

il est plus difficile pour ces personnes d'exercer leurs droits. Une analyse d'impact relative à la protection des données devrait également être effectuée lorsque des données à caractère personnel sont traitées en vue de prendre des décisions relatives à des personnes physiques spécifiques à la suite d'une évaluation systématique et approfondie d'aspects personnels propres à des personnes physiques sur la base du profilage desdites données ou à la suite du traitement de catégories particulières de données à caractère personnel, de données biométriques ou de données relatives à des condamnations pénales et à des infractions, ou encore à des mesures de sûreté connexes. Une analyse d'impact relative à la protection des données est de même requise aux fins de la surveillance à grande échelle de zones accessibles au public, en particulier lorsque des dispositifs opto-électroniques sont utilisés, ou pour toute autre opération pour laquelle l'autorité de contrôle compétente considère que le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, en particulier parce qu'elles empêchent ces personnes d'exercer un droit ou de bénéficier d'un service ou d'un contrat, ou parce qu'elles sont effectuées systématiquement à grande échelle. Le traitement de données à caractère personnel ne devrait pas être considéré comme étant à grande échelle si le traitement concerne les données à caractère personnel de patients ou de clients par un médecin, un autre professionnel de la santé ou un avocat exerçant à titre individuel. Dans de tels cas, une analyse d'impact relative à la protection des données ne devrait pas être obligatoire.

- (92) Il existe des cas dans lesquels il peut être raisonnable et économique d'élargir la portée de l'analyse d'impact relative à la protection des données au-delà d'un projet unique, par exemple lorsque des autorités publiques ou organismes publics entendent mettre en place une application ou une plateforme de traitement commune, ou lorsque plusieurs responsables du traitement envisagent de créer une application ou un environnement de traitement communs à tout un secteur ou segment professionnel, ou pour une activité transversale largement utilisée.
- (93) Au moment de l'adoption du droit d'un État membre qui fonde l'exercice des missions de l'autorité publique ou de l'organisme public concernés et qui réglemente l'opération ou l'ensemble d'opérations de traitement spécifiques, les États membres peuvent estimer qu'une telle analyse est nécessaire préalablement aux activités de traitement.
- (94) Lorsqu'il ressort d'une analyse d'impact relative à la protection des données que, en l'absence des garanties, de mesures de sécurité et de mécanismes pour atténuer le risque, le traitement engendrerait un risque élevé pour les droits et libertés des personnes physiques et que le responsable du traitement est d'avis que le risque ne peut être atténué par des moyens raisonnables compte tenu des techniques disponibles et des coûts de mise en œuvre, il y a lieu de consulter l'autorité de contrôle avant le début des opérations de traitement. Certains types de traitements et l'ampleur et la fréquence des traitements sont susceptibles d'engendrer un tel risque élevé et peuvent également causer un dommage ou porter atteinte aux droits et libertés d'une personne physique. L'autorité de contrôle devrait répondre à la demande de consultation dans un délai déterminé. Toutefois, l'absence de réaction de l'autorité de contrôle dans le délai imparti devrait être sans préjudice de toute intervention de sa part effectuée dans le cadre de ses missions et de ses pouvoirs prévus par le présent règlement, y compris le pouvoir d'interdire des opérations de traitement. Dans le cadre de ce processus de consultation, les résultats d'une analyse d'impact relative à la protection des données réalisée en ce qui concerne le traitement en question peuvent être soumis à l'autorité de contrôle, notamment les mesures envisagées pour atténuer le risque pour les droits et libertés des personnes physiques.
- (95) Le sous-traitant devrait aider le responsable du traitement, si nécessaire et sur demande, à assurer le respect des obligations découlant de la réalisation des analyses d'impact relatives à la protection des données et de la consultation préalable de l'autorité de contrôle.
- (96) L'autorité de contrôle devrait également être consultée au stade de la préparation d'une mesure législative ou réglementaire qui prévoit le traitement de données à caractère personnel, afin d'assurer que le traitement prévu respecte le présent règlement et, en particulier, d'atténuer le risque qu'il comporte pour la personne concernée.
- (97) Lorsque le traitement est réalisé par une autorité publique, à l'exception des juridictions ou des autorités judiciaires indépendantes agissant dans l'exercice de leur fonction juridictionnelle, lorsque, dans le secteur privé, il est effectué par un responsable du traitement dont les activités de base consistent en opérations de traitement exigeant un suivi régulier et systématique à grande échelle des personnes concernées, ou lorsque les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données à caractère personnel et de données relatives à des condamnations pénales et à des infractions, une personne possédant des connaissances spécialisées de la législation et des pratiques en matière de protection des données devrait aider le responsable du traitement ou le sous-traitant à vérifier le respect, au niveau interne, du présent règlement. Dans le secteur privé, les activités de base d'un responsable du traitement ont trait à ses activités principales et ne concernent pas le traitement des données à caractère personnel en tant qu'activité auxiliaire. Le niveau de connaissances spécialisées requis devrait être déterminé notamment en fonction

des opérations de traitement de données effectuées et de la protection exigée pour les données à caractère personnel traitées par le responsable du traitement ou le sous-traitant. De tels délégués à la protection des données, qu'ils soient ou non des employés du responsable du traitement, devraient être en mesure d'exercer leurs fonctions et missions en toute indépendance.

- (98) Il y a lieu d'encourager les associations ou autres organismes représentant des catégories de responsables du traitement ou de sous-traitants à élaborer des codes de conduite, dans les limites du présent règlement, de manière à en faciliter la bonne application, compte tenu des spécificités des traitements effectués dans certains secteurs et des besoins spécifiques des micro, petites et moyennes entreprises. Ces codes de conduite pourraient, en particulier, définir les obligations qui incombent aux responsables du traitement et aux sous-traitants, compte tenu du risque que le traitement peut engendrer pour les droits et libertés des personnes physiques.
- (99) Lors de l'élaboration d'un code de conduite, ou lors de sa modification ou prorogation, les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants devraient consulter les parties intéressées, y compris les personnes concernées lorsque cela est possible, et tenir compte des contributions transmises et des opinions exprimées à la suite de ces consultations.
- (100) Afin de favoriser la transparence et le respect du présent règlement, la mise en place de mécanismes de certification ainsi que de labels et de marques en matière de protection des données devrait être encouragée pour permettre aux personnes concernées d'évaluer rapidement le niveau de protection des données offert par les produits et services en question.
- (101) Les flux de données à caractère personnel à destination et en provenance de pays en dehors de l'Union et d'organisations internationales sont nécessaires au développement du commerce international et de la coopération internationale. L'augmentation de ces flux a créé de nouveaux enjeux et de nouvelles préoccupations en ce qui concerne la protection des données à caractère personnel. Cependant, il importe que, lorsque des données à caractère personnel sont transférées de l'Union à des responsables du traitement, sous-traitants ou autres destinataires dans des pays tiers ou à des organisations internationales, le niveau de protection des personnes physiques garanti dans l'Union par le présent règlement ne soit pas compromis, y compris en cas de transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale à des responsables du traitement ou sous-traitants dans le même pays tiers ou dans un pays tiers différent, ou à une autre organisation internationale. En tout état de cause, les transferts vers des pays tiers et à des organisations internationales ne peuvent avoir lieu que dans le plein respect du présent règlement. Un transfert ne pourrait avoir lieu que si, sous réserve des autres dispositions du présent règlement, les dispositions du présent règlement relatives au transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales sont respectées par le responsable du traitement ou le sous-traitant.
- (102) Le présent règlement s'entend sans préjudice des accords internationaux conclus entre l'Union et les pays tiers en vue de réglementer le transfert des données à caractère personnel, y compris les garanties appropriées au bénéfice des personnes concernées. Les États membres peuvent conclure des accords internationaux impliquant le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales dans la mesure où ces accords n'affectent pas le présent règlement ou toute autre disposition du droit de l'Union et prévoient un niveau approprié de protection des droits fondamentaux des personnes concernées.
- (103) La Commission peut décider, avec effet dans l'ensemble de l'Union, qu'un pays tiers, un territoire ou un secteur déterminé dans un pays tiers, ou une organisation internationale offre un niveau adéquat de protection des données, assurant ainsi une sécurité juridique et une uniformité dans l'ensemble l'Union en ce qui concerne le pays tiers ou l'organisation internationale qui est réputé offrir un tel niveau de protection. Dans ce cas, les transferts de données à caractère personnel vers ce pays tiers ou cette organisation internationale peuvent avoir lieu sans qu'il soit nécessaire d'obtenir une autre autorisation. La Commission peut également décider, après en avoir informé le pays tiers ou l'organisation internationale et lui avoir fourni une justification complète, de révoquer une telle décision.
- (104) 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, d'un territoire ou d'un secteur déterminé dans un pays tiers, prendre en considération la manière dont un pays tiers déterminé respecte l'état de droit, garantit l'accès à la justice et observe les règles et normes internationales dans le domaine des droits de l'homme, 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 tenir compte de critères clairs et objectifs, telles que les activités de traitement spécifiques et le champ d'application des normes juridiques applicables et de la législation en vigueur dans le pays tiers. Le pays tiers devrait offrir des garanties pour assurer un niveau adéquat de protection essentiellement équivalent à celui qui est garanti dans l'Union, en particulier

quand les données à caractère personnel 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 et juridictionnel.

- (105) Outre les engagements internationaux pris par le pays tiers ou l'organisation internationale, la Commission devrait tenir compte des obligations découlant de la participation du pays tiers ou de l'organisation internationale à des systèmes multilatéraux ou régionaux, notamment en ce qui concerne la 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. Lorsqu'elle évalue le niveau de protection offert par des pays tiers ou des organisations internationales, la Commission devrait consulter le comité.
- (106) 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, et surveiller le fonctionnement des décisions adoptées sur la base de l'article 25, paragraphe 6, ou de l'article 26, paragraphe 4, de la directive 95/46/CE. 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 présentant un intérêt dans le pays tiers ou au sein de l'organisation internationale. Aux fins de la surveillance et de la réalisation des examens périodiques, la Commission devrait prendre en considération les observations et les conclusions du Parlement européen et du Conseil, ainsi que d'autres organes et sources pertinents. La Commission devrait évaluer le fonctionnement desdites décisions dans un délai raisonnable et communiquer toute conclusion pertinente au comité au sens du règlement (UE) n° 182/2011 du Parlement européen et du Conseil ⁽¹⁾ établi en vertu du présent règlement, au Parlement européen et au Conseil.
- (107) La Commission peut 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 du présent règlement relatives aux transferts faisant l'objet de garanties appropriées, y compris des règles d'entreprise contraignantes et des dérogations pour des situations particulières, soient respectées. Dans ce cas, il y aurait lieu de prévoir des consultations 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 avec ceux-ci en vue de remédier à la situation.
- (108) En l'absence de décision d'adéquation, le responsable du traitement ou le sous-traitant devrait prendre des mesures pour compenser l'insuffisance de la protection des données dans le pays tiers par des garanties appropriées en faveur de la personne concernée. Ces garanties peuvent consister à recourir à des règles d'entreprise contraignantes, des clauses types de protection des données adoptées par la Commission, des clauses types de protection des données adoptées par une autorité de contrôle ou des clauses contractuelles autorisées par une autorité de contrôle. Ces garanties devraient assurer le respect des exigences en matière de protection des données et des droits des personnes concernées d'une manière appropriée au traitement au sein de l'Union, y compris l'existence de droits opposables de la personne concernée et de voies de droit effectives, ce qui comprend le droit d'engager un recours administratif ou juridictionnel effectif et d'introduire une action en réparation, dans l'Union ou dans un pays tiers. Ces garanties devraient porter, en particulier, sur le respect des principes généraux concernant le traitement des données à caractère personnel et des principes de protection des données dès la conception et de protection des données par défaut. Des transferts peuvent également être effectués par des autorités publiques ou des organismes publics avec des autorités publiques ou des organismes publics dans des pays tiers ou avec des organisations internationales exerçant des missions ou fonctions correspondantes, y compris sur la base de dispositions à intégrer dans des arrangements administratifs, telles qu'un protocole d'accord, prévoyant des droits opposables et effectifs pour les personnes concernées. L'autorisation de l'autorité de contrôle compétente devrait être obtenue lorsque ces garanties sont prévues dans des arrangements administratifs qui ne sont pas juridiquement contraignants.
- (109) La possibilité qu'ont les responsables du traitement et les sous-traitants de recourir à des clauses types de protection des données adoptées par la Commission ou par une autorité de contrôle ne devrait pas les empêcher

⁽¹⁾ Règlement (UE) n° 182/2011 du Parlement européen et du Conseil du 16 février 2011 établissant les règles et principes généraux relatifs aux modalités de contrôle par les États membres de l'exercice des compétences d'exécution par la Commission (JO L 55 du 28.2.2011, p. 13).

d'inclure ces clauses dans un contrat plus large, tel qu'un contrat entre le sous-traitant et un autre sous-traitant, ni d'y ajouter d'autres clauses ou des garanties supplémentaires, à condition que celles-ci ne contredisent pas, directement ou indirectement, les clauses contractuelles types adoptées par la Commission ou par une autorité de contrôle et qu'elles ne portent pas atteinte aux libertés et droits fondamentaux des personnes concernées. Les responsables du traitement et les sous-traitants devraient être encouragés à fournir des garanties supplémentaires par l'intermédiaire d'engagements contractuels qui viendraient compléter les clauses types de protection.

- (110) Un groupe d'entreprises ou un groupe d'entreprises engagées dans une activité économique conjointe devrait pouvoir recourir à des règles d'entreprise contraignantes approuvées pour ses transferts internationaux de l'Union vers des entités du même groupe d'entreprises, ou du même groupe d'entreprises engagées dans une activité économique conjointe, à condition que ces règles d'entreprise incluent tous les principes essentiels et les droits opposables pour assurer des garanties appropriées pour les transferts ou catégories de transferts de données à caractère personnel.
- (111) Il y a lieu de prévoir la possibilité de transferts dans certains cas où la personne concernée a donné son consentement explicite, lorsque le transfert est occasionnel et nécessaire dans le cadre d'un contrat ou d'une action en justice, qu'il s'agisse d'une procédure judiciaire, administrative ou extrajudiciaire, y compris de procédures devant des organismes de régulation. Il convient également de prévoir la possibilité de transferts lorsque des motifs importants d'intérêt public établis par le droit de l'Union ou le droit d'un État membre l'exigent, ou lorsque le transfert intervient au départ d'un registre établi par la loi et destiné à être consulté par le public ou par des personnes ayant un intérêt légitime. Dans ce dernier cas, ce transfert ne devrait pas porter sur la totalité des données à caractère personnel ni sur des catégories entières de données contenues dans le registre et, lorsque celui-ci est destiné à être consulté par des personnes ayant un intérêt légitime, le transfert ne devrait être effectué qu'à la demande de ces personnes ou lorsqu'elles doivent en être les destinataires, compte dûment tenu des intérêts et des droits fondamentaux de la personne concernée.
- (112) Ces dérogations devraient s'appliquer en particulier aux transferts de données requis et nécessaires pour des motifs importants d'intérêt public, par exemple en cas d'échange international de données entre autorités de la concurrence, administrations fiscales ou douanières, entre autorités de surveillance financière, entre services chargés des questions de sécurité sociale ou relatives à la santé publique, par exemple aux fins de la recherche des contacts des personnes atteintes de maladies contagieuses ou en vue de réduire et/ou d'éliminer le dopage dans le sport. Le transfert de données à caractère personnel devrait également être considéré comme licite lorsqu'il est nécessaire pour protéger un intérêt essentiel pour la sauvegarde des intérêts vitaux, y compris l'intégrité physique ou la vie, de la personne concernée ou d'une autre personne, si la personne concernée se trouve dans l'incapacité de donner son consentement. En l'absence d'une décision d'adéquation, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories particulières de données vers un pays tiers ou à une organisation internationale. Les États membres devraient notifier ces dispositions à la Commission. Tout transfert vers une organisation humanitaire internationale de données à caractère personnel d'une personne concernée qui se trouve dans l'incapacité physique ou juridique de donner son consentement, en vue d'accomplir une mission relevant des conventions de Genève ou de respecter le droit humanitaire international applicable dans les conflits armés, pourrait être considéré comme nécessaire pour des motifs importants d'intérêt public ou parce que ce transfert est dans l'intérêt vital de la personne concernée.
- (113) Les transferts qui peuvent être qualifiés de non répétitifs et qui ne touchent qu'un nombre limité de personnes concernées pourraient également être autorisés aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement, lorsque ces intérêts prévalent sur les intérêts ou les libertés et droits fondamentaux de la personne concernée et lorsque le responsable du traitement a évalué toutes les circonstances entourant le transfert de données. Le responsable du traitement devrait accorder une attention particulière à la nature des données à caractère personnel, à la finalité et à la durée de la ou des opérations de traitement envisagées ainsi qu'à la situation dans le pays d'origine, le pays tiers et le pays de destination finale, et devrait prévoir des garanties appropriées pour protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement de leurs données à caractère personnel. De tels transferts ne devraient être possibles que dans les cas résiduels dans lesquels aucun des autres motifs de transfert ne sont applicables. À des fins de recherche scientifique ou historique ou à des fins statistiques, il y a lieu de prendre en considération les attentes légitimes de la société en matière de progrès des connaissances. Le responsable du traitement devrait informer l'autorité de contrôle et la personne concernée du transfert.
- (114) En tout état de cause, lorsque la Commission ne s'est pas prononcée sur le caractère adéquat du niveau de protection des données dans un pays tiers, le responsable du traitement ou le sous-traitant devrait adopter des solutions qui garantissent aux personnes concernées des droits opposables et effectifs en ce qui concerne le traitement de leurs données dans l'Union une fois que ces données ont été transférées, de façon à ce que lesdites personnes continuent de bénéficier des droits fondamentaux et des garanties.

- (115) Certains pays tiers adoptent des lois, des règlements et d'autres actes juridiques qui visent à réglementer directement les activités de traitement effectuées par des personnes physiques et morales qui relèvent de la compétence des États membres. Il peut s'agir de décisions de juridictions ou d'autorités administratives de pays tiers qui exigent d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel, et qui ne sont pas fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre. L'application extraterritoriale de ces lois, règlements et autres actes juridiques peut être contraire au droit international et faire obstacle à la protection des personnes physiques garantie dans l'Union par le présent règlement. Les transferts ne devraient être autorisés que lorsque les conditions fixées par le présent règlement pour les transferts vers les pays tiers sont remplies. Ce peut être le cas, entre autres, lorsque la divulgation est nécessaire pour un motif important d'intérêt public reconnu par le droit de l'Union ou le d'un État membre auquel le responsable du traitement est soumis.
- (116) Lorsque des données à caractère personnel franchissent les frontières extérieures de l'Union, cela peut accroître le risque que les personnes physiques ne puissent exercer leurs droits liés à la protection des données, notamment pour se protéger de l'utilisation ou de la divulgation illicite de ces informations. 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, par l'hétérogénéité des régimes juridiques et par des obstacles pratiques tels que le manque de ressources. En conséquence, il est nécessaire de favoriser une coopération plus étroite entre les autorités de contrôle de la protection des données, pour les aider à échanger des informations et mener des enquêtes avec leurs homologues internationaux. Aux fins d'élaborer des mécanismes de coopération internationale destinés à faciliter et à mettre en place une assistance mutuelle internationale pour faire appliquer la législation relative à la protection des données à caractère personnel, la Commission et les autorités de contrôle devraient échanger des informations et coopérer dans le cadre d'activités liées à l'exercice de leurs compétences avec les autorités compétentes dans les pays tiers, sur une base réciproque et conformément au présent règlement.
- (117) La mise en place d'autorités de contrôle dans les États membres, habilitées à exercer leurs missions et leurs pouvoirs en toute indépendance, est un élément essentiel de la protection des personnes physiques à l'égard du traitement des données à caractère personnel. Les États membres devraient pouvoir mettre en place plusieurs autorités de contrôle en fonction de leur structure constitutionnelle, organisationnelle et administrative.
- (118) L'indépendance des autorités de contrôle ne devrait pas signifier que celles-ci ne peuvent être soumises à des mécanismes de contrôle ou de suivi de leur gestion financière ni à un contrôle juridictionnel.
- (119) Lorsqu'un État membre met en place plusieurs autorités de contrôle, il devrait établir par la loi des dispositifs garantissant la participation effective de ces autorités au mécanisme de contrôle de la cohérence. Il devrait en particulier désigner l'autorité de contrôle qui sert de point de contact unique, permettant une participation efficace de ces autorités au mécanisme, afin d'assurer une coopération rapide et aisée avec les autres autorités de contrôle, le comité et la Commission.
- (120) Il convient que chaque autorité de contrôle soit dotée des 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.
- (121) Les conditions générales applicables au(x) membre(s) de l'autorité de contrôle devraient être fixées par la loi dans chaque État membre et devraient prévoir notamment que ces membres sont nommés, selon une procédure transparente, par le parlement, le gouvernement ou le chef d'État de cet État membre, sur proposition du gouvernement ou d'un membre du gouvernement, ou du parlement ou d'une chambre du parlement, ou par un organisme indépendant qui en a été chargé en vertu du droit d'un État membre. Afin de garantir l'indépendance de l'autorité de contrôle, il convient que le membre ou les membres de celle-ci agissent avec intégrité, s'abstiennent de tout acte incompatible avec leurs fonctions et n'exercent, pendant la durée de leur mandat, aucune activité professionnelle incompatible, rémunérée ou non. Chaque autorité de contrôle devrait disposer de ses propres agents, choisis par elle-même ou un organisme indépendant établi par le droit d'un État membre, qui devraient être placés sous les ordres exclusifs du membre ou des membres de l'autorité de contrôle.
- (122) Chaque autorité de contrôle devrait être compétente sur le territoire de l'État membre dont elle relève pour exercer les missions et les pouvoirs dont elle est investie conformément au présent règlement. Cela devrait

7. L'analyse contient au moins:
- a) une description systématique des opérations de traitement envisagées et des finalités du traitement, y compris, le cas échéant, l'intérêt légitime poursuivi par le responsable du traitement;
 - b) une évaluation de la nécessité et de la proportionnalité des opérations de traitement au regard des finalités;
 - c) une évaluation des risques pour les droits et libertés des personnes concernées conformément au paragraphe 1; et
 - d) les mesures envisagées pour faire face aux risques, y compris les garanties, mesures et mécanismes de sécurité visant à assurer la protection des données à caractère personnel et à apporter la preuve du respect du présent règlement, compte tenu des droits et des intérêts légitimes des personnes concernées et des autres personnes affectées.
8. Le respect, par les responsables du traitement ou sous-traitants concernés, de codes de conduite approuvés visés à l'article 40 est dûment pris en compte lors de l'évaluation de l'impact des opérations de traitement effectuées par lesdits responsables du traitement ou sous-traitants, en particulier aux fins d'une analyse d'impact relative à la protection des données.
9. Le cas échéant, le responsable du traitement demande l'avis des personnes concernées ou de leurs représentants au sujet du traitement prévu, sans préjudice de la protection des intérêts généraux ou commerciaux ou de la sécurité des opérations de traitement.
10. Lorsque le traitement effectué en application de l'article 6, paragraphe 1, point c) ou e), a une base juridique dans le droit de l'Union ou dans le droit de l'État membre auquel le responsable du traitement est soumis, que ce droit réglemente l'opération de traitement spécifique ou l'ensemble des opérations de traitement en question et qu'une analyse d'impact relative à la protection des données a déjà été effectuée dans le cadre d'une analyse d'impact générale réalisée dans le cadre de l'adoption de la base juridique en question, les paragraphes 1 à 7 ne s'appliquent pas, à moins que les États membres n'estiment qu'il est nécessaire d'effectuer une telle analyse avant les activités de traitement.
11. Si nécessaire, le responsable du traitement procède à un examen afin d'évaluer si le traitement est effectué conformément à l'analyse d'impact relative à la protection des données, au moins quand il se produit une modification du risque présenté par les opérations de traitement.

Article 36

Consultation préalable

1. Le responsable du traitement consulte l'autorité de contrôle préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données effectuée au titre de l'article 35 indique que le traitement présenterait un risque élevé si le responsable du traitement ne prenait pas de mesures pour atténuer le risque.
2. Lorsque l'autorité de contrôle est d'avis que le traitement envisagé visé au paragraphe 1, constituerait une violation du présent règlement, 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 huit 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 peut faire usage des pouvoirs visés à l'article 58. Ce délai peut être prolongé de six semaines, en fonction de la complexité du traitement envisagé. L'autorité de contrôle informe le responsable du traitement et, le cas échéant, le sous-traitant de la prolongation du délai ainsi que des motifs du retard, dans un délai d'un mois à compter de la réception de la demande de consultation. Ces délais peuvent être suspendus jusqu'à ce que l'autorité de contrôle ait obtenu les informations qu'elle a demandées pour les besoins de la consultation.
3. Lorsque le responsable du traitement consulte l'autorité de contrôle en application du paragraphe 1, il lui communique:
 - a) le cas échéant, les responsabilités respectives du responsable du traitement, des responsables conjoints et des sous-traitants participant au traitement, en particulier pour le traitement au sein d'un groupe d'entreprises;
 - b) les finalités et les moyens du traitement envisagé;
 - c) les mesures et les garanties prévues afin de protéger les droits et libertés des personnes concernées en vertu du présent règlement;
 - d) le cas échéant, les coordonnées du délégué à la protection des données;

- e) l'analyse d'impact relative à la protection des données prévue à l'article 35; et
- f) toute autre information que l'autorité de contrôle demande.

4. Les États membres consultent l'autorité de contrôle 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.

5. Nonobstant le paragraphe 1, le droit des États membres peut exiger que les responsables du traitement consultent l'autorité de contrôle et obtiennent son autorisation préalable en ce qui concerne le traitement effectué par un responsable du traitement dans le cadre d'une mission d'intérêt public exercée par celui-ci, y compris le traitement dans le cadre de la protection sociale et de la santé publique.

Section 4

Délégué à la protection des données

Article 37

Désignation du délégué à la protection des données

1. Le responsable du traitement et le sous-traitant désignent en tout état de cause un délégué à la protection des données lorsque:
 - a) le traitement est effectué par une autorité publique ou un organisme public, à l'exception des juridictions agissant dans l'exercice de leur fonction juridictionnelle;
 - b) les activités de base du responsable du traitement ou du sous-traitant consistent en des opérations de traitement qui, du fait de leur nature, de leur portée et/ou de leurs finalités, exigent un suivi régulier et systématique à grande échelle des personnes concernées; ou
 - c) les activités de base du responsable du traitement ou du sous-traitant consistent en un traitement à grande échelle de catégories particulières de données visées à l'article 9 et de données à caractère personnel relatives à des condamnations pénales et à des infractions visées à l'article 10.
2. Un groupe d'entreprises peut désigner un seul délégué à la protection des données à condition qu'un délégué à la protection des données soit facilement joignable à partir de chaque lieu d'établissement.
3. Lorsque le responsable du traitement ou le sous-traitant est une autorité publique ou un organisme public, un seul délégué à la protection des données peut être désigné pour plusieurs autorités ou organismes de ce type, compte tenu de leur structure organisationnelle et de leur taille.
4. Dans les cas autres que ceux visés au paragraphe 1, le responsable du traitement ou le sous-traitant ou les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent désigner ou, si le droit de l'Union ou le droit d'un État membre l'exige, sont tenus de désigner un délégué à la protection des données. Le délégué à la protection des données peut agir pour ces associations et autres organismes représentant des responsables du traitement ou des sous-traitants.
5. 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 accomplir les missions visées à l'article 39.
6. Le délégué à la protection des données peut être un membre du personnel du responsable du traitement ou du sous-traitant, ou exercer ses missions sur la base d'un contrat de service.
7. Le responsable du traitement ou le sous-traitant publient les coordonnées du délégué à la protection des données et les communiquent à l'autorité de contrôle.

Article 38

Fonction du délégué à la protection des données

1. Le responsable du traitement et le sous-traitant veillent 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 et le sous-traitant aident le délégué à la protection des données à exercer les missions visées à l'article 39 en fournissant les ressources nécessaires pour exercer ces missions, ainsi que l'accès aux données à caractère personnel et aux opérations de traitement, et lui permettant d'entretenir ses connaissances spécialisées.
3. Le responsable du traitement et le sous-traitant veillent à ce que le délégué à la protection des données ne reçoive aucune instruction en ce qui concerne l'exercice des missions. Le délégué à la protection des données ne peut être relevé de ses fonctions ou pénalisé par le responsable du traitement ou le sous-traitant pour l'exercice de ses missions. Le délégué à la protection des données fait directement rapport au niveau le plus élevé de la direction du responsable du traitement ou du sous-traitant.
4. Les personnes concernées peuvent prendre contact avec le délégué à la protection des données au sujet de toutes les questions relatives au traitement de leurs données à caractère personnel et à l'exercice des droits que leur confère le présent règlement.
5. Le délégué à la protection des données est soumis au secret professionnel ou à une obligation de confidentialité en ce qui concerne l'exercice de ses missions, conformément au droit de l'Union ou au droit des États membres.
6. Le délégué à la protection des données peut exécuter d'autres missions et tâches. Le responsable du traitement ou le sous-traitant veillent à ce que ces missions et tâches n'entraînent pas de conflit d'intérêts.

Article 39

Missions du délégué à la protection des données

1. Les missions du délégué à la protection des données sont au moins les suivantes:
 - a) informer et conseiller le responsable du traitement ou le sous-traitant ainsi que les employés qui procèdent au traitement sur les obligations qui leur incombent en vertu du présent règlement 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 du présent règlement, 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 ou du sous-traitant en matière de protection des données à caractère personnel, y compris en ce qui concerne la répartition des responsabilités, la sensibilisation et la formation du personnel participant aux 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 35;
 - 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 36, et mener des consultations, le cas échéant, sur tout autre sujet.
2. Le délégué à la protection des données tient dûment compte, dans l'accomplissement de ses missions, du risque associé aux opérations de traitement compte tenu de la nature, de la portée, du contexte et des finalités du traitement.

Section 5

Codes de conduite et certification

Article 40

Codes de conduite

1. Les États membres, les autorités de contrôle, le comité et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer à la bonne application du présent règlement, compte tenu de la spécificité des différents secteurs de traitement et des besoins spécifiques des micro, petites et moyennes entreprises.
2. Les associations et autres organismes représentant des catégories de responsables du traitement ou de sous-traitants peuvent élaborer des codes de conduite, les modifier ou les proroger, aux fins de préciser les modalités d'application du présent règlement, telles que:
 - a) le traitement loyal et transparent;

- b) les intérêts légitimes poursuivis par les responsables du traitement dans des contextes spécifiques;
- c) la collecte des données à caractère personnel;
- d) la pseudonymisation des données à caractère personnel;
- e) les informations communiquées au public et aux personnes concernées;
- f) l'exercice des droits des personnes concernées;
- g) les informations communiquées aux enfants et la protection dont bénéficient les enfants et la manière d'obtenir le consentement des titulaires de la responsabilité parentale à l'égard de l'enfant;
- h) les mesures et les procédures visées aux articles 24 et 25 et les mesures visant à assurer la sécurité du traitement visées à l'article 32;
- i) la notification aux autorités de contrôle des violations de données à caractère personnel et la communication de ces violations aux personnes concernées;
- j) le transfert de données à caractère personnel vers des pays tiers ou à des organisations internationales; ou
- k) les procédures extrajudiciaires et autres procédures de règlement des litiges permettant de résoudre les litiges entre les responsables du traitement et les personnes concernées en ce qui concerne le traitement, sans préjudice des droits des personnes concernées au titre des articles 77 et 79.

3. Outre leur application par les responsables du traitement ou les sous-traitants soumis au présent règlement, les codes de conduite qui sont approuvés en vertu du paragraphe 5 du présent article et qui sont d'application générale en vertu du paragraphe 9 du présent article peuvent aussi être appliqués par des responsables du traitement ou des sous-traitants qui ne sont pas soumis au présent règlement en vertu de l'article 3, afin de fournir des garanties appropriées dans le cadre des transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale dans les conditions visées à l'article 46, paragraphe 2, point e). Ces responsables du traitement ou sous-traitants prennent l'engagement contraignant et doté de force obligatoire au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

4. Le code de conduite visé au paragraphe 2 du présent article comprend les mécanismes permettant à l'organisme visé à l'article 41, paragraphe 1, de procéder au contrôle obligatoire du respect de ses dispositions par les responsables du traitement ou les sous-traitants qui s'engagent à l'appliquer, sans préjudice des missions et des pouvoirs de l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56.

5. Les associations et autres organismes visés au paragraphe 2 du présent article qui ont l'intention d'élaborer un code de conduite ou de modifier ou proroger un code de conduite existant soumettent le projet de code, la modification ou la prorogation à l'autorité de contrôle qui est compétente en vertu de l'article 55. L'autorité de contrôle rend un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte le présent règlement et approuve ce projet de code, cette modification ou cette prorogation si elle estime qu'il offre des garanties appropriées suffisantes.

6. Lorsque le projet de code, la modification ou la prorogation est approuvé conformément au paragraphe 5, et lorsque le code de conduite concerné ne porte pas sur des activités de traitement menées dans plusieurs États membres, l'autorité de contrôle enregistre et publie le code de conduite.

7. Lorsque le projet de code de conduite concerne des activités de traitement menées dans plusieurs États membres, l'autorité de contrôle qui est compétente en vertu de l'article 55 soumet le projet de code, la modification ou la prorogation, avant approbation, selon la procédure visée à l'article 63, au comité, qui rend un avis sur la question de savoir si le projet de code, la modification ou la prorogation respecte le présent règlement ou, dans la situation visée au paragraphe 3 du présent article, s'il offre des garanties appropriées.

8. Lorsque l'avis visé au paragraphe 7 confirme que le projet de code, la modification ou la prorogation respecte le présent règlement ou, dans la situation visée au paragraphe 3, offre des garanties appropriées, le comité soumet son avis à la Commission.

9. La Commission peut décider, par voie d'actes d'exécution, que le code de conduite, la modification ou la prorogation approuvés qui lui ont été soumis en vertu du paragraphe 8 du présent article sont d'application générale au sein de l'Union. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

10. La Commission veille à garantir une publicité appropriée aux codes approuvés dont elle a décidé qu'ils sont d'application générale conformément au paragraphe 9.

11. Le comité consigne dans un registre tous les codes de conduite, les modifications et les prorogations approuvés et les met à la disposition du public par tout moyen approprié.

Article 41

Suivi des codes de conduite approuvés

1. Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente au titre des articles 57 et 58, le contrôle du respect du code de conduite en vertu de l'article 40 peut être effectué par un organisme qui dispose d'un niveau d'expertise approprié au regard de l'objet du code et qui est agréé à cette fin par l'autorité de contrôle compétente.

2. Un organisme visé au paragraphe 1 peut être agréé pour contrôler le respect d'un code de conduite lorsque cet organisme a:

- a) démontré, à la satisfaction de l'autorité de contrôle compétente, son indépendance et son expertise au regard de l'objet du code;
- b) établi des procédures qui lui permettent d'apprécier si les responsables du traitement et les sous-traitants concernés satisfont aux conditions pour appliquer le code, de contrôler le respect de ses dispositions et d'examiner périodiquement son fonctionnement;
- c) établi des procédures et des structures pour traiter les réclamations relatives aux violations du code ou à la manière dont le code a été ou est appliqué par un responsable du traitement ou un sous-traitant, et pour rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public; et
- d) démontré, à la satisfaction de l'autorité de contrôle compétente, que ses tâches et ses missions n'entraînent pas de conflit d'intérêts.

3. L'autorité de contrôle compétente soumet le projet de critères d'agrément d'un organisme visé au paragraphe 1 du présent article au comité en application du mécanisme de contrôle de la cohérence visé à l'article 63.

4. Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente et des dispositions du chapitre VIII, un organisme visé au paragraphe 1 du présent article prend, sous réserve des garanties appropriées, des mesures appropriées en cas de violation du code par un responsable du traitement ou un sous-traitant, et peut notamment suspendre ou exclure le responsable du traitement ou le sous-traitant concerné de l'application du code. Il informe l'autorité de contrôle compétente de ces mesures et des raisons pour lesquelles elles ont été prises.

5. L'autorité de contrôle compétente révoque l'agrément d'un organisme visé au paragraphe 1 si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme constituent une violation du présent règlement.

6. Le présent article ne s'applique pas au traitement effectué par les autorités publiques et les organismes publics.

Article 42

Certification

1. Les États membres, les autorités de contrôle, le comité et la Commission encouragent, en particulier au niveau de l'Union, la mise en place de mécanismes de certification en matière de protection des données ainsi que de labels et de marques en la matière, aux fins de démontrer que les opérations de traitement effectuées par les responsables du traitement et les sous-traitants respectent le présent règlement. Les besoins spécifiques des micro, petites et moyennes entreprises sont pris en considération.

2. Outre l'application par les responsables du traitement ou les sous-traitants soumis au présent règlement, les mécanismes de certification, les labels ou les marques en matière de protection des données approuvés en vertu du paragraphe 5 du présent article peuvent être établis aux fins de démontrer que des responsables du traitement ou des sous-traitants qui ne sont pas soumis au présent règlement en vertu de l'article 3 fournissent des garanties appropriées dans le cadre des transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale dans les conditions visées à l'article 46, paragraphe 2, point f). Ces responsables du traitement ou sous-traitants prennent l'engagement contraignant et exécutoire, au moyen d'instruments contractuels ou d'autres instruments juridiquement contraignants, d'appliquer ces garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.
3. La certification est volontaire et accessible via un processus transparent.
4. Une certification en vertu du présent article ne diminue par la responsabilité du responsable du traitement ou du sous-traitant quant au respect du présent règlement et est sans préjudice des missions et des pouvoirs des autorités de contrôle qui sont compétentes en vertu de l'article 55 ou 56.
5. Une certification en vertu du présent article est délivrée par les organismes de certification visés à l'article 43 ou par l'autorité de contrôle compétente sur la base des critères approuvés par cette autorité de contrôle compétente en application de l'article 58, paragraphe 3, ou par le comité en application de l'article 63. Lorsque les critères sont approuvés par le comité, cela peut donner lieu à une certification commune, le label européen de protection des données.
6. Le responsable du traitement ou le sous-traitant qui soumet son traitement au mécanisme de certification fournit à l'organisme de certification visé à l'article 43 ou, le cas échéant, à l'autorité de contrôle compétente toutes les informations ainsi que l'accès à ses activités de traitement, qui sont nécessaires pour mener la procédure de certification.
7. La certification est délivrée à un responsable du traitement ou à un sous-traitant pour une durée maximale de trois ans et peut être renouvelée dans les mêmes conditions tant que les exigences applicables continuent d'être satisfaites. La certification est retirée, s'il y a lieu, par les organismes de certification visés à l'article 43 ou par l'autorité de contrôle compétente lorsque les exigences applicables à la certification ne sont pas ou plus satisfaites.
8. Le comité consigne dans un registre tous les mécanismes de certification et les labels ou les marques en matière de protection des données et les met à la disposition du public par tout moyen approprié.

Article 43

Organismes de certification

1. Sans préjudice des missions et des pouvoirs de l'autorité de contrôle compétente au titre des articles 57 et 58, les organismes de certification disposant d'un niveau d'expertise approprié en matière de protection des données délivrent et renouvellent les certifications, après en avoir informé l'autorité de contrôle pour qu'elle puisse exercer au besoin les pouvoirs qui lui sont dévolus en vertu de l'article 58, paragraphe 2, point h). Les États membres veillent à ce que ces organismes de certification soient agréés par une des entités suivantes ou les deux:
 - a) l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56;
 - b) l'organisme national d'accréditation désigné conformément au règlement (CE) n° 765/2008 du Parlement européen et du Conseil ⁽¹⁾, conformément à la norme EN-ISO/IEC 17065/2012 et aux exigences supplémentaires établies par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56.
2. Les organismes de certification visés au paragraphe 1 ne sont agréés conformément audit paragraphe que lorsqu'ils ont:
 - a) démontré, à la satisfaction de l'autorité de contrôle compétente, leur indépendance et leur expertise au regard de l'objet de la certification;

⁽¹⁾ Règlement (CE) n° 765/2008 du Parlement européen et du Conseil du 9 juillet 2008 fixant les prescriptions relatives à l'accréditation et à la surveillance du marché pour la commercialisation des produits et abrogeant le règlement (CEE) n° 339/93 du Conseil (JO L 218 du 13.8.2008, p. 30).

- b) pris l'engagement de respecter les critères visés à l'article 42, paragraphe 5, et approuvés par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56 ou par le comité, en vertu de l'article 63;
- c) mis en place des procédures en vue de la délivrance, de l'examen périodique et du retrait d'une certification, de labels et de marques en matière de protection des données;
- d) établi des procédures et des structures pour traiter les réclamations relatives aux violations de la certification ou à la manière dont la certification a été ou est appliquée par un responsable du traitement ou un sous-traitant, et pour rendre ces procédures et structures transparentes à l'égard des personnes concernées et du public; et
- e) démontré, à la satisfaction de l'autorité de contrôle compétente, que leurs tâches et leurs missions n'entraînent pas de conflit d'intérêts.

3. L'agrément des organismes de certification visés aux paragraphes 1 et 2 du présent article se fait sur la base de critères approuvés par l'autorité de contrôle qui est compétente en vertu de l'article 55 ou 56 ou, par le comité en vertu de l'article 63. En cas d'agrément en application du paragraphe 1, point b), du présent article, ces exigences complètent celles prévues dans le règlement (CE) n° 765/2008 et les règles techniques qui décrivent les méthodes et procédures des organismes de certification.

4. Les organismes de certification visés au paragraphe 1 sont chargés de procéder à l'évaluation appropriée conduisant à la délivrance de la certification ou au retrait de cette certification, sans préjudice de la responsabilité du responsable du traitement ou du sous-traitant en ce qui concerne le respect du présent règlement. L'agrément est délivré pour une durée maximale de cinq ans et peut être renouvelé dans les mêmes conditions tant que l'organisme de certification satisfait aux exigences énoncées au présent article.

5. Les organismes de certification visés au paragraphe 1 communiquent aux autorités de contrôle compétentes les raisons de la délivrance ou du retrait de la certification demandée.

6. Les exigences visées au paragraphe 3 du présent article et les critères visés à l'article 42, paragraphe 5, sont publiés par les autorités de contrôle sous une forme aisément accessible. Les autorités de contrôle transmettent aussi ces exigences et ces critères au comité. Le comité consigne dans un registre tous les mécanismes de certification et les labels en matière de protection des données et les met à la disposition du public par tout moyen approprié.

7. Sans préjudice du chapitre VIII, l'autorité de contrôle compétente ou l'organisme national d'accréditation révoque l'agrément d'un organisme de certification en application du paragraphe 1 du présent article si les conditions d'agrément ne sont pas ou ne sont plus réunies ou si les mesures prises par l'organisme de certification constituent une violation du présent règlement.

8. La Commission est habilitée à adopter des actes délégués en conformité avec l'article 92, aux fins de préciser les exigences à prendre en considération en ce qui concerne les mécanismes de certification en matière de protection des données visés à l'article 42, paragraphe 1.

9. La Commission peut adopter des actes d'exécution visant à fixer des normes techniques pour les mécanismes de certification, les labels et les marques en matière de protection des données, ainsi que les mécanismes aux fins de la promotion et de la reconnaissance de ces mécanismes de certification, labels et marques. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

CHAPITRE V

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

Article 44

Principe général applicable aux transferts

Un transfert, vers un pays tiers ou à une organisation internationale, de données à caractère personnel qui font ou sont destinées à faire l'objet d'un traitement après ce transfert ne peut avoir lieu que si, sous réserve des autres dispositions du présent règlement, les conditions définies dans le présent chapitre sont respectées par le responsable du traitement et le sous-traitant, y compris pour les transferts ultérieurs de données à caractère personnel au départ du pays tiers ou de l'organisation internationale vers un autre pays tiers ou à une autre organisation internationale. Toutes les dispositions du présent chapitre sont appliquées de manière à ce que le niveau de protection des personnes physiques garanti par le présent règlement ne soit pas compromis.

Article 45

Transferts fondés sur une décision d'adéquation

1. 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 ainsi que 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 décider, par voie d'actes d'exécution, qu'un pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans un pays tiers, 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 93, 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 du présent article et des décisions adoptées sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE.

5. Lorsque les informations disponibles révèlent, en particulier à l'issue 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 si nécessaire, abroge, modifie ou suspend 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 93, 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 93, 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. Une décision adoptée en vertu du paragraphe 5 du présent article est sans préjudice des transferts de données à caractère personnel vers le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou à l'organisation internationale en question, effectués en application des articles 46 à 49.

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.

9. Les décisions adoptées par la Commission sur la base de l'article 25, paragraphe 6, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation par une décision de la Commission adoptée conformément au paragraphe 3 ou 5 du présent article.

Article 46

Transferts moyennant des garanties appropriées

1. En l'absence de décision en vertu de l'article 45, paragraphe 3, le responsable du traitement ou le sous-traitant ne peut transférer des données à caractère personnel vers un pays tiers ou à une organisation internationale que s'il a prévu des garanties appropriées et à la condition que les personnes concernées disposent de droits opposables et de voies de droit effectives.

2. Les garanties appropriées visées au paragraphe 1 peuvent être fournies, sans que cela ne nécessite une autorisation particulière d'une autorité de contrôle, par:

- a) un instrument juridiquement contraignant et exécutoire entre les autorités ou organismes publics;
- b) des règles d'entreprise contraignantes conformément à l'article 47;
- c) des clauses types de protection des données adoptées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;
- d) des clauses types de protection des données adoptées par une autorité de contrôle et approuvées par la Commission en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2;
- e) un code de conduite approuvé conformément à l'article 40, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées; ou
- f) un mécanisme de certification approuvé conformément à l'article 42, assorti de l'engagement contraignant et exécutoire pris par le responsable du traitement ou le sous-traitant dans le pays tiers d'appliquer les garanties appropriées, y compris en ce qui concerne les droits des personnes concernées.

3. Sous réserve de l'autorisation de l'autorité de contrôle compétente, les garanties appropriées visées au paragraphe 1 peuvent aussi être fournies, notamment, par:

- a) des clauses contractuelles entre le responsable du traitement ou le sous-traitant et le responsable du traitement, le sous-traitant ou le destinataire des données à caractère personnel dans le pays tiers ou l'organisation internationale; ou
- b) des dispositions à intégrer dans des arrangements administratifs entre les autorités publiques ou les organismes publics qui prévoient des droits opposables et effectifs pour les personnes concernées.

4. L'autorité de contrôle applique le mécanisme de contrôle de la cohérence visé à l'article 63 dans les cas visés au paragraphe 3 du présent article.

5. Les autorisations accordées par un État membre ou une autorité de contrôle sur le fondement de l'article 26, paragraphe 2, de la directive 95/46/CE demeurent valables jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par ladite autorité de contrôle. Les décisions adoptées par la Commission sur le fondement de l'article 26, paragraphe 4, de la directive 95/46/CE demeurent en vigueur jusqu'à leur modification, leur remplacement ou leur abrogation, si nécessaire, par une décision de la Commission adoptée conformément au paragraphe 2 du présent article.

Article 47

Règles d'entreprise contraignantes

1. L'autorité de contrôle compétente approuve des règles d'entreprise contraignantes conformément au mécanisme de contrôle de la cohérence prévu à l'article 63, à condition que:

- a) ces règles soient juridiquement contraignantes, et soient mises en application par toutes les entités concernées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe, y compris leurs employés;

- b) elles confèrent expressément aux personnes concernées des droits opposables en ce qui concerne le traitement de leurs données à caractère personnel; et
 - c) elles répondent aux exigences prévues au paragraphe 2.
2. Les règles d'entreprise contraignantes visées au paragraphe 1 précisent au moins:
- a) la structure et les coordonnées du groupe d'entreprises ou du groupe d'entreprises engagées dans une activité économique conjointe et de chacune de leurs entités;
 - b) les transferts ou l'ensemble des transferts de données, y compris les catégories de données à caractère personnel, le type de traitement et ses finalités, le type de personnes concernées affectées et le nom du ou des pays tiers en question;
 - c) leur nature juridiquement contraignante, tant interne qu'externe;
 - d) l'application des principes généraux relatifs à la protection des données, notamment la limitation de la finalité, la minimisation des données, la limitation des durées de conservation des données, la qualité des données, la protection des données dès la conception et la protection des données par défaut, la base juridique du traitement, le traitement de catégories particulières de données à caractère personnel, les mesures visant à garantir la sécurité des données, ainsi que les exigences en matière de transferts ultérieurs à des organismes qui ne sont pas liés par les règles d'entreprise contraignantes;
 - e) les droits des personnes concernées à l'égard du traitement et les moyens d'exercer ces droits y compris le droit de ne pas faire l'objet de décisions fondées exclusivement sur un traitement automatisé, y compris le profilage, conformément à l'article 22, le droit d'introduire une réclamation auprès de l'autorité de contrôle compétente et devant les juridictions compétentes des États membres conformément à l'article 79 et d'obtenir réparation et, le cas échéant, une indemnisation pour violation des règles d'entreprise contraignantes;
 - f) l'acceptation, par le responsable du traitement ou le sous-traitant établi sur le territoire d'un État membre, de l'engagement de sa responsabilité pour toute violation des règles d'entreprise contraignantes par toute entité concernée non établie dans l'Union; le responsable du traitement ou le sous-traitant ne peut être exonéré, en tout ou en partie, de cette responsabilité que s'il prouve que le fait générateur du dommage n'est pas imputable à l'entité en cause;
 - g) la manière dont les informations sur les règles d'entreprise contraignantes, notamment en ce qui concerne les éléments mentionnés aux points d), e) et f) du présent paragraphe sont fournies aux personnes concernées, en sus des informations visées aux articles 13 et 14;
 - h) les missions de tout délégué à la protection des données, désigné conformément à l'article 37, ou de toute autre personne ou entité chargée de la surveillance du respect des règles d'entreprise contraignantes au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, ainsi que le suivi de la formation et le traitement des réclamations;
 - i) les procédures de réclamation;
 - j) les mécanismes mis en place au sein du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe pour garantir que le contrôle du respect des règles d'entreprise contraignantes. Ces mécanismes prévoient des audits sur la protection des données et des méthodes assurant que des mesures correctrices seront prises pour protéger les droits de la personne concernée. Les résultats de ce contrôle devraient être communiqués à la personne ou à l'entité visée au point h) et au conseil d'administration de l'entreprise qui exerce le contrôle du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, et devraient être mis à la disposition de l'autorité de contrôle compétente sur demande;
 - k) les mécanismes mis en place pour communiquer et consigner les modifications apportées aux règles et pour communiquer ces modifications à l'autorité de contrôle;
 - l) le mécanisme de coopération avec l'autorité de contrôle mis en place pour assurer le respect des règles par toutes les entités du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, notamment en mettant à la disposition de l'autorité de contrôle les résultats des contrôles des mesures visés au point j);
 - m) les mécanismes permettant de communiquer à l'autorité de contrôle compétente toutes les obligations juridiques auxquelles une entité du groupe d'entreprises, ou du groupe d'entreprises engagées dans une activité économique conjointe, est soumise dans un pays tiers qui sont susceptibles d'avoir un effet négatif important sur les garanties fournies par les règles d'entreprise contraignantes; et
 - n) la formation appropriée en matière de protection des données pour le personnel ayant un accès permanent ou régulier aux données à caractère personnel.

3. La Commission peut, pour les règles d'entreprise contraignantes au sens du présent article, préciser la forme de l'échange d'informations entre les responsables du traitement, les sous-traitants et les autorités de contrôle, ainsi que les procédures qui s'y rapportent. Ces actes d'exécution sont adoptés en conformité avec la procédure d'examen visée à l'article 93, paragraphe 2.

Article 48

Transferts ou divulgations non autorisés par le droit de l'Union

Toute décision d'une juridiction ou d'une autorité administrative d'un pays tiers exigeant d'un responsable du traitement ou d'un sous-traitant qu'il transfère ou divulgue des données à caractère personnel ne peut être reconnue ou rendue exécutoire de quelque manière que ce soit qu'à la condition qu'elle soit fondée sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre, sans préjudice d'autres motifs de transfert en vertu du présent chapitre.

Article 49

Déroghations pour des situations particulières

1. En l'absence de décision d'adéquation en vertu de l'article 45, paragraphe 3, ou de garanties appropriées en vertu de l'article 46, y compris des règles d'entreprise contraignantes, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale ne peut avoir lieu qu'à l'une des conditions suivantes:

- a) la personne concernée a donné son consentement explicite au transfert envisagé, après avoir été informée des risques que ce transfert pouvait comporter pour elle en raison de l'absence de décision d'adéquation et de garanties appropriées;
- b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement ou à la mise en œuvre de mesures précontractuelles prises à la demande de la personne concernée;
- c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu dans l'intérêt de la personne concernée entre le responsable du traitement et une autre personne physique ou morale;
- d) le transfert est nécessaire pour des motifs importants d'intérêt public;
- e) le transfert est nécessaire à la constatation, à l'exercice ou à la défense de droits en justice;
- f) le transfert est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'autres personnes, lorsque la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement;
- g) le transfert a lieu au départ d'un registre qui, conformément au droit de l'Union ou au droit d'un État membre, est destiné à fournir des informations au public et est ouvert à la consultation du public en général ou de toute personne justifiant d'un intérêt légitime, mais uniquement dans la mesure où les conditions prévues pour la consultation dans le droit de l'Union ou le droit de l'État membre sont remplies dans le cas d'espèce.

Lorsqu'un transfert ne peut pas être fondé sur une disposition de l'article 45 ou 46, y compris les dispositions relatives aux règles d'entreprise contraignantes, et qu'aucune des dérogations pour des situations particulières visées au premier alinéa du présent paragraphe n'est applicable, un transfert vers un pays tiers ou à une organisation internationale ne peut avoir lieu que si ce transfert ne revêt pas de caractère répétitif, ne touche qu'un nombre limité de personnes concernées, est nécessaire aux fins des intérêts légitimes impérieux poursuivis par le responsable du traitement sur lesquels ne prévalent pas les intérêts ou les droits et libertés de la personne concernée, et si le responsable du traitement a évalué toutes les circonstances entourant le transfert de données et a offert, sur la base de cette évaluation, des garanties appropriées en ce qui concerne la protection des données à caractère personnel. Le responsable du traitement informe l'autorité de contrôle du transfert. Outre qu'il fournit les informations visées aux articles 13 et 14, le responsable du traitement informe la personne concernée du transfert et des intérêts légitimes impérieux qu'il poursuit.

2. Un transfert effectué en vertu du paragraphe 1, premier alinéa, point g), ne porte pas sur la totalité des données à caractère personnel ni sur des catégories entières de données à caractère personnel contenues dans le registre. Lorsque le registre est destiné à être consulté par des personnes justifiant d'un intérêt légitime, le transfert n'est effectué qu'à la demande de ces personnes ou lorsqu'elles en sont les destinataires.

3. Les points a), b), et c) du premier alinéa du paragraphe 1 et le deuxième alinéa du paragraphe 1 ne sont pas applicables aux activités des autorités publiques dans l'exercice de leurs prérogatives de puissance publique.
4. L'intérêt public visé au paragraphe 1, premier alinéa, point d), est reconnu par le droit de l'Union ou le droit de l'État membre auquel le responsable du traitement est soumis.
5. En l'absence de décision d'adéquation, le droit de l'Union ou le droit d'un État membre peut, pour des motifs importants d'intérêt public, fixer expressément des limites au transfert de catégories spécifiques de données à caractère personnel vers un pays tiers ou à une organisation internationale. Les États membres notifient de telles dispositions à la Commission.
6. Le responsable du traitement ou le sous-traitant documente, dans les registres visés à l'article 30, l'évaluation ainsi que les garanties appropriées visées au paragraphe 1, deuxième alinéa, du présent article.

Article 50

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

La Commission et les autorités de contrôle prennent, à l'égard des pays tiers et des organisations internationales, les mesures appropriées pour:

- a) élaborer des mécanismes de coopération internationale 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, y compris 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 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 51

Autorité de contrôle

1. Chaque État membre prévoit qu'une ou plusieurs autorités publiques indépendantes sont chargées de surveiller l'application du présent règlement, 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 dénommée «autorité de contrôle»).
2. Chaque autorité de contrôle contribue à l'application cohérente du présent règlement 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. Lorsqu'un État membre institue plusieurs autorités de contrôle, il désigne celle qui représente ces autorités au comité et définit le mécanisme permettant de s'assurer du respect, par les autres autorités, des règles relatives au mécanisme de contrôle de la cohérence visé à l'article 63.
4. Chaque État membre notifie à la Commission les dispositions légales qu'il adopte en vertu du présent chapitre, au plus tard, le 25 mai 2018 et, sans tarder, toute modification ultérieure les affectant.