NORMES DE PROTECTION DES DONNÉES PERSONNELLES

RÉSEAU IBÉRO-AMÉRICAIN DE PROTECTION DES DONNÉES

NORMES DE PROTECTION
DES DONNÉES PERSONNELLES
POUR LES ÉTATS IBÉRO-AMÉRICAINS

Dans le cadre de la XVe Rencontre Ibéro-américaine sur la protection des données, le Réseau Ibéro-américain de protection des données (RIPD ou Réseau) a approuvé et présenté officiellement les « Normes de protection des données des États ibéro-américains », donnant suite ainsi à un objectif poursuivi de longue date par toutes les entités membres, ainsi qu'à l'un des accords adoptés lors du XXVe Sommet Ibéro-américain des chefs d'État et de gouvernement, qui s'est tenu les 28 et 29 octobre 2016 en Colombie, qui porte sur la demande au Réseau d'élaborer une proposition de coopération efficace concernant la protection des données personnelles et la vie privée.

Le texte adopté vise à répondre à l'un des axes de la stratégie convenue par le RIPD en novembre 2016 à Montevideo, reflété dans le document « RIPD 2020 », pour « promouvoir et contribuer au renforcement et à l'adaptation des processus de réglementation dans la région à travers l'élaboration de lignes directrices qui servent de paramètre pour les réglementations futures ou pour la révision de celles existantes ».

En ce sens, les Normes ibéro-américaines constituent un ensemble de lignes directrices qui contribuent à la diffusion d'initiatives réglementaires pour la protection des données personnelles dans la région ibéro-américaine des pays qui ne disposent pas encore de ces règlements ou, le cas échéant, servent de référence pour la modernisation et la mise à jour de la législation existante.

Parmi les objectifs des Normes ibéro-américaines, on peut citer :

- Établir un ensemble de principes et de droits communs pour la protection des données personnelles que les États ibéro-américains puissent adopter et développer dans leur législation nationale, dans le but d'avoir des règles homogènes dans la région.

- Garantir l'exercice effectif et la défense du droit à la protection des données personnelles d'une personne physique dans les États ibéro-américains, en établissant des règles communes qui garantissent le traitement adéquat de ses données personnelles.

- Faciliter le flux de données personnelles entre les États ibéro-américains et au-delà de leurs frontières, afin de contribuer à la croissance économique et sociale de la région.

- Favoriser la coopération internationale entre les autorités de contrôle des États ibéro-américains avec d'autres autorités de contrôle non régionales et les autorités et agences internationales en la matière.

Comme antécédents directs de ces Normes on peut citer, d'une part, l'adoption par le RIPD lui-même, en 2007, des « Lignes directrices pour l'harmonisation de la protection des données dans la Communauté ibéro-américaine » à l'occasion de la Ve Rencontre ibéro-américaine pour la protection des données, visant à établir un « cadre harmonisé » de référence pour les initiatives réglementaires nationales émergentes dans la région en matière de protection des données. Et, d'autre part, les normes qui ont été approuvées à la Conférence internationale des autorités chargées de la protection des données et de la vie privée, tenue à Madrid en 2009, appelées les « Normes de Madrid », qui ont constitué une avance dans la recherche de solutions et dispositions spécifiques « qui pourraient être appliquées indépendamment des différences pouvant exister entre les diverses modèles existants de protection des données et de la vie privée ».

Dans l'élaboration des Normes ibéro-américaines, d'autres instruments internationaux et emblématiques sur la protection des données personnelles ont également été retenus comme référence, tels que les Lignes directrices pour la protection de la vie privée et la circulation transfrontalière des données à caractère personnel de l'Organisation de coopération et développement économique ; la Convention n° 108 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatique des données à caractère personnel et de son Protocole ; le Cadre de protection de la vie privée du Forum de coopération économique Asie-Pacifique et le Règlement du Parlement européen et du Conseil sur la protection des personnes physiques en ce qui concerne le traitement des données à caractère personnel et la libre circulation de ces données, entre autres.

L'itinéraire qui a été suivi pour leur élaboration comprend les étapes suivantes :

- Juin 2016 : à la XIVe Rencontre ibéro-américaine sur la protection des données, tenue le 8 juin 2016 à Santa Marta, en Colombie, il a été décidé l'élaboration des Normes ibéro-américaines par l'Institut national de la transparence, l'accès à l'information et la protection de données personnelles (INAI), à ce moment en sa qualité de président du Réseau.

- Novembre 2016: lors du Séminaire du RIPD au Centre de coopération espagnole à Montevideo, tenu les 8 et 9 novembre à Montevideo, en Uruguay, l'INAI a produit aux membres présents du Réseau l'avant-projet de Normes ibéro-américaines. Dans ce séminaire, il a été convenu qu'au cours du mois de décembre 2016, l'avant-projet de Normes ibéro-américaines serait ouvert aux commentaires et aux observations des membres du Réseau.

- Mai 2017 : dans l'atelier du RIPD au Centre de Coopération espagnole à Cartagena de Indias, la version des Normes ibéro-américaines qui avait été le résultat de toutes les contributions reçues au cours du mois de décembre 2016 a été étudiée et débattue du point de vue technique. Les autorités membres du RIPD et une représentation du Contrôleur européen de la protection des données et de l'Organisation des États américains ont participé à cet atelier, ainsi que l'Unité des flux internationaux de la Commission européenne, par vidéoconférence.

- Juin 2017 : lors de la XVe Rencontre ibéro-américaine de protection des données, tenue du 20 au 22 juin 2017 à Santiago du Chili, la version découlant du travail effectué au cours de l'atelier de Cartagena de Indias a été approuvée à l'unanimité lors de la séance à huis clos de la réunion, et elle a été proclamée formellement lors de la Séance Ouverte.

Grâce à l'approbation de ces Normes, le RIPD dispose d'un outil essentiel qui lui permet d'aborder de manière rigoureuse le suivi et le soutien des futurs développements législatifs dans la Région, étant donné que les Normes ibéro-américaines se caractérisent par un modèle normatif qui :

- Répond aux besoins et aux exigences nationaux et internationaux requis par le droit à la protection des données personnelles, dans une société où les technologies de l'information et du savoir deviennent de plus en plus importantes dans toutes les tâches de la vie quotidienne.

- Comprend les meilleures pratiques nationales et internationales en la matière.

- Propose une série de normes très flexibles qui facilitent leur adoption chez les États ibéro-américains, sans en rien contrevenir à leur droit interne, de telle sorte que ce document constitue une réalité vivante et viable dans la région ibéro-américaine au bénéfice du titulaire lui-même.

- Garantit un niveau adéquat de protection des données personnelles dans la région ibéro-américaine, dans le but de ne pas constituer des obstacles à la libre circulation de ces derniers dans les États ibéro-américains et, par conséquent, favoriser les activités commerciales entre la région, ainsi qu'avec d'autres régions économiques.

D'autre part, et non des moindres, les Normes ibéro-américaines permettront de renforcer le positionnement du Réseau sur la scène internationale. À cette fin, des initiatives seront lancées dans les différents forums internationaux (la Commission européenne, la Conférence internationale des autorités chargées de la protection des données et de la vie privée, l'Organisation des États américains, etc.), en essayant de trouver la diffusion la plus large possible.

En bref, le travail effectué par les entités qui composent le RIPD, qui a finalement conduit à l'adoption des Normes susmentionnées, constitue une expérience concrète de coopération qui, à notre avis, peut être très utile pour d'autres organisations. Elles sont, donc, disponibles pour toutes les entités et les professionnels qui en puissent bénéficier, afin d'assurer l'exercice et la défense, le plus efficacement possible, du droit à la protection des données dans la région ibéro-américaine et dans un contexte international.

Les États ibéro-américains :

(1) Considérant que la protection des personnes physiques par rapport au traitement de leurs données personnelles est un droit fondamental qui est reconnu au maximum dans la plupart des Constitutions politiques des États ibéro-américains sous la forme du droit à la protection des données personnelles ou habeas data, et que dans certains cas elle a été définie du point de vue de la jurisprudence par leurs tribunaux ou juridictions constitutionnelles ;

(2) Déterminant que le droit à la protection des données personnelles a été conceptualisé dans certains pays ibéro-américains, du point de vue législatif ou de la jurisprudence, comme un droit de nature différente aux droits à la vie privée et familiale, à l'intimité, à l'honneur, au bon nom et d'autres droits similaires qui, dans l'ensemble, garantissent le libre développement de la personnalité de la personne physique pour donner forme à un droit autonome, avec ses propres caractéristiques et dynamiques, dont le but est de sauvegarder le pouvoir de disposition et de contrôle que chaque personne physique a par rapport aux informations lui concernent, notamment quant à l'utilisation des technologies de l'information et des communications qui sont de plus en plus importantes dans toutes les tâches de la vie quotidienne ;

(3) Admettant que la sauvegarde du droit des personnes physiques à l'égard du traitement de leurs données personnelles est compatible avec l'objectif de garantir et de protéger d'autres droits reconnus comme indivisibles et interdépendants entre eux et qui nécessitent une protection appropriée pour préserver les personnes physiques contre les intrusions illégales ou arbitraires, y compris celles dérivées du traitement des données personnelles. Ce qui précède n'empêche pas que le droit à la protection des données personnelles soit applicable aux personnes morales conformément au droit interne des États ibéro-américains ;

(4) Rappelant que le Réseau ibéro-américain de protection des données a été créé à la suite de l'accord conclu lors de la Rencontre ibéro-américaine de protection des données tenue à La Antigua, au Guatemala, du 1er au 6 juin 2003, avec la présence de représentants de 14 pays ibéro-américains. Cette initiative a eu un soutien politique dès le départ, comme en témoignent la Déclaration finale du XIIIe Sommet des chefs d'État et de gouvernement des pays ibéro-américains, tenue à Santa Cruz de la Sierra, en Bolivie, les 14 et 15 novembre 2003, conscients de la nature de la protection des données personnelles en tant que droit fondamental ;

(5) Ayant à l'esprit que, à l'occasion de la Résolution adoptée lors du XXVème Sommet ibéro-américain des chefs d'État et de gouvernement tenue à Cartagena de Indias (Colombie) les 28 et 29 octobre 2016, il a été réaffirmé que l'adoption, l'élaboration et la promotion de divers manuels, programmes, initiatives et projets renforceraient la gestion et l'impact des actions de coopération entre les pays ibéro-américains ;

(6) Admettant que le Réseau ibéro-américain de protection des données constitue un forum permanent pour l'échange d'informations ouvert à tous les pays membres de la Communauté ibéro-américaine et qui permet l'implication des secteurs public, privé et social dans le but de promouvoir les développements normatifs nécessaires pour assurer une réglementation avancée du droit à la protection des données personnelles dans un contexte démocratique et mondial ;

(7) Rappelant que, à l'occasion de la réunion tenue à Santa Cruz de la Sierra, en Bolivie, du 3 au 5 mai 2006, le document intitulé Lignes directrices pour l'harmonisation de la protection des données dans la Communauté ibéro-américaine a été établi, et que ce document contient des dispositions qui visent à contribuer à l'élaboration des initiatives réglementaires de protection des données qui apparaissent dans la Communauté ibéro-américaine, se constituant comme référence pour l'élaboration de ces Normes ;

(8) Compte tenu du fait que l'Union européenne a adopté un nouveau cadre réglementaire en la matière dans le but de moderniser ses dispositions et d'assurer une plus grande solidité et cohérence dans la protection efficace du droit fondamental à la protection des données à caractère personnel dans l'Union européenne, et dans le but de générer de la confiance dans la société en général et, à son tour, de faciliter le développement de l'économie numérique, tant sur son marché intérieur que dans ses relations à l'échelle mondiale ; ce cadre normatif se positionne comme une référence obligatoire et déterminante pour l'élaboration des législations nationales de protection des données dans les pays ibéro-américains ;

(9) Reconnaissant qu'il y a un manque d'harmonisation dans les États ibéro-américains concernant la reconnaissance, l'adoption, la définition et le développement des figures, des principes, des droits et des procédures qui donnent du contenu au droit à la protection des données personnelles dans leurs législations nationales, ce qui, sans aucun doute, rend difficile, actuellement, de faire face aux nouveaux défis, pour la protection de ce droit, dérivés de l'évolution technologique constante et vertigineuse et de la mondialisation dans divers domaines ;

(10) Étant impératif, dans le contexte de l'innovation technologique constante, d'adopter des instruments réglementaires qui garantissent, d'une part, la protection

des personnes physiques par rapport au traitement de leurs données personnelles et, d'autre part, la libre circulation des données personnelles qui constituent actuellement la base du développement, du renforcement et de l'échange de biens et de services dans une économie mondiale et numérique, sur lesquelles reposent les économies des États ibéro-américains ;

(11) Convenant que, pour garantir un niveau élevé de protection des droits et des libertés des personnes physiques il faut, entre autres, un niveau uniforme et élevé de protection des personnes physiques en ce qui concerne leurs informations personnelles, qui réponde aux besoins et aux demandes actuels dans un contexte global, afin de ne pas entraver la libre circulation des données personnelles dans les États ibéro-américains et, par conséquent, favoriser les activités commerciales dans la région et avec les autres régions économiques ;

(12) Acceptant que, dans le but d'élargir et renforcer le régime de protection des personnes physiques en ce qui concerne le traitement de leurs données personnelles, il est impératif d'établir un équilibre entre les intérêts de tous les acteurs du secteur public, privé et social et les parties prenantes impliquées, y compris l'établissement d'exceptions pour des questions d'intérêt public qui soient raisonnables et compatibles avec les droits et les libertés, pour éviter de tomber dans des restrictions ou limitations injustifiées ou disproportionnées qui ne soient pas conformes aux objectifs poursuivis dans les sociétés démocratiques ;

(13) Conscients des risques potentiels qui peuvent survenir dans le domaine des personnes physiques dans le cadre du traitement de leurs données personnelles à grande échelle par des organismes publics et privés et, notamment, en tenant compte de la vulnérabilité particulière des enfants et les adolescents, qui demandent des garanties appropriées et suffisantes de protection contre l'utilisation abusive ou arbitraire de leurs informations personnelles, préservant ainsi leur intérêt supérieur, le libre développement de leur personnalité, leur sécurité et d'autres valeurs qui font l'objet d'un maximum de protection par les États ibéro-américains ;

(14) Acceptant que le développement technologique facilite le traitement de nouvelles catégories de données personnelles qui présentent des risques spécifiques, en particulier leur utilisation inappropriée, il est très pertinent de parvenir à un consensus minimum concernant les catégories de données personnelles considérées comme sensibles ou particulièrement protégées, ainsi que les règles pour leur traitement, en tenant compte du fait que les conséquences négatives et les interférences qui peuvent résulter de l'utilisation abusive de ce type de données personnelles peut engendrer des conditions injustes ou discriminatoires pour les personnes physiques ;

(15) Admettant que pas tous les États ibéro-américains ne disposent d'une législation en la matière, une situation qui peut entraîner des affectations dans la sauvegarde et le traitement des informations personnelles, compte tenu de l'utilisation accélérée des technologies de l'information qui facilitent et permettent une communication massive de données personnelles de façon immédiate et presque illimitée ;

(16) Établissant que la législation sur la protection des données personnelles des États ibéro-américains doit adopter les modèles contenus dans ces Normes pour disposer d'un cadre réglementaire harmonisé qui offre un niveau de protection aux personnes physiques en ce qui concerne le traitement de leurs données personnelles et, à son tour, garantissant le développement commercial et économique de la région ;

(17) Reconnaissant qu'à l'heure actuelle, les bases légales qui authentifient un organisme public ou privé pour traiter les données personnelles qu'ils possèdent sont le consentement du titulaire, le respect d'une disposition légale, la conformité à une décision judiciaire, à une résolution ou à un mandat fondé et motivé d'une autorité publique compétente, l'exercice de pouvoirs propres aux autorités publiques, la reconnaissance ou la défense des droits du titulaire devant une autorité publique compétente, l'exécution d'un contrat ou d'un précontrat dans lequel le titulaire est partie, le respect d'une obligation légale applicable au responsable, la protection des intérêts essentiels du titulaire ou d'une autre personne physique, l'intérêt légitime de l'organisation publique ou privée, ou des raisons d'intérêt public ;

(18) Soulignant la nécessité pour les États ibéro-américains de traiter les données personnelles selon les mêmes normes et des règles homogènes qui offrent aux titulaires les mêmes garanties de protection, par l'établissement d'un catalogue de principes d'application obligatoire répondant aux normes nationales et internationales actuelles en la matière, ainsi qu'aux exigences demandées par un exercice effectif et le respect de ce droit fondamental ;

(19) Reconnaissant que, dans le but de garantir efficacement le droit à la protection des données personnelles, il est nécessaire d'adopter un cadre réglementaire qui reconnaisse à toute personne physique, en tant que titulaire de ses données personnelles, la possibilité d'exercer, en règle générale sans frais et exceptionnellement avec les coûts associés pour des raisons naturelles de reproduction, d'envoi, de certification ou autre, les droits d'accès, de rectification, de suppression, d'opposition et à la portabilité, même dans le cadre du traitement des données personnelles effectué par des moteurs Internet ou des moteurs de recherche, des droits qui complètent les conditions nécessaires pour que les titulaires exercent pleinement leur droit à l'autodétermination informative ;

(20) Soulignant l'importance et le rôle fondamental joué par les fournisseurs de services qui traitent les données personnelles au nom et pour le compte du responsable, y compris ceux qui fournissent des services de cloud computing et d'autres questions, ce qui fait que les États ibéro-américains adoptent, dans un monde globalisé, un régime qui leur permette de réglementer ce type de services afin d'établir une série de garanties pour la protection des données personnelles qu'en raison de leur mission ils possèdent et traitent, sans exonérer le responsable des obligations et responsabilités devant les titulaires et les autorités de contrôle ;

(21) Considérant que le développement des nouvelles technologies de l'information et des communications, ainsi que les services développés dans le contexte de l'économie numérique contribuent à la croissance continue des flux transfrontaliers de données personnelles au sein d'une société mondiale, l'obligation d'établir une base minimale pour faciliter et permettre aux responsables et préposés, en tant qu'exportateurs, de procéder à des transferts internationaux de données à caractère personnel dans le plein respect des droits des titulaires devient incontournable ;

(22) Compte tenu du fait que via Internet il est possible d'accéder et de recueillir des informations disponibles dans n'importe quel pays, ainsi que d'effectuer un traitement de ces informations, comme la collecte de données provenant de millions de personnes sans y être domicilié physiquement, une circonstance qui ne devrait pas être un facteur qui empêche une protection efficace des droits et libertés des individus dans le cyberespace ;

(23) Reconnaissant l'importance de prendre des mesures préventives pour permettre au responsable de répondre de manière proactive aux éventuels problèmes liés au droit à la protection des données personnelles, telles que l'adoption de schémas d'autorégulation contraignants ou de systèmes de certification en la matière, la désignation d'un agent de protection des données personnelles, l'élaboration d'évaluations d'impact sur la protection des données personnelles et la vie privée par défaut et par conception, entre autres, ce qui est essentiel dans le domaine des technologies de l'information et des télécommunications ;

(24) Admettant la nécessité impérieuse de chaque État ibéro-américain d'avoir une autorité de contrôle indépendante et impartiale dans ses attributions dont les décisions ne puissent faire l'objet d'un recours que par un contrôle judiciaire, indépendant de toute influence extérieure, avec des pouvoirs de surveillance et de recherche sur la protection des données personnelles et responsable de contrôler le respect de la législation nationale en la matière, qui soit dotée de ressources humaines et matérielles suffisantes pour assurer l'exercice de ses pouvoirs et l'efficacité de ses fonctions;

(25) Reconnaissant que les États ibéro-américains sont tenus d'adopter un régime qui garantisse aux titulaires une série de mécanismes et de procédures pour adresser leurs réclamations à l'autorité de contrôle lorsqu'ils considèrent que leurs droits à la protection des données personnelles ont été violés, ainsi que pour être indemnisés lorsqu'ils ont subi des dommages et intérêts en raison d'une violation de leur droit ;

(26) Soulignant l'importance d'établir une base minimale pour la coopération internationale entre les autorités de contrôle latino-américaines et, entre celles-ci et celles des pays tiers, afin de favoriser et faciliter la mise en œuvre de la législation en la matière et une protection efficace des titulaires ;

Ils ont convenu d'adopter ces Normes comme une priorité absolue dans la Communauté ibéro-américaine afin que, en tant que lignes directrices, elles contribuent à la mise en place d'initiatives réglementaires pour la protection des données personnelles dans la région des pays qui n'ont pas encore de telles réglementations ou, le cas échéant, qu'elles puissent servir de guide pour moderniser et mettre à jour la législation en vigueur, favorisant l'adoption d'un cadre réglementaire harmonisé qui offre un niveau adéquat de protection des personnes physiques en ce qui concerne le traitement de leurs données personnelles et, à leur tour, garantir le développement commercial et économique de la région, selon ce qui suit :

Chapitre I

Dispositions générales

1. Objet

1.1 Ces Normes ont pour objet de :

a. Établir un ensemble de principes et de droits pour la protection des données personnelles que les États ibéro-américains puissent adopter et développer dans leur législation nationale, dans le but de garantir le traitement adéquat des données personnelles et d'avoir des règles homogènes dans la région.

b. Augmenter le niveau de protection des personnes physiques en ce qui concerne le traitement de leurs données personnelles, ainsi qu'entre les États ibéro-américains, qui réponde aux besoins et aux exigences internationaux que le droit à la protection des données personnelles demande dans une société dans laquelle les technologies de l'information et du savoir sont de plus en plus importantes dans toutes les tâches de la vie quotidienne.

c. Garantir l'exercice effectif et la défense du droit à la protection des données personnelles de toute personne physique dans les États ibéro-américains, en établissant des règles communes qui garantissent le traitement adéquat de ses données personnelles.

d. Faciliter le flux de données personnelles entre les États ibéro-américains et au-delà de leurs frontières, afin de contribuer à la croissance sociale et économique de la région.

e. Promouvoir le développement de mécanismes de coopération internationale entre les autorités de contrôle des États ibéro-américains, les autorités de contrôle non régionales et les autorités et entités internationales en la matière.

2. Définitions

2.1. Aux fins des présentes Normes, il faut entendre par :

a. **Anonymisation** : l'application de mesures de quelque nature que ce soit visant à empêcher l'identification ou la ré-identification d'une personne physique sans efforts disproportionnés.

b. **Consentement** : manifestation de la volonté, libre, spécifique, sans équivoque et informée du titulaire par laquelle il accepte et autorise le traitement des données personnelles le concernant.

c. **Données personnelles** : toute information concernant une personne physique identifiée ou identifiable, exprimée sous forme numérique, alphabétique, graphique, photographique, alphanumérique, acoustique ou autre. Une personne est considérée comme identifiable lorsque son identité peut être déterminée directement ou indirectement, dans la mesure où cela ne nécessite pas de délais ou d'activités disproportionnées.

d. **Données personnelles sensibles** : celles qui concernent la sphère intime du titulaire ou dont l'utilisation inappropriée peut donner lieu à une discrimination ou entraîner un risque grave pour le titulaire. De manière énonciative, les données personnelles considérées comme sensibles sont celles qui puissent révéler des aspects tels que l'origine raciale ou ethnique, des croyances ou convictions religieuses, philosophiques et morales, l'affiliation syndicale, des opinions politiques, des données relatives à la santé, à la vie, à la préférence ou à l'orientation sexuelle, des données génétiques ou des données biométriques visant à identifier de façon univoque une personne physique.

e. **Préposé** : un fournisseur de services qui, au titre de personne physique ou morale ou autorité publique, étrangère à l'organisation du responsable, traite des données personnelles au nom et pour le compte de ce dernier.

f. **Exportateur** : une personne physique ou morale de nature privée, une autorité publique, des services, un organisme ou un fournisseur de services situé sur le territoire d'un État qui effectue des transferts internationaux de données à caractère personnel, conformément aux dispositions des présentes Normes.

g. **Responsable**: une personne physique ou morale de nature privée, une autorité publique, des services ou un organisme qui, seul ou conjointement avec d'autres, détermine les objectifs, les moyens, la portée et d'autres questions liées au traitement des données personnelles.

h. **Titulaire** : une personne physique concernée par les données personnelles.

i. **Traitement** : toute opération ou ensemble d'opérations effectuées au moyen de procédures physiques ou automatisées accomplies sur des données personnelles, liées, sans limitation, à l'obtention, l'accès, l'enregistrement, l'organisation, la structuration, l'adaptation, l'indexation, la modification, l'extraction, la consultation, le stockage, la conservation, l'élaboration, le transfert, la diffusion, la possession, l'exploitation et, en général, toute utilisation ou disposition de données personnelles.

3. Champ d'application subjectif

3.1. Ces Normes seront applicables aux personnes physiques ou morales privées, aux autorités et aux organismes publics qui traitent des données personnelles dans l'exercice de leurs activités et fonctions.

4. Champ d'application objectif

4.1. Ces Normes seront applicables au traitement des données personnelles sur des supports physiques, totalement ou partiellement automatisés, ou sur les deux supports, quelle que soit la forme ou la modalité de leur création, le type de support, le traitement, le stockage et l'organisation.

4.2. En règle générale, ces Normes seront applicables aux données personnelles des personnes physiques, ce qui n'empêche pas que les États ibéro-américains, dans leur législation nationale, disposent que les informations des personnes morales soient protégées en accord avec le droit à la protection des données personnelles, conformément aux dispositions de leur droit interne.

4.3. Les Normes ne seront pas applicables dans les cas suivants :

a. Lorsque les données personnelles seront destinées à des activités exclusivement dans le cadre de la vie familiale ou domestique d'une personne physique, c'est-à-dire, l'utilisation de données personnelles dans un environnement d'amitié, de parenté ou de groupe personnel proche et non destiné à être divulgué ou utilisé de façon commerciale.

b. Les informations anonymes, c'est-à-dire, les informations qui ne sont pas liées à une personne physique identifiée ou identifiable, ainsi que les données personnelles soumises à un processus d'anonymisation de telle sorte que le titulaire ne puisse pas être identifié ou ré-identifié.

4.4. La législation nationale des États ibéro-américains applicable en la matière pourra établir des catégories de données personnelles auxquelles le régime de protection prévu dans ces Normes ne sera pas applicable, conformément à leur droit interne.

5. Champ d'application territoriale

5.1. Les Normes seront applicables au traitement des données personnelles effectué :

a. Par un responsable ou préposé établi sur le territoire des États ibéro-américains.

b. Par un responsable ou préposé non établi sur le territoire des États ibéro-américains, lorsque les activités de traitement seront liées à l'offre de biens ou de services adressés aux résidents des États ibéro-américains, ou bien elles seront liées au contrôle de leur comportement dans la mesure où ce contrôle sera effectué dans les États ibéro-américains.

c. Par un responsable ou préposé qui ne soit pas établi dans un État ibéro-américain mais dont la législation nationale de cet État lui résulte applicable suite à la passation d'un contrat ou en vertu du droit international public.

d. Par un responsable ou préposé non établi sur le territoire des États ibéro-américains et qui utilise ou fasse appel à des moyens, automatisés ou non automatisés, situés sur ce territoire, pour traiter des données personnelles, à moins que ces moyens ne soient utilisés qu'à des fins de transit.

5.2. Aux fins de ces Normes, il faudra entendre par établissement le lieu de l'administration centrale ou principale du responsable ou du préposé qui devra être déterminé selon des critères objectifs et impliquer l'exercice effectif et réel des activités de gestion qui déterminent les décisions principales en ce qui concerne les fins et les moyens du traitement des données personnelles effectués, par des modalités stables.

5.3. La présence et l'utilisation de moyens techniques et de technologies pour le traitement des données personnelles ou des activités de traitement ne constitueront pas, en eux-mêmes, un établissement principal et ne seront pas considérés comme des critères déterminants pour la définition de l'établissement principal du responsable ou du préposé.

5.4. Lorsque le traitement des données personnelles sera effectué par un groupe d'entreprises, l'établissement principal de l'entreprise qui exerce le contrôle devra être considéré l'établissement principal du groupe d'entreprises, sauf lorsque les fins et les moyens du traitement seront effectivement déterminés par une autre des entreprises du groupe.

6. Exceptions générales au droit à la protection des données personnelles.

6.1. La législation nationale des États ibéro-américains applicable en la matière pourra limiter le droit à la protection des données afin de protéger la sécurité nationale, la sécurité publique, la protection de la santé publique, la protection des droits et des libertés de tiers, ainsi que pour des raisons d'intérêt public.

6.2. Les limitations et restrictions seront expressément reconnues en droit, afin de fournir suffisamment de certitudes aux titulaires sur la nature et la portée de la mesure.

6.3. Toute loi ayant pour objet de limiter le droit à la protection des données personnelles contiendra, au minimum, des dispositions relatives :

a. Au but du traitement.

b. Aux catégories de données personnelles en question.

c. À la portée des limitations établies.

d. Aux garanties appropriées pour empêcher l'accès ou les transferts illégaux ou disproportionnés.

e. À la détermination du responsable ou des responsables.

f. Aux délais de conservation des données personnelles.

g. Aux risques éventuels pour les droits et les libertés des titulaires.

h. Au droit des titulaires d'être informés de la limitation, à moins qu'elle soit nuisible ou incompatible aux fins de celle-ci.

6.4. Les lois seront les nécessaires, appropriées et proportionnelles dans une société démocratique, et devront respecter les droits et les libertés fondamentales des titulaires.

7. Pondération du droit à la protection des données personnelles.

7.1. Les États ibéro-américains pourront, dans leur droit interne, exempter le respect des principes et des droits énoncés dans ces Normes, uniquement dans la mesure où il sera nécessaire de concilier le droit à la protection des données personnelles avec d'autres droits et libertés fondamentaux.

7.2. Cette exemption devra requérir un exercice de pondération afin de déterminer la nécessité, l'adéquation et la proportionnalité de la restriction ou de l'exception selon les règles et critères établis par les États ibéro-américains dans leur droit interne.

8. Traitement des données personnelles des enfants et des adolescents

8.1. Dans le traitement des données personnelles concernant les enfants et les adolescents, les États ibéro-américains privilégieront la protection de leur intérêt supérieur, conformément à la Convention relative aux droits de l'enfant et à d'autres instruments internationaux qui visent leur bien-être et leur protection intégrale.

8.2. Les États ibéro-américains favoriseront l'utilisation responsable, adéquate et sûre des technologies de l'information et des communications et informeront les risques potentiels qu'ils rencontreront dans les environnements numériques concernant le traitement inadéquat de leurs données personnelles dans la formation scolaire des enfants et des adolescents, ainsi que le respect de leurs droits et libertés.

9. Traitement des données personnelles sensibles

9.1. En règle générale, le responsable ne pourra pas traiter des données personnelles sensibles, à moins que ce soit le cas de l'une des hypothèses suivantes :

a. Qu'elles soient strictement nécessaires pour l'exercice et le respect des attributions et des obligations expressément prévues dans les normes qui réglementent son activité.

b. Par mandat juridique.

c. Qu'il existe le consentement exprès par écrit du titulaire.

d. Qu'elles soient nécessaires pour des raisons de sécurité nationale, de sécurité publique, d'ordre public, de santé publique ou de protection des droits et libertés d'autrui.

9.2. La législation nationale des États ibéro-américains applicable en la matière pourra établir des exceptions, des garanties et des conditions supplémentaires pour assurer le traitement approprié des données personnelles sensibles, conformément à leur droit interne.

Chapitre II

Principes de protection des données personnelles

10. Principes applicables au traitement des données personnelles

10.1. Dans le traitement des données personnelles, le responsable devra respecter les principes de légitimation, de légalité, de fidélité, de transparence, de finalité, de proportionnalité, de qualité, de responsabilité, de sécurité et de confidentialité.

11. Principe de légitimation

11.1. En règle générale, le responsable ne pourra traiter les données personnelles que lorsque l'une des circonstances suivantes se produit :

a. Le titulaire donne son consentement pour un ou plusieurs objectifs spécifiques.

b. Le traitement est nécessaire pour l'exécution d'un ordre judiciaire, une résolution ou un mandat fondé et motivé par une autorité publique compétente.

c. Le traitement est nécessaire pour l'exercice de pouvoirs propres aux autorités publiques ou s'effectue en vertu d'une autorisation légale.

d. Le traitement est nécessaire pour la reconnaissance ou la défense des droits du titulaire devant une autorité publique.

e. Le traitement est nécessaire pour l'exécution d'un contrat ou d'un précontrat dans lequel le titulaire est partie.

f. Le traitement est nécessaire pour l'exécution d'une obligation légale applicable au responsable.

g. Le traitement est nécessaire pour protéger les intérêts vitaux du titulaire ou d'une autre personne physique.

h. Le traitement est nécessaire pour des raisons d'intérêt public établies ou prévues par la loi.

i. Le traitement est nécessaire pour répondre aux intérêts légitimes poursuivis par le responsable ou par un tiers, à condition que sur ces intérêts ne prévalent pas les intérêts ou les droits et libertés fondamentaux du titulaire qui nécessite la protection des données personnelles, notamment lorsque le titulaire est un enfant ou un adolescent. Ce qui précède ne sera pas applicable au traitement des données personnelles par les autorités publiques dans l'exercice de leurs fonctions.

11.2. Dans le cas de ce dernier paragraphe, le traitement des données personnelles de contact qui s'avère essentiel pour la localisation des personnes physiques qui rendent leurs services au responsable sera entendu protégé par l'intérêt légitime, afin de maintenir tout type de relation avec ce dernier.

12. Conditions pour le consentement

12.1. Lorsqu'il sera nécessaire d'obtenir le consentement du titulaire, le responsable devra démontrer de façon certaine que le titulaire a donné son consentement, soit par une déclaration, soit par une action affirmative claire.

12.2. Le titulaire pourra révoquer à tout moment le consentement pour le traitement des données personnelles lorsqu'il lui sera requis ; pour ce faire, le responsable établira des mécanismes simples, agiles, efficaces et gratuits.

13. Consentement pour le traitement des données personnelles des enfants et des adolescents

13.1. En obtenant le consentement des enfants et des adolescents, le responsable obtiendra l'autorisation du titulaire de l'autorité parentale ou de la tutelle, conformément aux règles de représentation prévues par le droit interne des États ibéro-américains ou, le cas échéant, demandera directement l'autorisation du mineur si le droit interne de chaque État ibéro-américain a établi un âge minimum pour qu'il puisse l'accorder directement et sans aucune représentation du titulaire de l'autorité parentale ou de la tutelle.

13.2. Le responsable fera des efforts raisonnables pour vérifier que le consentement a été accordé par le titulaire de l'autorité parentale ou la tutelle, ou par le mineur, selon son âge, conformément au droit interne de chaque État ibéro-américain, en tenant compte de la technologie disponible.

14. Principe de légalité

14.1. Le responsable traitera les données personnelles en sa possession avec un attachement et respect stricts des dispositions du droit interne de l'Etat ibéro-américain applicable, du droit international et des droits et libertés des personnes.

14.2. Le traitement des données personnelles effectué par les autorités publiques sera soumis aux pouvoirs ou aux attributions accordés expressément par le droit interne de l'Etat ibéro-américain en question, en plus des dispositions du paragraphe précédent des présentes Normes.

15. Principe de fidélité

15.1. La personne responsable traitera les données personnelles en sa possession privilégiant la protection des intérêts du titulaire et s'abstenant de les traiter par des moyens trompeurs ou frauduleux.

15.2. Aux fins des présentes Normes, les traitements des données personnelles qui entraînent une discrimination injuste ou arbitraire à l'encontre des titulaires seront considérés comme déloyaux.

16. Principe de transparence

16.1. Le responsable informera le titulaire de l'existence et des caractéristiques principales du traitement auquel ses données personnelles seront soumises afin qu'il puisse prendre des décisions éclairées à cet égard.

16.2. Le responsable fournira au titulaire, au moins, les informations suivantes :

a. Son identité et ses coordonnées.

b. Les objectifs du traitement auquel ses données personnelles seront soumises.

c. Les communications, nationales ou internationales, de données personnelles qu'il compte effectuer, y compris les destinataires et les objectifs qui motivent leur réalisation.

d. L'existence, la forme et les mécanismes ou les procédures par lesquels il pourra exercer les droits d'accès, de rectification, de suppression, d'opposition et à la portabilité.

e. Le cas échéant, l'origine des données personnelles si le responsable ne les a pas obtenues directement du propriétaire.

16.3. Les informations fournies au titulaire devront être suffisantes et facilement accessibles, ainsi que rédigées et structurées dans un langage clair, simple et facile à comprendre pour les titulaires auxquelles elles sont adressées, en particulier s'il s'agit d'enfants et d'adolescents.

16.4. Tous les responsables auront des politiques transparentes pour le traitement des données personnelles qu'ils effectueront.

17. Principe de finalité

17.1. Tout traitement des données personnelles se limitera à la réalisation de finalités spécifiques, explicites et légitimes.

17.2. Le responsable ne pourra pas traiter les données personnelles en sa possession à d'autres fins que celles qui ont motivé leur traitement original, à moins que l'une quelconque des causes permettant un nouveau traitement de données selon le principe de légitimation ne se produise.

17.3. Le traitement ultérieur des données personnelles à des fins d'archivage, de recherche scientifique et historique ou à des fins statistiques, dans l'intérêt public, ne sera pas considéré comme incompatible avec les finalités initiales.

18. Principe de proportionnalité

18.1 Le responsable ne traitera que les données personnelles qui s'avèrent adéquates, pertinentes et limitées au minimum nécessaire par rapport aux finalités qui justifient leur traitement.

19. Principe de qualité

19.1. Le responsable prendra les mesures nécessaires pour que les données personnelles en sa possession demeurent identiques, complètes et à jour, de sorte que leur véracité ne soit pas modifiée pour la réalisation des fin qui ont motivé leur traitement.

19.2. Lorsque les données personnelles ont cessé d'être nécessaires pour remplir les fins qui ont motivé leur traitement, le responsable les supprimera ou les éliminera de ses fichiers, registres, bases de données, dossiers ou systèmes d'information ou, le cas échéant, les soumettra à une procédure d'anonymisation.

19.3. Dans l'élimination des données personnelles, le responsable mettra en œuvre des méthodes et des techniques visant à éliminer de façon définitive et sûre ces données.

19.4. Les données personnelles ne seront conservées que pour le temps nécessaire pour remplir les fins qui justifient leur traitement ou celles liées aux exigences légales applicables au responsable. Toutefois, la législation nationale des États ibéro-américains applicable en la matière pourra établir des exceptions concernant la durée de conservation des données personnelles, dans le plein respect des droits et garanties du titulaire.

20. Principe de responsabilité

20.1. Le responsable mettra en œuvre les mécanismes nécessaires pour prouver le respect des principes et obligations établis dans ces Normes, ainsi que pour rendre des comptes sur le traitement des données personnelles en sa possession au titulaire et à l'autorité de contrôle ; pour ce faire, il pourra utiliser des normes, les meilleures pratiques nationales ou internationales, des schémas d'autorégulation, des systèmes de certification ou tout autre mécanisme qu'il juge approprié à ces fins.

20.2. Ce qui précède s'appliquera lorsque les données personnelles seront traitées par une personne au nom du responsable, ainsi qu'au moment d'effectuer des transferts de données personnelles.

20.3. Le responsable pourra adopter les mécanismes suivants, parmi d'autres, pour respecter le principe de responsabilité :

a. Consacrer des ressources pour la mise en œuvre de programmes et de politiques pour la protection des données personnelles.

b. Mettre en place des systèmes de gestion des risques liés au traitement des données personnelles.

c. Élaborer des politiques et des programmes pour la protection des données personnelles obligatoires et exigibles dans l'organisation du responsable.

d. Mettre en œuvre un programme de formation et de mise à jour du personnel sur les obligations relatives à la protection des données personnelles.

e. Examiner périodiquement les politiques et les programmes de sécurité des données personnelles pour déterminer les modifications nécessaires.

f. Établir un système de contrôle et de surveillance interne et/ou externe, y compris des audits, pour vérifier le respect des politiques de protection des données personnelles.

g. Établir des procédures pour répondre aux questions et aux plaintes des titulaires.

20.4. Le responsable examinera et évaluera à tout moment les mécanismes qu'il adoptera de façon volontaire pour respecter le principe de responsabilité, afin de mesurer son niveau d'efficacité quant au respect de la législation nationale applicable.

21. Principe de sécurité

21.1. Le responsable établira et maintiendra, indépendamment du type de traitement effectué, des mesures administratives, physiques et techniques suffisantes pour garantir la confidentialité, l'intégrité et la disponibilité des données personnelles.

21.2. Pour la détermination des mesures visées au paragraphe précédent, le responsable tiendra compte des facteurs suivants :

a. Le risque pour les droits et les libertés des titulaires, en particulier, pour la valeur quantitative et qualitative potentielle que les données personnelles traitées pourraient avoir pour une tierce personne non autorisée à les avoir.

b. L'état de l'art.

c. Les coûts de la mise en œuvre.

d. La nature des données personnelles traitées, en particulier s'il s'agit de données personnelles sensibles.

e. La portée, le contexte et les fins du traitement.

f. Les transferts internationaux de données personnelles exécutés ou destinés à être exécutés.

g. Le nombre de titulaires.

h. Les conséquences possibles qui résulteraient d'une violation des droits pour les titulaires.

i. Les violations antérieures qui ont eu lieu lors du traitement des données personnelles.

21.3. Le responsable mènera régulièrement une série d'actions visant à assurer l'établissement, la mise en œuvre, l'opération, le suivi, l'examen, le maintien et l'amélioration continue des mesures de sécurité applicables au traitement des données personnelles.

22. Notification des violations de la sécurité des données personnelles

22.1. Lorsque le responsable prendra connaissance qu'une violation de la sécurité des données personnelles s'est produite à n'importe quel stade du traitement, considérée comme tout dommage, perte, altération, destruction, accès et, en général, toute utilisation illégale ou non autorisée de données personnelles, même si cela se produit de manière accidentelle, il informera immédiatement l'autorité de contrôle et les titulaires concernés de l'incident.

22.2. Ce qui précède ne sera pas applicable si le responsable peut démontrer, conformément au principe de la responsabilité proactive, l'improbabilité de la violation de la sécurité qui s'est produite ou qu'elle ne représente pas un risque pour les droits et les libertés des titulaires concernés.

22.3. La notification faite par le responsable aux titulaires concernés sera rédigée dans un langage clair et simple.

22.4. La notification visée aux paragraphes précédents contiendra, au moins, les informations suivantes :

a. La nature de l'incident.

b. Les données personnelles mises en danger.

c. Les mesures correctives prises immédiatement.

d. Les recommandations au titulaire sur les mesures qu'il peut prendre pour protéger ses intérêts.

e. Les moyens disponibles pour le titulaire pour obtenir plus d'informations.

22.5. Le responsable documentera toute violation de la sécurité des données personnelles survenue dans n'importe quelle phase du traitement et identifiera, parmi d'autres, la date à laquelle elle s'est produite, le motif de la violation, les faits qui y sont liés et ses effets, et les mesures correctives mises en œuvre immédiatement et définitivement, ce qui sera à la disposition de l'autorité de contrôle.

22.6. La législation nationale des États ibéro-américains applicable en la matière établira les effets des notifications de violations de sécurité que le responsable présentera à l'autorité de contrôle en ce qui concerne les procédures, la forme et les conditions de son intervention dans le but de protéger les intérêts, les droits et les libertés des titulaires concernés.

23. Principe de confidentialité

23.1. Le responsable établira des contrôles ou des mécanismes pour que ceux qui participeront à une phase quelconque du traitement des données personnelles maintiennent et respectent leur confidentialité, une obligation qui subsistera même après la fin de sa relation avec le titulaire.

Chapitre III

Droits du titulaire

24. Droits ARCO

24.1. En tout moment, le titulaire ou son représentant pourront demander au responsable l'accès, la rectification, la suppression, l'opposition et la portabilité des données personnelles qui lui concernent.

24.2. L'exercice de l'un des droits visés au paragraphe précédent n'est pas une condition préalable, ni n'empêche l'exercice d'un autre.

25. Droit d'accès

25.1. Le titulaire aura le droit de demander l'accès à ses données personnelles détenues par le responsable, ainsi que de connaître toute information relative aux conditions générales et spécifiques de son traitement.

26. Droit de rectification

26.1. Le titulaire aura le droit d'obtenir du responsable la rectification ou la correction de ses données personnelles, lorsque celles-ci seront inexactes, incomplètes ou pas à jour.

27. Droit de suppression

27.1. Le titulaire aura le droit de demander la suppression ou l'élimination de ses données personnelles des fichiers, des registres, des dossiers et des systèmes du responsable, afin qu'elles ne soient plus en sa possession et qu'il ne les traite plus.

28. Droit d'opposition

28.1. Le titulaire pourra s'opposer au traitement de ses données personnelles dans les cas suivants :

a. S'il a une raison légitime découlant de sa situation particulière.

b. Si le traitement de ses données personnelles est destiné au marketing direct, y compris l'établissement de profils, dans la mesure où il soit lié à une telle activité.

28.2 Dans le cas du paragraphe précédent, si le titulaire s'oppose au traitement à des fins de marketing direct, ses données personnelles ne seront plus traitées à ces fins.

29. Droit à ne pas faire l'objet de décisions individuelles automatisées

29.1. Le titulaire aura le droit à ne pas faire l'objet de décisions lui produisant des effets juridiques ou l'affectant de manière significative fondées uniquement sur des traitements automatisés conçus pour évaluer, sans intervention humaine, certains de ses aspects personnels ou analyser ou prédire en particulier sa performance professionnelle, son statut économique, son état de santé, ses préférences sexuelles, sa fiabilité ou son comportement.

29.2. Les dispositions du paragraphe précédent ne seront pas applicables si le traitement automatisé des données personnelles est nécessaire pour la passation ou l'exécution d'un contrat entre le titulaire et le responsable, s'il est autorisé par le droit interne des États ibéro-américains ou s'il est fondé sur le consentement démontrable du titulaire.

29.3. Toutefois, lorsqu'il sera nécessaire pour la relation contractuelle ou si le titulaire a exprimé son consentement, il aura le droit d'obtenir l'intervention humaine, recevoir une explication sur la décision prise, exprimer son point de vue et contester la décision.

29.4. Le responsable ne pourra pas faire des traitements automatisés des données personnelles ayant pour effet de discriminer les titulaires par leur origine raciale ou ethnique, leurs croyances ou convictions religieuses, philosophiques et morales, leur affiliation syndicale, leurs opinions politiques, des données relatives à la santé, à la vie, à la préférence ou à l'orientation sexuelle, ainsi que des données génétiques ou des données biométriques.

30. Droit à la portabilité des données personnelles

30.1. Lorsque les données personnelles seront traitées par voie électronique ou par des moyens automatisés, le titulaire aura le droit d'obtenir une copie des données personnelles qu'il aurait fournies au responsable ou qui feraient l'objet de traitement, dans un format électronique structuré, d'usage courant et de lecture mécanique, qui lui permette de continuer à les utiliser et les transférer à un autre responsable, si nécessaire.

30.2. Le titulaire pourra demander que ses données personnelles soient transférées directement de responsable à responsable lorsque cela sera techniquement possible.

30.3. Le droit à la portabilité des données personnelles ne nuira pas aux droits et libertés d'autrui.

30.4. Sous réserve d'autres droits du titulaire, le droit à la portabilité des données personnelles ne sera pas approprié lorsqu'il s'agit d'informations déduites, dérivées, créées, générées ou obtenues à partir de l'analyse ou du traitement effectué par le responsable en fonction de données personnelles fournies par le titulaire, comme c'est le cas des données personnelles qui auraient été soumis à un processus de personnalisation, de recommandation, de catégorisation ou de création de profils.

31. Droit à la limitation du traitement des données personnelles

31.1. Le titulaire aura droit à ce que le traitement de données personnelles soit limité au stockage pendant la période entre une demande de rectification ou d'opposition jusqu'à sa résolution par le responsable.

31.2. Le titulaire aura droit à la limitation du traitement de ses données personnelles lorsqu'ils ne seront pas nécessaires pour le responsable, mais il en aura besoin pour faire une réclamation.

32. Exercice des droits ARCO et à la portabilité

32.1. Le responsable établira des moyens et des procédures simples, rapides, accessibles et gratuites qui permettent au titulaire d'exercer ses droits d'accès, de rectification, de suppression, d'opposition et à la portabilité.

32.2. La législation nationale des États ibéro-américains applicable en la matière établira les exigences, les délais, les termes et les conditions dans lesquels les titulaires pourront exercer leurs droits d'accès, de rectification, de suppression, d'opposition et à la portabilité, ainsi que les motifs d'irrecevabilité pour les exercer, tels que, parmi d'autres :

a. Lorsque le traitement sera nécessaire pour la réalisation d'un objectif important d'intérêt public.

b. Lorsque le traitement sera nécessaire pour l'exercice des fonctions propres aux autorités publiques.

c. Lorsque le responsable prouvera avoir des raisons légitimes pour faire prévaloir le traitement sur les intérêts, les droits et les libertés du titulaire.

d. Lorsque le traitement sera nécessaire pour le respect d'une disposition légale.

e. Lorsque les données personnelles seront nécessaires pour le maintien ou l'exécution d'une relation juridique ou contractuelle.

32.3. La législation nationale des États ibéro-américains applicable en la matière pourra reconnaître que les personnes physiques liées à des personnes décédées ou désignées par celles-ci exerceront les droits visés dans la présente Norme concernant les données personnelles des personnes décédées qui les concernent.

32.4. La législation nationale des États ibéro-américains applicable en la matière reconnaîtra le droit du titulaire d'être en désaccord ou de contester les réponses données par le responsable face à une demande d'exercice des droits visés au présent paragraphe ou, en l'absence de réponse, devant l'autorité de surveillance et, le cas échéant, devant les organes judiciaires conformément au droit interne de chaque État ibéro-américain.

Chapitre IV

Préposé

33. Portée du préposé

33.1. Le préposé effectuera le traitement des données personnelles sans aucun pouvoir de décision sur sa portée et son contenu, et limitera ses actions aux conditions fixées par le responsable.

34. Formalisation de la prestation de services du préposé

34.1. La prestation de services entre le responsable et le préposé sera formalisée par la signature d'un contrat ou de tout autre instrument juridique considéré par les États ibéro-américains dans la législation nationale applicable en la matière.

34.2. Le contrat ou l'instrument juridique établira au moins l'objet, la portée, le contenu, la durée, la nature et le but du traitement, le type de données personnelles, les catégories des titulaires, ainsi que les obligations et les responsabilités du responsable et du préposé.

34.3. Le contrat ou l'instrument juridique établira au moins les clauses générales suivantes relatives aux services fournis par le préposé :

a. Effectuer le traitement des données personnelles selon les instructions du responsable.

b. S'abstenir de traiter les données personnelles à des fins autres que celles indiquées par le responsable.

c. Mettre en œuvre des mesures de sécurité conformément aux instruments juridiques applicables.

d. Informer le responsable lorsqu'il y aura une violation des données personnelles qu'il traite selon ses instructions.

e. Maintenir la confidentialité en ce qui concerne les données personnelles traitées.

f. Supprimer, rendre ou communiquer à un nouveau préposé désigné par le responsable les données personnelles faisant l'objet du traitement, une fois la relation juridique avec le responsable finie ou selon ses instructions, sauf qu'une disposition légale exige la conservation des données personnelles, ou que le responsable autorise la communication de ceux-ci à un autre préposé.

g. S'abstenir de transférer les données personnelles sauf par décision du responsable, ou que la communication provienne d'une sous-traitance, ou par mandat express de l'autorité de contrôle.

h. Permettre au responsable ou à l'autorité de contrôle les inspections et les vérifications sur place.

i. Générer, mettre à jour et conserver la documentation nécessaire qui lui permettra de prouver ses obligations.

j. Collaborer avec le responsable en tout ce qui concerne le respect de la législation nationale de l'État ibéro-américain applicable en la matière.

34.4. Lorsque le préposé ne respecte pas les instructions du responsable et décide lui-même de la portée, du contenu, des moyens et d'autres questions relatives au traitement des données personnelles, il assumera la condition de responsable conformément à la législation nationale de l'État ibéro-américain applicable en la matière.

35. Sous-traitance des services

35.1. Le préposé pourra, à son tour, sous-traiter des services impliquant le traitement de données personnelles, à condition qu'il y ait une autorisation préalable par écrit, spécifique ou générale du responsable, ou que cela soit stipulé expressément dans le contrat ou l'instrument juridique signé entre le responsable et le préposé.

35.2. Le sous-traité assumera le caractère de préposé dans les termes stipulés par la législation nationale de l'État ibéro-américain applicable en la matière.

35.3. Le préposé formalisera la prestation des services du sous-traité par un contrat ou tout autre instrument juridique déterminé par la législation nationale de l'État ibéro-américain applicable en la matière.

35.4. Si le sous-traité manque à ses obligations et ses responsabilités concernant le traitement des données personnelles en application des instructions du préposé, il assumera la condition de responsable conformément à la législation nationale de l'État ibéro-américain applicable en la matière.

Chapitre V

Transferts internationaux de données personnelles

36. Règles générales pour le transfert de données personnelles

36.1. Le responsable et le préposé pourront effectuer des transferts internationaux de données personnelles dans l'un des cas suivants :

a. Si le pays, une partie de son territoire, un secteur, une activité ou une organisation internationale recevant les données personnelles avait été reconnu avec un niveau adéquat de protection des données personnelles par le pays transférant, conformément à la législation nationale de ce pays applicable en la matière, ou le pays destinataire ou plusieurs secteurs prouvaient avoir des conditions minimales et suffisantes pour assurer un niveau adéquat de protection des données personnelles.

b. Si l'exportateur offre des garanties suffisantes pour le traitement des données personnelles dans le pays de destination et celui-ci certifie, à son tour, le respect des conditions minimales et suffisantes établies dans la législation nationale de chaque État ibéro-américain applicable en la matière.

c. Si l'exportateur et le destinataire concluent des clauses contractuelles ou tout autre instrument juridique qui offre des garanties suffisantes et qui permet de démontrer la portée du traitement des données personnelles, les obligations et les responsabilités assumées par les parties et les droits des titulaires. L'autorité de contrôle pourra valider les clauses contractuelles ou les instruments juridiques conformément à la législation nationale des États ibéro-américains applicables en la matière.

d. Si l'exportateur et le destinataire adoptent un schéma d'autorégulation contraignant ou un mécanisme de certification agréé, à condition qu'il soit conforme aux dispositions de la législation nationale de l'État ibéro-américain applicable en la matière, que l'exportateur doit respecter.

e. Si l'autorité de contrôle de l'État ibéro-américain du pays de l'exportateur autorise le transfert, en vertu de la législation nationale applicable en la matière.

36.2. La législation nationale des États ibéro-américains applicable en la matière pourra expressément établir des limites sur les transferts internationaux de catégories de données personnelles pour des raisons de sécurité nationale, de sécurité publique, de protection de la santé publique, protection des droits et des libertés de tiers, ainsi que pour des raisons d'intérêt public.

Chapitre VI

Mesures proactives dans le traitement des données personnelles

37. Reconnaissance des mesures proactives

37.1. La législation nationale des États ibéro-américains applicable en la matière pourra reconnaître et mettre en place des mesures qui favorisent un meilleur respect de sa législation et contribuent à renforcer et à augmenter les contrôles de la protection des données personnelles mis en œuvre par le responsable. Certaines de ces mesures sont mentionnées dans ce Chapitre.

38. Protection de la vie privée par conception et protection de la vie privée par défaut

38.1. Le responsable appliquera, à partir de la conception, des mesures préventives de nature différente qui permettent une application effective des principes, des droits et d'autres obligations prévues dans la législation nationale de l'État ibéro-américain pouvant être applicable, dans la détermination des moyens de traitement des données personnelles, pendant le traitement et avant la collecte des données personnelles.

38.2. Le responsable veillera à ce que ses programmes, services, systèmes ou plateformes informatiques, applications électroniques ou toute autre technologie qui implique le traitement de données personnelles respectent par défaut ou soient conformes aux principes, droits et autres obligations énoncés dans la législation nationale de l'État ibéro-américain applicable. Plus précisément, dans le but que seul le minimum de données personnelles soit traité et de limiter l'accessibilité sans l'intervention du titulaire à un nombre indéterminé de personnes.

39. Agent de protection des données personnelles

39.1. Le responsable désignera un agent de protection des données personnelles ou un équivalent dans les cas prévus par la législation nationale des États ibéro-américains applicables en la matière et lorsque :

a. Il sera une autorité publique.

b. Il effectuera des traitements des données personnelles visant une observation habituelle et systématique du comportement du titulaire.

c. Il effectuera des traitements des données personnelles où il est probable que cela implique un risque élevé d'affecter le droit à la protection des données personnelles des titulaires, compte tenu, entre autres facteurs et de manière non limitative, des catégories de données personnelles traitées, en particulier lorsqu'il s'agit de données sensibles, les transferts effectués, le nombre de titulaires, la portée du traitement, les technologies de l'information utilisées ou leurs objectifs.

39.2. Le responsable qui n'est pas dans l'un des motifs prévus au paragraphe précédent pourra désigner un agent de protection des données personnelles s'il le juge approprié.

39.3. Le responsable sera tenu de soutenir l'agent de protection des données personnelles dans l'exercice de ses fonctions, en lui fournissant les ressources nécessaires pour exécuter son travail et pour le maintien de ses connaissances spécialisées et leur mise à jour.

39.4. L'agent de protection des données personnelles aura, au moins, les tâches suivantes :

a. Conseiller le responsable sur les sujets soumis à leur examen en matière de protection des données personnelles.

b. Coordonner, dans l'organisation du responsable, les politiques, programmes, actions et autres activités visant à l'application de la législation nationale de l'État ibéro-américain applicable en la matière.

c. Superviser, dans l'organisation du responsable, le respect de la législation nationale de l'État ibéro-américain applicable en la matière.

40. Mécanismes d'autorégulation

40.1. Le responsable pourra adhérer volontairement à des schémas d'autorégulation contraignants, dont le but sera, entre autres, de contribuer à l'application correcte de la législation nationale de l'État ibéro-américain applicable en la matière et d'établir des procédures pour résoudre les conflits entre le responsable et le titulaire, sous réserve d'autres mécanismes établis par la législation nationale de la matière applicable, compte tenu des caractéristiques spécifiques des traitements des données personnelles effectués, ainsi que de l'exercice effectif et du respect des droits du titulaire.

40.2. Aux fins du paragraphe précédent, des codes de déontologie et des systèmes de certification et leurs cachets de confiance respectifs pourront, entre autres, être développés pour contribuer aux objectifs indiqués dans ce paragraphe.

40.3. La législation nationale des États ibéro-américains applicable en la matière établira les règles correspondantes pour la validation, la confirmation ou la reconnaissance des mécanismes d'autorégulation mentionnés.

41. Évaluation de l'impact à la protection des données personnelles.

41.1. Lorsque le responsable aura l'intention d'effectuer un type de traitement de données personnelles qui, par sa nature, sa portée, son contexte ou son objet, risque d'affecter le droit à la protection des données personnelles des titulaires réalisera, avant sa mise en œuvre, une évaluation de l'impact pour la protection des données personnelles.

41.2. La législation nationale des États ibéro-américains applicable en la matière indiquera les traitements ayant besoin d'une évaluation d'impact à la protection des données personnelles, leur contenu, les cas dans lesquels il sera approprié de présenter le résultat à l'autorité de contrôle, ainsi que les exigences de cette présentation, entre autres.

Chapitre VII

Autorités de contrôle

42. Nature des autorités de contrôle et de surveillance

42.1. Chaque État ibéro-américain devra avoir une ou plusieurs autorités de contrôle en matière de protection des données personnelles avec une autonomie totale, conformément à sa législation nationale applicable en la matière.

42.2 Les autorités de contrôle pourront être des organismes à un seul membre ou à plusieurs membres ; elles agiront de manière impartiale et indépendante dans leurs pouvoirs, seront indépendantes de toute influence extérieure, directe ou indirecte, et ne demanderont ni n'admettront aucune ordonnance ou instruction.

42.3. Le membre ou les membres des organes de direction des autorités de contrôle devront avoir l'expérience et les compétences, notamment en ce qui concerne l'étendue de la protection des données personnelles, nécessaires à l'exercice de leurs fonctions et de leurs pouvoirs. Ils seront nommés par une procédure transparente en vertu de la législation nationale applicable et ne pourront être destitués que pour des causes graves établies dans le droit interne de chaque État ibéro-américain, conformément aux règles de procédure régulière.

42.4. La législation nationale des États ibéro-américains applicable en la matière devra conférer aux autorités de contrôle des pouvoirs suffisants d'enquête, de supervision, de décision, de promotion, de sanction et d'autres qui soient nécessaires pour garantir son respect effectif, ainsi que l'exercice et le respect du droit à la protection des données personnelles.

42.5. Les décisions des autorités de contrôle ne feront l'objet que du contrôle judiciaire, conformément aux mécanismes établis dans la législation nationale des États ibéro-américains applicables en la matière et à leur droit interne.

42.6. Les autorités de contrôle devront disposer des ressources humaines et matérielles nécessaires pour s'acquitter de leurs tâches.

Chapitre VIII

Réclamations et Sanctions

43. Régime de réclamations et imposition de sanctions

43.1. Tout titulaire aura le droit de présenter sa réclamation à l'autorité de contrôle, ainsi que de faire appel à la protection judiciaire pour faire respecter ses droits en vertu de la législation nationale de l'État ibéro-américain applicable en la matière.

43.2. La législation nationale des États ibéro-américains applicable en la matière établira un régime qui permettra au titulaire de déposer une plainte auprès de l'autorité de contrôle lorsqu'il estime que le traitement de ses données personnelles viole la législation nationale en la matière, ainsi que pour demander une protection judiciaire.

43.3. La législation nationale des États ibéro-américains applicable en la matière établira un régime qui permettra de prendre des mesures correctives et de sanctionner les comportements qui aillent à l'encontre des dispositions des lois nationales correspondantes, indiquant au moins le plafond et les critères objectifs pour les sanctions correspondantes, en fonction de la nature, de la gravité, de la durée de l'infraction et de ses conséquences, ainsi que les mesures mises en œuvre par le responsable pour assurer le respect de leurs obligations en la matière.

Chapitre IX

Droit à l'indemnisation

44. Dédommagement

44.1. La législation nationale des États ibéro-américains applicable en la matière reconnaîtra le droit du titulaire d'être indemnisé lorsqu'il a subi des dommages et intérêts en raison d'une violation de son droit à la protection des données personnelles.

44.2. Le droit interne des États ibéro-américains indiquera l'autorité compétente pour connaître de ce type d'actions déposées par le titulaire concerné, ainsi que les termes, les exigences et les conditions dans le cadre desquels il sera indemnisé, le cas échéant.

Chapitre X

Coopération internationale

45. Mise en place de mécanismes de coopération internationale

45.1. Les États ibéro-américains pourront adopter des mécanismes de coopération internationale pour faciliter l'application des législations nationales applicables en la matière, qui pourront inclure, entre autres :

a. La mise en place de mécanismes pour renforcer l'assistance et la coopération internationales dans la mise en œuvre de la législation nationale respective en la matière.

b. L'assistance entre les autorités de contrôle par la notification et le renvoi de plaintes, l'assistance aux enquêtes et l'échange d'informations.

c. L'adoption de mécanismes axés sur le savoir et l'échange des meilleures pratiques et expériences dans le domaine de la protection des données personnelles, y compris les conflits de compétence avec les pays tiers.