Ministerio de Justicia

DÉCRET ROYAL 1720/2007, DU 21 DÈCEMBRE, PORTANT APROBATION DU RÈGLAMENT D´ APPLICATION DE LA LOI ORGANIQUE 15/1999, DU 13 DÉCEMBRE, RELATIVE À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

2012

Colección: Traducciones del derecho español

Edita:

Ministerio de Justicia- Secretaría General Técnica

NIPO: 051-12-031-7

Traducción realizada por: Verbatim, S.A

Maquetación: Subdirección General de Documentación y Publicaciones

DÉCRET ROYAL 1720/2007, DU 21 DÉCEMBRE, PORTANT APPROBATION DU RÈGLEMENT D'APPLICATION DE LA LOI ORGANIQUE 15/1999, DU 13 DÉCEMBRE, RELATIVE À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL.

Publication : BOE numéro 17, du 19.01.2008

L'actuelle loi organique 15/1999, du 13 décembre, relative à la protection des données à caractère personnel a adapté notre système juridique aux dispositions de la directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, abrogeant ainsi la loi organique 5/1992, du 29 octobre, sur la régulation du traitement automatisé de données à caractère personnel, qui était en vigueur.

La nouvelle loi, qui a vu le jour avec une vocation marquée de généralité, stipule dans son article 1er « qu'elle a pour but de garantir et de protéger, en ce qui concerne le traitement de données à caractère personnel, les libertés publiques et les droits fondamentaux des personnes physiques et, en particulier, leur honneur et leur intimité personnelle ». Elle vise par conséquent les traitements automatisés et non automatisés de données à caractère personnel.

Afin de garantir la sécurité juridique nécessaire dans un domaine aussi sensible pour les droits fondamentaux qu'est celui de la protection des données, le législateur a déclaré le maintien des normes réglementaires existantes et, en particulier, du décret royal 428/1993, du 26 mars, portant approbation du statut de l'Agence de protection des données, du décret royal 1332/1994, du 20 juin, développant certains aspects de la loi organique 5/1992, du 29 octobre, sur la régulation du traitement automatisé de données à caractère personnel et du décret royal 994/1999, du 11 juin, portant approbation du règlement des mesures de sécurité des fichiers automatisés contenant des données à caractère personnel, tout en autorisant le gouvernement à approuver ou à modifier les dispositions réglementaires nécessaires à l'application et au développement de la loi organique 15/1999.

Par ailleurs, la loi 34/2002, du 11 juillet, sur les services de la société de l'information et du commerce électronique, et la loi 32/2003, du 3 novembre, à caractère général sur les télécommunications attribuent des compétences en matière de sanction à l'Agence espagnole de protection des données. Celles-ci doivent faire l'objet d'un développement réglementaire avec la particularité que les deux normes citées sont soumises à la tutelle non seulement des droits des personnes physiques, mais également des personnes morales.

II

Ce règlement partage avec la loi organique la mission d'affronter les risques que la collecte et le traitement de données à caractère personnel peuvent supposer pour les droits de la personnalité. Il faut par conséquent souligner que cette norme réglementaire est née avec la vocation de ne pas réitérer les contenus de la norme supérieure et de développer non seulement les préceptes contenus dans la loi organique en vertu des principes qui émanent de la directive, mais également ceux dont l'application pendant cette période de validité de la loi a démontré la nécessité d'un développement normatif plus important.

Ce règlement est donc approuvé en partant de la nécessité d'assurer la cohérence de la norme réglementaire dans tous les aspects liés à la transposition de la directive et de développer les aspects novateurs de la loi organique 15/1999 ainsi que ceux pour lesquels l'expérience a recommandé un certain degré de précision qui attribue une sécurité juridique au système.

III

Le règlement couvre le domaine visé auparavant par les décrets royaux 1332/1994, du 20 juin, et 994/1999, du 11 juin, en tenant compte de la nécessité de fixer des critères applicables aux fichiers et aux traitements non automatisés de données à caractère personnel. Par ailleurs, la loi 34/2002, du 11 juillet, sur les services de la société de l'information et du commerce électronique, et la loi 32/2003, du 3 novembre, à caractère général, sur les télécommunications attribuent des compétences en matière de sanction à l'Agence espagnole de protection des données.

Le règlement s'articule autour de neuf titres dont les contenus développent les principaux aspects dans ce domaine.

Le titre Ier aborde l'objet et le champ d'application du règlement. On a ressenti la nécessité, tout au long de la validité de la loi organique 15/1999, de développer l'alinéa 2 de l'article 2 de la loi citée afin de préciser ce que recouvrent les notions de fichiers et de traitements liés aux activités personnelles ou domestiques, un aspect très important dès lors que ces notions sont exclues de la norme relative à la protection des données à caractère personnel.

Par ailleurs, le présent règlement ne contient aucune disposition concernant les traitements de données à caractère personnel visés à l'alinéa 3 de l'article 2 de la loi organique, étant donné qu'ils sont régis par leurs dispositions spécifiques et, le cas échéant, par les dispositions spécifiquement établies à ce sujet par la propre loi organique 15/1999. Ceci signifie qu'on maintiendra le régime juridique propre de ces traitements et fichiers.

Ce titre contient également une série de définitions qui contribueront à la bonne compréhension de la norme, ce qui s'avère particulièrement nécessaire dans un domaine aussi technicisé que celui de la protection des données à caractère personnel. D'autre part, il fixe le critère à suivre en matière de calcul des délais afin d'uniformiser cette question et d'éviter les distinctions qui impliqueraient des différences de traitement entre les fichiers publics et les fichiers privés.

Le titre II se réfère aux principes de la protection des données. La réglementation du mode d'obtention du consentement est particulièrement importante car elle tient compte d'aspects très spécifiques comme le cas des services de communications électroniques et, en particulier, la collecte de données auprès des mineurs. Ce titre propose également ce qui peut être défini comme un statut de la personne chargée du traitement, qui contribuera sans aucun doute à clarifier tout ce qui a trait à cette figure. Les dispositions dans ce domaine sont complétées par les dispositions du titre VIII en matière de sécurité, qui inscrivent l'action de la personne chargée du traitement dans un cadre cohérent.

Le titre III aborde une question aussi essentielle que celle des droits des personnes dans ce domaine. Ces droits d'accès, de rectification, d'annulation et d'opposition au traitement, comme l'a affirmé la Cour constitutionnelle dans son jugement 292/2000, constituent la gamme de facultés qui émanent du droit fondamental à la protection des données et qui « servent à la fonction capitale que remplit ce droit fondamental : garantir à la personne un pouvoir de contrôle sur ses données à caractère personnel, ce qui n'est possible et efficace que si l'on impose aux tiers les obligations citées ».

Ensuite, les titres IV à VII permettent de clarifier des aspects importants pour le trafic ordinaire tels que l'application de critères spécifiques à un certain type de fichiers privé, qui l'exigeraient en raison de leur importance – ceux qui ont trait à la solvabilité patrimoniale et au crédit et ceux qui sont utilisés dans des activités de publicité et de prospection commerciale –, l'ensemble des obligations matérielles et formelles qui doivent amener les responsables à la création et à l'inscription des fichiers, les critères et les procédures pour effectuer des transferts internationaux de données et, enfin, la réglementation d'un instrument, le code type, qui est appelé à jouer un rôle de plus en plus important comme facteur dynamisant du droit fondamental à la protection des données.

Le titre VIII régit un aspect essentiel pour la tutelle du droit fondamental à la protection des données – la sécurité –qui a des répercussions sur de nombreux aspects organisationnels, de gestion et même d'investissement, dans toutes les organisations qui traitent des données à caractère personnel. La répercussion de l'obligation de sécurité exigeait une rigueur particulière étant donné que cette matière était le point de convergence de différents éléments très importants. D'une part, l'expérience provenant de l'application du décret royal 994/1999 a permis de connaître les difficultés qu'avaient rencontrées les responsables et d'identifier les points faibles et les points forts de la réglementation. D'autre part, la société réclamait l'adaptation de la réglementation dans différents domaines. Dans ce sens, le règlement cherche à être particulièrement rigoureux dans l'attribution des niveaux de sécurité, dans l'établissement des mesures qui doivent être adoptées dans chaque cas et dans la révision de celles-ci lorsque cela s'avère nécessaire. Par ailleurs, il ordonne de façon plus précise le contenu et les obligations liées au maintien du document de sécurité. En outre, on a cherché à réglementer la matière de sorte à tenir compte des multiples formes d'organisation matérielle et personnelle de la sécurité qui existent dans la pratique. Enfin, le règlement régit un ensemble de mesures destinées aux fichiers et aux traitements structurés et non automatisés, qui offrent un champ d'action clair aux responsables.

Finalement, il a été décidé dans le titre IX, qui est consacré aux procédures réalisées par l'Agence espagnole de protection des données, de réglementer exclusivement les particularités qui différencient les diverses procédures réalisées par l'Agence des normes générales prévues pour les procédures dans la loi 30/1992, du 26 novembre, relative au régime juridique des administrations publiques et de la procédure administrative commune, qui s'appliquera de façon supplétoire au présent règlement.

En foi de quoi, suite à la proposition du ministre de la Justice et après avoir obtenu l'approbation de la ministre des Administrations publiques, en conformité avec le Conseil d'État et après délibération du Conseil des ministres réuni le 21 décembre 2007,

IL A ÉTÉ DÉCIDÉ CE QUI SUIT:

Article unique. Approbation du règlement.

Le règlement d'application de la loi organique 15/1999, du 13 décembre, relative à la protection des données à caractère personnel, dont le texte est inclus ci-dessous, est approuvé.

Première disposition transitoire. Adaptation des codes type inscrits au registre général de protection des données.

Les modifications qui devront être apportées aux codes type inscrits au registre général de protection des données afin d'adapter leur contenu aux dispositions du titre VII de ce décret royal devront être notifiées à l'Agence espagnole de protection des données dans le délai de un an à compter de l'entrée en vigueur de ce décret royal.

Deuxième disposition transitoire. Délais de mise en œuvre des mesures de sécurité.

La mise en œuvre des mesures de sécurité prévues dans ce décret royal devra être réalisée conformément aux règles suivantes:

1er. En ce qui concerne les fichiers automatisés qui existeront à la date d'entrée en vigueur de ce décret royal:

a) On appliquera, dans le délai de un an à compter de son entrée en vigueur, les mesures de sécurité de niveau moyen qui sont exigibles aux fichiers suivants:

1. Les fichiers dont sont responsables les sociétés de gestion et de services communs de la sécurité sociale et qui ont trait à l'exercice de leurs compétences.

2. Les fichiers dont sont responsables les mutuelles d'accidents de travail et de maladies professionnelles de la sécurité sociale.

3. Les fichiers contenant un ensemble de données à caractère personnel qui offrent une définition des caractéristiques ou de la personnalité des citoyens et qui permettent d'évaluer certains aspects de la personnalité ou du comportement de ces derniers, alors que des mesures de ce niveau ne seraient pas exigibles conformément aux dispositions de l'article 4.4 du règlement des mesures de sécurité des fichiers automatisés de données à caractère personnel, approuvé dans le décret royal 994/1999, du 11 juin.

b) On appliquera, dans le délai de un an à compter de l'entrée en vigueur du décret, les mesures de sécurité de niveau moyen et, dans le délai de dix–huit mois à compter de cette date, celles du niveau supérieur qui sont exigibles aux fichiers suivants:

1. Les fichiers contenant des données issues d'actes de violence conjugale.

2. Les fichiers dont sont responsables les opérateurs qui fournissent des services de communication électronique disponibles au public ou qui exploitent des réseaux publics de communication électronique en ce qui concerne les données de trafic et les données de localisation.

c) Dans les autres cas, lorsque le présent règlement exige la mise en œuvre d'une mesure additionnelle, non prévue dans le règlement des mesures de sécurité des fichiers automatisés de données à caractère personnel, approuvé dans le décret royal 994/1999, du 11 juin, cette mesure devra être mise en œuvre dans le délai de un an à compter de l'entrée en vigueur du présent décret royal.

2me. En ce qui concerne les fichiers non automatisés qui existeront à la date d'entrée en vigueur de ce décret royal:

a) Les mesures de sécurité de niveau élémentaire devront être mises en œuvre dans le délai de un an à compter de son entrée en vigueur.

b) Les mesures de sécurité de niveau moyen devront être mises en œuvre dans le délai de dix-huit mois à compter de son entrée en vigueur.

c) Les mesures de sécurité de niveau supérieur devront être mises en œuvre dans le délai de deux ans à compter de son entrée en vigueur.

3me. Les fichiers, qu'ils soient ou non automatisés, qui seront créés après la date d'entrée en vigueur du présent décret royal devront avoir intégré, dès le moment de leur création, l'ensemble des mesures de sécurité régies dans ce décret.

Troisième disposition transitoire. Régime transitoire des demandes concernant l'exercice des droits des personnes.

Le présent décret royal ne sera pas applicable aux demandes concernant l'exercice des droits d'accès, d'opposition, de rectification et d'annulation qui auraient été introduites avant son entrée en vigueur. Ces demandes seront régies par le règlement antérieur.

Quatrième disposition transitoire. Régime transitoire des procédures.

Le présent décret royal ne sera pas applicable aux procédures qui auraient été engagées avant son entrée en vigueur. Ces procédures seront régies par le règlement antérieur.

Cinquième disposition transitoire. Régime transitoire des actes préliminaires.

Le présent décret royal ne sera pas applicable aux actes préliminaires qui auraient été engagés avant son entrée en vigueur. Ces actes seront régis par le règlement antérieur.

Le présent décret royal s'appliquera aux actes préliminaires qui seraient engagés après son entrée en vigueur.

Disposition abrogatoire unique. Abrogation réglementaire.

Sont abrogés le décret royal 1332/1994, du 20 juin, développant certains aspects de la loi organique 5/1992, du 29 octobre, sur la régulation du traitement automatisé de données à caractère personnel, le décret royal 994/1999, du 11 juin, portant approbation du règlement des mesures de sécurité des fichiers automatisés contenant des données à caractère personnel et toutes les normes d'un rang égal ou inférieur qui contrediraient ou s'opposeraient aux dispositions du présent décret royal.

Première disposition finale. Attribution de compétence.

Le titre Ier, exception faite de la lettre c) de l'article 4, les titres II, III, VII et VIII, ainsi que les articles 52, 53.3, 53.4, 54, 55.1, 55.3, 56, 57, 58 et 63.3 du règlement sont énoncés conformément aux dispositions de l'article 149.1.1. de la Constitution, qui attribue à l'État la compétence exclusive de régir les conditions de base garantissant l'égalité de tous les citoyens espagnols dans l'exercice des droits et dans le respect des obligations constitutionnelles.

Seconde disposition finale. Entrée en vigueur.

Le présent décret royal entrera en vigueur trois mois après sa publication intégrale au Journal officiel de l'État espagnol.

RÈGLEMENT D'APPLICATION DE LA LOI ORGANIQUE 15/1999, DU 13 DÉCEMBRE, RELATIVE À LA PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

TITRE IER

Dispositions générales

Article 1. Objet.

1. Le présent règlement a pour objet l'application de la loi organique 15/1999, du 13 décembre, relative à la protection des données à caractère personnel.

2. Par ailleurs, le chapitre III du titre IX de ce règlement développe les dispositions relatives à l'exercice du pouvoir de sanction par l'Agence espagnole de protection des données, en application des dispositions de la loi organique 15/1999, du 13 décembre, du titre VII de la loi 34/2002, du 11 juillet, sur les services de la société de l'information et du commerce électronique, et du titre VIII de la loi 32/2003, du 3 novembre, à caractère général, sur les télécommunications.

Article 2. Champ objectif d'application.

1. Le présent règlement s'appliquera aux données à caractère personnel enregistrées sur un support physique, qui les rendrait susceptibles d'être traitées, et à toute modalité d'utilisation ultérieure de ces données par les secteurs public et privé.

2. Ce règlement ne sera pas applicable aux traitements de données concernant des personnes morales ni aux fichiers qui se limiteraient à introduire les données des personnes physiques fournissant leurs services au sein de celles–ci, qui ne comprendraient que leur nom, les fonctions ou postes exercés ainsi que l'adresse postale ou électronique, les numéros de téléphone et de fax professionnels.

3. De même, on considérera que les données concernant des entrepreneurs individuels seront exclues du régime d'application de la protection des données à caractère personnel si elles font référence à ceux-ci en leur qualité de commerçants, d'industriels ou d'armateurs.

4. Ce règlement ne sera pas applicable aux données concernant des personnes décédées. Ceci étant, les personnes liées au défunt pour des raisons familiales ou analogues, pourront s'adresser aux responsables des fichiers ou des traitements qui contiendraient des données de ce dernier dans le but de notifier le décès moyennant la présentation des documents requis à cet effet et demander, le cas échéant, l'annulation des données.

Article 3. Champ territorial d'application.

1. Le présent règlement régira tout traitement de données à caractère personnel:

a) Lorsque le traitement est effectué dans le cadre des activités d'un établissement du responsable du traitement, à condition que cet établissement soit situé sur le territoire espagnol.

   Si la disposition visée au paragraphe précédent n'est pas applicable, mais qu'il existe un responsable du traitement établi en Espagne, le traitement sera soumis aux normes contenues dans le titre VIII du présent règlement.

b) Lorsque le responsable du traitement établi hors du territoire espagnol est soumis à la législation espagnole en vertu des normes de droit international public.

c) Lorsque le responsable du traitement n'est pas établi sur le territoire de l'Union européenne et utilise, dans le traitement des données, des moyens situés sur le territoire espagnol, sauf si ces moyens sont utilisés uniquement à des fins de transit.

   Dans ce cas, le responsable du traitement devra désigner un représentant établi sur le territoire espagnol.

2. Aux fins prévues aux alinéas précédents, on entendra par établissement, quelle que soit sa forme juridique, toute installation stable qui permet l'exercice effectif et réel d'une activité.

Article 4. Fichiers ou traitements exclus.

Le régime de protection des données à caractère personnel qui est établi dans le présent règlement ne sera pas applicable aux fichiers et traitements suivants

a) À ceux qui sont réalisés ou maintenus par des personnes physiques dans l'exercice d'activités exclusivement personnelles ou domestiques.

Ne seront considérés liés à des activités personnelles ou domestiques que les traitements concernant les activités qui s'inscrivent dans le cadre de la vie privée ou familiale des particuliers.

b) À ceux qui sont soumis au règlement sur la protection des matières classées.

c) À ceux qui sont établis pour la recherche du terrorisme et de formes graves de délinquance organisée. Ceci dit, le responsable du fichier communiquera au préalable l'existence du fichier, ses caractéristiques générales et sa finalité à l'Agence espagnole de protection des données.

Article 5. Définitions.

1. Aux fins de ce règlement, on entend par:

a) Personne concernée ou intéressé: la personne physique titulaire des données qui font l'objet du traitement.

b) Annulation: la procédure en vertu de laquelle le responsable cesse d'utiliser les données. L'annulation impliquera le blocage des données, qui consistera en l'identification et en la réserve de ces dernières afin d'empêcher leur traitement si ce n'est pour les mettre à la disposition des administrations publiques, des juges et des tribunaux afin d'assumer les éventuelles responsabilités issues du traitement et ce, uniquement pendant le délai de prescription de ces responsabilités. Ce délai écoulé, on devra procéder à la suppression des données.

c) Cession ou communication de données: le traitement de données qui implique la transmission de celles-ci à une personne différente de l'intéressé.

d) Consentement de l'intéressé: toute manifestation de volonté libre, sans équivoque, spécifique et informée par laquelle l'intéressé accepte le traitement de données à caractère personnel le concernant.

e) Donnée dissociée: celle qui ne permet pas l'identification d'une personne concernée.

f) Données à caractère personnel: toute information numérique, alphabétique, graphique, photographique, acoustique ou d'une quelconque autre nature concernant des personnes physiques identifiées ou identifiables.

g) Données à caractère personnel liées à la santé: les informations concernant la santé passée, présente et future, physique ou mentale, d'un individu. En particulier, on considère comme données liées à la santé des personnes celles qui ont trait à leur pourcentage de handicap et à leur information génétique.

h) Destinataire ou cessionnaire: la personne physique ou morale, publique ou privée, ou l'organe administratif auquel sont révélées les données.

Les entités dépourvues de personnalité juridique qui interviennent dans le trafic en qualité de sujets différenciés pourront également être des destinataires.

i) Personne chargée du traitement: la personne physique ou morale, publique ou privée, ou l'organe administratif qui, seul ou conjointement avec d'autres, traite des données à caractère personnel pour le compte du responsable du traitement ou du responsable du fichier suite à l'existence d'une relation juridique qui le lie à celui-ci et qui délimite son champ d'action aux fins de la prestation du service.

Les entités dépourvues de personnalité juridique, qui interviennent dans le trafic en qualité de sujets différenciés, pourront également être chargées du traitement.

j) Exportateur de données à caractère personnel: la personne physique ou morale, publique ou privée, ou l'organe administratif situé sur le territoire espagnol qui réalise, conformément aux dispositions du présent règlement, un transfert de données à caractère personnel vers un pays tiers.

k) Fichier: tout ensemble structuré de données à caractère personnel qui permet l'accès aux données selon des critères déterminés, quelle que soit la forme ou la modalité de sa création, de son stockage, de son organisation et de son accès.

l) Fichiers privés: les fichiers dont sont responsables les personnes, les entreprises ou les entités de droit privé, quels que soient les détenteurs de leur capital ou la provenance de leurs ressources économiques, ainsi que les fichiers dont sont responsables les corporations de droit public, lorsque ceux–ci ne sont pas strictement liés à l'exercice des pouvoirs de droit public qui leur sont attribués par leur réglementation spécifique.

m) Fichiers publics: les fichiers dont sont responsables les organes constitutionnels ou à caractère constitutionnel de l'État ou les institutions régionales ayant des fonctions analogues à ceux–ci, les administrations publiques territoriales ainsi que les entités ou organismes liés ou dépendant de celles–ci et les corporations de droit public à condition que leur finalité soit l'exercice des pouvoirs de droit public

n) Fichier non automatisé: tout ensemble de données à caractère personnel organisé de façon non automatisée et structuré conformément à des critères spécifiques concernant des personnes physiques, qui permet d'accéder sans efforts disproportionnés à leurs données à caractère personnel, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.

ñ) Importateur de données à caractère personnel: la personne physique ou morale, publique ou privée, ou l'organe administratif récepteur des données en cas de transfert international de ces dernières à un pays tiers, qu'il s'agisse du responsable du traitement, de la personne chargée du traitement ou d'un tiers.

o) Personne identifiable: toute personne dont l'identité peut être déterminée, directement ou indirectement, au moyen de n'importe quelle information concernant son identité physique, physiologique, psychique, économique, culturelle ou sociale. Une personne physique ne sera pas réputée identifiable si cette identification requiert des délais ou des activités disproportionnés.

p) Procédure de dissociation: tout traitement de données à caractère personnel qui permet l'obtention de données dissociées.

q) Responsable du fichier ou du traitement: la personne physique ou morale, de nature publique ou privée, ou l'organe administratif qui, seul ou conjointement avec d'autres, décide de la finalité, du contenu et de l'utilisation du traitement, même s'il n'en est pas l'auteur matériel.

   Les entités dépourvues de personnalité juridique, qui interviennent dans le trafic en qualité de sujets différenciés, pourront également être responsables du fichier ou du traitement.

r) Tiers: la personne physique ou morale, publique ou privée, ou l'organe administratif autre que l'intéressé, que le responsable du traitement, que le responsable du fichier, que la personne chargée du traitement et que les personnes autorisées à traiter les données sous l'autorité directe du responsable du traitement ou de la personne chargée du traitement.

   Les entités dépourvues de personnalité juridique, qui interviennent dans le trafic en qualité de sujets différenciés, pourront également être des tiers.

s) Transfert international de données: le traitement de données impliquant une transmission de celles–ci à l'extérieur du territoire de l'espace économique européen, qu'il constitue une cession ou une communication de données ou qu'il ait pour objet la réalisation d'un traitement de données pour le compte du responsable du fichier établi sur le territoire espagnol

t) Traitement de données: toute opération ou tout procédé technique, automatisé ou non, qui permet la collecte, l'enregistrement, la conservation, l'élaboration, la modification, la consultation, l'utilisation, l'annulation, le blocage ou la suppression ainsi que les cessions de données résultant de communications, de consultations, d'interconnexion et de transferts.

2. En particulier, au sujet des dispositions du titre VIII de ce règlement, on entend par:

a) Accès autorisés: les autorisations concédées à un utilisateur concernant l'utilisation des différentes ressources. Le cas échéant, ils incluront les autorisations ou fonctions qui auront été attribuées à un utilisateur par délégation du responsable du fichier ou du traitement ou du responsable de la sécurité.

b) Authentification: la procédure de vérification de l'identité d'un utilisateur.

c) Mot de passe: l'information confidentielle, souvent constituée d'une chaîne de caractères, qui peut être utilisée dans l'authentification d'un utilisateur ou pour accéder à une ressource.

d) Contrôle d'accès: le mécanisme qui, en fonction de l'identification authentifiée au préalable, permet d'accéder aux données ou aux ressources.

e) Copie de sécurité: la copie des données d'un fichier automatisé sur un support qui permet de les récupérer.

f) Document: tout écrit, graphique, son, image ou n'importe quel type d'information qui peut être traitée dans un système d'information en tant qu'unité différenciée.

g) Fichiers temporaires: les fichiers de travail créés par des utilisateurs ou des procédés qui sont nécessaires aux fins d'un traitement occasionnel ou comme étape intermédiaire pendant la réalisation d'un traitement.

h) Identification: la procédure de reconnaissance de l'identité d'un utilisateur.

i) Incident: toute anomalie qui affecte ou peut affecter la sécurité des données.

j) Profil d'utilisateur: les accès autorisés à un groupe d'utilisateurs.

k) Ressource: n'importe quel élément faisant partie d'un système d'information.

l) Responsable de sécurité: la personne ou les personnes auxquelles le responsable du fichier a assigné formellement la fonction de coordonner et de contrôler les mesures de sécurité applicables.

m) Système d'information: l'ensemble de fichiers, de traitements, de programmes, de supports et, le cas échéant, d'appareils utilisés pour le traitement de données à caractère personnel.

n) Système de traitement: le mode d'organisation ou d'utilisation d'un système d'information. Selon le système de traitement choisi, les systèmes d'information pourront être automatisés, non automatisés ou partiellement automatisés.

ñ) Support: l'objet physique qui stocke ou contient des données ou des documents, ou l'objet susceptible d'être traité dans un système d'information et sur lequel on peut enregistrer et récupérer des données.

o) Transmission de documents: tout transfert, communication, envoi, remise ou divulgation de l'information contenue dans ces documents.

p) Utilisateur: le sujet ou le processus autorisé à accéder aux données ou aux ressources. Seront considérés utilisateurs les processus qui permettent d'accéder aux données ou aux ressources sans identification d'un utilisateur physique.

Article 6. Calcul des délais.

Dans le cas où ce règlement indiquera un délai par jour, on ne comptera que les jours ouvrables. Si le délai est établi par mois, on le calculera d'une date à une autre.

Article 7. Sources accessibles au public.

1. Aux effets de l'article 3, lettre j) de la loi organique 15/1999, on estimera que les sources accessibles au public seront exclusivement:

a) Le recensement à des fins promotionnelles, régi conformément aux dispositions de la loi organique 15/1999, du 13 décembre.

b) Les guides de services de communication électronique dans les conditions prévues par leur règlement spécifique.

c) Les listes de personnes appartenant à des groupes de professionnels qui ne comprendront que les données concernant le nom, le titre, la profession, l'activité, le grade universitaire, l'adresse professionnelle et l'indication de leur appartenance au groupe. L'adresse professionnelle pourra inclure les données du siège social complet, le numéro de téléphone, le numéro de fax et l'adresse électronique. Dans le cas des ordres professionnels, on pourra indiquer comme données d'appartenance au groupe celles relatives au numéro de membre, à la date d'inscription et à la situation d'exercice professionnel.

d) Les journaux et bulletin officiels.

e) Les moyens de communication sociale.

2. En tout état de cause, pour que les cas mentionnés à l'alinéa précédent puissent être considérés comme des sources accessibles au public, il faudra que la consultation de ces sources puisse être réalisée par n'importe quelle personne, sans être soumise à une norme limitative, ou, le cas échéant, sans autre exigence que le versement d'une contre–prestation.

TITRE II

Des principes de la protection des données

CHAPITRE IER

De la qualité des données

Article 8. Principes relatifs à la qualité des données.

1. Les données à caractère personnel devront être traitées de façon loyale et licite. La collecte de données par des moyens frauduleux, déloyaux ou illicites est interdite.

2. Les données à caractère personnel ne pourront être collectées que pour satisfaire des finalités déterminées, explicites et légitimes du responsable du traitement.

3. Les données à caractère personnel qui feront l'objet d'un traitement ne pourront pas être utilisées pour des finalités incompatibles avec celles pour lesquelles elles auront été collectées.

4. Ne pourront faire l'objet d'un traitement que les données qui seront adéquates, pertinentes et non excessives au regard des finalités déterminées, explicites et légitimes pour lesquelles elles auront été obtenues.

5. Les données à caractère personnel seront exactes et mises à jour de sorte à refléter de façon véridique la situation actuelle de la personne concernée. Les données qui auront été recueillies directement de la personne concernée seront considérées exactes.

Si les données à caractère personnel soumises au traitement s'avèrent inexactes, en tout ou en partie, ou incomplètes, on les annulera et les remplacera d'office par les données rectifiées ou complétées correspondantes dans le délai de dix jours à partir du moment où l'on aura pris connaissance de l'inexactitude, sauf si la législation applicable au fichier prévoit une procédure ou un délai spécifique à cet effet.

Si les données ont été communiquées au préalable, le responsable du fichier ou du traitement devra notifier la rectification ou l'annulation réalisée au cessionnaire, pour autant que ce dernier soit connu, dans le délai de dix jours.

Le cessionnaire qui conserverait le traitement des données devra procéder à la rectification et à l'annulation notifiée, dans le délai de dix jours à compter de la réception de la notification.

Cette actualisation des données à caractère personnel n'exigera aucune communication à l'intéressé, sans préjudice de l'exercice par les intéressés des droits qui sont reconnus dans la loi organique 15/1999, du 13 décembre.

Les dispositions de cet alinéa s'entendent sans préjudice des facultés que reconnaît le titre III de ce règlement aux personnes concernées.

6. Les données à caractère personnel seront annulées lorsqu'elles auront cessé d'être nécessaires ou pertinentes au regard de la finalité pour laquelle elles auront été collectées ou enregistrées.

Elles pourront néanmoins être conservées aussi longtemps que pourra être exigé un quelconque type de responsabilité découlant d'une relation ou d'une obligation juridique ou de l'exécution d'un contrat ou de l'application de mesures précontractuelles demandées par l'intéressé.

Une fois que la période visée aux paragraphes précédents se sera écoulée, les données ne pourront être conservées qu'après avoir été dissociées, sans préjudice de l'obligation de blocage prévue dans la loi organique 15/1999, du 13 décembre, et dans le présent règlement.

7. Les données à caractère personnel seront traitées de sorte qu'elles permettent l'exercice du droit d'accès aussi longtemps qu'il n'y aura pas lieu de les annuler.

Article 9. Traitements à des fins statistiques, historiques ou scientifiques.

1. Le traitement de données à caractère personnel à des fins historiques, statistiques ou scientifiques ne sera pas considéré incompatible aux effets prévus à l'alinéa 3 de l'article précédent.

Pour déterminer les fins visées au paragraphe précédent, on s'en tiendra à la législation qui sera applicable dans chaque cas et, en particulier, aux dispositions de la loi 12/1989, du 9 mai, portant régulation de la fonction statistique publique, de la loi 16/1985, du 25 juin, sur le patrimoine historique espagnol et de la loi 13/1986, du 14 avril, sur la

promotion et la coordination générale de la recherche scientifique et technique, et de leurs dispositions d'application respectives, ainsi qu'au règlement régional dans ces matières.

2. À titre d'exception aux dispositions de l'alinéa 6 de l'article précédent, l'Agence espagnole de protection des données ou, le cas échéant, les autorités de contrôle des Communautés autonomes pourront décider, à la demande du responsable du traitement et conformément à la procédure établie dans la deuxième section du chapitre VII du titre IX du présent règlement, de maintenir intégralement certaines données en raison de leurs valeurs historiques, statistiques ou scientifiques conformément aux normes citées à l'alinéa précédent.

Article 10. Cas légitimant le traitement ou la cession des données.

1. Les données à caractère personnel ne pourront faire l'objet d'un traitement ou d'une cession que si l'intéressé y a consenti au préalable.

2. Ceci dit, le traitement ou la cession de données à caractère personnel sera possible sans consentement de l'intéressé:

a) Lorsqu'il sera autorisé par une norme ayant rang de loi ou par une norme de droit communautaire et, en particulier, lorsque se présentera un des cas suivants:

   Si le traitement ou la cession a pour objet la satisfaction d'un intérêt légitime du responsable du traitement ou du cessionnaire reconnu par ces normes, pour autant que ne prévalent pas l'intérêt ou les droits et les libertés fondamentales des intéressés qui sont prévus à l'article 1er de la loi organique 15/1999, du 13 décembre.

   Si le traitement ou la cession des données est nécessaire pour que le responsable du traitement remplisse une obligation qui lui serait imposée par une de ces normes.

b) (Annulé)[1]

3. Les données à caractère personnel pourront être traitées sans consentement de l'intéressé:

a) Si elles sont recueillies aux fins de l'exercice des fonctions propres des administrations publiques dans le cadre des compétences que leur attribue une norme ayant rang de loi ou une norme de droit communautaire.

b) Si elles sont recueillies par le responsable du traitement à l'occasion de la passation d'un contrat ou d'un précontrat ou de l'existence d'une relation d'affaires, de travail ou administrative à laquelle la personne concernée est partie et si elles sont nécessaires pour la maintenir ou l'exécuter.

c) Si le traitement des données a pour finalité la protection d'un intérêt vital de l'intéressé aux termes de l'alinéa 6 de l'article 7 de la loi organique 15/1999, du 13 décembre.

4. La cession des données à caractère personnel sans disposer du consentement de l'intéressé sera possible :

a) Lorsque la cession fait suite à l'acceptation libre et légitime d'une relation juridique dont le développement, l'exécution et le contrôle impliquent la communication des données. Dans ce cas, la communication ne sera légitime que dans la mesure où elle se limitera à la finalité qui la justifie.

b) Lorsque la communication qui doit être réalisée a pour destinataire le Médiateur, le Ministère public, les juges ou tribunaux, la Cour des comptes ou les institutions régionales ayant des fonctions analogues au Médiateur ou à la Cour des Comptes et qu'elle se produit dans le cadre des fonctions que la loi leur attribue expressément.

c) Lorsque la cession se réalise entre des administrations publiques et qu'un des cas suivants se présente :

   Si elle a pour objet le traitement des données à des fins historiques, statistiques ou scientifiques.

   Si les données à caractère personnel ont été collectées ou élaborées par une administration publique afin d'être transmises à une autre.

   Si la communication est réalisée aux fins de l'exercice de compétences identiques ou qui traitent des mêmes matières.

5. Les données jouissant d'une protection spéciale pourront être traitées et cédées dans les conditions prévues aux articles 7 et 8 de la loi organique 15/1999, du 13 décembre.

[1] Le paragraphe 2.b) est annulé par arrêts du Tribunal Supremo du 8 février 2012.

En particulier, le consentement de l'intéressé ne sera pas nécessaire pour communiquer des données à caractère personnel relatives à la santé, y compris par des moyens électroniques, entre des organismes, des centres et des services du système national de la santé, lorsque cette communication sera réalisée aux fins de l'attention sanitaire des personnes, conformément aux dispositions du chapitre V de la loi 16/2003, du 28 mai, relative à la cohésion et à la qualité du système national de la santé.

Article 11. Vérification de données dans des demandes présentées aux administrations publiques.

(Annulé)

CHAPITRE II

Du consentement au traitement des données et du devoir d'information

SECTION 1RE. OBTENTION DU CONSENTEMENT DE LA PERSONNE CONCERNÉE

Article 12. Principes généraux.

1. Le responsable du traitement devra obtenir le consentement de l'intéressé au traitement de ses données à caractère personnel, sauf dans les cas où ce consentement ne sera pas exigible conformément aux dispositions légalement établies.

La demande de consentement devra se rapporter à un traitement ou à une série de traitements concrets, en précisant la finalité pour laquelle ces données sont collectées ainsi que les autres conditions affectant le traitement ou la série de traitements.

2. Lorsqu'on demande le consentement de la personne concernée en vue de réaliser une cession de ses données, celle-ci doit être informée de sorte qu'elle connaisse clairement la finalité à laquelle seront destinées les données pour la communication desquelles on lui demande son consentement ainsi que le type d'activité réalisée par le cessionnaire. Dans le cas contraire, le consentement sera nul.

3. Il incombera au responsable du traitement de démontrer l'existence du consentement de la personne concernée à l'aide de n'importe quel moyen de preuve légalement admissible.

Article 13. Consentement au traitement de données de mineurs.

1. On pourra traiter les données des plus de quatorze ans avec leur consentement, sauf dans les cas où la loi exige pour leur prestation l'assistance des titulaires de l'autorité parentale ou de la tutelle. Dans le cas des enfants de moins de quatorze ans, on exigera le consentement des parents ou des tuteurs.

2. On ne pourra en aucun cas demander au mineur des données permettant d'obtenir des informations sur les autres membres du groupe familial ou sur les caractéristiques de ce dernier, comme des données relatives à l'activité professionnelle des parents, des informations économiques, des données sociologiques ou d'une quelconque autre nature sans le consentement des titulaires de ces données. On pourra néanmoins demander les données d'identité et l'adresse du père, de la mère ou du tueur dans le seul but d'obtenir l'autorisation prévue à l'alinéa précédent.

3. Lorsque le traitement porte sur des données de mineurs, l'information qui sera adressée à ces derniers devra être rédigée dans un langage qui leur sera facilement compréhensible en indiquant expressément les dispositions de cet article.

4. Il incombera au responsable du fichier ou du traitement d'établir les procédures garantissant qu'on aura effectivement vérifié l'âge du mineur et l'authenticité du consentement qui aurait éventuellement été donné par les parents, les tuteurs ou les représentants légaux.

Article 14. Mode d'obtention du consentement.

1. Le responsable du traitement pourra demander le consentement de l'intéressé à travers la procédure établie dans cet article, sauf lorsque la loi exige à ce dernier d'obtenir un consentement exprès au traitement des données.

2. Le responsable pourra s'adresser à la personne concernée pour l'informer dans les conditions prévues dans les articles 5 de la loi organique 15/1999, du 13 décembre, et 12.2 de ce règlement et devra lui concéder un délai de

trente jours pour qu'il puisse manifester son refus du traitement, en l'informant que son absence de réponse à cet égard signifiera qu'il acceptera le traitement de ces données à caractère personnel.

En particulier, lorsqu'il s'agit de responsables qui fournissent à la personne concernée un service générant des informations régulières ou réitérées, ou une facturation régulière, la communication pourra être adressée conjointement à ces informations ou à la facturation du service fourni, à condition qu'elle soit réalisée de façon bien visible.

3. En tout état de cause, il faudra que le responsable du traitement puisse savoir si la communication a été refusée pour une cause quelconque, auquel cas il ne pourra pas procéder au traitement des données concernant cette personne.

4. Il faudra mettre à la disposition de l'intéressé un moyen simple et gratuit pour refuser le traitement de ses données. En particulier, on considérera conformes au présent règlement les procédures dans lesquelles ce refus pourra se matérialiser, entre autres, par l'envoi d'une lettre préaffranchie au responsable du traitement ou par l'appel d'un numéro de téléphone gratuit ou des services d'attention au public que celui-ci aurait établis.

5. Lorsqu'on demande le consentement de l'intéressé par le biais de la procédure établie dans cet article, il ne sera pas possible de le redemander pour les mêmes traitements et pour les mêmes finalités dans le délai de un an à compter de la date de la demande précédente.

Article 15. Demande de consentement dans le cadre d'une relation contractuelle à des fins non liées directement à celle–ci.

Si le responsable du traitement demande le consentement de la personne concernée pendant le processus de passation d'un contrat pour des finalités qui n'ont pas de rapport direct avec le maintien, le développement ou le contrôle de la relation contractuelle, il devra permettre à la personne concernée de manifester expressément son refus du traitement ou de la communication des données.

En particulier, on estimera que cette obligation sera satisfaite si l'on permet à la personne concernée de cocher une case bien visible et qui n'est pas activée à l'avance dans le document qui lui est remis pour la passation du contrat ou si l'on prévoit une procédure équivalente qui lui permette de manifester son refus du traitement.

Article 16. Traitement des données de facturation et de trafic dans les services de communication électronique.

La demande de consentement au traitement ou à la cession des données de trafic, de facturation et de localisation par les sujets qui y sont obligés ou, le cas échéant, la révocation de celui–ci, selon la législation régissant les télécommunications, sera soumise aux dispositions de son règlement spécifique et, pour tout ce qui ne sera pas contraire à ce dernier, aux dispositions contenues dans la présente section.

Article 17. Révocation du consentement.

1. La personne concernée pourra révoquer son consentement en utilisant un moyen simple, gratuit et qui ne produira aucun revenu au responsable du fichier ou du traitement. En particulier, on considérera conforme au présent règlement la procédure dans laquelle ce refus pourra s'effectuer, entre autres, en envoyant une lettre préaffranchie au responsable du traitement ou en appelant un numéro de téléphone gratuit ou les services clientèle que celui–ci aurait établis.

Ne seront pas considérés conformes aux dispositions de la loi organique 15/1999, du 13 décembre, les cas dans lesquels les moyens établis par le responsable pour que la personne concernée puisse manifester son refus du traitement seraient l'envoi de lettres recommandées ou d'une nature équivalente, l'utilisation de services de télécommunication impliquant un tarif supplémentaire pour la personne concernée ou tout autre moyen représentant un coût supplémentaire à celle–ci.

2. Le responsable cessera le traitement des données dans un délai maximum de dix jours à compter du jour de réception de la révocation du consentement, sans préjudice de son obligation de bloquer les données conformément aux dispositions de l'article 16.3 de la loi organique 15/1999, du 13 décembre.

3. Si l'intéressé a demandé au responsable du traitement de lui confirmer la cessation du traitement de ses données, ce dernier devra répondre expressément à sa demande.

4. Dans le cas où les données auraient été cédées au préalable, le responsable du traitement – une fois que le consentement aura été révoqué – devra le signaler aux cessionnaires dans le délai prévu à l'alinéa 2 afin que ces derniers cessent le traitement des données, pour autant qu'ils le réalisent encore, conformément à l'article 16.4 de la loi organique 15/1999, du 13 décembre.

SECTION 2. DEVOIR D'INFORMATION DE L'INTÉRESSÉ

Article 18. Justification de l'exécution du devoir d'information.

(Annulé)

Article 19. Cas spéciaux.

Dans le cas où le responsable du fichier changerait suite à une opération de fusion, de scission, de cession globale d'actifs et de passifs, d'apport ou de transmission d'une activité ou d'une branche d'activité professionnelle, ou suite à n'importe quelle opération de restructuration sociétaire d'une nature analogue, prévue par la législation commerciale, la cession de données ne pourra pas avoir lieu sans préjudice du respect par le responsable des dispositions de l'article 5 de la loi organique 15/1999, du 13 décembre.

CHAPITRE III

De la personne chargée du traitement

Article 20. Relations entre le responsable et la personne chargée du traitement.

1. L'accès aux données par une personne chargée du traitement qui serait nécessaire pour assurer la prestation d'un service au responsable ne sera pas considéré comme une communication de données à condition que les dispositions contenues dans la loi organique 15/1999, du 13 décembre, et dans le présent chapitre, soient respectées.

Le service fourni par la personne chargée du traitement pourra ou non avoir un caractère rémunéré et être temporaire ou d'une durée indéterminée.

Ceci étant, on considérera qu'il existera une communication de données lorsque l'accès a pour objet l'établissement d'un nouveau lien entre la personne qui accède aux données et la personne concernée.

2. Lorsqu'il souscrit la prestation d'un service qui comporte un traitement de données à caractère personnel soumis aux dispositions de ce chapitre, le responsable du traitement devra veiller à ce que la personne chargée du traitement réunisse les garanties concernant le respect des dispositions contenues dans ce règlement.

3. Dans le cas où la personne chargée du traitement destinerait les données à une autre finalité, les communiquerait ou les utiliserait en infraction aux clauses du contrat visé à l'alinéa 2 de l'article 12 de la loi organique 15/1999, du 13 décembre, elle sera également considérée responsable du traitement et répondra des infractions qu'elle aurait commises à titre personnel.

En revanche, la personne chargée du traitement ne sera pas tenue responsable si elle communique les données, sur indication expresse du responsable, à un tiers désigné par ce dernier auquel elle aurait confié la prestation d'un service conformément aux dispositions de ce présent chapitre.

Article 21. Possibilité de sous-traitance des services.

1. La personne chargée du traitement ne pourra sous–traiter à un tiers la réalisation d'aucun traitement que lui aurait confié le responsable du traitement, à moins qu'elle n'ait obtenu de ce dernier l'autorisation de le faire. Dans ce cas, la sous–traitance s'effectuera toujours au nom et pour le compte du responsable du traitement.

2. Nonobstant les dispositions de l'alinéa précédent, la sous-traitance pourra s'effectuer sans autorisation pour autant que les conditions suivantes soient réunies:

a) Que soient indiqués dans le contrat les services qui peuvent faire l'objet de sous-traitance et, si possible, l'entreprise à laquelle ils vont être sous-traités.

   Si l'entreprise à laquelle le traitement va être sous-traité n'a pas été identifiée dans le contrat, la personne chargée du traitement devra communiquer au responsable les données identifiant celle-ci avant de procéder à la sous–traitance.

b) Que le traitement de données à caractère personnel par le sous-traitant soit conforme aux instructions du responsable du fichier.

c) Que la personne chargée du traitement et la société sous-traitante passent le contrat dans les conditions prévues à l'article précédent.

   Dans ce cas, le sous-traitant sera considéré comme étant la personne chargée du traitement et se verra appliquer les dispositions de l'article 20.3 de ce règlement.

3. S'il est nécessaire, pendant la prestation du service, de sous-traiter une partie de ce dernier alors que cette circonstance n'a pas été prévue dans le contrat, il faudra soumettre au responsable du traitement les informations signalées à l'alinéa précédent.

Article 22. Conservation des données par la personne chargée du traitement.

1. Une fois que la prestation contractuelle aura été fournie, les données à caractère personnel devront être détruites ou rendues au responsable du traitement ou à la personne chargée du traitement que ce dernier aurait désignée, au même titre que n'importe quel support ou document qui contiendrait une quelconque donnée à caractère personnel ayant fait l'objet du traitement.

Il n'y aura pas lieu de détruire les données s'il existe une disposition légale qui exige de les conserver, auquel cas il faudra les restituer tout en garantissant cette conservation au responsable du fichier.

2. La personne chargée du traitement conservera les données, dûment bloquées, aussi longtemps que sa relation avec le responsable du traitement pourrait entraîner des responsabilités.

TITRE III

Des droits d'accès, de rectification, d'annulation et d'opposition

CHAPITRE IER

Dispositions générales

Article 23. Caractère personnel.

1. Les droits d'accès, de rectification, d'annulation et d'opposition sont intimement liés à la personne et seront exercés par la personne concernée.

2. Ces droits seront exercés:

a) Par la personne concernée, après avoir justifié son identité, de la façon prévue à l'article suivant.

b) Si la personne concernée se trouve dans une situation d'incapacité ou de minorité d'âge qui l'empêche d'exercer personnellement ces droits, ceux-ci pourront être exercés par son représentant légal qui devra justifier cette condition.

c) Les droits pourront également être exercés par l'intermédiaire d'un représentant volontaire, qui aura été expressément désigné pour exercer ces droits. Dans ce cas, il faudra que soient clairement indiquées l'identité du mandant à travers la présentation de la copie de sa carte d'identité ou du document équivalent, et la représentation concédée par ce dernier.

Si le responsable du fichier est un organe des administrations publiques ou de l'administration judiciaire, la représentation pourra être justifiée par n'importe quel moyen valide en droit qui fera foi ou par une déclaration faite lors de la comparution de l'intéressé.

3. Les droits seront refusés si la demande est présentée par une personne autre que la personne concernée et s'il n'est pas justifié qu'elle intervienne au nom de celle–ci.

Article 24. Conditions générales de l'exercice des droits d'accès, de rectification, d'annulation et d'opposition.

1. Les droits d'accès, de rectification, d'annulation et d'opposition sont des droits indépendants de sorte qu'on ne peut considérer que l'exercice de l'un quelconque de ces droits soit une condition préalable à l'exercice d'un autre.

2. Il faudra mettre à la disposition de l'intéressé un moyen simple et gratuit pour qu'il puisse exercer ses droits d'accès, de rectification, d'annulation et d'opposition.

3. L'exercice par la personne concernée de ses droits d'accès, de rectification, d'annulation et d'opposition sera gratuit et ne pourra en aucun cas produire un revenu supplémentaire au responsable du traitement devant lequel ils seraient exercés.

Ne seront pas considérés conformes aux dispositions de la loi organique 15/1999, du 13 décembre, et du présent règlement les cas dans lesquels les moyens établis par le responsable du traitement pour que l'intéressé puisse exercer ses droits seraient l'envoi de lettres recommandées ou d'une nature équivalente, l'utilisation de services de télécommunication impliquant un tarif supplémentaire pour la personne concernée ou tout autre moyen qui occasionnerait un coût excessif à l'intéressé.

4. Si le responsable du fichier ou du traitement dispose de services de n'importe quelle nature qui sont destinés à l'attention de sa clientèle ou à l'exercice de réclamations liées au service fourni ou aux produits proposés à celle–ci, il pourra concéder à la personne concernée la possibilité d'exercer ses droits d'accès, de rectification, d'annulation et d'opposition à travers ces services. On considérera dans ce cas que l'identité de l'intéressé sera justifiée par les moyens établis aux fins de l'identification des clients du responsable dans la prestation de ses services ou dans la souscription de ses produits.

5. Le responsable du fichier ou du traitement devra répondre à la demande d'accès, de rectification, d'annulation ou d'opposition présentée par la personne concernée, même si celle–ci n'a pas utilisé la procédure spécifiquement établie à cet effet par celui-ci, à condition que l'intéressé ait utilisé un moyen qui permette de justifier l'envoi et la réception de la demande, et que celle-ci contienne les éléments visés au paragraphe 1er de l'article suivant.

Article 25. Procédure.

1. Hormis dans le cas indiqué au paragraphe 4 de l'article précédent, l'exercice des droits devra s'effectuer à travers une communication adressée au responsable du fichier, qui contiendra:

a) Les noms et prénoms de la personne concernée; la photocopie de sa carte d'identité ou de son passeport ou d'un autre document valide l'identifiant et, le cas échéant, de la personne qui le représenterait ou les instruments électroniques équivalents, ainsi que le document ou l'instrument électronique justifiant cette représentation. L'utilisation de la signature électronique identificatrice de la personne concernée la libérera de la présentation des photocopies de sa carte d'identité ou du document équivalent.

   Le paragraphe précédent s'entendra sans préjudice du règlement spécifique applicable à la vérification des données d'identité par les administrations publiques dans les procédures administratives.

b) Le document concrétisant la demande.

c) L'adresse aux effets de notifications, la date et la signature du demandeur.

d) Le cas échéant, les documents justificatifs de la demande présentée.

2. Le responsable du traitement devra toujours répondre à la demande qui lui sera adressée, indépendamment du fait que ses fichiers contiennent ou non des données à caractère personnel de la personne concernée.

3. Si la demande ne réunit pas les conditions indiquées au premier alinéa, le responsable du fichier devra demander la correction des données indiquées dans celle–ci.

4. La réponse devra être conforme aux conditions prévues pour chaque cas dans le présent titre.

5. Le responsable du traitement sera tenu de prouver que l'obligation de réponse visée à l'alinéa 2 a été respectée et conservera la justification du respect de l'obligation citée.

6. Le responsable du fichier devra prendre les mesures opportunes afin de garantir que les membres de son organisation qui ont accès à des données à caractère personnel sont en mesure de donner des informations sur la procédure que la personne concernée devra suivre pour exercer ses droits.

7. L'exercice des droits d'accès, de rectification, d'annulation et d'opposition pourra être adapté pour des raisons de sécurité publique dans les cas et la mesure prévus dans les lois.

8. Lorsque les lois applicables à certains fichiers concrets prévoient une procédure spéciale pour la rectification ou l'annulation des données contenues dans ceux–ci, on s'en tiendra aux dispositions de ces lois.

Article 26. Exercice des droits auprès d'une personne chargée du traitement.

Si les intéressés exercent leurs droits auprès d'une personne chargée du traitement et demandent à exercer leur droit auprès de celle-ci, cette personne devra transmettre la demande au responsable afin qu'il l'a satisfasse lui-même, sauf si la relation qui l'unit au responsable du traitement prévoit précisément que la personne chargée du traitement administrera, pour le compte du responsable, les demandes d'exercice par les intéressés de leurs droits d'accès, de rectification, d'annulation ou d'opposition.

CHAPITRE II

Du droit d'accès

Article 27. Droit d'accès.

1. Le droit d'accès est le droit de la personne concernée à obtenir des informations pour savoir si ses propres données à caractère personnel font l'objet d'un traitement et pour connaître la finalité du traitement qui serait éventuellement réalisé ainsi que les informations disponibles sur l'origine de ces données et les communications réalisées ou prévues de celles–ci.

2. En vertu du droit d'accès, la personne concernée pourra obtenir du responsable du traitement des informations sur des données concrètes, sur des données incluses dans un fichier déterminé ou sur l'ensemble des données faisant l'objet d'un traitement.

Ceci étant, lorsque des motifs d'une complexité particulière le justifient, le responsable du fichier pourra demander

à la personne concernée de préciser les fichiers sur lesquels il souhaite exercer son droit d'accès, ce pour quoi il devra lui remettre une liste de tous les fichiers concernés.

3. Le droit d'accès est indépendant du droit qui est attribué aux personnes concernées par les lois spéciales et, en particulier, par la loi 30/1992, du 26 novembre, relative au régime juridique des administrations publiques et de la procédure administrative commune.

Article 28. Exercice du droit d'accès.

1. La personne concernée qui exerce le droit d'accès pourra choisir de recevoir l'information à travers un ou plusieurs des systèmes suivants de consultation du fichier:

a) Visualisation à l'écran.

b) Document, copie ou photocopie remise par courrier, recommandé ou non.

c) Télécopie.

d) Courrier électronique ou autres systèmes de communication électronique.

e) Tout autre système, proposé par le responsable, qui sera adapté à la configuration ou à l'implantation matérielle du fichier ou à la nature du traitement.

2. Les systèmes de consultation du fichier prévus à l'alinéa précédent pourront être restreints en fonction de la configuration ou de l'implantation matérielle du fichier ou de la nature du traitement, à condition que le système qui sera proposé à la personne concernée soit gratuit et garantisse la communication écrite si elle l'exige ainsi.

3. En permettant l'accès, le responsable du fichier devra respecter les dispositions figurant au titre VIII de ce règlement.

Si ce responsable propose un système déterminé pour exercer le droit d'accès et la personne concernée le refuse, il ne répondra pas des risques éventuels que pourrait occasionner ce choix pour la sécurité de l'information.

De la même façon, si le responsable propose une procédure pour exercer le droit d'accès et la personne concernée exige que celui–ci se matérialise à travers une procédure impliquant un coût disproportionné, alors que le système proposé par le responsable a le même effet et garantit la même sécurité, la personne concernée prendra à sa charge les frais résultant de son choix.

Article 29. Octroi de l'accès.

1. Le responsable du fichier se prononcera sur la demande d'accès dans le délai maximum de un mois à compter de la réception de la demande. Si ce délai s'écoule sans que le responsable n'ait répondu de façon expresse à la demande d'accès, l'intéressé pourra présenter la réclamation prévue à l'article 18 de la loi organique 15/1999, du 13 décembre.

S'il ne dispose pas de données à caractère personnel des personnes concernées, il devra également le communiquer dans le même délai.

2. Si la demande est acceptée et le responsable ne joint pas à sa communication l'information visée à l'article 27.1, l'accès sera effectif dans les dix jours suivant cette communication.

3. L'information qui sera fournie, quel que soit le support sur lequel elle serait présentée, sera remise de façon lisible et intelligible, sans utiliser de codes qui exigeraient l'utilisation de dispositifs mécaniques spécifiques.

Cette information comprendra toutes les données de base de la personne concernée, les données résultant de n'importe quelle élaboration ou processus informatique, l'information disponible sur l'origine des données, sur les cessionnaires de ces dernières ainsi que la spécification des utilisations et des finalités concrètes pour lesquelles elles ont été stockées.

Article 30. Refus de l'accès.

1. Le responsable du fichier ou du traitement pourra refuser l'accès aux données à caractère personnel si le droit a déjà été exercé dans les douze mois précédant la demande, sauf si l'on peut justifier l'existence d'un intérêt légitime à cet effet.

2. L'accès pourra également être refusé lorsque le prévoit une loi ou une norme de droit communautaire d'application directe ou si cette loi ou norme empêche le responsable du traitement de révéler aux personnes concernées le traitement des données sur lesquelles porte l'accès.

3. En tout état de cause, le responsable du fichier informera la personne concernée de son droit à solliciter la protection de l'Agence espagnole de protection des données ou, le cas échéant, des autorités de contrôle des Communautés autonomes, conformément aux dispositions de l'article 18 de la loi organique 15/1999, du 13 décembre.

CHAPITRE III

Des droits de rectification et d'annulation

Article 31. Droits de rectification et d'annulation.

1. Le droit de rectification est le droit que possède la personne concernée d'obtenir la modification des données qui seraient inexactes ou incomplètes.

2. L'exercice du droit d'annulation donnera lieu à la suppression des données qui seraient inadéquates ou excessives, sans préjudice de l'obligation de blocage prévue dans ce règlement.

Dans le cas où l'intéressé invoquerait l'exercice du droit d'annulation pour révoquer le consentement donné au préalable, on s'en tiendra aux dispositions de la loi organique 15/1999, du 13 décembre, et du présent règlement.

Article 32. Exercice des droits de rectification et d'annulation.

1. La demande de rectification devra indiquer les données visées et la correction qui devra être réalisée, et devra être accompagnée de la documentation justifiant la demande.

Dans la demande d'annulation, l'intéressé devra indiquer les données visées en apportant, le cas échéant, la documentation justifiant l'annulation.

2. Le responsable du fichier se prononcera sur la demande de rectification ou d'annulation dans le délai maximum de dix jours à compter de la réception de la demande. Si ce délai s'écoule sans que le responsable n'ait répondu de façon expresse à la demande, l'intéressé pourra présenter la réclamation prévue à l'article 18 de la loi organique 15/1999, du 13 décembre.

S'il ne dispose pas de données à caractère personnel de la personne concernée, il devra également le lui communiquer dans le même délai.

3. Si les données rectifiées ou annulées ont été cédées au préalable, le responsable du fichier devra communiquer, dans le même délai, la rectification ou l'annulation réalisée au cessionnaire afin que ce dernier procède, également dans le délai de dix jours à compter de la réception de cette communication, à la rectification ou à l'annulation des données.

La rectification ou l'annulation réalisée par le cessionnaire n'exigera aucune communication à l'intéressé, sans préjudice de l'exercice des droits par les personnes concernées qui sont reconnus dans la loi organique 15/1999, du 13 décembre.

Article 33. Refus des droits de rectification et d'annulation.

1. Il n'y aura pas lieu à annulation si les données à caractère personnel doivent être conservées pendant les délais prévus dans les dispositions applicables ou, le cas échéant, dans les relations contractuelles établies entre la personne ou l'entité responsable du traitement et l'intéressé, qui auront justifié le traitement des données.

2. Les droits de rectification ou d'annulation pourront également être refusés lorsque le prévoit une loi ou une norme de droit communautaire d'application directe ou si cette loi ou norme empêche le responsable du traitement de révéler aux personnes concernées le traitement des données sur lesquelles porte l'accès.

3. En tout état de cause, le responsable du fichier informera la personne concernée de son droit à solliciter la protection de l'Agence espagnole de protection des données ou, le cas échéant, des autorités de contrôle des Communautés autonomes, conformément aux dispositions de l'article 18 de la loi organique 15/1999, du 13 décembre.

CHAPITRE IV

Du droit d'opposition

Article 34. Droit d'opposition.

Le droit d'opposition est le droit que possède la personne concernée à s'opposer au traitement de ses données à caractère personnel ou à obtenir la cessation du traitement dans les cas suivants:

a) Lorsque son consentement au traitement n'est pas nécessaire étant donné l'existence d'un motif légitime et fondé concernant sa situation personnelle concrète qui le justifie, à condition qu'aucune loi ne prévoie le contraire.

b) Lorsqu'il s'agit de fichiers ayant pour objet la réalisation d'activités publicitaires et de prospection commerciale, dans les conditions prévues à l'article 51 de ce règlement, quelle que soit la société responsable de leur création.

c) Lorsque le traitement a pour objet la prise d'une décision affectant la personne concernée et fondée uniquement sur un traitement automatisé de ses données à caractère personnel, dans les conditions prévues à l'article 36 de ce règlement.

Article 35. Exercice du droit d'opposition.

1. Le droit d'opposition sera exercé à travers une demande adressée au responsable du traitement.

Lorsque l'opposition est invoquée en fonction de la lettre a) de l'article précédent, la demande devra indiquer les motifs fondés et légitimes se rapportant à une situation personnelle concrète de la personne concernée, qui justifient l'exercice de ce droit.

2. Le responsable du fichier se prononcera sur la demande d'opposition dans le délai maximum de dix jours à compter de la réception de la demande. Si ce délai s'écoule sans que le responsable n'ait répondu de façon expresse à la demande, l'intéressé pourra présenter la réclamation prévue à l'article 18 de la loi organique 15/1999, du 13 décembre.

S'il ne dispose pas de données à caractère personnel des personnes concernées, il devra également le communiquer dans le même délai.

3. Le responsable du fichier ou du traitement devra exclure du traitement les données relatives à la personne concernée qui exercera son droit d'opposition ou refuser de façon motivée la demande de l'intéressé dans le délai prévu à l'alinéa 2 de cet article.

Article 36. Droit d'opposition aux décisions fondées uniquement sur un traitement automatisé des données.

1. Les intéressés ont le droit de ne pas être soumis à une décision produisant des effets juridiques à leur égard ou les affectant d'une façon significative, qui serait prise sur le seul fondement d'un traitement automatisé des données destiné à évaluer certains aspects de leur personnalité tels que leur rendement professionnel, leur crédit, leur fiabilité ou leur comportement.

2. Les personnes concernées pourront néanmoins être soumises à une des décisions prévues à l'alinéa 1er si cette décision:

a) A été prise dans le cadre de la conclusion ou de l'exécution d'un contrat à la demande de l'intéressé, à condition qu'on lui donne la possibilité de présenter les allégations pertinentes pour défendre son droit ou ses intérêts. En tout état de cause, le responsable du fichier devra indiquer au préalable à la personne concernée, d'une façon claire et précise, que des décisions présentant les caractéristiques indiquées à l'alinéa 1er vont être prises et qu'il annulera les données dans le cas où le contrat ne serait finalement pas conclu.

b) Est autorisée par une norme ayant rang de loi qui établirait des mesures garantissant l'intérêt légitime de la personne concernée.

TITRE IV

Des dispositions applicables à certains fichiers privés

CHAPITRE IER

Des fichiers d'information sur la solvabilité patrimoniale et le crédit

SECTION 1RE. DISPOSITIONS GÉNÉRALES

Article 37. Régime applicable.

1. Le traitement de données à caractère personnel sur la solvabilité patrimoniale et le crédit, prévu à l'alinéa 1er de l'article 29 de la loi organique 15/1999, du 13 décembre, sera soumis, de façon générale, aux dispositions établies dans ladite loi organique et dans le présent règlement.

2. L'exercice des droits d'accès, de rectification, d'annulation et d'opposition dans le cas des fichiers visés à l'alinéa précédent sera régi par les dispositions des chapitres I à IV du titre III du présent règlement, selon les critères suivants:

a) Si la demande d'exercice des droits est adressée au responsable du fichier, celui-ci sera tenu de satisfaire ces droits en toute circonstance.

b) Si la demande est adressée aux personnes et aux entités auxquelles est fourni le service, celles-ci ne devront communiquer à la personne concernée que les données la concernant qui leur auront été communiquées et indiquer l'identité du responsable afin qu'elle puisse, le cas échéant, exercer ses droits auprès de ce dernier.

3. Conformément à l'alinéa 2 de l'article 29 de la loi organique 15/1999, du 13 décembre, on pourra également traiter les données à caractère personnel relatives à l'exécution ou à l'inexécution d'obligations financières, qui auront été fournies par le créancier ou par une personne agissant pour son compte ou dans son intérêt.

Ces données devront être conservées dans des fichiers créés dans le seul but de fournir une information de crédit sur la personne concernée et leur traitement sera régi par les dispositions du présent règlement et, en particulier, par les dispositions contenues dans la seconde section de ce chapitre.

SECTION 2. TRAITEMENT DE DONNÉES RELATIVES À L'EXÉCUTION OU L'INEXÉCUTION D'OBLIGATIONS FINANCIÈRES FOURNIES PAR LE CRÉANCIER OU PAR UNE PERSONNE AGISSANT POUR SON COMPTE OU DANS SON INTÉRÊT

Article 38. Conditions de l'inclusion des données.

1. Seules les données à caractère personnel qui seront déterminantes pour évaluer la solvabilité économique de la personne concernée pourront être incluses dans ces fichiers, à condition que les conditions suivantes soient réunies:

a) Il doit exister au préalable une dette certaine, échue, exigible, qui n'a pas été payée et *qui n'a pas fait l'objet de réclamation judiciaire, d'arbitrage ou administrative, ou, s'agissant de services financiers, qui n'a pas fait l'objet d'une réclamation dans les conditions prévues dans le Règlement des commissions pour la défense du client de services financiers, approuvé par le décret royal 303/2004, du 20 février.*

b) Un délai de six ans ne peut pas s'être écoulé depuis la date à laquelle le paiement de la dette aurait dû se produire ou depuis l'échéance de l'obligation ou du délai concret si celle-ci était assortie d'une échéance périodique.

c) Une mise en demeure doit avoir été adressée au préalable à la personne devant exécuter l'obligation.

2. (Annulé)

3. Le créancier ou la personne qui agit pour son compte ou dans son intérêt sera tenu de conserver à la disposition du responsable du fichier commun et de l'Agence espagnole de protection des données la documentation suffisante qui justifiera le respect des conditions établies dans cet article et de la mise en demeure préalable à laquelle fait référence l'article suivant.

Article 39. Information préalable à l'inclusion.

Le créancier devra informer le débiteur, au moment de la passation du contrat et, en tout état de cause au moment de l'exécution de la mise en demeure visée à la lettre c) de l'alinéa 1er de l'article précédent, que si le paiement n'est pas réalisé dans le délai prévu à cet effet et si les conditions prévues à l'article cité sont remplies, les données relatives au non-paiement pourront être transmises dans des fichiers relatifs à l'exécution ou à l'inexécution d'obligations financières.

Article 40. Notification de l'inclusion.

1. Le responsable du fichier commun devra notifier aux intéressés dont on aura enregistré des données à caractère personnel, dans le délai de trente jours à compter de cet enregistrement, une référence des données qui auront été incluses et leur indiquera qu'ils auront la possibilité d'exercer leurs droits d'accès, de rectification, d'annulation et d'opposition dans les conditions prévues par la loi organique 15/1999, du 13 décembre.

2. Chaque dette concrète et déterminée donnera lieu à une notification indépendamment que celle-ci soit associée au même créancier ou à différents créanciers.

3. La notification devra être réalisée à l'aide d'un moyen fiable, vérifiable et indépendant de l'entité de notification, qui lui permettra de justifier la réalisation effective des envois.

4. En tout état de cause, il faudra que le responsable du fichier puisse savoir si la notification a fait l'objet d'un renvoi pour une cause quelconque, auquel cas il ne pourra pas procéder au traitement des données concernant cet intéressé.

Les renvois dans lesquels le destinataire aurait refusé d'accepter l'envoi ne seront pas considérés un motif suffisant pour ne pas procéder au traitement des données relatives à un intéressé.

5. Si la notification d'inclusion est refusée, le responsable du fichier commun vérifiera auprès de l'organisme de crédit que l'adresse utilisée pour effectuer cette notification correspond à l'adresse convenue dans le contrat avec le client aux fins de communication et ne procédera pas au traitement des données si l'organisme cité ne confirme pas l'exactitude de cette donnée.

Article 41. Conservation des données.

1. Seules les données qui reflètent de façon véridique la situation de la dette à chaque moment concret pourront faire l'objet d'un traitement.

Le paiement ou la satisfaction de la dette déterminera l'annulation immédiate de toute donnée la concernant.

2. Dans les autres cas, les données devront être annulées après une période de six ans à compter de l'échéance de l'obligation ou du délai concret si celle-ci est assortie d'une échéance périodique.

Article 42. Accès à l'information contenue dans le fichier.

1. Les données contenues dans le fichier commun ne pourront être consultées par des tiers que lorsqu'ils devront évaluer la solvabilité économique de la personne concernée. En particulier, on estimera que cette circonstance se produira dans les cas suivants :

a) Lorsque la personne concernée maintient avec le tiers une relation contractuelle de n'importe quel type qui n'est pas encore échue.

b) Lorsque la personne concernée a l'intention de conclure avec le tiers un contrat qui implique le paiement différé du prix.

c) Lorsque la personne concernée a l'intention de conclure avec le tiers la prestation d'un service à facturation périodique.

2. Les tiers devront informer par écrit les personnes se trouvant dans les cas visés ci-dessus aux lettres b) et c) de leur droit à consulter le fichier.

En cas de souscription téléphonique des produits ou services auxquels fait référence le paragraphe précédent, l'information ne devra pas nécessairement s'effectuer par écrit, le tiers étant responsable de prouver que le devoir d'information aura été respecté.

Article 43. Responsabilité.

1. Le créancier ou la personne qui agit pour son compte ou dans son intérêt devra s'assurer de l'existence de toutes les conditions exigées aux articles 38 et 39 au moment de notifier les données adverses au responsable du fichier commun.

2. Le créancier ou la personne qui agit pour son compte ou dans son intérêt sera responsable de l'inexistence ou de l'inexactitude des données qu'il aurait fournies aux fins de leur inclusion dans le fichier, dans les conditions prévues dans la loi organique 15/1999, du 13 décembre.

Article 44. Exercice des droits d'accès, de rectification, d'annulation et d'opposition.

1. L'exercice des droits d'accès, de rectification, d'annulation et d'opposition sera régi par les dispositions des chapitres I à IV du titre III du présent règlement, sans préjudice des dispositions figurant dans le présent article.

2. Lorsque l'intéressé exerce son droit d'accès concernant l'inclusion de ses données dans un fichier régi par l'article 29.2 de la loi organique 15/1999, du 13 décembre, on tiendra compte des règles suivantes:

1. Si la demande est adressée au titulaire du fichier commun, celui-ci devra communiquer à la personne concernée toutes les données la concernant qui figureront dans le fichier.

   Dans ce cas, le propriétaire du fichier commun devra non seulement respecter les dispositions établies dans le présent règlement, mais également fournir les évaluations et les appréciations qui auront été communiquées sur la personne concernée pendant les six derniers mois ainsi que le nom et l'adresse des cessionnaires.

2. Si la demande est adressée à n'importe quelle autre entité participant au système, celle-ci devra communiquer à la personne concernée toutes les données la concernant auxquelles elle pourra accéder ainsi que l'identité et l'adresse du titulaire du fichier commun afin que la personne concernée puisse exercer son droit d'accès.

3. Lorsque l'intéressé exerce ses droits de rectification ou d'annulation concernant l'inclusion de ses données dans un fichier régi par l'article 29.2 de la loi organique 15/1999, du 13 décembre, on tiendra compte des règles suivantes:

1. Si la demande est adressée au propriétaire du fichier commun, celui-ci prendra les mesures opportunes pour transmettre cette demande à l'organisme qui aura fourni les données afin qu'il y réponde. Si le responsable du fichier commun ne reçoit pas de réponse de la part de l'organisme dans le délai de sept jours, il procédera à la rectification ou à l'annulation conservatoire de ces données.

2. Si la demande est adressée à quiconque aura fourni les données au fichier commun, il procédera à la rectification ou à l'annulation de ces données dans ses fichiers, l'indiquera au propriétaire du fichier commun dans le délai de dix jours et répondra à l'intéressé dans les conditions prévues à l'article 33 de ce règlement.

3. Si la demande est adressée à une autre entité participant au système, qui n'aurait pas fourni les données au fichier commun, cette entité signalera ce fait à la personne concernée dans le délai maximum de dix jours et lui fournira l'identité et l'adresse du propriétaire du fichier commun pour qu'elle puisse, le cas échéant, exercer ses droits auprès de ce dernier.

CHAPITRE II

Des traitements concernant les activités publicitaires et de prospection commerciale

Article 45. Données susceptibles de traitement et information destinée à l'intéressé.

1. Les personnes qui se consacrent à la collecte d'adresses, à la distribution de documents, à la publicité, à la vente à distance, à la prospection commerciale et à d'autres activités analogues, ainsi que celles qui exercent ces activités dans le but de commercialiser leurs propres produits ou services ou ceux de tiers ne pourront utiliser les noms et les adresses ou d'autres données à caractère personnel que lorsque ces données se trouveront dans un des cas suivants:

a) Si elles figurent dans une des sources accessibles au public visées à la lettre j) de l'article 3 de la loi organique 15/1999, du 13 décembre, et à l'article 7 de ce règlement, et si la personne concernée n'a pas manifesté son refus ou son opposition au traitement de ses données pour les activités décrites dans cet alinéa.

b) Si elles ont été fournies par les propres intéressés ou obtenues avec leur consentement pour des finalités déterminées, explicites et légitimes liées à l'activité publicitaire ou de prospection commerciale, après que les intéressés ont été informés des secteurs d'activité spécifiques et concrets sur lesquels ils pourront recevoir des informations ou de la publicité.

2. Lorsque les données proviennent de sources accessibles au public et sont destinées à l'activité publicitaire ou de prospection commerciale, il faudra indiquer à l'intéressé, dans chaque communication qui lui sera adressée, l'origine des données et l'identité du responsable du traitement ainsi que les droits qu'il pourra faire valoir en précisant auprès de qui il pourra les exercer.

À cet effet, l'intéressé devra être informé que ses données ont été obtenues dans des sources accessibles au public en indiquant l'entité auprès de laquelle elles auraient été obtenues.

Article 46. Traitement de données lors de campagnes publicitaires.

1. Pour qu'une entité puisse réaliser par elle-même une activité publicitaire de ses produits ou services auprès de ses clients, il faudra que le traitement se fasse sous le couvert d'un des cas prévus à l'article 6 de la loi organique 15/1999, du 13 décembre.

2. Si une entité engage les services de tiers ou leur confie la réalisation d'une campagne publicitaire déterminée de ses produits ou services, en leur demandant de réaliser le traitement de certaines données, on appliquera les normes suivantes:

a) Si les paramètres identificateurs des destinataires de la campagne sont fixés par l'entité qui commande la campagne, celle-ci sera responsable du traitement des données.

b) Si les paramètres sont déterminés uniquement par l'entité ou les entités engagées pour réaliser le traitement, ces entités seront les responsables du traitement.

c) Si les deux entités interviennent dans la détermination des paramètres, elles seront toutes les deux responsables du traitement.

3. Dans le cas prévu à l'alinéa précédent, l'entité qui commande la campagne publicitaire devra adopter les mesures nécessaires pour s'assurer que l'entité engagée à cet effet a obtenu les données en respectant les exigences établies dans la loi organique 15/1999, du 13 décembre, et du présent règlement.

4. Aux fins de cet article, on entend par paramètres identificateurs des destinataires les variables utilisées pour identifier le public cible ou destinataire d'une campagne ou d'une promotion commerciale de produits ou services qui permettent de délimiter les destinataires individuels de celle-ci.

Article 47. Nettoyage de données à caractère personnel.

Lorsque deux ou plusieurs responsables ont l'intention, par eux-mêmes ou par l'intermédiaire de tiers, sans avoir obtenu le consentement des personnes concernées, à des fins de promotion ou de commercialisation de leurs produits ou services et en procédant à un traitement croisé de leurs fichiers, de déterminer les personnes qui auraient la condition de clients de l'un ou l'autre ou de plusieurs d'entre eux, le traitement ainsi réalisé constituera une cession ou une communication de données.

Article 48. Fichiers d'exclusion de l'envoi de communications commerciales.

Les responsables auxquels la personne concernée aura manifesté son refus de recevoir de la publicité pourront conserver les données minimales qui seront indispensables pour l'identifier et pour prendre les mesures nécessaires afin d'éviter de lui envoyer de la publicité.

Article 49. Fichiers communs d'exclusion de l'envoi de communications commerciales.

1. Il sera possible de créer des fichiers communs, de caractère général ou sectoriel, dans lesquels seront traitées les données à caractère personnel qui seront nécessaires pour éviter l'envoi de communications commerciales aux intéressés qui auront manifesté leur refus ou leur opposition à recevoir de la publicité.

À cet effet, les fichiers cités pourront contenir les données minimales indispensables pour identifier la personne concernée.

2. Lorsque la personne concernée indique à un responsable concret son refus ou son opposition à voir ses données traitées à des fins publicitaires ou de prospection commerciale, elle devra être informée de l'existence des fichiers communs d'exclusion généraux ou sectoriels ainsi que de l'identité de leur responsable, de leur domicile et de la finalité du traitement.

La personne concernée pourra demander d'être exclue d'un fichier ou d'un traitement concret ou d'être incluse dans des fichiers communs de personnes exclues à caractère général ou sectoriel.

3. L'entité responsable du fichier commun pourra traiter les données des personnes concernées qui auraient déclaré leur refus ou leur opposition à voir leurs données traitées à des fins publicitaires ou de prospection commerciale, en respectant les autres obligations établies dans la loi organique 15/1999, du 13 décembre, et dans le présent règlement.

4. Quiconque a l'intention d'effectuer un traitement associé à des activités publicitaires ou de prospection commerciale devra consulter au préalable les fichiers communs qui pourraient affecter son action afin d'éviter de traiter les données des personnes concernées qui auraient déclaré leur refus ou leur opposition à ce traitement.

Article 50. Droits d'accès, de rectification et d'annulation.

1. L'exercice des droits d'accès, de rectification et d'annulation concernant les traitements associés à des activités publicitaires et de prospection commerciale sera soumis aux dispositions des chapitres I à IV du titre III de ce règlement.

2. Si le droit est exercé auprès d'une entité qui a confié à un tiers la réalisation d'une campagne publicitaire, cette entité aura l'obligation, dans le délai de dix jours à compter de la réception de la communication de la demande d'exercice des droits de la personne concernée, de communiquer la demande au responsable du fichier afin que celui-ci octroie le droit en question à la personne concernée dans le délai de dix jours à compter de la réception de la communication et l'informe de la situation.

Les dispositions du paragraphe précédent s'entendront sans préjudice de l'obligation imposée à l'entité mentionnée à l'alinéa précédent, en tout état de cause, en vertu du paragraphe deux de l'article 5.5 de la loi organique 15/1999, du 13 décembre.

Article 51. Droit d'opposition.

1. Les intéressés auront le droit de s'opposer, sur demande et sans frais, au traitement des données les concernant, auquel cas ils seront désinscrits du traitement et obtiendront que les informations figurant à leur sujet dans ce dernier soient supprimées à leur simple demande.

L'opposition visée au paragraphe précédent s'entendra sans préjudice du droit de l'intéressé à révoquer, s'il l'estime opportun, le consentement qu'il aurait éventuellement donné pour le traitement des données.

2. L'intéressé devra se voir offrir à cet effet un moyen simple et gratuit pour s'opposer au traitement. En particulier, on estimera que cette règle sera respectée si les droits peuvent être exercés en appelant un numéro de téléphone gratuit ou en envoyant un courriel.

3. Lorsque le responsable du fichier ou du traitement dispose de services de n'importe quelle nature qui sont destinés à l'attention de ses clients ou à l'exercice de réclamations liées au service fourni ou aux produits proposés à ces derniers, il pourra concéder à la personne concernée la possibilité d'exercer son opposition à travers ces services.

Ne seront pas considérés conformes aux dispositions de la loi organique 15/1999, du 13 décembre, les cas dans lesquels les moyens établis par le responsable du traitement pour que l'intéressé puisse exercer son opposition seraient l'envoi de lettres recommandées ou d'une nature équivalente, l'utilisation de services de télécommunication impliquant un tarif supplémentaire pour la personne concernée ou tout autre moyen qui occasionnerait un coût excessif à celle-ci.

En tout état de cause, l'exercice des droits par la personne concernée ne pourra pas produire de revenu supplémentaire au responsable du traitement auprès duquel ils seront exercés.

4. Si le droit d'opposition est exercé auprès d'une entité qui a confié à un tiers la réalisation d'une campagne publicitaire, cette entité aura l'obligation, dans le délai de dix jours à compter de la réception de la communication de la demande d'exercice des droits de la personne concernée, de communiquer la demande au responsable du fichier afin que celui-ci octroie le droit en question à la personne concernée dans le délai de dix jours à compter de la réception de la communication et l'informe de la situation.

Les dispositions du paragraphe précédent s'entendront sans préjudice de l'obligation imposée à l'entité mentionnée à l'alinéa précédent, en tout état de cause, en vertu du paragraphe deux de l'article 5.5 de la loi organique 15/1999, du 13 décembre.

TITRE V

Des obligations préalables au traitement des données

CHAPITRE IER

De la création, de la modification ou de la suppression de fichiers publics

Article 52. Disposition ou décision de création, de modification ou de suppression du fichier.

1. La création, la modification ou la suppression des fichiers publics ne pourra s'effectuer qu'à travers une disposition générale ou une décision publiée au Journal officiel de l'État ou au journal officiel correspondant.

2. En tout état de cause, la disposition ou la décision devra être adoptée et publiée avant la création, la modification ou la suppression du fichier.

Article 53. Forme de la disposition ou de la décision.

1. Lorsque la disposition fait référence aux organes de l'administration générale de l'État ou aux entités ou organismes liés ou dépendant de celle-ci, elle devra prendre la forme d'un arrêté ministériel ou d'une résolution du titulaire de l'entité ou de l'organisme correspondant.

2. Dans le cas des organes constitutionnels de l'État, on s'en tiendra aux normes qui les régissent.

3. En ce qui concerne les fichiers dont sont responsables les Communautés autonomes, les collectivités locales et les entités ou organismes liés ou dépendant de celles-ci, les universités publiques ainsi que les organes des Communautés autonomes ayant des fonctions analogues aux organes constitutionnels de l'État, on s'en tiendra à la législation spécifique.

4. La création, la modification ou la suppression des fichiers dont sont responsables les corporations de droit public et qui sont liés à l'exercice par celles-ci de pouvoirs de droit public devra s'effectuer au moyen d'une décision prise par leurs organes de gouvernance, dans les conditions qui seront établies dans leurs statuts respectifs, qui devra également être publiée au Journal officiel de l'État ou au journal officiel correspondant.

Article 54. Contenu de la disposition ou de la décision.

1. La disposition ou décision relative à la création du fichier devra contenir les points suivants:

a) L'identification du fichier ou du traitement, en indiquant sa dénomination, ainsi que la description de sa finalité et de ses utilisations prévues.

b) L'origine des données en indiquant le collectif de personnes au sujet desquelles on a l'intention d'obtenir des données à caractère personnel ou qui sont obligées de les fournir, la procédure de collecte des données et leur origine.

c) La structure de base du fichier à travers la description détaillée des données identificatrices et, le cas échéant, des données spécialement protégées ainsi que des autres catégories de données à caractère personnel incluses dans ce dernier et le système de traitement utilisé dans leur organisation.

d) Les communications de données préalables en indiquant, le cas échéant, les destinataires ou les catégories de destinataires.

e) Les transferts internationaux de données prévus vers des pays tiers en indiquant, le cas échéant, les pays de destination des données.

f) Les organes responsables du fichier.

g) Les services ou unités auprès desquels peuvent être exercés les droits d'accès, de rectification, d'annulation et d'opposition.

h) Le niveau élémentaire, moyen ou supérieur de sécurité qui sera exigible conformément aux dispositions du titre VIII du présent règlement.

2. La disposition ou décision relative à la modification du fichier devra indiquer les modifications affectant n'importe lequel des points visés à l'alinéa précédent.

3. Les dispositions ou décisions qui seront prises aux fins de la suppression des fichiers devront indiquer la destination qui sera réservée aux données ou, le cas échéant, les dispositions qui seront prises pour les détruire.

CHAPITRE II

De la notification et de l'inscription des fichiers publics ou privés

Article 55. Notification des fichiers.

1. Tout fichier public de données à caractère personnel sera notifié à l'Agence espagnole de protection des données par l'organe compétent de l'administration responsable du fichier aux fins de son inscription au registre général de protection des données, dans le délai de trente jours à compter de la publication de sa norme ou de sa décision de création au journal officiel correspondant.

2. Les fichiers privés de données à caractère personnel seront notifiés à l'Agence espagnole de protection des données, avant leur création, par la personne ou l'entité privée qui a l'intention de les créer. La notification devra préciser l'identification du responsable du fichier et du fichier proprement dit, ses finalités et les utilisations prévues, le système de traitement utilisé dans son organisation, le collectif de personnes au sujet desquelles sont obtenues les données, la procédure et l'origine des données, les catégories de données, le service ou l'unité d'accès, l'indication du niveau élémentaire, moyen ou supérieur exigible pour les mesures de sécurité et, le cas échéant, l'identification de la personne chargée du traitement dans lequel figure le fichier ainsi que les destinataires des cessions et des transferts internationaux de données.

3. Lorsque l'obligation de notifier concerne des fichiers qui sont du ressort de l'autorité de contrôle d'une Communauté autonome qui aura créé son propre registre de fichiers, la notification sera adressée à l'autorité régionale compétente qui communiquera l'inscription au registre général de protection des données.

Le registre général de protection des données pourra demander aux autorités de contrôle des Communautés autonomes le transfert auquel fait référence le paragraphe précédent et, à défaut, réaliser l'inclusion d'office du fichier dans le registre.

4. La notification s'effectuera selon la procédure établie à la première section du chapitre IV du titre IX du présent règlement.

Article 56. Traitement de données sur différents supports.

1. La notification d'un fichier de données à caractère personnel est indépendante du système de traitement utilisé dans son organisation et du support ou des supports utilisés dans le traitement des données.

2. Lorsque les données à caractère personnel qui font l'objet d'un traitement sont stockées sur différents supports, automatisés et non automatisés, ou lorsqu'il existe une copie sur un support non automatisé d'un fichier automatisé, seule une notification devra être émise concernant ce fichier.

Article 57. Fichiers dont il existe plus d'un responsable.

Lorsqu'il est prévu de créer un fichier dont plusieurs personnes ou entités seraient responsables en même temps, chacune d'elles devra notifier la création du fichier correspondant afin de procéder à son inscription au registre général de protection des données et, le cas échéant, aux registres de fichiers créés par les autorités de contrôle des Communautés autonomes.

Article 58. Notification de la modification ou de la suppression de fichiers.

1. L'inscription du fichier devra être actualisée à tout moment. Toute modification qui affecterait le contenu de l'inscription d'un fichier devra être notifiée au préalable à l'Agence espagnole de protection des données ou aux autorités de contrôle régionales compétentes afin de procéder à son inscription au registre correspondant conformément aux dispositions de l'article 35.

2. Si le responsable du fichier décide de le supprimer, il devra le notifier afin que l'inscription soit annulée dans le registre correspondant.

3. Dans le cas des fichiers publics, si l'on souhaite réaliser la modification affectant une des conditions prévues à l'article 55 ou la suppression du fichier, il faudra avoir adopté, avant la notification, la norme ou la décision correspondante dans les conditions prévues au chapitre Ier de ce titre.

Article 59. Modèles et supports pour la notification.

1. L'Agence espagnole de protection des données publiera, à travers la résolution correspondante du Directeur, les modèles ou formulaires électroniques de notification de la création, de la modification ou de la suppression de

fichiers, qui permettront de les présenter par voie télématique ou sur support papier ainsi que, après avoir consulté les autorités de protection des données des Communautés autonomes, les formats destinés à la communication télématique de fichiers publics par les autorités de contrôle régionales, conformément aux dispositions des articles 55 et 58 du présent règlement.

2. Les modèles ou formulaires électroniques de notification pourront être obtenus gratuitement sur le site web de l'Agence espagnole de protection des données.

3. Le Directeur de l'Agence espagnole de protection des données pourra établir des procédures simplifiées de notification en fonction des circonstances qui affecteront le traitement ou le type de fichier objet de la notification.

Article 60. Inscription des fichiers.

1. Agissant sur proposition du registre général de protection des données, le Directeur de l'Agence espagnole de protection des données émettra une résolution autorisant, selon le cas, l'inscription, après que la procédure prévue au chapitre IV du titre IX aura été accomplie.

2. L'inscription comprendra le code assigné par le registre, l'identification du responsable du fichier, l'identification du fichier ou du traitement, la description de sa finalité et des utilisations prévues, le système de traitement utilisé dans son organisation, le cas échéant, le collectif de personnes au sujet desquelles sont obtenues les données, la procédure et l'origine des données, les catégories de données, le service ou l'unité d'accès et l'indication du niveau de mesures de sécurité exigible conformément aux dispositions de l'article 81.

On inclura également, selon le cas, l'identification de la personne chargée du traitement où se trouvera le fichier et des destinataires des cessions et des transferts internationaux.

Dans le cas des fichiers publics, on indiquera également la référence à la disposition générale en vertu de laquelle il aura été créé et, le cas échéant, il aura été modifié.

3. L'inscription d'un fichier au registre général de protection des données ne dispensera pas le responsable de respecter les autres obligations prévues dans la loi organique 15/1999, du 13 décembre, et les autres dispositions réglementaires.

Article 61. Annulation de l'inscription.

1. Si le responsable du traitement communique la suppression du fichier en vertu des dispositions de l'article 58 de ce règlement, le Directeur de l'Agence espagnole de protection des données, une fois que la procédure établie à la première section du chapitre IV du titre IX aura été accomplie, émettra une résolution annulant l'inscription correspondant au fichier.

2. Le Directeur de l'Agence espagnole de protection des données pourra décider d'office, dans l'exercice de ses compétences, d'annuler l'inscription d'un fichier lorsque se présentent des circonstances qui justifient l'impossibilité de son existence, une fois que la procédure établie dans la deuxième section du chapitre IV du titre IX de ce règlement aura été accomplie.

Article 62. Rectification d'erreurs.

Le registre général de protection des données pourra rectifier à n'importe quel moment, d'office ou à la demande des intéressés, les erreurs matérielles, de fait ou arithmétiques, qui pourraient exister dans les inscriptions, conformément aux dispositions de l'article 105 de la loi 30/1992, du 26 novembre.

Article 63. Inscription d'office de fichiers publics.

1. Dans certains cas exceptionnels, on pourra procéder à l'inscription d'office d'un fichier déterminé au registre général de protection des données dans le but de garantir le droit à la protection des données des personnes concernées et ce, sans préjudice de l'obligation de notification.

2. Pour que la disposition de l'alinéa précédent soit applicable, il sera indispensable que la norme correspondante ou la décision régissant les fichiers qui contiendront des données à caractère personnel ait été publiée au journal officiel correspondant et soit conforme aux conditions requises dans la loi organique 15/1999, du 13 décembre et dans le présent règlement.

3. Le directeur de l'Agence espagnole de protection des données pourra décider, à la demande du registre général de protection des données, d'inscrire le fichier public au registre, décision qu'il notifiera à l'organe responsable du fichier.

Lorsque l'inscription concerne des fichiers qui sont du ressort de l'autorité de contrôle d'une Communauté autonome qui aura créé son propre registre de fichiers, elle sera communiquée à l'autorité de contrôle régionale visée afin qu'elle procède, selon le cas, à l'inscription d'office.

Article 64. Collaboration avec les autorités de contrôle des Communautés autonomes.

Le Directeur de l'Agence espagnole de protection des données pourra conclure avec les directeurs des autorités de contrôle des Communautés autonomes les conventions de collaboration ou les accords qu'il estimera pertinents afin de garantir l'inscription au registre général de protection des données des fichiers qui sont du ressort de ces autorités régionales.

TITRE VI

Des transferts internationaux de données

CHAPITRE IER

Dispositions générales

Article 65. Application des dispositions de la loi organique 15/1999, du 13 décembre.

Le transfert international de données n'exclut en aucun cas l'application des dispositions contenues dans la loi organique 15/1999, du 13 décembre, et dans le présent règlement.

Article 66. Autorisation et notification.

1. Pour que le transfert international de données puisse être considéré conforme aux dispositions de la loi organique 15/1999, du 13 décembre, et du présent règlement, il faudra disposer de l'autorisation du Directeur de l'Agence espagnole de protection des données, qui sera concédée si l'exportateur fournit les garanties visées à l'article 70 du présent règlement.

L'autorisation sera concédée selon la procédure établie à la première section du chapitre V du titre IX de ce règlement.

2. L'autorisation ne sera pas nécessaire:

a) Si l'État dans lequel se trouve l'importateur offre un niveau adéquat de protection conformément aux dispositions du chapitre II de ce titre.

b) Si le transfert correspond à l'un des cas visés aux alinéas a) à j) de l'article 34 de la loi organique 15/1999, du 13 décembre.

3. En tout état de cause, le transfert international de données devra être notifié afin de procéder à son inscription au registre général de protection des données, conformément à la procédure établie dans la première section du chapitre IV du titre IX du présent règlement.

CHAPITRE II

Des transferts vers des États qui offrent un niveau adéquat de protection

Article 67. Niveau adéquat de protection déclaré par l'Agence espagnole de protection des données.

1. Un transfert international de données n'exigera pas l'autorisation du Directeur de l'Agence espagnole de protection des données si les normes applicables à l'État où se trouve l'importateur offrent ce niveau adéquat de protection selon l'appréciation du Directeur de l'Agence espagnole de protection des données.

Le caractère adéquat du niveau de protection qu'offre le pays de destination sera évalué en analysant toutes les circonstances dans lesquelles se produit le transfert ou la catégorie de transfert de données. En particulier, on tiendra compte de la nature des données, de la finalité et de la durée du traitement ou des traitements prévus, du pays d'origine et du pays de destination, des normes de droit - générales ou sectorielles - en vigueur dans le pays tiers en question, du contenu des rapports de la Commission de l'Union européenne ainsi que des normes professionnelles et des mesures de sécurité en vigueur dans ces pays.

Les résolutions du Directeur de l'Agence espagnole de protection des données en vertu desquelles il est décidé qu'un pays déterminé offre un niveau adéquat de protection des données seront publiées au Journal officiel de l'État.

2. Le Directeur de l'Agence espagnole de protection des données autorisera la publication de la liste des pays dont le niveau de protection aura été considéré d'un niveau équivalent en vertu des dispositions de l'alinéa précédent.

Cette liste sera publiée et maintenue à jour à l'aide de moyens informatiques ou télématiques.

Article 68. Niveau adéquat de protection déclaré sur décision de la Commission européenne.

L'autorisation du Directeur de l'Agence espagnole de protection des données ne sera pas nécessaire pour réaliser un transfert international de données dont l'importateur serait une personne ou entité, publique ou privée,

située sur le territoire d'un État au sujet duquel la Commission européenne aurait déclaré l'existence d'un niveau adéquat de protection.

Article 69. Suspension provisoire des transferts.

1. Dans les cas prévus aux articles précédents, le Directeur de l'Agence espagnole de protection des données, faisant usage du pouvoir que lui confère l'article 37.1 f) de la loi organique 15/1999, du 13 décembre, pourra décider, après avoir entendu l'exportateur, la suspension provisoire du transfert de données vers un importateur situé dans un État tiers au sujet duquel on aura déclaré l'existence d'un niveau adéquat de protection, si l'une ou l'autre des circonstances suivantes se présente:

a) Si les autorités de protection des données de l'État importateur ou toute autre autorité compétente dans le cas où les premières n'existeraient pas décident que l'importateur a enfreint les normes de protection des données établies dans son droit interne.

b) S'il existe des indices rationnels indiquant que les normes ou, le cas échéant, les principes de protection des données sont violés par la société importatrice du transfert et si les autorités compétentes dans l'État où se trouve l'importateur n'ont pas pris ou n'envisagent pas de prendre à l'avenir des mesures opportunes pour résoudre le cas en question, alors qu'elles ont été averties de la situation par l'Agence espagnole de protection des données. Dans ce cas, le transfert pourra être suspendu si son maintien peut occasionner un risque imminent de grave préjudice aux personnes concernées.

2. La suspension sera décidée une fois que la procédure établie à la deuxième section du chapitre V du titre IX du présent règlement aura été accomplie.

Dans ce cas, la décision du Directeur de l'Agence espagnole de protection des données sera notifiée à la Commission européenne.

CHAPITRE III

Des transferts vers des États qui n'offrent pas un niveau adéquat de protection

Article 70. Transferts sujets à l'autorisation du Directeur de l'Agence espagnole de protection des données.

1. L'autorisation du Directeur de l'Agence espagnole de protection des données devra être demandée lorsque le transfert est destiné à un État au sujet duquel ni la Commission européenne ni le Directeur de l'Agence espagnole de protection des données n'a déclaré ou estimé l'existence d'un niveau adéquat de protection.

L'autorisation du transfert sera traitée selon la procédure établie à la première section du chapitre V du titre IX de ce règlement.

2. L'autorisation pourra être concédée si le responsable du fichier ou du traitement présente un contrat écrit, conclu entre l'exportateur et l'importateur, qui offre les garanties nécessaires de respect de la protection de la vie privée des personnes concernées et de leurs droits et libertés fondamentales et qui garantit l'exercice de leurs droits respectifs.

À cet effet, on considérera que les garanties adéquates seront établies dans les contrats qui auront été conclus conformément aux dispositions des décisions de la Commission européenne 2001/497/CE, du 15 juin 2001, 2002/16/CE, du 27 décembre 2001, et 2004/915/CE, du 27 décembre 2004 ou aux dispositions des décisions de la Commission en application de l'article 26.4 de la directive 95/46/CE.

3. Dans le cas prévu à l'alinéa précédent, le Directeur de l'Agence espagnole de protection des données pourra refuser ou, faisant usage du pouvoir que lui octroie l'article 37.1 f) de la loi organique 15/1999, du 13 décembre, suspendre provisoirement le transfert, après avoir entendu l'exportateur, si l'une ou l'autre des circonstances suivantes se présente:

a) Si la situation de protection des droits fondamentaux et des libertés publiques dans le pays de destination ou sa législation empêche de garantir l'exécution intégrale du contrat et l'exercice par les personnes concernées des droits garantis par le contrat.

b) Si l'entité destinataire a enfreint au préalable les garanties établies dans des clauses contractuelles de ce type.

c) S'il existe des indices rationnels que les garanties offertes par le contrat ne sont pas ou ne seront pas respectées par l'importateur.

d) S'il existe des indices rationnels que les mécanismes d'application du contrat ne sont pas ou ne seront pas effectifs.

e) Si le transfert, ou le maintien de ce dernier s'il a déjà commencé, peut provoquer une situation de risque de préjudice effectif aux personnes concernées.

La suspension sera décidée une fois que la procédure établie à la deuxième section du chapitre V du titre IX du présent règlement aura été accomplie.

Les résolutions du Directeur de l'Agence espagnole de protection des données en vertu desquelles un transfert international de données sera refusé ou suspendu provisoirement en vertu des causes visées à cet alinéa seront notifiées à la Commission des Communautés européennes lorsque la loi l'exigera.

4. L'autorisation relative à un transfert international de données au sein de groupes multinationaux d'entreprises pourra également être accordée s'ils ont été adoptés par les mêmes normes ou règles internes comprenant les garanties nécessaires de respect de la protection de la vie privée et le droit fondamental à la protection des données des personnes concernées et si l'on garantit également le respect des principes et l'exercice des droits reconnus dans la loi organique 15/1999, du 13 décembre, et dans le présent règlement.

Dans ce cas, le Directeur de l'Agence espagnole de protection des données pourra autoriser le transfert si les normes ou les règles sont contraignantes pour les entreprises du groupe et sont exigibles conformément au système juridique espagnol.

En tout état de cause, l'autorisation du Directeur de l'Agence espagnole de protection des données impliquera l'exigibilité des dispositions contenues dans les normes ou les règles internes aussi bien par l'Agence que par les personnes concernées dont les données auraient fait l'objet d'un traitement.

TITRE VII

Des codes type

Article 71. Objet et nature.

1. Les codes type auxquels fait référence l'article 32 de la loi organique 15/1999, du 13 décembre, ont pour objet d'adapter les dispositions figurant dans la ladite loi organique et dans le présent règlement aux particularités des traitements effectués par les personnes qui y adhèrent.

À cet effet, ils contiendront des règles ou des standards spécifiques qui permettront d'harmoniser les traitements de données réalisés par les adhérents, de faciliter l'exercice des droits des personnes concernées et de favoriser le respect des dispositions de la loi organique 15/1999, du 13 décembre, et du présent règlement.

2. Les codes type auront le caractère de codes déontologiques ou de pratique d'excellence professionnelle et seront contraignants pour ceux qui y adhéreront.

Article 72. Initiative et champ d'application.

1. Les codes type auront un caractère volontaire.

2. Les codes type de caractère sectoriel pourront faire référence à l'ensemble ou à une partie des traitements réalisés par des entités appartenant à un même secteur et devront être formulés par des organisations représentatives de ce secteur, au moins dans leur champ territorial d'application, sans préjudice de la faculté qu'auront ces entités d'adapter le code type à leurs particularités.

3. Les codes type promus par une entreprise devront affecter l'ensemble des traitements réalisés par celle-ci.

4. Les administrations publiques et les corporations de droit public pourront adopter des codes type conformément aux dispositions établies dans les normes qui leur seront applicables.

Article 73. Contenu.

1. Les codes type devront être rédigés dans des termes clairs et accessibles.

2. Les codes type doivent respecter le règlement en vigueur et contenir, d'une façon suffisamment précise, au moins les informations suivantes:

a) L'identification claire et précise de leur champ d'application, les activités auxquelles fait référence le code et les traitements soumis à ce dernier.

b) Les dispositions spécifiques concernant l'application des principes de protection des données.

c) L'établissement de standard homogènes aux fins du respect par les adhérents au code des obligations établies dans la loi organique 15/1999, du 13 décembre.

d) L'établissement de procédures qui faciliteront l'exercice par les personnes concernées de leurs droits d'accès, de rectification, d'annulation et d'opposition.

e) La détermination des cessions et des transferts internationaux de données qui seraient prévus, en indiquant les garanties qui devront être octroyées.

f) Les actions de formation en matière de protection des données destinées aux personnes qui les traiteront, en particulier en ce qui concerne leur relation avec les personnes concernées.

g) Les mécanismes de supervision à travers lesquels on garantira le respect par les adhérents des dispositions contenues dans le code type, dans les conditions prévues à l'article 74 de ce règlement.

3. En particulier, le code devra contenir :

a) Des clauses type visant l'obtention du consentement des personnes concernées au traitement ou à la cession de leurs données.

b) Des clauses type visant à informer les personnes concernées du traitement lorsque les données ne sont pas obtenues auprès de celles-ci.

c) Des modèles pour l'exercice par les personnes concernées de leurs droits d'accès, de rectification, d'annulation et d'opposition.

d) Des modèles de clauses concernant le respect des conditions formelles exigibles, le cas échéant, pour l'engagement d'une personne chargée du traitement.

Article 74. Engagements supplémentaires.

1. Les codes type pourront inclure tout autre engagement supplémentaire que les adhérents assumeraient dans le but d'assurer une meilleure application de la législation en vigueur en matière de protection des données.

2. Ils pourront également contenir n'importe quel autre engagement que pourront prendre les entités de promotion, notamment:

a) L'adoption de mesures de sécurité complémentaires aux mesures exigées par la loi organique 15/1999, du 13 décembre, et par le présent règlement.

b) L'identification des catégories de cessionnaires ou d'importateurs des données.

c) Les mesures concrètes adoptées en matière de protection des mineurs ou de certains collectifs de personnes concernées.

d) L'établissement d'un label de qualité qui identifierait les adhérents au code.

Article 75. Garanties du respect des codes type.

1. Les codes type devront inclure des procédures de supervision indépendantes afin de garantir le respect des obligations contractées par les adhérents et établir un régime de sanction adéquat, efficace et dissuasif.

2. La procédure qui sera prévue devra garantir:

a) L'indépendance et l'impartialité de l'organe responsable de la supervision.

b) La simplicité, l'accessibilité, la rapidité et la gratuité lors de la présentation de plaintes et de réclamations auprès de cet organe pour cause d'éventuelles inexécutions du code type.

c) Le principe de contradiction.

d) Une graduation des sanctions qui permette d'ajuster celles-ci à la gravité de l'infraction. Ces sanctions devront être dissuasives et pourront impliquer la suspension de l'adhésion au code ou l'expulsion de l'entité adhérente. Le cas échéant, on pourra également prévoir la publicité de ces sanctions.

e) La notification de la décision adoptée à la personne concernée.

3. Par ailleurs et sans préjudice des dispositions de l'article 19 de la loi organique 15/1999, du 13 décembre, les codes type pourront prévoir des procédures visant à déterminer des mesures réparatrices dans le cas où l'inexécution du code type aurait causé préjudice aux personnes concernées.

4. Les dispositions de cet article s'appliqueront sans préjudice des compétences de l'Agence espagnole de protection des données et, le cas échéant, des autorités de contrôle des Communautés autonomes.

Article 76. Liste des adhérents.

Le code type devra inclure en annexe une liste des adhérents, qui devra être constamment actualisée et mise à la disposition de l'Agence espagnole de protection des données.

Article 77. Dépôt et publicité des codes type.

1. Afin qu'ils puissent être considérés comme tels aux effets prévus à l'article 32 de la loi organique 5/1999, du 13 décembre, et dans le présent règlement, les codes type devront être déposés et inscrits au registre général de protection des données de l'Agence espagnole de protection des données ou, selon le cas, au registre qui aurait été créé par les Communautés autonomes, qui les transmettront aux fins de leur inclusion dans le registre général de protection des données.

2. À cet effet, les codes type devront être présentés devant l'autorité correspondante et, s'ils sont soumis à la décision de l'Agence espagnole de protection des données, seront inscrits conformément à la procédure établie au chapitre VI du titre IX de ce règlement.

3. En tout état de cause, l'Agence espagnole de protection des données fera la publicité des codes type inscrits, de préférence en utilisant des moyens informatiques ou télématiques.

Article 78. Obligations ultérieures à l'inscription du code type.

Les entités de promotion ou les organes, les personnes ou les entités qui seraient désignées à cet effet dans le propre code type auront les obligations suivantes, une fois que ce dernier aura été publié:

a) Maintenir l'accessibilité du public à l'information actualisée concernant les entités de promotion, le contenu du code type, les procédures d'adhésion et de garantie de son respect et la liste des adhérents à laquelle fait référence l'article précédent.

   Cette information devra être présentée d'une façon claire et concise, et être accessible de façon permanente par des moyens électroniques.

b) Remettre à l'Agence espagnole de protection des données un rapport annuel sur les activités réalisées pour diffuser le code type et promouvoir l'adhésion à ce dernier, sur les actions de vérification de l'application du code et leurs résultats, sur les plaintes et les réclamations présentées et sur la suite qui leur aurait été réservée ainsi que sur n'importe quel autre aspect que les entités de promotion estimeraient opportun de signaler.

   Lorsqu'il s'agit de codes type inscrits au registre d'une autorité de contrôle d'une Communauté autonome, ce rapport sera remis à cette autorité qui le transmettra au registre général de protection des données.

c) Évaluer de façon régulière l'efficacité du code type en mesurant le degré de satisfaction des personnes concernées et, le cas échéant, actualiser son contenu afin de l'adapter à la réglementation générale ou sectorielle de protection des données existant à chaque instant.

   Cette évaluation devra être réalisée au moins tous les quatre ans, à moins qu'il ne soit nécessaire d'adapter les engagements du code à la modification de la réglementation applicable dans un délai plus court.

d) Favoriser l'accessibilité de toutes les personnes à toute l'information disponible sur le code type, en veillant tout particulièrement à celles qui présenteraient un handicap ou qui auraient un âge avancé.

TITRE VIII

Des mesures de sécurité dans le traitement de données à caractère personnel

CHAPITRE IER

Dispositions générales

Article 79. Étendue.

Les responsables des traitements ou des fichiers et les personnes chargées du traitement devront implanter les mesures de sécurité conformément aux dispositions de ce titre, quel que soit le système de traitement qui sera utilisé.

Article 80. Niveaux de sécurité.

Les mesures de sécurité exigibles aux fichiers et aux traitements sont classées dans trois niveaux : élémentaire, moyen et supérieur.

Article 81. Application des niveaux de sécurité.

1. Tous les fichiers ou traitements de données à caractère personnel devront adopter les mesures de sécurité dites de niveau élémentaire.

2. Il faudra mettre en œuvre les mesures de niveau moyen, en plus des mesures de sécurité de niveau élémentaire, dans les fichiers ou traitements de données à caractère personnel suivants:

a) Ceux qui concernent la commission d'infractions administratives ou pénales.

b) Ceux dont le fonctionnement est régi par l'article 29 de la loi organique 15/1999, du 13 décembre.

c) Ceux dont sont responsables les administrations fiscales et qui ont trait à l'exercice de leurs pouvoirs fiscaux.

d) Ceux dont sont responsables les organismes financiers au regard de finalités liées à la prestation de services financiers.

e) Ceux dont sont responsables les sociétés de gestion et de services communs de la sécurité sociale et qui ont trait à l'exercice de leurs compétences. Il en va de même pour ceux dont sont responsables les mutuelles d'accidents de travail et de maladies professionnelles de la sécurité sociale.

f) Ceux qui contiennent un ensemble de données à caractère personnel qui offrent une définition des caractéristiques ou de la personnalité des citoyens et qui permettent d'évaluer certains aspects de la personnalité ou du comportement de ces derniers.

3. On appliquera les mesures de niveau supérieur, en plus des mesures de niveau élémentaire et moyen, aux fichiers ou traitements de données à caractère personnel suivants:

a) Ceux qui font référence à des données sur l'idéologie, l'affiliation syndicale, la religion, les croyances, l'origine raciale, la santé ou la vie sexuelle.

b) Ceux qui contiennent ou font référence à des données collectées à des fins policières sans le consentement des personnes concernées.

c) Ceux qui contiennent des données issues d'actes de violence conjugale.

4. La mesure de sécurité de niveau supérieur prévue à l'article 103 de ce règlement sera appliquée, en plus des mesures de sécurité des niveaux élémentaire et moyen, aux fichiers dont sont responsables les opérateurs qui fournissent des services de communication électronique disponibles au public ou qui exploitent de réseaux publics de communication électronique en ce qui concerne les données de trafic et les données de localisation.

5. Dans le cas des fichiers ou des traitements de données concernant l'idéologie, l'affiliation syndicale, la religion, les croyances, l'origine raciale, la santé ou la vie sexuelle, l'application des mesures de sécurité du niveau élémentaire sera suffisante:

a) Si les données sont utilisées dans le seul but de réaliser un transfert financier aux entités dont les personnes concernées sont des associées ou des membres.

b) S'il s'agit de fichiers ou de traitements qui contiennent ces données de façon accidentelle ou accessoire et sans lien avec leur finalité.

6. Les mesures de sécurité du niveau élémentaire pourront également être mises en œuvre dans les fichiers ou les traitements qui contiennent des données relatives à la santé concernant exclusivement le degré de handicap ou la simple déclaration de la condition de handicap ou d'invalidité de la personne concernée, dans le cadre de l'exécution d'obligations publiques.

7. Les mesures incluses dans chacun des niveaux décrits ci-dessus sont considérées comme des niveaux minimums exigibles, sans préjudice des dispositions légales ou réglementaires spécifiques en vigueur qui pourraient être applicables dans chaque cas ou de celles que le responsable du fichier adopterait de sa propre initiative.

8. Dans le souci de faciliter l'application des dispositions de ce titre, lorsqu'un système d'information comprend des fichiers ou des traitements qui, en fonction de leur finalité ou de leur utilisation concrète, ou de la nature des données qu'ils contiennent, exigent l'application d'un niveau de mesures de sécurité différent de celui du système principal, on pourra les séparer de ce dernier et appliquer dans chaque cas le niveau de mesures de sécurité correspondant, à condition que l'on puisse délimiter les données concernées et les utilisateurs ayant accès à ces dernières et que cette séparation soit dûment indiquée dans le document de sécurité.

Article 82. Personne chargée du traitement.

1. Lorsque le responsable du fichier ou du traitement permet l'accès aux données, aux supports qui les contiennent ou aux ressources du système d'information qui les traite, à une personne chargée du traitement qui fournit ses services dans les locaux du premier cité, cette circonstance devra être mentionnée dans le document de sécurité dudit responsable et le personnel de la personne chargée du traitement devra s'engager à respecter les mesures de sécurité prévues dans le document en question.

Si cet accès est réalisé à distance parce qu'il a été interdit à la personne chargée du traitement d'incorporer ces données à des systèmes ou supports distincts de ceux du responsable, elle devra signaler cette circonstance dans le document de sécurité du responsable et le personnel de la personne chargée du traitement devra s'engager à respecter les mesures de sécurité prévues dans le document en question.

2. Si le service est fourni par la personne chargée du traitement dans ses propres locaux, différents de ceux du responsable du fichier, elle devra élaborer un document de sécurité dans les conditions exigées par l'article 88 de ce règlement ou compléter celui qu'elle aurait éventuellement élaboré en identifiant le fichier ou le traitement et le responsable de ce dernier et en introduisant les mesures de sécurité à appliquer à ce traitement.

3. En tout état de cause, l'accès aux données par la personne chargée du traitement sera soumis aux mesures de sécurité prévues dans ce règlement.

Article 83. Prestations de services sans accès à des données à caractère personnel.

Le responsable du fichier ou du traitement prendra les mesures adéquates pour limiter l'accès du personnel à des données à caractère personnel, aux supports qui les contiennent ou aux ressources du système d'information pour réaliser des travaux qui n'impliqueront pas le traitement de données à caractère personnel.

Lorsqu'il s'agit d'un personnel différent, le contrat de prestation de services mentionnera expressément l'interdiction d'accéder aux données à caractère personnel et l'obligation de garder le secret des données dont le personnel aurait pu prendre connaissance dans le cadre de la prestation du service.

Article 84. Délégation d'autorisations.

Les autorisations qui sont concédées dans ce titre au responsable du fichier ou du traitement pourront être déléguées aux personnes désignées à cet effet. Le document de sécurité devra mentionner les personnes autorisées à concéder ces autorisations ainsi que les bénéficiaires de cette délégation. Cette désignation ne constitue en aucun cas une délégation de la responsabilité qui incombe au responsable du fichier.

Article 85. Accès aux données à travers des réseaux de communication.

Les mesures de sécurité exigibles pour les accès à des données à caractère personnel à travers des réseaux de communication, qu'ils soient publics ou non, devront garantir un niveau de sécurité équivalant à celui qui sera applicable aux accès en mode local, selon les critères établis à l'article 80.

Article 86. Régime de travail hors des locaux du responsable du fichier ou de la personne chargée du traitement.

1. Lorsque les données à caractère personnel sont stockées dans des dispositifs portatifs ou sont traitées hors des locaux du responsable du fichier ou du traitement, ou de la personne chargée du traitement, il faudra veiller à ce

qu'il existe au préalable une autorisation du responsable du fichier ou du traitement et à ce que le niveau de sécurité correspondant au type de fichier traité soit garanti en toute circonstance.

2. L'autorisation visée au paragraphe précédent devra être mentionnée dans le document de sécurité et pourra être établie pour un utilisateur ou pour un profil d'utilisateurs en déterminant sa période de validité.

Article 87. Fichiers temporaires ou copies de travail de documents.

1. Les fichiers temporaires ou les copies de documents qui auraient été créés exclusivement pour la réalisation de travaux temporaires ou auxiliaires devront présenter le niveau de sécurité qui leur sera applicable en fonction des critères établis à l'article 81.

2. Tout fichier temporaire ou toute copie de travail ainsi créé sera effacé ou détruit lorsqu'il cessera d'être nécessaire aux fins qui auront justifié sa création.

CHAPITRE II

Du document de sécurité

Article 88. Le document de sécurité.

1. Le responsable du fichier ou du traitement élaborera un document de sécurité, qui contiendra les mesures de nature technique et organisationnelle conformes au règlement de sécurité en vigueur, qui sera obligatoirement applicable par le personnel ayant accès à des systèmes d'information.

2. Le document de sécurité pourra être unique et commun à tous les fichiers ou traitements, ou bien être propre à chaque fichier ou traitement. On pourra également élaborer différents documents de sécurité en regroupant des fichiers ou des traitements selon le système de traitement utilisé dans leur organisation ou bien en suivant les critères organisationnels du responsable. En tout état de cause, il aura le caractère de document interne de l'organisation.

3. Ce document devra contenir au moins les aspects suivants:

a) Son champ d'application avec une identification détaillée des ressources protégées.

b) Les mesures, les normes, les procédures d'action, les règles et les standard visant à garantir le niveau de sécurité exigé dans ce règlement.

c) Les fonctions et les obligations du personnel au sujet du traitement des données à caractère personnel incluses dans les fichiers.

d) La structure des fichiers contenant des données à caractère personnel et la description des systèmes d'information qui les traitent.

e) La procédure de notification, de gestion et de réponse en cas d'incidents.

f) Les procédures de réalisation de copies de sécurité et de récupération des données dans les fichiers ou traitements automatisés.

g) Les mesures qui devraient être adoptées pour le transport de supports et de documents, ainsi que pour la destruction des documents et des supports ou, selon le cas, pour la réutilisation de ces derniers.

4. Si les mesures de sécurité de niveau moyen ou les mesures de sécurité de niveau supérieur, qui sont énoncées dans ce titre, sont applicables aux fichiers, le document de sécurité devra contenir en outre:

a) L'identification du responsable ou des responsables de sécurité.

b) Les contrôles réguliers qui devront être réalisés pour vérifier l'application des dispositions contenues dans le propre document.

5. Dans le cas d'un traitement des données réalisé pour le compte de tiers, le document de sécurité devra inclure l'identification des fichiers ou des traitements qui seront traités en qualité de personne chargée du traitement avec une référence expresse au contrat ou au document qui régit les conditions de la commande, ainsi que l'identification du responsable et de la période de validité de la commande.

6. Dans le cas où des données à caractère personnel d'un fichier ou d'un traitement sont ajoutées et traitées de façon exclusive dans les systèmes de la personne chargée du traitement, le responsable devra l'indiquer dans son

document de sécurité. Si cette circonstance concerne une partie ou l'ensemble des fichiers ou des traitements du responsable, on pourra déléguer l'administration du document de sécurité à la personne chargée du traitement, sauf en ce qui concerne les données qui sont contenues dans des ressources propres. Ce fait sera indiqué expressément dans le contrat conclu sous le couvert de l'article 12 de la loi organique 15/1999, du 13 décembre, en spécifiant les fichiers ou les traitements concernés.

Dans ce cas, on s'en tiendra au document de sécurité de la personne chargée du traitement aux fins de l'application des dispositions de ce règlement.

7. Le document de sécurité devra être maintenu constamment à jour et sera révisé chaque fois que des modifications importantes seront apportées au système d'information, au système de traitement utilisé, à son organisation, au contenu de l'information incluse dans les fichiers ou les traitements ou, le cas échéant, à l'occasion des contrôles réguliers qui seront réalisés. En tout état de cause, on estimera qu'une modification sera importante lorsqu'elle pourra avoir des répercussions sur l'application des mesures de sécurité mises en œuvre.

8. Le contenu du document de sécurité devra s'ajuster, à tout moment, aux dispositions applicables en matière de sécurité des données à caractère personnel.

CHAPITRE III

Des mesures de sécurité applicables aux fichiers et aux traitements automatisés

SECTION 1RE. MESURES DE SÉCURITÉ DE NIVEAU ÉLÉMENTAIRE

Article 89. Fonctions et obligations du personnel.

1. Les fonctions et obligations de chaque utilisateur ou de chaque profil d'utilisateurs ayant accès aux données à caractère personnel et aux systèmes d'information seront clairement définies et documentées dans le document de sécurité.

On définira également les fonctions de contrôle ou les autorisations déléguées par le responsable du fichier ou du traitement.

2. Le responsable du fichier ou du traitement prendra les mesures nécessaires pour que le personnel connaisse et comprenne les normes de sécurité qui affecteront l'exercice de ses fonctions ainsi que les conséquences qu'il pourrait subir en cas d'inexécution.

Article 90. Registre d'incidents.

Il faudra prévoir une procédure de notification et de gestion des incidents qui affecteraient les données à caractère personnel et créer un registre dans lequel on indiquera le type d'incident, le moment où il s'est produit ou, le cas échéant, où il a été détecté, la personne qui effectue la notification, le destinataire de celle-ci, les effets que cet incident aurait causés et les mesures correctrices appliquées.

Article 91. Contrôle d'accès.

1. Les utilisateurs auront accès uniquement aux ressources dont ils auront besoin pour exercer leurs fonctions.

2. Le responsable du fichier veillera à ce qu'il existe une liste actualisée des utilisateurs et des profils d'utilisateurs ainsi que des accès autorisés pour chacun d'eux.

3. Le responsable du fichier établira des mécanismes afin d'éviter qu'un utilisateur ne puisse accéder à des ressources s'il ne possède pas les droits correspondants.

4. Seul le personnel qui aura été autorisé à cet effet dans le document de sécurité pourra concéder, modifier ou annuler l'accès autorisé aux ressources, selon les critères établis par le responsable du fichier.

5. Si un personnel étranger au responsable du fichier a accès aux ressources, il devra être soumis aux mêmes conditions et obligations de sécurité que le personnel propre.

Article 92. Gestion des supports et des documents.

1. Les supports et documents qui contiennent des données à caractère personnel devront permettre d'identifier le type d'information qu'ils contiennent, d'être inventoriés et ne devront être accessibles qu'au personnel autorisé à cet effet dans le document de sécurité.

Ces obligations ne seront pas applicables si les caractéristiques physiques du support empêchent de les exécuter, situation qui sera indiquée de façon motivée dans le document de sécurité.

2. La sortie de supports et de documents qui contiennent des données à caractère personnel, y compris ceux qui sont compris et/ou joints à un courriel, hors des locaux se trouvant sous le contrôle du responsable du fichier ou du traitement devra être autorisée par le responsable du fichier ou être dûment autorisée dans le document de sécurité.

3. Lors du transfert de la documentation, on prendra les mesures visant à éviter la subtilisation, la perte ou l'accès indus à l'information pendant le transport de celle-ci.

4. Chaque fois qu'un quelconque document ou support contenant des données à caractère personnel va être jeté, il faudra procéder à la destruction ou à l'effacement de ces données en prenant les mesures visant à éviter l'accès à l'information contenue dans ce dernier ou sa récupération ultérieure.

5. L'identification des supports contenant des données à caractère personnel que l'organisation estimerait spécialement sensibles pourra être réalisée en utilisant des systèmes d'étiquetage compréhensibles et ayant une signification, qui permettront aux utilisateurs autorisés à accéder à ces supports et à ces documents d'identifier leur contenu tout en empêchant leur identification par les autres personnes.

Article 93. Identification et authentification.

1. Le responsable du fichier ou du traitement devra prendre les mesures qui garantiront l'identification et l'authentification correctes des utilisateurs.

2. Le responsable du fichier ou du traitement établira un mécanisme qui permettra l'identification claire et personnalisée de tout utilisateur qui essaierait d'accéder au système d'information et la vérification de son autorisation.

3. Lorsque le mécanisme d'authentification se fonde sur l'existence de mots de passe, il devra exister une procédure d'assignation, de distribution et de stockage qui garantira leur confidentialité et leur intégrité.

4. Le document de sécurité établira la périodicité, qui ne sera jamais supérieure à un an, à laquelle il faudra modifier les mots de passe, qui devront être conservés de façon inintelligible aussi longtemps qu'ils seront valides.

Article 94. Copies de sécurité et récupération.

1. Il faudra établir des procédures d'intervention concernant la réalisation, au moins une fois par semaine, de copies de sécurité sauf si les données n'ont fait l'objet d'aucune mise à jour pendant cette période.

2. On établira également des procédures concernant la récupération des données qui garantiront à chaque instant leur reconstruction dans l'état où elles se trouvaient au moment où la perte ou la destruction se serait produite.

Ce n'est que dans le cas où la perte ou la destruction affecterait des fichiers ou des traitements partiellement automatisés, pour autant que l'existence d'une documentation permette d'atteindre l'objectif visé au paragraphe précédent, qu'on devra enregistrer manuellement les données en signalant ce fait de façon motivée dans le document de sécurité.

3. Le responsable du fichier se chargera de vérifier tous les six mois que la définition, le fonctionnement et l'application des procédures de réalisation de copies de sécurité et de récupération des données sont correctes.

4. Les essais préalables à l'implantation ou à la modification des systèmes d'information qui traitent des fichiers contenant des données à caractère personnel ne seront pas réalisés avec des données réelles, sauf si l'on garantit le niveau de sécurité correspondant au traitement réalisé et si l'on inscrit sa réalisation dans le document de sécurité.

Si l'on prévoit de réaliser des essais avec des données réelles, il faudra avoir effectué au préalable une copie de sécurité de ces données.

SECTION 2. MESURES DE SÉCURITÉ DE NIVEAU MOYEN

Article 95. Responsable de sécurité.

Il faudra désigner dans le document de sécurité un ou plusieurs responsables de sécurité chargés de coordonner et de contrôler les mesures définies dans ce dernier. Cette désignation peut être unique pour tous les fichiers ou traitements de données à caractère personnel ou être différenciée selon les systèmes utilisés, circonstance qui devra être clairement indiquée dans le document de sécurité.

Cette désignation ne constitue en aucun cas une exonération de la responsabilité qui incombe au responsable du fichier ou à la personne chargée du traitement aux termes de ce règlement.

Article 96. Audit.

1. À partir du niveau moyen, les systèmes d'information et les installations de traitement et de stockage de données seront soumis, au moins tous les deux ans, à un audit interne ou externe qui vérifiera le respect des dispositions de ce titre.

Cet audit devra être réalisé à titre extraordinaire chaque fois qu'on effectuera des modifications substantielles dans le système d'information qui pourraient avoir des répercussions sur l'application des mesures de sécurité mises en œuvre dans le but de vérifier l'adaptation, l'ajustement et l'efficacité de ces dernières. Cet audit fera courir la période de deux ans indiquée au paragraphe précédent.

2. Le rapport d'audit devra évaluer la conformité des mesures et des contrôles à la loi et à son développement règlementaire, identifier leurs déficiences et proposer les mesures correctrices ou complémentaire nécessaires. Il devra également inclure les données, les faits et les observations sur lesquels se fondent les évaluations réalisées et les recommandations proposées.

3. Les rapports d'audit seront analysés par le responsable de sécurité compétent, qui transmettra les conclusions au responsable du fichier ou du traitement afin qu'il prenne les mesures correctrices adéquates, et seront mis à la disposition de l'Agence espagnole de protection des données ou, selon le cas, des autorités de contrôle des Communautés autonomes.

Article 97. Gestion des supports et des documents.

1. Il faudra établir un système de registre d'entrée des supports qui permettra de connaître, directement ou indirectement, le type de document ou de support, la date et l'heure, l'expéditeur, le nombre de documents ou de supports inclus dans l'envoi, le type d'information qu'ils contiennent, le mode d'envoi et la personne responsable de la réception qui devra être dûment autorisée à cet effet.

2. On créera également un système de registre de sortie des supports qui permettra de connaître, directement ou indirectement, le type de document ou de support, la date et l'heure, le destinataire, le nombre de documents ou de supports inclus dans l'envoi, le type d'information qu'ils contiennent, le mode d'envoi et la personne responsable de la remise qui devra être dûment autorisée à cet effet.

Article 98. Identification et authentification.

Le responsable du fichier ou du traitement établira un mécanisme qui limitera la possibilité d'essayer de façon répétée d'accéder sans autorisation au système d'information.

Article 99. Contrôle d'accès physique.

Seul le personnel autorisé dans le document de sécurité pourra avoir accès aux lieux où seront installés les équipements physiques qui serviront de support aux systèmes d'information.

Article 100. Registre d'incidents.

1. Il faudra également consigner dans le registre prévu à l'article 90 les procédures de récupération des données qui auront été réalisées en indiquant la personne qui aura exécuté le processus, les données restaurées et, selon le cas, les données qui auront dû être enregistrées manuellement dans le processus de récupération.

2. L'autorisation du responsable du fichier sera nécessaire pour exécuter les procédures de récupération des données.

SECTION 3. MESURES DE SÉCURITÉ DE NIVEAU SUPÉRIEUR

Article 101. Gestion et distribution des supports.

1. L'identification des supports devra être réalisée en utilisant des systèmes d'étiquetage compréhensibles et ayant une signification, qui permettront aux utilisateurs autorisés à accéder à ces supports et à ces documents d'identifier leur contenu tout en empêchant leur identification par les autres personnes.

2. La distribution des supports qui contiennent des données à caractère personnel s'effectuera en chiffrant ces données ou en utilisant un autre mécanisme qui garantira que cette information ne sera pas accessible ni manipulée pendant leur transport.

On chiffrera également les données que contiennent les dispositifs portatifs lorsque ceux-ci seront situés hors des installations qui se trouvent sous le contrôle du responsable du fichier.

3. Il faudra éviter le traitement de données à caractère personnel dans des dispositifs portatifs qui ne permettent pas de les chiffrer. Si c'est strictement nécessaire, on l'indiquera de façon motivée dans le document de sécurité et on prendra des mesures qui tiendront compte des risques associés au fait de réaliser des traitements dans des environnements non protégés.

Article 102. Copies de sécurité et récupération.

Il faudra conserver une copie de sécurité des données et des procédures de récupération de ces dernières à un endroit différent de celui où se trouvent les équipements informatiques qui les traitent, qui devra satisfaire en toute circonstance aux mesures de sécurité exigées dans ce titre ou en utilisant des éléments qui garantiront l'intégrité et la récupération de l'information de sorte qu'il soit possible de les récupérer.

Article 103. Registre d'accès.

1. De chaque tentative d'accès, on conservera au moins l'identification de l'utilisateur, la date et l'heure à laquelle il s'est produit, le fichier consulté, le type d'accès et si ce dernier a été autorisé ou refusé.

2. Si l'accès a été autorisé, il faudra conserver l'information qui permettra d'identifier le registre ayant fait l'objet de l'accès.

3. Les mécanismes qui permettent d'enregistrer les accès se trouveront sous le contrôle direct du responsable de sécurité compétent mais ne doivent permettre ni la désactivation ni la manipulation de ces derniers.

4. La période minimale de conservation des données enregistrées sera de deux ans.

5. Le responsable de sécurité veillera à réviser au moins une fois par mois l'information de contrôle enregistrée et rédigera un rapport des révisions réalisées et des problèmes détectés.

6. L'enregistrement des accès qui est défini dans cet article ne sera pas nécessaire si les circonstances suivantes se produisent:

a) Si le responsable du fichier ou du traitement est une personne physique.

b) Si le responsable du fichier ou du traitement garantit qu'il est le seul à avoir accès et à traiter les données à caractère personnel.

La coïncidence des deux circonstances visées à l'alinéa précédent devra être consignée de façon expressedans le document de sécurité.

Article 104. Télécommunications.

Lorsqu'il est nécessaire, aux termes de l'article 81.3, de mettre en œuvre les mesures de sécurité de niveau supérieur, la transmission de données à caractère personnel à travers des réseaux publics ou des réseaux sans fil de communication électronique s'effectuera en chiffrant ces données ou en utilisant tout autre mécanisme qui garantira que l'information ne sera pas intelligible et ne pourra pas être manipulée par des tiers.

CHAPITRE IV

Des mesures de sécurité applicables aux fichiers et aux traitements non automatisés

SECTION 1RE. MESURES DE SÉCURITÉ DE NIVEAU ÉLÉMENTAIRE

Article 105. Obligations communes.

1. Les fichiers non automatisés se verront appliquer, outre les dispositions figurant dans ce chapitre, les dispositions des chapitres I et II du présent titre en ce qui concerne :

a) L'étendue.

b) Les niveaux de sécurité.

c) La personne chargée du traitement.

d) Les prestations de services sans accès à des données à caractère personnel.

e) La délégation d'autorisations.

f) Le régime de travail hors des locaux du responsable du fichier ou de la personne chargée du traitement.

g) Les copies de travail de documents.

h) Le document de sécurité.

2. Ils se verront également appliquer les dispositions de la première section du chapitre III du présent titre concernant:

a) Les fonctions et les obligations du personnel.

b) Le registre d'incidents.

c) Le contrôle d'accès.

d) La gestion des supports.

Article 106. Critères d'archivage.

L'archivage des supports ou documents s'effectuera selon les critères prévus dans leur législation respective. Ces critères devront garantir la bonne conservation des documents, la localisation et la consultation de l'information, et permettre l'exercice des droits d'opposition au traitement, d'accès, de rectification et d'annulation.

Dans les cas où il n'existerait pas de norme applicable, le responsable du fichier devra établir les critères et les procédures d'action qui devront être suivis pour l'archivage.

Article 107. Dispositifs de stockage.

Les dispositifs de stockage des documents qui contiennent des données à caractère personnel devront être assortis de mécanismes empêchant leur ouverture. Si les caractéristiques physiques de ces derniers ne permettent pas d'appliquer cette mesure, le responsable du fichier ou du traitement prendra des mesures qui empêcheront l'accès des personnes non autorisées.

Article 108. Garde des supports.

Aussi longtemps que la documentation contenant des données à caractère personnel ne sera pas archivée dans les dispositifs de stockage établis à l'article précédent, parce qu'elle se trouve en cours de révision ou de traitement préalable ou postérieur à son archivage, la personne qui en a la charge devra la garder et empêcher en tout moment qu'une personne non autorisée puisse y accéder.

SECTION 2. MESURES DE SÉCURITÉ DE NIVEAU MOYEN

Article 109. Responsable de sécurité.

On désignera un ou plusieurs responsables de sécurité dans les conditions et avec les fonctions prévues à l'article 95 de ce règlement.

Article 110. Audit.

Les fichiers compris dans la présente section seront soumis, au moins tous les deux ans, à un audit interne ou externe qui vérifiera le respect des dispositions du présent titre.

SECTION 3. MESURES DE SÉCURITÉ DE NIVEAU SUPÉRIEUR

Article 111. Stockage de l'information.

1. Les armoires, classeurs ou autres éléments dans lesquels seront stockés les fichiers non automatisés contenant des données à caractère personnel devront être installés dans des lieux dont l'accès sera protégé à l'aide de portes munies de systèmes d'ouverture à clef ou d'un autre dispositif équivalent. Ces lieux devront être fermés lorsqu'il ne sera pas nécessaire d'accéder aux documents inclus dans le fichier.

2. Si les caractéristiques des locaux dont dispose le responsable du fichier ou du traitement ne permettent pas de respecter les dispositions de l'alinéa précédent, le responsable prendra des mesures alternatives qui seront indiquées de façon motivée dans le document de sécurité.

Article 112. Copie ou reproduction.

1. La génération de copies ou la reproduction des documents ne pourra s'effectuer que sous le contrôle du personnel autorisé dans le document de sécurité.

2. Il faudra procéder à la destruction des copies ou des reproductions jetées afin d'empêcher l'accès à l'information contenue dans celles-ci ou leur récupération ultérieure.

Article 113. Accès à la documentation.

1. L'accès à la documentation sera exclusivement réservé au personnel autorisé.

2. On établira des mécanismes qui permettront d'identifier les accès réalisés dans le cas de documents qui peuvent être utilisés par de multiples utilisateurs.

3. L'accès de personnes non incluses au paragraphe précédent devra être dûment enregistré selon la procédure établie à cet effet dans le document de sécurité.

Article 114. Transfert de la documentation.

Chaque fois qu'on réalisera le transfert physique de la documentation contenue dans un fichier, il faudra prendre des mesures visant à empêcher l'accès ou la manipulation de l'information faisant l'objet du transfert.

TITRE IX

Des procédures réalisées par l'Agence espagnole de protection des données

CHAPITRE IER

Dispositions générales

Article 115. Régime applicable.

1. Les procédures réalisées par l'Agence espagnole de protection des données seront régies par des dispositions de ce titre et, à titre supplétoire, par la loi 30/1992, du 26 novembre, relative au régime juridique des administrations publiques et de la procédure administrative commune.

2. Les normes régissant la procédure administrative commune s'appliqueront de façon spécifique au régime de représentation dans les procédures citées.

Article 116. Publicité des résolutions.

1. L'Agence espagnole de protection des données rendra publiques ses résolutions, hormis celles qui concerneront l'inscription d'un fichier ou d'un traitement au registre général de protection des données et celles qui auront trait à l'inscription des codes type dans ce dernier, pour autant qu'elles se réfèrent à des procédures qui auraient été ouvertes après le 1er janvier 2004 ou qui correspondraient à l'archivage d'actions d'inspection engagées à partir de cette date.

2. La publication de ces résolutions s'effectuera de préférence au moyen de leur insertion sur le site web de l'Agence espagnole de protection des données dans le délai de un mois à compter de la date de leur notification aux intéressés.

3. Les personnes concernées seront expressément informées, dans la notification des résolutions, de la publicité qui est prévue à l'article 37.2 de la loi organique 15/1999, du 13 décembre.

4. La publication sera réalisée en appliquant les critères de dissociation des données à caractère personnel qui seront établis à cet effet au moyen d'une résolution du Directeur de l'Agence.

CHAPITRE II

De la procédure de tutelle des droits d'accès, de rectification, d'annulation et d'opposition

Article 117. Instruction de la procédure.

1. La procédure sera ouverte à la demande de la personne concernée ou des personnes concernées en indiquant clairement le contenu de leur réclamation et les dispositions de la loi organique 15/1999, du 13 décembre, qui auraient été violées.

2. Une fois qu'elle aura été reçue par l'Agence espagnole de protection des données, la réclamation sera transmise au responsable du fichier afin qu'il présente, dans le délai de quinze jours, les allégations qu'il estimerait pertinentes.

3. Lorsque les allégations auront été reçues ou le délai prévu à l'alinéa précédent se sera écoulé, l'Agence espagnole de protection des données se prononcera sur la réclamation présentée, après avoir réalisé les rapports, les essais et d'autres actes d'instruction pertinents comprenant l'audition de la personne concernée et une nouvelle audition du responsable du fichier.

Article 118. Durée de la procédure et effets de l'absence de résolution expresse.

1. Le délai maximum pour émettre et notifier la résolution dans la procédure de tutelle des droits sera de six mois à compter de la date de dépôt de la réclamation de la personne concernée ou des personnes concernées à l'Agence espagnole de protection des données.

2. Si aucune résolution expresse n'a été émise ni notifiée dans ce délai, la personne concernée pourra considérer que sa réclamation aura été admise en vertu du silence administratif positif.

Article 119. Exécution de la résolution.

Si la résolution de tutelle est admise, il sera exigé au responsable du fichier qu'il permette l'exercice des droits objet de la tutelle dans le délai de dix jours suivant la notification et qu'il communique par écrit, dans le même délai, l'exécution de cette obligation à l'Agence espagnole de protection des données.

CHAPITRE III

Des procédures relatives à l'exercice du pouvoir de sanction

SECTION 1RE. DISPOSITIONS GÉNÉRALES

Article 120. Champ d'application.

1. Les dispositions contenues dans le présent chapitre seront applicables aux procédures relatives à l'exercice par l'Agence espagnole de protection des données du pouvoir de sanction qui lui est attribué par la loi organique 15/1999, du 13 décembre, relative à la protection des données à caractère personnel, dans la loi 34/2002, du 11 juillet, sur les services de la société de l'information et du commerce électronique, et dans la loi 32/2003, du 3 novembre, à caractère général, sur les télécommunications.

2. Ceci dit, les dispositions prévues à l'article 121 et dans la quatrième section de ce chapitre ne seront applicables qu'aux procédures concernant l'exercice du pouvoir de sanction prévue dans la loi organique 15/1999, du 13 décembre.

Article 121. Immobilisation de fichiers.

1. Dans le cas qualifié d'infraction très grave par la loi organique 15/1999, du 13 décembre, qui impliquerait l'utilisation ou la cession illicite des données à caractère personnel dans laquelle on empêcherait ou on porterait atteinte gravement à l'exercice des droits des citoyens et au libre développement de la personnalité qui est garanti par la Constitution et par les lois, le Directeur de l'Agence espagnole de protection des données pourra requérir, à n'importe quel moment de la procédure, les responsables des fichiers ou des traitements de données à caractère personnel, aussi bien publics que privés, de cesser l'utilisation ou la cession illicite des données.

2. La requête devra être satisfaite dans le délai non prorogeable de trois jours pendant lequel le responsable du fichier pourra formuler les allégations qu'il estimerait opportunes afin d'obtenir la levée de la mesure.

3. Si la requête n'est pas satisfaite, le Directeur de l'Agence espagnole de protection des données pourra décider, moyennant une résolution motivée, d'immobiliser ces fichiers ou traitements aux seules fins de restaurer les droits des personnes concernées.

SECTION 2. ACTES PRÉLIMINAIRES

Article 122. Ouverture de la procédure.

1. Des actes préliminaires pourront être réalisés avant d'entamer la procédure de sanction afin de déterminer l'existence éventuelle de circonstances qui justifieraient cette ouverture. En particulier, ces actes viseront à déterminer, de la façon la plus précise possible, les faits qui pourraient justifier l'ouverture de la procédure, à identifier la personne ou l'organe qui pourrait être responsable et à établir les principales circonstances qui pourraient exister dans ce cas.

2. Les actes préliminaires seront exécutés d'office par l'Agence espagnole de protection des données, soit de sa propre initiative, soit du fait de l'existence d'une plainte ou d'une demande raisonnée émanant d'un autre organe.

3. Lorsque les actes sont exécutés du fait de l'existence d'une plainte ou d'une demande raisonnée émanant d'un autre organe, l'Agence espagnole de protection des données accusera réception de la plainte ou de la demande et pourra demander toute la documentation qu'elle estimerait nécessaire pour pouvoir vérifier les faits susceptibles de motiver l'ouverture de la procédure de sanction.

4. Ces actes préliminaires auront une durée maximale de douze mois à compter de la date à laquelle la plainte ou la demande raisonnée visée à l'alinéa 2 aurait été reçue par l'Agence espagnole de protection des données ou, si celle-ci n'existe pas, à partir du moment où le Directeur de l'Agence déciderait de les exécuter.

L'expiration du délai sans qu'une décision d'ouverture de la procédure de sanction n'ait été émise rendra caduques les actes préliminaires.

Article 123. Personnel compétent pour la réalisation des actes préliminaires.

1. Les actes préliminaires seront exercés par le personnel du département d'inspection des données qui sera autorisé à exercer des fonctions d'inspection.

2. (Annulé)

3. Les fonctionnaires exerçant l'inspection qui sont visés aux deux alinéas précédents seront considérés comme une autorité publique dans l'exercice de leurs fonctions.

Ils seront tenus de garder secrètes les informations dont ils prendraient connaissance pendant l'exercice des fonctions citées, y compris après avoir cessé leurs fonctions.

Article 124. Obtention d'information.

Les inspecteurs pourront demander toutes les informations dont ils auront besoin pour remplir leur mission. À cette fin, ils pourront exiger la présentation ou l'envoi des documents et des données et les examiner à l'endroit où ils seront déposés, obtenir des copies de ces derniers, examiner les équipements physiques et logiques, et exiger l'exécution des traitements et des programmes ou procédures de gestion et de support du fichier ou des fichiers faisant l'objet d'un examen en accédant aux endroits où ils seront installés.

Article 125. Actes présentiels.

1. Les inspecteurs désignés pourront réaliser, dans le cadre des actes préliminaires, des visites d'inspection dans les locaux ou au siège de la personne faisant l'objet d'une inspection ou, le cas échéant, à l'endroit où se trouveront les fichiers. Pour ce faire, les inspecteurs auront été autorisés au préalable par le Directeur de l'Agence espagnole de protection des données.

Les inspections pourront être réalisées au domicile de la personne inspectée, au siège ou dans un local concret associé à celle-ci ou dans n'importe lequel de ses locaux, y compris dans ceux où le traitement sera réalisé par une personne chargée du traitement.

L'autorisation se limitera à indiquer l'habilitation de l'inspecteur autorisé et l'identification de la personne ou de l'organe faisant l'objet de l'inspection.

2. Dans le cas prévu à l'alinéa précédent, les inspections s'achèveront par la rédaction du procès-verbal correspondant dans lequel on inscrira les actes réalisés pendant la visite ou les visites d'inspection.

3. Le procès-verbal, qui sera émis en double exemplaire, sera signé par les inspecteurs intervenants et par la personne inspectée, qui pourra y consigner les allégations ou les déclarations qu'elle estimera opportunes.

Si la personne inspectée refuse de signer le procès-verbal, on signalera cette circonstance de façon expresse dans ce dernier. En tout état de cause, la signature du procès-verbal par la personne inspectée n'impliquera pas sa conformité, mais tout au plus la réception de ce document.

Un des originaux du procès-verbal d'inspection sera remis à la personne inspectée et l'autre sera joint aux actes.

Article 126. Résultat des actes préliminaires.

1. Une fois terminés, les actes préliminaires seront soumis à la décision du Directeur de l'Agence espagnole de protection des données.

Si les actes ne révèlent pas de faits susceptibles de motiver l'imputation d'une infraction quelconque, le Directeur de l'Agence espagnole de protection des données émettra une décision de classement sans suite qui sera notifiée à la personne inspectée et, selon le cas, à l'auteur de la plainte.

2. Si l'on apprécie l'existence d'indices susceptibles de motiver l'imputation d'une infraction, le Directeur de l'Agence espagnole de protection des données rendra une décision d'ouverture de procédure de sanction ou d'infraction des administrations publiques, qui sera exécutée selon les dispositions figurant respectivement aux sections trois et quatre de ce chapitre.

SECTION 3. PROCÉDURES DE SANCTION

Article 127. Ouverture de la procédure.

À titre spécifique, la décision d'ouvrir la procédure de sanction devra contenir :

a) L'identification de la personne ou des personnes présumées responsables.

b) La description succincte des faits imputés, leur qualification éventuelle et les sanctions qui pourraient être appliquées, sans préjudice du résultat de l'instruction.

c) L'indication que l'organe compétent pour résoudre la procédure est le Directeur de l'Agence espagnole de protection des données.

d) L'indication au responsable présumé qu'il peut reconnaître volontairement sa responsabilité, auquel cas la résolution sera directement émise.

e) La désignation de l'instructeur et, le cas échéant, du secrétaire, en indiquant expressément le régime de récusation de ceux-ci.

f) L'indication expresse du droit du responsable à présenter des allégations, à se faire entendre pendant la procédure et à proposer les preuves qu'il estimerait opportunes.

g) Les mesures de caractère provisoire qui pourraient avoir été convenues conformément aux dispositions de la première section du présent chapitre.

Article 128. Délai maximum pour statuer.

1. Le délai prévu pour émettre une résolution sera celui que détermineront les normes applicables à chaque procédure de sanction et sera calculé à partir de la date à laquelle aura été émise la décision d'engager la procédure jusqu'à ce que se produise la notification de la résolution de sanction ou que soit dûment justifiée la tentative de notification.

2. L'échéance dudit délai maximum sans qu'aucune résolution expresse n'ait été émise ni notifiée rendra caduque la procédure et provoquera le classement sans suite des actes.

SECTION 4. PROCÉDURE DE DÉCLARATION D'INFRACTION DE LA LOI ORGANIQUE 15/1999, DU 13 DÉCEMBRE, PAR LES ADMINISTRATIONS PUBLIQUES

Article 129. Disposition générale.

La procédure qui permettra de déclarer l'existence d'une infraction de la loi organique 15/1999, du 13 décembre, commise par les administrations publiques sera celle qui est établie dans la troisième section de ce chapitre.

CHAPITRE IV

Des procédures liées à l'inscription ou à l'annulation de fichiers

SECTION 1RE. PROCÉDURE D'INSCRIPTION DE LA CRÉATION, DE LA MODIFICATION OU DE LA SUPPRESSION DE FICHIERS

Article 130. Ouverture de la procédure.

1. La procédure sera déclenchée par la notification de la création, de la modification ou de la suppression du fichier par l'intéressé ou, selon le cas, par la communication effectuée par les autorités de contrôle des Communautés autonomes à laquelle fait référence le présent règlement.

2. La notification devra s'effectuer en remplissant les modèles ou formulaires électroniques publiés à cet effet par l'Agence espagnole de protection des données, en vertu des dispositions de l'aliéna 1er de l'article 59 de ce règlement.

S'il s'agit de la notification de la modification ou de la suppression d'un fichier, il faudra y indiquer le code d'inscription du fichier au registre général de protection des données.

3. La notification s'effectuera sur un support électronique, que ce soit par communication électronique à travers Internet à l'aide d'une signature électronique ou sur un support informatique, en utilisant à cet effet le programme d'aide à la génération de notifications que l'Agence mettra gratuitement à la disposition des intéressés.

La notification effectuée sur support papier sera tout aussi valide si elle a été présentée sur les modèles ou les formulaires publiés par l'Agence.

4. Dans la notification, le responsable du fichier devra déclarer un domicile aux fins des notifications dans le cadre de la procédure.

Article 131. Particularité concernant la notification de fichiers publics.

1. Lorsqu'il s'agit de la notification de fichiers publics, il faudra joindre à la notification une copie de la norme ou de la décision de création, de modification ou de suppression du fichier à laquelle fait référence l'article 52 du présent règlement.

Lorsque le journal officiel dans lequel est publiée ladite norme ou décision est accessible à travers Internet, il suffira d'indiquer dans la notification l'adresse électronique où elle pourra être localisée.

2. Si, une fois reçue, la notification ne contient pas l'information obligatoire ou si l'on y observe des défauts de forme, le registre général de protection des données exigera au responsable du fichier de compléter ou de corriger la notification. Le délai prévu pour corriger ou améliorer la demande sera de trois mois dans le cas où il serait nécessaire de modifier la norme ou la décision de création du fichier.

Article 132. Décision d'inscription ou d'annulation.

Si la notification relative à la création, à la modification ou à la suppression du fichier contient l'information obligatoire et si les autres exigences légales sont remplies, le Directeur de l'Agence espagnole de protection des données décidera, à la demande du registre général de protection des données, respectivement l'inscription du fichier en lui assignant le code d'inscription correspondant, la modification de l'inscription du fichier ou l'annulation de l'inscription correspondante.

Article 133. Inadmissibilité ou refus de l'inscription.

Le Directeur de l'Agence espagnole de protection des données, agissant sur proposition du registre général de protection des données, émettra une résolution refusant l'inscription, la modification ou l'annulation si les documents présentés par le responsable du fichier montrent que la notification n'est pas conforme aux dispositions de la loi organique 15/1999, du 13 décembre.

La résolution sera dûment motivée et indiquera expressément les causes qui empêcheraient l'inscription, la modification ou l'annulation.

Article 134. Durée de la procédure et effets de l'absence de résolution expresse.

1. Le délai maximum pour émettre et notifier une résolution concernant l'inscription, la modification ou l'annulation sera de un mois.

2. Si aucune résolution expresse n'a été émise ni notifiée dans ce délai, on considérera que le fichier aura été inscrit, modifié ou annulé à tous les effets.

SECTION 2. PROCÉDURE D'ANNULATION D'OFFICE DES FICHIERS INSCRITS

Article 135. Ouverture de la procédure.

La procédure d'annulation d'office des fichiers inscrits au registre général de protection des données sera toujours ouverte d'office, soit sur une propre initiative, soit en vertu d'une plainte, sur décision du Directeur de l'Agence espagnole de protection des données.

Article 136. Clôture du dossier.

Après audition de l'intéressé, la résolution indiquera s'il y a lieu ou non d'annuler le fichier.

Si la résolution décide d'annuler le fichier, on fera part de cette décision au registre général de protection des données afin qu'il procède à l'annulation.

CHAPITRE V

Des procédures liées aux transferts internationaux de données

SECTION 1RE. PROCÉDURE D'AUTORISATION DE TRANSFERTS INTERNATIONAUX DE DONNÉES

Article 137. Ouverture de la procédure.

1. La procédure visant à obtenir l'autorisation d'effectuer des transferts internationaux de données vers des pays tiers auxquels font référence l'article 33 de la loi organique 15/1999, du 13 décembre, et l'article 70 de ce règlement sera toujours ouverte à la demande de l'exportateur qui souhaiterait réaliser le transfert.

2. Outre les conditions légales requises, l'exportateur devra toujours indiquer dans sa demande :

a) L'identification du fichier ou des fichiers sur les données desquelles porte le transfert international, en indiquant la dénomination et le code d'inscription du fichier au registre général de protection des données.

b) Le transfert ou les transferts qui font l'objet de la demande d'autorisation en indiquant la finalité qui la justifie.

c) La documentation contenant les garanties exigibles pour l'obtention de l'autorisation et, le cas échéant, le respect des conditions légales nécessaires pour la réalisation du transfert.

Si l'autorisation repose sur l'existence d'un contrat conclu entre l'exportateur et l'importateur des données, il faudra présenter une copie de ce dernier et justifier que les parties au contrat possèdent la capacité juridique suffisante.

Si l'on souhaite fonder l'autorisation sur les dispositions de l'alinéa 4 de l'article 70, il faudra présenter les normes ou règles adoptées au sujet du traitement des données au sein du groupe, ainsi que la documentation justifiant leur caractère obligatoire et leur efficacité au sein du groupe. Il faudra également présenter la documentation qui justifiera que la personne concernée ou l'Agence espagnole de protection des données aura la possibilité d'exiger la responsabilité correspondante en cas de préjudice causé à la personne concernée ou en cas de violation des normes de protection des données par n'importe quelle société importatrice.

Article 138. Instruction de la procédure.

1. Si le Directeur de l'Agence espagnole de protection des données décide, en vertu des dispositions de l'article 86.1 de la loi 30/1992, du 26 novembre, l'ouverture d'une période d'information publique, le délai prévu pour la présentation d'allégations sera de dix jours à compter de la publication au Journal officiel de l'État de l'avis prévu dans cette loi.

2. Il ne sera pas possible d'accéder à l'information du dossier dans quel se produisent les circonstances établies à l'article 37.5 de la loi 30/1992, du 26 novembre.

3. Passé le délai prévu à l'alinéa 1er, si des allégations ont été formulées, elles seront transmises au demandeur de l'autorisation afin qu'il puisse formuler à son tour les allégations qu'il estimerait pertinentes dans un délai de dix jours.

Article 139. Actes réalisés après la résolution.

1. S'il décide d'autoriser le transfert international de données, le Directeur de l'Agence espagnole de protection des données communiquera sa décision d'autorisation au registre général de protection des données afin de procéder à son inscription.

Le registre général de protection des données inscrira d'office l'autorisation de transfert international.

2. En tout état de cause, on communiquera la décision d'autoriser ou de refuser l'autorisation du transfert international de données au ministère de la Justice afin qu'il la notifie à la Commission européenne et aux autres États membres de l'Union européenne conformément aux dispositions de l'article 26.3 de la directive 95/46/CE.

Article 140. Durée de la procédure et effets de l'absence de résolution expresse.

1. Le délai maximum prévu pour émettre et notifier la résolution sera de trois mois à compter de la date de réception de la demande par l'Agence espagnole de protection des données.

2. Si aucune résolution expresse n'a été émise ni notifiée dans ce délai, on considérera que l'autorisation du transfert international de données aura été autorisée.

SECTION 2. PROCÉDURE DE SUSPENSION PROVISOIRE DE TRANSFERTS INTERNATIONAUX DE DONNÉES

Article 141. Ouverture de la procédure.

1. Le Directeur de l'Agence espagnole de protection des données pourra décider de suspendre provisoirement un transfert international de données dans les cas prévus à l'article 69 et à l'alinéa 3 de l'article 70.

2. Dans ces cas, le Directeur rendra une décision visant à engager la procédure de suspension provisoire du transfert. La décision devra être motivée et se fonder sur les cas prévus dans ce règlement.

Article 142. Instruction et résolution.

1. La décision sera communiquée à l'exportateur afin qu'il présente les allégations qu'il estimerait pertinentes dans le délai de quinze jours.

2. Lorsque les allégations auront été reçues ou lorsque le délai indiqué se sera écoulé, le Directeur émettra une résolution prévoyant, le cas échéant, la suspension provisoire du transfert international de données.

Article 143. Actes réalisés après la résolution.

1. Le Directeur de l'Agence espagnole de protection des données communiquera la résolution au registre général de protection des données afin qu'elle soit inscrite au registre.

Le registre général de protection des données inscrira d'office la suspension provisoire du transfert international.

2. En tout état de cause, on communiquera la résolution au ministère de la Justice afin qu'il la notifie à la Commission européenne et aux autres États membres de l'Union européenne conformément aux dispositions de l'article 26.3 de la directive 95/46/CE.

Article 144. Levée de la suspension provisoire.

1. La suspension sera levée, dès que cesseront les causes qui l'auront justifiée, moyennant une résolution du Directeur de l'Agence espagnole de protection des données qui sera communiquée à l'exportateur.

2. Le Directeur de l'Agence espagnole de protection des données communiquera la résolution au registre général de protection des données afin qu'elle soit inscrite au registre.

Le registre général de protection des données inscrira d'office la levée de la suspension provisoire du transfert international.

3. La décision sera communiquée à l'exportateur et au ministère de la Justice afin qu'il la notifie à la Commission européenne et aux autres États membres de l'Union européenne conformément aux dispositions de l'article 26 de la directive 95/46/CE.

CHAPITRE VI

De la procédure d'inscription des codes type

Article 145. Ouverture de la procédure.

1. La procédure relative à l'inscription des codes type au registre général de protection des données sera toujours déclenchée à la demande de l'entité, de l'organe ou de l'association promotrice du code type.

2. La demande, qui devra être conforme aux conditions légales établies, devra être accompagnée des documents suivants:

a) La justification de la représentation que possède la personne qui introduit la demande.

b) Le contenu de la décision, de la convention ou de la décision en vertu de laquelle est approuvé, dans le domaine correspondant, le code type présenté.

c) Si le code type provient d'une convention sectorielle ou d'une décision d'une entreprise, la certification concernant l'adoption de la convention et la légitimation de l'organe qui l'a adoptée.

d) Dans le cas mentionné à la lettre précédente, une copie des statuts de l'association, de l'organisation sectorielle ou de l'entité dans le cadre de laquelle le code aura été approuvé.

e) Dans le cas des codes type présentés par des associations ou des organisations à caractère sectoriel, la documentation concernant leur représentativité dans le secteur.

f) Dans le cas des codes type fondés sur des décisions d'entreprise, la description des traitements auxquels fait référence le code type.

g) Le code type soumis à l'Agence espagnole de protection des données.

Article 146. Analyses des aspects substantiels du code type.

1. Pendant les trente jours suivant la notification ou la correction des défauts, le registre général de protection des données pourra convoquer les demandeurs pour obtenir des explications ou des précisions sur le contenu substantiel du code type.

2. Au terme du délai indiqué à l'alinéa précédent, le registre général de protection des données rédigera un rapport sur les caractéristiques du projet de code type.

3. La documentation présentée et le rapport du registre seront remis au bureau juridique afin que celui-ci évalue le respect des conditions établies au titre VII de ce règlement.

Article 147. Information publique.

1. Si le Directeur de l'Agence espagnole de protection des données décide, en vertu des dispositions de l'article 86.1 de la loi 30/1992, du 26 novembre, l'ouverture d'une période d'information publique, le délai prévu pour la présentation d'allégations sera de dix jours à compter de la publication au Journal officiel de l'État de l'avis prévu dans cette loi.

2. Il ne sera pas possible d'accéder à l'information du dossier dans quel se produisent les circonstances établies à l'article 37.5 de la loi 30/1992, du 26 novembre.

Article 148. Amélioration du code type.

S'il s'avère nécessaire, dans le courant de la procédure, de présenter de nouveaux documents ou de modifier le code type présenté, l'Agence espagnole de protection des données pourra sommer le demandeur d'introduire les modifications nécessaires dans le délai de trente jours et d'envoyer le texte amendé à l'Agence espagnole de protection des données.

L'inexécution de cette requête par le demandeur provoquera la suspension de la procédure.

Article 149. Procédure de consultation.

Si des allégations ont été formulées lors des formalités prévues à l'article 148, on les transmettra au demandeur de l'autorisation afin qu'il puisse faire à son tour les allégations qu'il estimerait pertinentes dans un délai de dix jours.

Article 150. Résolution.

1. Lorsque les conditions établies aux articles précédents auront été remplies, le Directeur de l'Agence décidera s'il convient d'inscrire le code type au registre général de protection des données.

2. Si le Directeur de l'Agence espagnole de protection des données décide d'autoriser l'inscription du code type, il communiquera sa décision au registre général de protection des données afin de procéder à son inscription.

Article 151. Durée de la procédure et effets de l'absence de résolution expresse.

1. Le délai maximum prévu pour émettre et notifier la résolution sera de six mois à compter de la date de réception de la demande par l'Agence espagnole de protection des données.

2. Si aucune résolution expresse n'a été émise ni notifiée dans ce délai, le demandeur pourra considérer que sa demande aura été admise.

Article 152. Publication des codes type par l'Agence espagnole de protection des données.

L'Agence espagnole de protection des données fera la publicité du contenu des codes type inscrits au registre général de protection des données en utilisant de préférence des moyens électroniques et télématiques.

CHAPITRE VII

Des autres procédures réalisées par l'Agence espagnole de protection des données

SECTION 1RE. PROCÉDURE D'EXEMPTION DU DEVOIR D'INFORMATION DE L'INTÉRESSÉ

Article 153. Ouverture de la procédure.

1. La procédure visant à obtenir de l'Agence espagnole de protection des données l'exemption du devoir d'information de l'intéressé au sujet du traitement de ses données à caractère personnel lorsque ce devoir est impossible ou qu'il requiert des efforts disproportionnés, telle qu'elle est prévue à l'alinéa 5 de l'article 5 de la loi organique 15/1999, du 13 décembre, sera toujours déclenchée à la demande du responsable qui souhaiterait obtenir l'application de l'exemption.

2. Dans le document de la demande, outre les conditions établies à l'article 70 de la loi 30/1992, du 26 novembre, le responsable devra:

a) Identifier clairement le traitement des données auquel il souhaite appliquer l'exemption du devoir d'information.

b) Motiver de façon expresse les causes sur lesquelles il fonde l'impossibilité ou le caractère disproportionné de l'effort qu'impliquerait le respect du devoir d'information.

c) Exposer en détailles les mesures de compensation qu'il envisage d'appliquer en cas d'exemption du respect du devoir d'information.

d) Présenter une clause informative qui, moyennant sa diffusion dans les conditions indiquées dans la demande, permettrait de compenser l'exemption du devoir d'information.

Article 154. Proposition de nouvelles mesures de compensation.

1. Si elle estime que les mesures de compensation proposées par le demandeur sont insuffisantes, l'Agence espagnole de protection des données pourra décider l'adoption de mesures complétant ou remplaçant celles qu'il aura énoncées dans sa demande.

2. La décision sera communiquée au demandeur afin qu'il présente les allégations qu'il estimerait pertinentes dans le délai de quinze jours.

Article 155. Fin de la procédure.

Une fois que les formalités prévues dans les articles précédents auront été terminées, le Directeur de l'Agence émettra une résolution concédant ou refusant l'exemption du devoir d'information. La résolution pourra imposer l'adoption de mesures complémentaires à celles qui sont visées à l'article précédent.

Article 156. Durée de la procédure et effets de l'absence de résolution expresse.

1. Le délai maximum prévu pour émettre et notifier la résolution dans la procédure sera de six mois à compter de la date de réception de la demande du responsable du fichier par l'Agence espagnole de protection des données.

2. Si aucune résolution expresse n'a été émise ni notifiée dans ce délai, la personne concernée pourra considérer que sa demande aura été admise en vertu du silence administratif positif.

SECTION 2. PROCÉDURE RELATIVE À L'AUTORISATION DE CONSERVATION DE DONNÉE À DES FINS HISTORIQUES, STATISTIQUES OU SCIENTIFIQUES

Article 157. Ouverture de la procédure.

1. La procédure visant à obtenir de l'Agence espagnole de protection des données la déclaration de l'existence, dans un traitement déterminé, de données de valeurs historiques, scientifiques ou statistiques, aux fins prévues dans la loi organique 15/1999, du 13 décembre, et dans le présent règlement, sera toujours déclenchée à la demande du responsable qui souhaiterait obtenir la déclaration.

2. Dans le document de la demande, le responsable devra :

a) Identifier clairement le traitement des données auquel il souhaite appliquer l'exception.

b) Motiver expressément les causes qui justifieraient la déclaration.

c) Exposer en détail les mesures que le responsable du fichier a l'intention de mettre en œuvre pour garantir le droit des citoyens.

3. La demande devra être accompagnée de tous les documents ou preuves qui seraient nécessaires pour justifier l'existence des valeurs historiques, scientifiques ou statistiques qui justifieraient la déclaration de l'Agence.

Article 158. Durée de la procédure et effets de l'absence de résolution expresse.

1. Le délai maximum prévu pour émettre et notifier la résolution dans la procédure sera de trois mois à compter de la date de réception de la demande du responsable du fichier par l'Agence espagnole de protection des données.

2. Si aucune résolution expresse n'a été émise ni notifiée dans ce délai, la personne concernée pourra considérer que sa demande aura été admise.

Disposition additionnelle unique. Produits logiciels.

Les produits logiciels destinés au traitement automatisé de données à caractère personnel devront inclure dans leur description technique le niveau de sécurité élémentaire, moyen ou supérieur qu'ils pourront atteindre conformément aux dispositions du titre VIII de ce règlement.

Disposition finale unique. Application supplétive.

Pour toutes les questions qui ne sont pas établies au chapitre III du titre IX, les procédures de sanction introduites par l'Agence espagnole de protection des données seront soumises aux dispositions contenues dans le règlement de la procédure concernant l'exercice du pouvoir de sanction, approuvé par le décret royal 1398/1993, du 4 août.