Adoption de politiques harmonisées pour le marché des TIC dans les pays ACP

Protection de données:

Loi type de la Communauté de développement de l'Afrique australe (SADC)

HIPSSA

Harmonisation des politiques en matière de TIC en Afrique Subsaharienne

Commission européenne

Adoption de politiques harmonisées pour le marché des TIC dans les pays ACP

Protection de données :

Loi type de la Communauté de développement de l'Afrique australe (SADC)

HIPSSA

Harmonisation des politiques en matière de TIC en Afrique Subsaharienne

Avis de non-responsabilité

Le présent document a été réalisé avec l'aide financière de l'Union européenne. Les opinions exprimées dans les présentes ne reflètent pas nécessairement la position de l'Union européenne.

Les appellations utilisées et la présentation de matériels, notamment des cartes, n'impliquent en aucun cas l'expression d'une quelconque opinion de la part de l'UIT concernant le statut juridique d'un pays, d'un territoire, d'une ville ou d'une région donnés, ou concernant les délimitations de ses frontières ou de ses limites. La mention de sociétés spécifiques ou de certains produits n'implique pas qu'ils sont agréés ou recommandés par l'UIT de préférence à d'autres non mentionnés d'une nature similaire.

La version française a été traduite au fin d'information uniquement et ne revêt aucun caractère officiel, seule la version anglaise fait foi.

Avant d'imprimer ce rapport, pensez à l'environnement.

Avant-propos

Les technologies de l'information et de la communication (TIC) sont à la base du processus de mondialisation. Conscients qu'elles permettent d'accélérer l'intégration économique de l'Afrique et donc, d'en renforcer la prospérité et la capacité de transformation sociale, les ministres responsables des communications et des technologies de l'information, réunis sous les auspices de l'Union africaine, ont adopté, en mai 2008, un cadre de référence pour l'harmonisation des politiques et réglementations des télécommunications/TIC, dont la mise en place se faisait d'autant plus nécessaire que les Etats étaient de plus en plus nombreux à adopter des politiques pour libéraliser ce secteur.

La coordination dans l'ensemble de la région est essentielle si l'on veut que les politiques, la législation et les pratiques résultant de la libéralisation dans chaque pays ne freinent pas, par leur diversité, le développement de marchés régionaux compétitifs.

Notre projet d'"Appui à l'harmonisation des politiques en matière de TIC en Afrique subsaharienne" (HIPSSA) cherche à remédier à ce problème potentiel en regroupant et accompagnant tous les pays de la région au sein du Groupe des Etats d'Afrique, des Caraïbes et du Pacifique (ACP). Ces pays formulent et adoptent des politiques, des législations et des cadres réglementaires harmonisés dans le domaine des TIC. Exécuté par l'Union internationale des télécommunications (UIT) sous la coprésidence de l'Union africaine, ce projet est entrepris en étroite collaboration avec les communautés économiques régionales (CER) et les associations régionales de régulateurs qui sont membres de son comité directeur. Un comité de pilotage global constitué de représentants du Secrétariat ACP et de la Direction générale du développement et de la coopération – EuropeAid (DEVCO, Commission européenne) supervise la mise en oeuvre du projet dans son ensemble.

Inscrit dans le cadre du programme ACP sur les technologies de l'information et de la communication (@CP-ICT), le projet est financé par le 9ème Fonds européen de développement (FED), principal vecteur de l'aide européenne à la coopération au service du développement dans les Etats ACP, et cofinancé par l'UIT. La finalité du programme @CT-ICT est d'aider les gouvernements et les institutions ACP à harmoniser leurs politiques dans le domaine des TIC, grâce à des conseils, des formations et des activités connexes de renforcement des capacités, fondés sur des critères mondiaux tout en étant adaptés aux réalités locales.

Pour tous les projets rassembleurs impliquant de multiples parties prenantes, l'objectif est double: créer un sentiment partagé d'appartenance et assurer des résultats optimaux pour toutes les parties. Une attention particulière est prêtée à ce problème, depuis les débuts du projet HIPSSA en décembre 2008. Une fois les priorités communes arrêtées, des groupes de travail réunissant des parties prenantes ont été créés pour agir concrètement. Les besoins propres aux régions ont ensuite été définis, de même que les pratiques régionales pouvant donner de bons résultats, qui ont été comparées aux pratiques et normes établies dans d'autres régions du monde.

Ces évaluations détaillées, qui tiennent compte des spécificités de la sous-région et de chaque pays, ont servi de point de départ à l'élaboration de modèles de politiques et de textes législatifs constituant un cadre législatif dont l'ensemble de la région peut être fier. Il ne fait aucun doute que ce projet servira d'exemple pour les parties prenantes qui cherchent à mettre le rôle de catalyseur joué par les TIC au service de l'accélération de l'intégration économique et du développement socio-économique.

Avant-propos

Je saisis cette occasion pour remercier la Commission européenne et le Secrétariat ACP pour leur soutien financier. Je remercie également la Communauté économique des Etats de l'Afrique de l'Ouest (CEDEAO), l'Union économique et monétaire ouest-africaine (UEMOA), la Communauté économique des Etats de l'Afrique centrale (CEEAC), la Communauté économique et monétaire de l'Afrique centrale (CEMAC), la Communauté d'Afrique de l'Est (CAE), le Marché commun de l'Afrique orientale et australe (COMESA), la Communauté de développement de l'Afrique australe (SADC), l'Autorité intergouvernementale pour le développement (IGAD) l'Association des régulateurs des communications de l'Afrique australe (CRASA), l'Association des régulateurs de télécommunications d'Afrique centrale (ARTAC), la Commission économique des Nations Unies pour l'Afrique (CEA) et l'Assemblée des régulateurs des télécommunications de l'Afrique de l'Ouest (ARTAO) d'avoir contribué à la réalisation du projet. Sans la volonté politique des pays bénéficiaires, les résultats auraient été bien maigres. Aussi, je tiens à exprimer ma profonde gratitude à tous les gouvernements des pays ACP pour leur détermination, qui a assuré le grand succès de ce projet.

Brahima Sanou
Directeur du BDT

Remerciements

Le présent document constitue l'un des résultats d'une activité régionale organisée dans le cadre du projet HIPSSA ("Appui à l'harmonisation des politiques dans le secteur des TIC en Afrique subsaharienne"), officiellement lancé en décembre 2008 à Addis-Abeba.

En réponse à la fois aux défis et aux possibilités qu'offrent les technologies de l'information et de la communication (TIC) en termes de développement politique, social, économique et environnemental, l'Union internationale des télécommunications (UIT) et la Commission européenne (CE) ont uni leurs forces et signé un accord (projet UIT-CE) destiné à fournir un "Appui pour l'établissement de politiques harmonisées sur le marché des TIC dans les pays ACP", dans le cadre du Programme "ACP-Technologies de l'information et de la communication" (@CP-TIC) financé par le 9ème Fonds européen de développement (FED). Il s'agit du projet UIT-CE-ACP.

Ce projet global UIT-CE-ACP est mené à bien dans le cadre de trois sous-projets distincts adaptés aux besoins spécifiques de chaque région: l'Afrique subsaharienne (HIPSSA), les Caraïbes (HIPCAR) et les Etats insulaires du Pacifique (ICB4PAC).

En tant que membres de la Commission de direction du projet HIPSSA – coprésidée par la Commission de l'Union africaine et l'UIT – le Secrétariat de la Communauté de développement de l'Afrique australe (SADC) et celui de la Communication Regulators' Association of Southern Africa (CRASA) ont fourni conseils et assistance aux consultants, M. Jan Marc Van Gyseghem et Mme Pria Chetty, qui ont préparé le projet de document. Ce dernier a été révisé, examiné et validé, par un large consensus, par les participants lors de l'atelier organisé en collaboration avec les Secrétariats de la CRASA et de la SADC, qui s'est déroulé à Gaborone (Botswana) du 27 février au 3 mars 2012. Il devrait être adopté par les Ministres des pays de la SADC chargés des télécommunications, des postes et des TIC, lors de la réunion qu'ils tiendront à Maurice en novembre 2012.

L'UIT souhaite remercier les délégués des ateliers issus des ministères chargés des TIC et des télécommunications des pays de la SADC, les régulateurs de contrôle des pays de la CRASA, le milieu universitaire, la société civile, les opérateurs et les organisations régionales, pour l'excellent travail qu'ils ont fourni et l'engagement dans l'élaboration du rapport final, dont ils ont fait preuve afin de produire le contenu. Nous remercions également très sincèrement les Secrétariats de la SADC et de la CRASA pour leurs contributions.

Sans la participation active de l'ensemble de ces parties prenantes, il aurait été impossible d'élaborer un tel document, qui reflète les exigences et les conditions générales de la région de la SADC tout en décrivant les meilleures pratiques internationales.

Les activités ont été mises en œuvre par Mme Ida Jallow, chargée de la coordination des activités en Afrique subsaharienne (Coordonnatrice principale du projet HIPSSA) et M. Sandro Bazzanella, chargé de la gestion de l'ensemble du projet couvrant l'Afrique subsaharienne, les Caraïbes et le Pacifique (Directeur du projet UIT-CE-ACP), avec l'appui de Mme Hiwot Mulugeta, Assistante du projet HIPSSA, et de Mme Silvia Villar, Assistante du projet UIT-CE-ACP. Le travail a été réalisé sous la direction générale de M. Cosmas Zavazava, Chef du Département de l'appui aux projets et de la gestion des connaissances. Le document a été établi sous la supervision directe de M. Jean-François Le Bihan, qui était alors Coordonnateur principal du projet, et ses auteurs ont bénéficié des commentaires de la Division de l'environnement réglementaire et commercial (RME) et de la Division des initiatives spéciales (SIS) du Bureau de développement des télécommunications (BDT) de l'UIT. Ils ont aussi bénéficié de l'appui de M. Marcelino Tayob, Conseiller principal au Bureau régional de l'UIT pour l'Afrique. L'équipe du Service de composition des publications de l'UIT a été chargée de la publication.

Table des matières

Table des matières

Pages

Table des matières

Préambule

De nombreuses institutions ou organisations internationales estiment que la protection des données est fondamentale pour le développement de la personne dans une société démocratique et pour la construction du bien-être. A ce titre, la protection des données est au service de l'individu, tant dans la sphère personnelle que sur le lieu de travail.

En raison des liens entre la protection des données et la protection de la vie privée, il convient toutefois de reconnaître que la protection des données couvre un champ d'application plus large. Plusieurs droits de l'homme sont en effet concernés, dont la liberté d'expression, la liberté d'association, etc. La protection des données empêche d'utiliser des données à caractère personnel pour opérer une distinction entre les personnes sur la base, entre autres, des croyances religieuses, de l'adhésion à un syndicat, du sexe, de la race, de la filiation et des informations liées à la santé.

Outre ces aspects basés sur les droits fondamentaux de l'homme, on assiste à une réelle explosion des technologies de l'information et de la communication qui pourrait affecter ce droit à la protection des données à caractère personnel dans les activités commerciales ainsi que dans les activités de gouvernement électronique (eGov). Le développement de ces technologies implique la prolifération de bases de données utilisées pour stocker et traiter une grande partie des données à caractère personnel. L'interconnexion de ces bases de données pourrait alors mener à la localisation illégitime de personnes dans leurs diverses activités, privées comme professionnelles. De plus, il est évident que les technologies de l'information et de la communication acquièrent une importance accrue dans la prise de décisions concernant les personnes, notamment au vu des informations contenues dans les bases de données décrites ci-dessus. La réglementation en matière de protection des données doit viser à s'assurer que les avantages liés à l'utilisation des technologies de l'information et de la communication ne sont pas associés à un affaiblissement de la protection des données à caractère personnel. Cela signifie que les informations doivent être correctes, mais aussi pertinentes pour l'objectif spécifié et déclaré. Le principe de ne collecter et de ne traiter que les données à caractère personnel nécessaires à un objectif spécifié et déclaré doit être mis en œuvre. De plus, le contrôleur (c'est-à-dire la personne qui détermine l'objectif ou le but du traitement et des moyens qui seront mis en œuvre) est tenu de mettre à jour les données et de poser des limites à leur collecte et à leur traitement.

Il est également nécessaire de s'assurer que les données ne sont pas divulguées sans l'autorisation de la personne ou d'une disposition juridique. Cela implique l'adoption de mesures organisationnelles et techniques garantissant la sécurité du traitement, concernant notamment la collecte et le stockage de données à caractère personnel.

Cette exigence implique un principe de responsabilité du contrôleur des données, mais aussi de son responsable du traitement des données selon la sensibilité des données traitées. Il existe, en réalité, des données moins sensibles que d'autres, pouvant exiger un niveau de protection inférieur. Par exemple, si une base de données contient uniquement les prénoms et les noms de famille, les données ne sont pas normalement sensibles. Par conséquent, le risque d'ingérence ou de vol est moindre et une sécurité moins sophistiquée est requise. En revanche, une base de données recueillant des données à caractère personnel liées à la santé ou révélant l'identité raciale exigerait une sécurité accrue.

Comme indiqué, deux catégories de données existent: les données sensibles pouvant affecter la vie privée d'une personne et les données qui ne sont pas sensibles. La première catégorie révèle l'affiliation religieuse, l'origine ethnique et l'état de santé d'une personne. Il peut s'agir aussi de données génétiques, qui ont la particularité de concerner de nombreuses personnes puisqu'elles sont communes à toute la famille. C'est pourquoi il faut définir des règles spécifiques pour cette catégorie particulière de données sensibles, tout en tenant compte du fait que certaines données sensibles ne sont pas traitées pour ce qu'elles contiennent ou révèlent (par exemple, la photo de quelqu'un écoutant des religieux sur un site Internet ou dans un annuaire). Les données (la photo) ne sont pas traitées dans le sens religieux, mais

uniquement pour la photo de la personne qui la montre sur le site Internet ou dans l'annuaire. Les règles doivent donc aborder cet aspect. Toutefois, cela n'est pas valable en ce qui concerne les données génétiques, biométriques et celles liées aux enfants, aux délits, aux sanctions pénales ou aux mesures de sécurité, qui sont des données extrêmement sensibles.

Dans le même temps, il convient de donner à l'individu la possibilité de contrôler ses propres informations, par le biais d'un droit d'accès duquel découlera, entre autre, un droit de rectification et d'opposition. Il peut s'avérer nécessaire, en outre, d'établir un système de sanctions pour conférer à la loi toute son efficacité. Une loi sans sanction risque en effet d'être violée, ce qui la rend totalement inefficace.

Il convient également de noter qu'avec la mondialisation, les frontières traditionnelles entre les régions et les pays deviennent de plus en plus perméables. De ce fait, les données à caractère personnel font, de plus en plus souvent, l'objet de traitements transfrontières. Les Etats doivent établir les règles qui régissent ces transferts, afin de les autoriser uniquement sous des conditions qui garantissent la protection des données à caractère personnel. Ces règles de protection des données seront plus facilement applicables si de nombreux pays promulguent des règles équivalentes. Cela mène par conséquent à l'adoption de textes à une échelle régionale. Il est en effet important que de nombreux pays adoptent un ensemble commun de règles pour assurer l'exercice réel du droit de protection des données à caractère personnel. L'objectif de la loi type proposée est la création d'un système uniforme dans une zone donnée afin de créer un environnement sûr pour les citoyens.

L'établissement d'un système uniforme de règles requiert la coopération entre les pays pour assurer la continuité dans l'uniformité. Cette coopération peut avoir lieu grâce à la collaboration en matière de protection des données à caractère personnel par l'intermédiaire d'un groupe de travail international.

De plus, le régime de protection des données à caractère personnel doit prendre en compte les coutumes sociales et religieuses ainsi que les politiques régionales existantes pour atteindre son objectif de protection et d'harmonisation. Les outils existants, tels que le projet de convention de l'Union africaine sur l'établissement d'un cadre juridique crédible pour la cyber-sécurité en Afrique, les textes de la Communauté de développement de l'Afrique australe (SADC), de la Communauté économique des Etats d'Afrique de l'Ouest (CDEAO) et les législations nationales existantes, y compris les dispositions constitutionnelles.

L'établissement d'un régime de protection des données à caractère personnel ne sera effectif qu'avec la création d'une Autorité de protection, visant à encourager le respect de la loi et la protection de la vie privée en général. Cette autorité doit également être dotée de pouvoirs réglementaires afin, par exemple, de clarifier certains principes de la loi type.

En gardant ceci à l'esprit, il est reconnu que la protection des données à caractère personnel implique l'établissement d'un régime spécifique et adapté aux particularités de chaque région, comme exposé dans la présente Loi type.

Titre I

Titre abrégé .

La présente législation peut être désignée sous le titre "Loi relative à la protection des données", et entrera en vigueur [le xxx/après sa publication au journal officiel].

Objectif

L'objectif de la législation en matière de protection des données en (au) [indiquer le nom du pays] est de combattre les violations de données susceptibles de découler de la collecte, du traitement, de la transmission, du stockage et de l'utilisation de données à caractère personnel.

TITRE I: DÉFINITIONS

Définitions 1.

(1) **Code de conduite:** fait référence aux chartes d'utilisation des données élaborées par le contrôleur de données afin d'instituer l'utilisation légitime de ressources informatiques, d'Internet et des communications électroniques de la structure concernée, et qui ont été approuvées par l'autorité de protection des données.

(2) **Consentement:** fait référence à toute manifestation d'une expression de volonté spécifique, non équivoque, librement donnée et éclairée, par laquelle la personne concernée ou son représentant légal, judiciaire ou légalement désigné accepte que ses données personnelles soient traitées.

(3) **Données:** fait référence à toutes les représentations d'informations, quel que soit le format ou le support.

(4) **Contrôleur de données ou contrôleur:** fait référence à une personne physique ou morale ou un organisme public qui, seul(e) ou conjointement avec d'autres, détermine l'objectif et les moyens du traitement des données à caractère personnel. Lorsque l'objectif et les moyens de traitement sont déterminés par ou en vertu d'une loi, d'un décret ou d'une ordonnance, le contrôleur est la personne physique ou morale ou l'organisme public qui a été désigné à ce titre par ou en vertu de cette loi, de ce décret ou de cette ordonnance.

(5) **Représentant du contrôleur de données ou représentant du contrôleur:** fait référence à une personne physique ou morale ou à un organisme public établi à titre permanent sur le territoire [du pays concerné], qui se substitue au contrôleur de données dans l'accomplissement des obligations énoncées par la présente loi type.

(6) **Responsable du traitement des données:** fait référence à une personne physique, morale ou à un organisme public qui traite des données personnelles pour et au nom du contrôleur et suivant les instructions du contrôleur de données, sauf pour les personnes qui, sous l'autorité directe du contrôleur, sont autorisées à traiter les données.

(7) **Responsable de la protection des données ou RPD:** fait référence à toute personne désignée par le contrôleur de données chargé d'assurer, de manière indépendante, le respect des obligations prévues dans la présente loi type, sauf lorsqu'il s'agit d'un transfert de données à caractère personnel à un Etat non-membre de la SADC.

(8) **Personne concernée:** fait référence à un individu qui fait l'objet du traitement de données à caractère personnel et qui est identifié ou identifiable.

(9) **Personne identifiable:**

(a) personne qui peut être identifiée, directement ou indirectement, en particulier par référence à un numéro d'identification ou à un ou plusieurs facteurs spécifiques à son identité physique, physiologique, mentale, économique, culturelle ou sociale.

(b) Pour déterminer si une personne est identifiable, il convient de tenir compte de tous les moyens raisonnablement susceptibles d'être utilisés soit par le contrôleur, soit par une autre personne pour identifier ladite personne.

(10) **Fichier:**

(a) fait référence à un ensemble structuré de données à caractère personnel qui sont accessibles selon des critères spécifiques, qu'ils soient centralisés, décentralisés ou dispersés sur une base fonctionnelle ou géographique.

(b) inclut les fichiers électroniques ou tout autre support.

(11) **Données génétiques:** fait référence aux informations issues d'une analyse de l'acide désoxyribonucléique (ADN).

(12) **Professionnel de santé:** fait référence à tout individu qualifié comme tel par la loi nationale.

(13) **Enfant:** fait référence à tout individu qui n'est pas majeur ou qui n'a pas de statut similaire selon sa loi nationale [ou la loi nationale de l'Etat appliquant la présente loi type].

(14) **Données à caractère personnel:** fait référence aux données relatives à toute personne concernée.

(15) **Traitement:** fait référence à toute opération ou ensemble d'opérations qui sont exécutées sur des données à caractère personnel, que ce soit ou non par des moyens automatiques, tels que l'obtention, l'enregistrement ou la détention de données ou l'exécution d'une opération ou d'un ensemble d'opérations sur des données, y compris:

(a) l'organisation, l'adaptation ou l'altération des données;

(b) l'extraction, la consultation ou l'utilisation des données; ou

(c) l'alignement, la combinaison, le verrouillage, l'effacement ou la destruction des données.

(16) **Autorité de protection ou Autorité:** fait référence à une autorité administrative indépendante responsable de s'assurer que les données à caractère personnel sont traitées conformément aux dispositions de la présente loi type. Cela implique un pouvoir décisionnaire indépendant de toute influence externe, directe ou indirecte, sur l'Autorité.

(17) **Destinataire:** personne physique ou morale, autorité publique, agence ou tout autre organisme auquel des données sont divulguées, qu'il s'agisse d'une tierce partie ou non; toutefois, les autorités pouvant recevoir des données dans le cadre d'une enquête juridique particulière ne sont pas considérées comme des destinataires.

(18) **Registre:** désigne le registre visé au Chapitre 3.

(19) **Données sensibles:**.

(a) fait référence aux données génétiques, aux données liées aux enfants, aux données liées aux délits, aux sentences pénales ou aux mesures de sécurité, aux données biométriques ainsi que, si elles sont traitées pour ce qu'elles révèlent ou contiennent, aux données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, la filiation, l'appartenance syndicale, le sexe et le traitement d'informations concernant la santé ou la vie sexuelle.

(b) fait référence aussi aux données à caractère personnel qui sont considérées par un Etat membre comme présentant un risque majeur pour les droits et les intérêts de la personne concernée, notamment la discrimination illégale ou arbitraire.

(20) **Tierce partie:** fait référence à une personne physique ou morale, une organisation non constituée en société ou une autorité publique autre que la personne concernée, le contrôleur, le responsable du traitement et toute personne qui, sous l'autorité directe du contrôleur ou du responsable du traitement, est autorisée à traiter les données.

(21) **Flux transfrontalier:** fait référence à des flux internationaux de données à caractère personnel au moyen de la transmission électronique ou par tout autre moyen de transmission, y compris la transmission de données par satellite.

(22) **Déclenchement d'alerte éthique ou *whistleblowing*:** fait référence au système juridique qui permet aux individus de signaler le comportement d'un membre de leur organisation, qu'ils estiment contraire à une loi, à un règlement ou aux règles fondamentales établies par leur organisation.

Titre II

TITRE II: CHAMP D'APPLICATION

Champ d'application

2. (1) La présente loi type s'applique au traitement de données à caractère personnel exécuté en tout ou partie par des moyens automatisés, et au traitement de données à caractère personnel autrement que par des moyens automatisés, qui fait partie d'un système de classement ou est destiné à en faire partie.

(2) La présente loi type s'applique:

(a) au traitement de données à caractère personnel exécuté dans le contexte des activités effectives et réelles d'un contrôleur établi à titre permanent sur le territoire [du pays donné] ou dans un endroit où la loi [du pays donné] s'applique en vertu du droit public international;

(b) au traitement de données à caractère personnel par un contrôleur qui n'est pas établi à titre permanent sur le territoire [du pays donné], si les moyens utilisés, qui peuvent être des moyens automatiques ou d'autres moyens situés sur le territoire d'un [pays donné], ne sont pas les mêmes que les moyens utilisés pour le traitement de données à caractère personnel uniquement aux fins du transit de données à caractère personnel sur le territoire (du pays donné).

(3) Dans les circonstances visées au paragraphe précédent sous (2)b, le contrôleur doit désigner un représentant établi sur le territoire (du pays donné], sans préjudice des procédures juridiques pouvant être intentées à l'encontre du contrôleur.

(4) La présente loi type ne s'applique pas au traitement de données à caractère personnel par une personne physique au cours d'activités purement personnelles ou ne dépassant pas le cadre d'un foyer.

(5) La présente loi type ne peut pas restreindre:

(a) les moyens de production des informations disponibles selon la loi nationale ou comme autorisé dans les règles régissant les procédures juridiques;

(b) le pouvoir d'une autorité judiciaire de contraindre un témoin à témoigner et produire des preuves.

Titre III

TITRE III: AUTORITÉ DE PROTECTION DES DONNÉES

Statut et composition

3. (1) Une autorité indépendante et administrative appelée Autorité de protection ou Autorité est établie et sera chargée du contrôle du respect de la présente loi type et de la vie privée sur le territoire national.

Cela implique un pouvoir décisionnaire indépendant de toute influence externe directe ou indirecte sur l'Autorité.

(2) L'Autorité sera composée de juges désignés par leurs pairs, d'un représentant du [Premier ministre ou Chef d'Etat], de députés désignés par leurs pairs, de personnes désignées par des organisations nationales œuvrant dans le domaine des droits fondamentaux de l'homme ou par des organisations non gouvernementales, de personnes désignées par des organisations nationales œuvrant dans le domaine des technologies de l'information et de la communication. Ce sont des membres permanents.

(3) L'Autorité inclura aussi des membres suppléants ayant un profil professionnel équivalent, qui remplaceront un membre permanent lorsqu'il est excusé, absent ou lorsque son poste devient vacant.

(4) Tous les membres permanents et suppléants possèderont les compétences requises en matière de protection des données à caractère personnel et de la vie privée ainsi que de technologies de l'information.

(a) Avoir la nationalité du pays.

(b) Être en pleine possession de leurs droits civils et politiques.

(c) Ne pas être membres d'un organe de la SADC ou du Parlement, à l'exception des parlementaires nommés membres de l'Autorité en vertu du paragraphe (2) qui précède.

[L'Etat membre doit établir des règles spécifiques relatives à l'incompatibilité entre la fonction de membres de l'Autorité et d'autres fonctions afin d'éviter des conflits d'intérêts survenant avant ou pendant le mandate des membres de l'Autorité.]

(6) Il n'est pas permis aux membres de l'Autorité d'assister aux délibérations sur des questions dans lesquelles eux-mêmes ou les membres de leur famille jusqu'au quatrième degré de parenté ont un intérêt personnel.

(7) Les membres de l'autorité sont soumis à l'obligation de respect du secret selon les règles juridiques (telles que le code pénal).

(8) Les membres de l'Autorité sont nommés pour une durée de [….] ans renouvelables […] fois.

(9) Les membres peuvent être démis de leur fonction par l'organe ou l'organisation qui les a nommés en cas de violation de leurs devoirs stipulés dans la présente loi type ou d'une atteinte à l'intégrité de leur fonction.

(10) Les membres de l'Autorité bénéficient de l'immunité pour les opinions qu'ils expriment dans l'exécution de leur fonction. Les membres ne peuvent pas être démis de leur fonction du fait des opinions exprimées ou des actes accomplis dans l'exercice de leur fonction en qualité de membres.

Titre III

(11) Dans l'exercice de leur fonction, les membres doivent rester indépendants de l'influence de toute autre autorité publique et ne sont soumis à aucune de ses instructions.

(12) Les délibérations de l'Autorité sont légitimes lorsqu'au moins la majorité de ses membres est présente pendant ses réunions. Les décisions sont prises à la majorité absolue. En cas de partage égal des voix, le Président de l'Autorité ou, en son absence, son suppléant ou sa suppléante a une voix prépondérante.

(13) Sauf dans les cas visés à l'Article 5(1) (c), tout le personnel, les consultants et les entrepreneurs de l'Autorité doivent se soumettre à l'obligation du secret selon les règles juridiques (telles que le code pénal) aux fins de respecter la confidentialité de tous les faits, actes et informations que cette personne ou ces personnes peuvent apprendre en raison de leur fonction.

(14) Le Président de l'Autorité doit être un juge ayant au moins cinq ans d'expérience, qui sera nommé à plein temps au sein de l'Autorité. Durant son mandat, le Président/ la Présidente ne peut pas exercer d'autre activité professionnelle. Son salaire est égal à celui en vigueur pour le poste de [….], y compris les augmentations de salaires et autres avantages du personnel.

(15) Avant d'exécuter leur mandat respectif, le Président de l'Autorité et les membres, permanents et suppléants, prêtent le serment suivant devant le Parlement:

"Je m'engage à remplir les devoirs de ma mission de manière consciencieuse et impartiale."

Pouvoirs

4.

(1) L'Autorité:

(a) doit veiller principalement à ce que le traitement du contrôleur de données à caractère personnel soit conforme à la présente loi type.

(b) émet son opinion, à sa propre initiative ou à la demande du Gouvernement ou du Parlement, sur toute question relative à l'application des principes fondamentaux de la protection de la vie privée, dans le contexte de la présente loi type et de toute loi contenant des dispositions relatives à la protection de la vie privée en rapport avec le traitement de données à caractère personnel.

(c) peut soumettre au Tribunal tout texte législatif ou administratif non conforme aux principes fondamentaux de la protection de la vie privée dans le cadre de la présente loi type ainsi que de toute loi contenant des dispositions concernant la protection de la vie privée en rapport avec le traitement de données à caractère personnel.

(d) peut, conformément à ses pouvoirs, publier des règlements aux termes de la présente loi type, qui seront exerçables par un acte statutaire ayant force de loi, lequel (sauf dans le cas des règlements initiaux) sera susceptible d'être annulé en vertu d'une résolution du Parlement adoptée par une majorité des deux tiers des membres du Parlement.

Titre III

(e)

(i.) peut mener des enquêtes, de son propre accord ou à la demande de la personne concernée ou de toute personne intéressée et, à cet effet, peut demander l'aide d'experts pour exécuter ses fonctions, c'est-à-dire donner des instructions à un ou plusieurs de ses membres, accompagnés d'un expert, le cas échéant, pour effectuer des enquêtes sur place.

(ii.) peut exiger, entre autres, la divulgation de documents susceptibles d'être utiles pour son enquête.

(iii.) a accès à tous les endroits raisonnablement suspectés d'être le lieu d'activités se rapportant à l'application de la présente loi type.

(f) reçoit, par la poste, par des moyens électroniques ou par tout autre moyen équivalent, les plaintes déposées contre un traitement de données à caractère personnel et assure un retour d'information aux demandeurs.

(g) reçoit, par la poste, par des moyens électroniques ou par tout autre moyen équivalent, les plaintes déposées dans l'exercice des droits de la personne concernée en vertu du Chapitre 7 de la présente loi type.

(h) peut conduire de fréquentes consultations avec des parties prenantes principales (telles que le Parlement, le ministère concerné, le public) sur des questions paraissant nécessaires pour garantir la protection effective des données pour les services, les installations, les appareils ou les annuaires au titre de la présente loi type.

Devoirs

5. (1) L'Autorité doit:

(a) répondre à toute demande d'avis concernant la protection de la vie privée en rapport avec le traitement de données à caractère personnel;

(b) recevoir la notification de traitement en vertu de l'Article 6 (1) et faire respecter sa conformité avec la présente loi type.

(c) sauf description différente de la loi, informer sans retard l'autorité judiciaire de toute infraction dont elle a connaissance et estime nécessaire de signaler à l'autorité judiciaire.

(2) prononcer des sanctions administratives, telles que l'annulation de l'autorisation de procéder au traitement, d'amendes ou de l'octroi de dommages et intérêts au profit de la personne lésée en cas de violation des dispositions de la présente loi type.

(3) accorder l'autorisation en vertu de l'Article 28;

(4) créer, tenir et mettre à jour le registre qui doit être accessible à toute personne en requérant l'accès sans aucun motif nécessaire

(5) recevoir des notifications des violations de la sécurité énoncées à l'Article 25;

(6) recevoir et donner l'autorisation concernant le projet, la modification ou l'extension des codes de conduite énoncés au Chapitre 12

(7) donner son avis sur la façon dont le cadre juridique de protection des données légales peut être simplifié et amélioré;

Titre III

(8) établir des mécanismes de coopération avec les autorités de protection de pays tiers, le cas échéant et principalement pour résoudre d'éventuels différends transfrontaliers au titre de la présente loi type lorsque le différend est du ressort de l'autorité nationale de protection des données de plusieurs Etats Membres;

(9) participer à toute négociation internationale sur les questions de protection de données;

(10) soumettre, une fois par an, un rapport d'activité à présenter à l'institution à laquelle l'Autorité rend compte;

6. (1) L'Autorité peut demander une ordonnance du Tribunal pour la préservation prompte des données, y compris des données de trafic, lorsqu'il existe des motifs raisonnables d'estimer que de telles données sont exposées au risque de perte ou de modification.

(2) Lorsque le Tribunal estime qu'une ordonnance peut être rendue au titre du paragraphe (1) précédent, il émettra une mesure conservatoire spécifiant une période qui ne doit pas excéder 90 jours durant laquelle l'ordonnance restera en vigueur.

(3) Le Tribunal peut, à la demande de l'Autorité, prolonger la période spécifiée au paragraphe (2) précédent pendant le temps que le juge estime approprié.

7. (1) L'Autorité doit élaborer ses règles de procédure dans un délai de [….] à compter de son établissement. Ces règles doivent être publiées.

(2) Ces règles établissent les procédures concernant:

(a) Les délibérations, l'instruction et la présentation des affaires;
(b) La plainte, l'enquête et la sanction;
(c) Toutes les autres procédures établies au présent chapitre.

(3) Les délibérations de l'Autorité ne sont légitimes que lorsqu'au moins la majorité de ses membres est présente pendant ses réunions. Elle prend ses décisions à la majorité absolue. En cas de partage égal des voix, le(la) Président(e) de l'Autorité ou, en son absence, son suppléant/sa suppléante a une voix prépondérante.

Accès à l'Autorité

8. (1) Toute personne prouvant son identité a le droit de s'adresser à l'Autorité, sans frais, par elle-même ou par l'intermédiaire de son avocat, d'une autre personne ou d'un organisme juridique légalement désigné.

Sanctions

9. (1) L'Autorité peut imposer ce qui suit:

(a) un avertissement à un contrôleur de données ne respectant pas les obligations de la présente loi type
(b) une mise en demeure de se conformer, adressée audit contrôleur de données, pour qu'il mette fin à la non-exécution dans un délai donné. En cas d'urgence, ce délai peut être limité à cinq jours.

(2) En cas de non-exécution par le contrôleur de la mise en demeure signifiée, l'Autorité pourrait prononcer les sanctions suivantes, après avoir dûment entendu les parties:

(a) Limitation ou cessation du traitement ou suspension de l'autorisation, pendant une période maximum de trois mois;

et/ou

(b) pénalité financière de (…);

(3) En cas de violation grave et immédiate des droits et des libertés individuels, l'Autorité peut décider, dans une procédure en référé:

(a) la limitation ou la cessation du traitement des données à caractère personnel;

ou

(b) l'accès temporaire ou définitif à certaines données à caractère personnel traitées;

(c) le traitement temporaire ou définitif non conforme aux dispositions de la présente loi type.

(4) Les sanctions et les décisions prises par l'Autorité peuvent faire l'objet d'un appel par le biais des autorités judiciaires.

Financement 10.

(1) Pour l'accomplissement de sa mission, l'Autorité recevra une subvention du Parlement qui assure sa capacité à exercer ses devoirs et ses pouvoirs.

(2) L'Autorité encaissera la sanction financière prononcée à l'encontre des contrôleurs de données en application de la présente loi type.

(3) L'Autorité présentera un rapport annuel à l'institution à laquelle l'Autorité rend compte.

TITRE IV: QUALITÉ DES DONNÉS

Qualité des données

11. (1) Le contrôleur de données doit s'assurer que les données à caractère personnel traitées sont:

(a) adéquates, pertinentes et non excessives par rapport aux objectifs pour lesquels elles sont collectées ou traitées ultérieurement;

(b) exactes et, si nécessaire, tenues à jour; toutes les mesures raisonnables doivent être prises pour s'assurer que les données inexactes ou incomplètes, au regard des objectifs pour lesquels elles sont collectées ou pour lesquels elles sont traitées ultérieurement, soient effacées ou rectifiées;

(c) conservées sous une forme permettant l'identification des personnes concernées, pendant une durée n'excédant pas celle nécessaire à la réalisation des objectifs pour lesquels elles sont collectées ou traitées ultérieurement. L'Autorité établira des mesures de protection appropriées concernant les données à caractère personnel qui sont conservées plus longtemps que permis ci-dessus à des fins de recherches historiques, statistiques ou scientifiques.

(2) Le contrôleur de données doit prendre toutes les mesures appropriées pour s'assurer que les données à caractère personnel traitées peuvent être exploitées, quel que soit le support utilisé, et s'assurer que l'évolution de la technologie ne sera pas un obstacle à cette opération.

(3) Le contrôleur assure la conformité avec les règles stipulées aux paragraphes (1) et (2) par toute personne travaillant sous son autorité ou par tout sous-traitant.

Titre V

TITRE V: RÈGLES GÉNÉRALES SUR LE TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL

Généralité

12. (1) Le contrôleur de données s'assurera que le traitement de données à caractère personnel est nécessaire et est effectué équitablement et en toute légalité.

Objectif

13. (1) Le contrôleur de données doit s'assurer que les données à caractère personnel sont collectées dans des objectifs spécifiés, explicites et légitimes et, en tenant compte de tous les facteurs pertinents, en particulier les attentes raisonnables de la personne concernée et les dispositions légales et réglementaires applicables, qu'elles ne sont pas traitées ultérieurement d'une façon incompatible avec ces objectifs.

Données non sensibles

14. (1) Le traitement de données à caractère personnel non sensibles est autorisé, sans le consentement de la personne concernée, si nécessaire:

(a) à l'exécution d'un contrat auquel la personne concernée est partie ou afin de prendre des mesures, à la demande de la personne concernée, avant de conclure un contrat;

ou

(b) pour la conformité avec une obligation à laquelle le contrôleur est soumis par ou en vertu d'une loi;

ou

(c) afin de protéger les intérêts vitaux de la personne concernée;

ou

(d) pour l'exécution d'une tâche effectuée dans l'intérêt public ou dans l'exercice de l'autorité officielle assignée au contrôleur ou à une tierce partie à laquelle les données sont divulguées;

ou

(e) pour la promotion des intérêts légitimes du contrôleur ou de la tierce partie à qui les données sont divulguées, sauf lorsque ces intérêts sont annulés par les intérêts ou les droits et libertés fondamentaux de la personne concernée réclamant la protection au titre de la présente loi type.

(2) L'Autorité peut spécifier les circonstances dans lesquelles la condition stipulée sous e) est considérée comme n'ayant pas été remplie.

Données sensibles

15. (1)

(a) Le traitement de données à caractère personnel, si elles sont traitées pour ce qu'elles révèlent ou contiennent, de données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, la filiation, l'appartenance syndicale ou le sexe, ainsi que le traitement de données concernant la vie sexuelle et de toutes données à caractère personnel qui sont considérées par un Etat membre comme présentant un risque majeur pour les droits et les intérêts de la personne concernée, en particulier la discrimination illégale ou arbitraire, sont interdits. Cette disposition ne s'applique pas si la personne concernée a donné son consentement par écrit pour ce traitement de données à caractère personnel, sauf si la loi déclare que l'interdiction ne peut pas être levée par le consentement écrit de la personne concernée.

(b) Ce consentement peut être retiré à tout moment par la personne concernée, sans explication et sans frais.

(c) L'Autorité peut déterminer les cas dans lesquels l'interdiction de traiter les données visées au présent article ne peut pas être levée même avec le consentement de la personne concernée.

(2) Le paragraphe (1) ci-dessus ne s'applique pas lorsque:

(a) le traitement est nécessaire pour remplir les obligations et les droits spécifiques du contrôleur dans le domaine du droit du travail; ou

(b) le traitement est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne, lorsque la personne concernée est physiquement ou légalement incapable de donner son consentement ou n'est pas représentée par son représentant légal, judiciaire ou désigné; ou

(c) le traitement est effectué au cours de ses activités légitimes par une fondation, une association ou une autre organisation à but non lucratif poursuivant un objectif politique, philosophique, religieux, d'assurance maladie ou syndical et à condition que le traitement se rapporte uniquement aux membres de l'organisation ou aux personnes qui ont un contact régulier avec elle en rapport avec ses objectifs et que les données ne soient pas divulguées à une tierce partie sans le consentement de la personne concernée; ou

(d) le traitement est nécessaire au respect des lois relatives à la sécurité sociale; ou

(e) le traitement est nécessaire, avec les garanties appropriées, à l'établissement, à l'exercice ou à la défense de réclamations légales; ou

(f) le traitement se rapporte à des données qui ont apparemment été rendues publiques par la personne concernée; ou

(g)

(i.) le traitement est nécessaire aux fins de la recherche scientifique.

(ii.) L'Autorité sera en droit de spécifier les conditions sous lesquelles ce traitement peut être effectué.

ou

(h) le traitement est effectué conformément à la législation relative aux statistiques publiques; ou

(i) le traitement est nécessaire aux fins de la médecine préventive ou du diagnostic médical, de la fourniture de soins ou de traitement à la personne concernée ou à l'un de ses parents, ou de la gestion de services de soins de santé fournis dans l'intérêt de la personne concernée, et lorsque les données sont traitées sous la surveillance d'un professionnel de santé; ou

(j) le traitement de données à caractère personnel visé est autorisé par une loi ou un texte législatif équivalent pour une autre raison d'intérêt public substantiel; ou

(k) le traitement est effectué par des associations dotées de la personnalité juridique ou d'organisations d'intérêt public dont l'objectif principal est la protection et la promotion de droits de l'homme et de libertés fondamentales, en vue de réaliser cet objectif, à condition que le traitement ait été autorisé par l'Autorité;

(3)

(a) Le traitement de données à caractère personnel visées au Paragraphe 2 (i) ci-dessus, sauf lorsque la personne concernée donne son consentement écrit ou lorsque le traitement est nécessaire pour empêcher un danger imminent ou l'atténuation d'une infraction pénale spécifique, ne peut être effectué que sous l'autorité d'un professionnel de santé.

(b) Dans ce cas, le professionnel de santé et ses mandataires sont soumis à l'obligation de confidentialité.

(4)

(a) Sans préjudice de l'application des Articles 16 à 19, le traitement de données à caractère personnel se rapportant à la vie sexuelle est autorisé s'il est effectué par une association dotée de la personnalité juridique ou par une organisation d'intérêt public dont le principal objectif, selon ses statuts, est l'évaluation, les conseils et le traitement de personnes dont la conduite sexuelle peut être qualifiée d'infraction, et qui a été reconnue et subventionnée pour la réalisation de cet objectif par l'organisme public compétent. Aux fins de ce traitement, dont l'objectif doit englober l'évaluation, les conseils et le traitement des personnes visées au présent paragraphe, et pour lequel le traitement de données à caractère personnel, s'il concerne la vie sexuelle, ne se rapporte qu'aux personnes susmentionnées, l'organisme public compétent doit accorder une autorisation individualisée spécifique, après avoir reçu l'avis de l'Autorité.

(b) Le consentement visé au paragraphe précédent (a) peut être retiré à tout moment par la personne concernée, sans indiquer de motif et sans frais;

(c) L'Autorité peut déterminer les cas dans lesquels l'interdiction de traiter les données, visée au présent article, ne peut pas être levée même avec le consentement de la personne concernée.

(2) Le paragraphe (1) qui précède ne s'applique pas lorsque:

(a) le traitement est nécessaire pour remplir les obligations et les droits spécifiques du contrôleur dans le domaine du droit du travail; ou

(b) le traitement est nécessaire pour se conformer aux lois relatives à la sécurité sociale; ou

(c) le traitement est nécessaire à la promotion et à la protection de la santé publique, y compris les examens médicaux de la population; ou

(d) le traitement est exigé par ou en vertu d'une loi ou d'un texte législatif équivalent pour des raisons d'intérêt public substantiel; ou

(e) le traitement est nécessaire pour protéger les intérêts vitaux de la personne concernée ou d'une autre personne, lorsque la personne concernée est physiquement ou légalement incapable de donner son consentement ou n'est pas représentée par son représentant légal, judiciaire ou convenu; ou

(f) le traitement est nécessaire à la prévention d'un danger imminent ou à l'atténuation d'une infraction pénale spécifique; ou

(g) le traitement se rapporte à des données qui ont apparemment été rendues publiques par la personne concernée; ou

(h) le traitement est nécessaire à l'établissement, à l'exercice ou à la défense de droits légaux; ou

(i)

(i.) le traitement est requis aux fins de la recherche scientifique.

(ii.) L'Autorité établit les conditions que ce traitement doit remplir.

Titre V

ou

(j) le traitement est nécessaire aux fins de la médecine préventive ou du diagnostic médical, de la fourniture de soins ou de traitement à la personne concernée ou à l'un de ses parents [à déterminer par l'Etat donné], ou de la gestion de services de soins de santé dans l'intérêt de la personne concernée, et lorsque les données sont traitées sous la surveillance d'un professionnel de santé;

(3)

(a) Les données à caractère personnel liées à la santé ne peuvent être traitées que sous la responsabilité d'un professionnel en soins de santé, sauf si la personne concernée a donné son consentement écrit ou si le traitement est nécessaire à la prévention d'un danger imminent ou à l'atténuation d'une infraction pénale spécifique.

(b) Les données à caractère personnel liées à la santé doivent être collectées auprès de la personne concernée.

(4) L'Autorité est en droit de spécifier les conditions sous lesquelles ce traitement peut être effectué.

(5) Elles ne peuvent être collectées à partir d'autres sources que si les paragraphes (3) et (4) ci-dessus sont respectés et si cela est nécessaire aux fins du traitement, ou si la personne concernée est incapable de fournir les données.

(6) Pour tout traitement visé au présent article, le professionnel de santé et ses mandataires sont soumis à l'obligation de confidentialité.

17. (1) Dans le champ d'application des Articles 15 (2) (i), 16 (2) (c) et 16 (2) (j), le traitement des données génétiques et des données à caractère personnel concernant la santé, si elles sont traitées pour ce qu'elles révèlent ou contiennent, exige la remise préalable au patient d'un identifiant unique, qui doit être différent de tout autre numéro d'identification, par l'autorité publique établie par la loi à cette fin.

(2) L'interconnectivité de cet identifiant unique de patient avec tout autre identifiant que peut permettre la personne concernée au sens de l'Article 1 (9) ne sera possible qu'avec l'autorisation de l'Autorité.

18. (1) Le traitement de données à caractère personnel se rapportant à des litiges qui ont été présentés devant des cours et des tribunaux ainsi que devant des organismes administratifs ou judiciaires, se rapportant à des présomptions, des poursuites ou des condamnations en matière de crime, de sanctions administratives ou de mesures de sécurité, est interdit, sauf si le traitement est effectué:

(a) sous la surveillance d'un organisme public ou d'un fonctionnaire ministériel tel que défini par la loi [de l'Etat donné] et si le traitement est nécessaire pour remplir ses fonctions; ou

(b) par d'autres personnes, si le traitement est nécessaire pour réaliser les objectifs qui ont été établis par la loi; ou

(c) par des personnes physiques ou des personnes juridiques privées ou publiques, dans la mesure où le traitement est nécessaire pour gérer leurs litiges; ou

(d) par des avocats ou d'autres conseillers juridiques, dans la mesure où le traitement est nécessaire à la protection des intérêts de leurs clients; ou

Titre V

(e) si le traitement effectué est nécessaire à la recherche scientifique. L'Autorité établit les conditions à suivre pour ce traitement.

(2) Les personnes autorisées aux termes du présent article pour traiter ces données à caractère personnel sont soumises à une obligation de confidentialité.

(3) L'Autorité devra établir les conditions spécifiques à remplir lors du traitement des données à caractère personnel visées au présent article.

19. Le traitement de données à caractère personnel d'un enfant est subordonné au respect des règles de représentation visées à l'Article 37.

20. (1) L'Autorité peut fixer des exceptions au présent chapitre, à l'Article 21 et l'Article 22 et au Chapitre 7 lorsque le traitement est conduit par une personne légalement soumise à une obligation de confidentialité de par la nature de sa fonction.

(2) Le paragraphe (1) ci-dessus ne s'applique pas au client/patient d'une personne à qui une telle exception s'applique.

Titre VI

TITRE VI: DEVOIRS DU CONTRÔLEUR DE DONNÉES ET DU RESPONSABLE DU TRAITEMENT DES DONNÉES

Informations

21. (1) Lorsque des données à caractère personnel se rapportant à la personne concernée sont obtenues directement auprès d'elle, le contrôleur ou son représentant fourniront simultanément à la personne concernée au moins les informations suivantes, sauf si la personne concernée a déjà reçu de telles informations:

(a) le nom et l'adresse du contrôleur et de son représentant, le cas échéant;

(b) les objectifs du traitement;

(c) l'existence du droit d'objection, par voie de requête et sans frais, au traitement prévu des données à caractère personnel la concernant, si elles sont obtenues aux fins du marketing direct;

(d) l'obligation éventuelle de conformité avec la demande d'informations, ainsi qu'une indication des conséquences de la non-conformité;

(e) en fonction des circonstances spécifiques dans lesquelles les données sont collectées, toute information complémentaire, s'il est nécessaire d'assurer un traitement juste pour la personne concernée, telle que:

(i.) les destinataires ou les catégories de destinataires des données;

(ii.) l'obligation éventuelle de répondre et les conséquences possibles de la non-réponse;

(iii.) l'existence du droit d'accès et de rectification des données à caractère personnel la concernant, sauf lorsque ces informations supplémentaires, compte tenu des circonstances spécifiques dans lesquelles les données sont collectées, ne sont pas nécessaires pour garantir le traitement correct eu égard à la personne concernée.

(f) d'autres informations en fonction de la nature spécifique du traitement, comme spécifié par l'Autorité.

22. (1) Lorsque les données à caractère personnel ne sont pas recueillies auprès de la personne concernée elle-même, le contrôleur ou son représentant doit lui fournir au moins les informations ci-dessous lors de l'enregistrement des données à caractère personnel ou s'il est envisagé de les communiquer à une tierce partie, et ce au plus tard lorsque les données sont divulguées pour la première fois, sauf si la personne concernée a déjà reçu de telles informations:

(a) le nom et l'adresse du contrôleur et de son représentant, le cas échéant;

(b) les objectifs du traitement;

(c) l'obligation éventuelle de conformité avec la demande d'informations, ainsi qu'une indication des conséquences de la non-conformité;

(d) l'existence du droit d'objection, par voie de requête et sans frais, au traitement prévu de données à caractère personnel la concernant, si elles sont obtenues aux fins du marketing direct; dans ce cas, la personne concernée doit être informée avant la première divulgation à une tierce partie des données à caractère personnel ou avant la première utilisation des données aux fins du marketing direct pour le compte de tierces parties;

(e) en fonction des circonstances spécifiques dans lesquelles les données sont collectées, toute information complémentaire, s'il est nécessaire d'assurer un traitement juste pour la personne concernée, telle que:

Titre VI

(i.) les catégories de données concernées,

(ii.) les destinataires ou les catégories de destinataires des données;

(iii.) l'existence du droit d'accès et de rectification des données à caractère personnel la concernant, sauf lorsque ces informations supplémentaires, compte tenu des circonstances spécifiques dans lesquelles les données sont collectées, ne sont pas nécessaires pour garantir le traitement juste eu égard à la personne concernée.

(f) d'autres informations spécifiées par l'Autorité en fonction de la nature spécifique du traitement.

(2) Le paragraphe (1) qui précède ne s'applique pas:

(a) s'il se révèle impossible d'informer la partie concernée ou si cela implique un effort disproportionné, notamment pour les données recueillies à des fins de statistiques ou aux fins de la recherche historique ou scientifique, ou pour les besoins de l'examen médical de la population en vue d'assurer la protection ou la promotion de la santé publique;

ou

(b) si les données à caractère personnel sont enregistrées ou fournies en vue de l'application d'une disposition stipulée par ou en vertu d'une loi, d'un décret ou d'une ordonnance.

(3) L'Autorité établira les conditions pour l'application du présent paragraphe.

Autorité en matière de traitement

23. Toute personne ayant accès aux données à caractère personnel et agissant sous l'autorité du contrôleur ou du responsable du traitement, tout comme le responsable du traitement lui-même, est tenue de suivre les instructions du contrôleur pour traiter les données à caractère personnel, sans préjudice de tout devoir imposé par la loi.

(2) Le paragraphe 1 ne s'applique pas lorsque l'utilisateur du service agit sous l'autorité ou le contrôle de l'hébergeur.

(3) Si l'hébergeur retire le contenu après avoir reçu une injonction conforme au paragraphe 1, il est exempté de l'obligation contractuelle auprès de son client d'assurer la disponibilité du service.

Sécurité

24. (1)

(a) Afin d'assurer la sécurité des données à caractère personnel, le contrôleur ou son représentant, le cas échéant, ainsi que le responsable du traitement, doivent prendre les mesures techniques et organisationnelles appropriées qui sont nécessaires pour protéger les données à caractère personnel contre la destruction fautive et non autorisée, la perte fautive, ainsi que l'altération, l'accès et tout autre traitement non autorisé des données à caractère personnel.

(b) Ces mesures doivent assurer un niveau de sécurité approprié, compte tenu du stade de développement technologique dans ce domaine et du coût de la mise en œuvre des mesures d'un côté, et de la nature des données à protéger ainsi que des risques potentiels de l'autre.

(c) L'Autorité peut émettre des normes appropriées relatives à la sécurité des informations pour toutes les catégories de traitement ou certaines d'entre elles.

Titre VI

(2) Le contrôleur de données doit choisir, aux fins de tout traitement effectué pour son compte, un responsable du traitement des données qui donne suffisamment de garanties relatives aux mesures de sécurité techniques et organisationnelles concernant le traitement à effectuer et doit assurer le respect de ces mesures.

(3)

(a) Tout recours au responsable du traitement de données doit être régi par un contrat ou par toute autre loi qui lie le responsable du traitement des données au contrôleur de données.

(b) Le contrat ou le texte législatif doit établir:

(i.) que le responsable du traitement des données agit uniquement sur instruction du contrôleur de données;

(ii.) que le responsable du traitement des données doit aussi s'acquitter des obligations énoncées au paragraphe (1) précédent.

25. (1) Le contrôleur de données ou son représentant doit notifier à l'Autorité, sans retard excessif, toute violation de la sécurité affectant les données à caractère personnel.

(2) Le responsable du traitement des données doit notifier au contrôleur de données, sans retard excessif, toute violation de la sécurité affectant les données à caractère personnel qu'il traite pour le compte du contrôleur de données.

Obligation de notification à l'Autorité

26. (1)

(a) Avant toute opération ou série d'opérations entièrement ou partiellement automatisées destinées à servir un objectif unique ou plusieurs objectifs liés, le contrôleur ou son représentant, le cas échéant, doit le notifier à l'Autorité.

(b) Toute modification des informations données conformément à l'Article 27 doit être notifiée à l'Autorité.

(2) Le paragraphe (1) précédent ne s'applique pas aux opérations dont le seul objectif est de tenir un registre destiné à fournir des informations au public en vertu d'une loi, d'un décret ou d'une ordonnance et qui est ouvert pour consultation soit par le public, soit par toute personne démontrant un intérêt légitime.

(3) L'Autorité peut exonérer certaines catégories de la notification au titre du présent article si:

(a) compte tenu des données en cours de traitement, il n'y a pas de risque apparent d'atteinte aux droits et libertés de la personne concernée, et si les objectifs du traitement, les catégories de données en cours de traitement, les catégories de personnes concernées, les catégories de destinataires et la période de conservation des données sont spécifiés.

(b)

(i.) Le contrôleur des données a désigné un responsable de la protection des données.

(ii.) La désignation du responsable de la protection des données doit être notifiée à l'Autorité.

(iii.) Le responsable de la protection des données:

- doit être une personne dotée des qualifications requises pour exercer ses fonctions;

- doit tenir une liste du traitement effectué, qui soit immédiatement accessible à toute personne présentant une demande d'accès, et ne peut pas être sanctionné par son employeur du fait de l'exercice de ses fonctions.

(iv.) Il peut formuler une demande auprès de l'Autorité lorsqu'il rencontre des difficultés dans l'exercice de ses fonctions.

(v.) En cas de non-conformité avec les dispositions de la présente loi type, l'Autorité ordonne au contrôleur de données d'accomplir les formalités indiquées au paragraphe précédent (1).

(vi.) En cas de non-respect de ses devoirs, le représentant sera démis de ses fonctions à la demande de l'Autorité ou après consultation de celle-ci.

(vii.) L'Autorité établit les règles spécifiques définissant la fonction du responsable de la protection des données.

(4) Si l'exonération du devoir de notification a été accordée pour le traitement automatique conformément au paragraphe précédent, le contrôleur des données doit divulguer, à toute personne qui en fait la demande, les éléments d'informations mentionnés à l'Article 27.

(5) Le traitement exécuté par les autorités publiques ne peut pas bénéficier de l'exonération de notification établie par le paragraphe (3).

Contenu de la notification

27. (1) La notification doit mentionner au moins:

(a) la date de notification et la loi, le décret, l'ordonnance ou l'acte réglementaire permettant le traitement automatique, le cas échéant;

(b) le nom de famille, les prénoms et l'adresse complète ou le nom et le siège social du contrôleur et de son représentant, le cas échéant;

(c) l'appellation du traitement automatique;

(d) l'objectif ou l'ensemble d'objectifs liés au traitement automatique;

(e) les catégories de données personnelles traitées et une description détaillée des données visées aux Articles 7 à 11;

(f) une description de la catégorie ou des catégories de personnes concernées;

(g) les sauvegardes qui doivent être liées à la divulgation des données aux tierces parties;

(h) la manière dont les personnes concernées sont informées, le service permettant l'exercice du droit d'accès et les mesures prises pour faciliter l'exercice de ce droit;

(i) les interconnexions prévues ou toute autre forme de lien avec un autre traitement;

(j) le délai après lequel les données ne peuvent plus être stockées, utilisées ou divulguées;

(k) une description générale contenant une évaluation préliminaire de la pertinence des mesures de sécurité prises en vertu du Chapitre 6, Article 3 ci-dessus;

(l) le recours à un responsable du traitement de données;

(m) les transferts de données vers un pays tiers comme prévu par le contrôleur de données;

(2) L'Autorité peut préciser d'autres informations qui doivent être mentionnées dans la notification.

Titre VI

(3) Lorsque l'Autorité estime que le traitement ou le transfert de données par un contrôleur de données implique des risques spécifiques pour les droits à la vie privée des personnes concernées, elle peut examiner et évaluer les mesures de sécurité avant le début du traitement ou du transfert.

(4) L'Autorité peut, à tout moment raisonnable durant les heures ouvrées, procéder à des examens et une évaluation plus approfondis des mesures de sécurité imposées à un contrôleur de données.

Autorisation

28. (1) L'Autorité établit les catégories de traitement qui représentent des risques spécifiques vis-à-vis des droits fondamentaux de la personne concernée et qui exigent une autorisation de l'Autorité.

(2) Cette autorisation est donnée après réception de la notification du contrôleur de données ou du responsable de la protection des données qui, en cas de doute, doit demander conseil à l'Autorité.

Transparence du traitement

29. (1)

(a) L'Autorité tient un registre de toutes les opérations de traitement automatique des données à caractère personnel.

(b) Toute écriture dans le registre doit inclure les informations mentionnées à l'Article 27.

(c) La consultation du registre par tous les membres du public s'effectue d'une manière déterminée par l'Autorité.

(2) Dans le cas du traitement exonéré de notification par la présente loi type, l'Autorité peut, par vertu de son mandat ou à la demande de la personne concernée, imposer au contrôleur l'obligation de divulguer à la personne concernée tout ou partie des informations mentionnées à l'Article 27.

Responsabilité

30. (1) Le contrôleur de données doit:

(a) prendre toutes les mesures nécessaires pour respecter les principes et les obligations énoncés dans la présente loi type, y compris les Chapitres 4 et 5.

et

(b) avoir mis en place les mécanismes internes nécessaires pour démontrer ce respect tant aux personnes concernées qu'à l'Autorité dans l'exercice de ses pouvoirs.

Titre VII

TITRE VII: DROITS DE LA PERSONNE CONCERNÉE

Droit d'accès

31. (1) Toute personne concernée qui prouve son identité a le droit d'obtenir, sans explication et sans frais, de la part du contrôleur ou de son représentant, le cas échéant:

(a) des informations sur l'existence d'un traitement éventuel des données qui la concernent, ainsi que des informations relatives aux objectifs du traitement, aux catégories de données auxquelles le traitement se rapporte et aux catégories de destinataires auxquels les données sont divulguées;

(b) la communication sous une forme intelligible des données qui sont traitées ainsi que de toute source d'information disponible;

(c) des informations sur la logique de base impliquée dans tout traitement automatique de données la concernant dans le cas d'une prise de décision automatisée;

(d) des informations concernant son droit de déposer des plaintes au titre du présent chapitre et son droit de consulter le registre visé à l'Article 29, si nécessaire.

(2)

(a) Pour obtenir ces informations, la personne concernée devra présenter au contrôleur ou au responsable de la protection des données une demande signée et datée.

(b) L'Autorité sera habilitée à spécifier d'autres conditions pour l'application du présent paragraphe (2) (a).

(3)

(a) Lorsque les données à caractère personnel sensibles sont traitées aux fins de la recherche scientifique, qu'il n'y a pas de risque évident d'atteinte au droit de la personne concernée à la protection de sa vie privée et que les données ne sont pas utilisées afin de prendre des mesures et des décisions affectant un individu, le fait d'informer la personne concernée peut être reporté au plus tard jusqu'au moment où la recherche prend fin, mais seulement dans la mesure où informer la personne concernée compromettrait gravement la recherche.

(b) Dans ce cas, la personne concernée doit avoir donné au contrôleur de données son consentement écrit préalable au traitement des données à caractère personnel qui la concernent à des fins de recherche scientifique et au report, pour cette raison, du moment auquel elle est informée.

(4) La renonciation au paiement de frais en vertu du paragraphe (1) ci-dessus peut être refusée par le contrôleur de données en cas d'utilisation indue de la demande par la personne concernée.

(5) La décision du contrôleur de données peut faire l'objet d'une plainte adressée à l'Autorité par la personne concernée, conformément à l'Article 4.

Droit de rectification, de radiation et de limitation temporaire d'accès

32. (1)

(a) La personne concernée a le droit, selon le cas et sans frais, de rectification et de radiation des données à caractère personnel la concernant ou de limitation temporaire d'accès à ces données à caractère personnel si le traitement n'est pas en conformité avec la présente loi type, notamment si les données à caractère personnel ne sont pas complètes ou exactes.

Titre VII

(b) Toute personne a aussi le droit d'obtenir sans frais la radiation de ou l'interdiction d'utiliser toutes les données à caractère personnel la concernant qui sont incomplètes ou non pertinentes en vue du traitement ou lorsque l'enregistrement, la divulgation ou le stockage des données est interdit, ou lorsqu'elles ont été stockées pendant une durée plus longue que la période de temps autorisée.

(2) La personne concernée a le droit d'obtenir du contrôleur la notification à des tierces parties auxquelles les données ont été divulguées de toute rectification, radiation ou limitation temporaire en vertu du paragraphe (1), sauf si cela se révèle impossible ou implique un effort disproportionné.

(3) La gratuité en vertu du paragraphe (1) peut être refusée par le contrôleur de données en cas de mauvaise utilisation de la demande par la personne concernée.

(4) La décision du contrôleur de données peut faire l'objet d'une plainte adressée à l'Autorité par la personne concernée conformément à l'Article 6.

Droit d'objection

33. (1) La personne concernée est en droit:

(a)

(i.) de faire objection, à tout moment et sans frais, pour des motifs légitimes impérieux se rapportant à sa situation particulière (telle qu'une procédure judiciaire), au traitement de données la concernant, sauf si la légalité du traitement est basée sur les raisons visées aux Articles 14(1) (a), 14(1) (b), 15(2) (a), 15(2) (d), 15 (2) (j), 16(2) (a), 16(2) (b) et 17(2) (d).

(ii.) Lorsqu'il existe une objection justifiée, le traitement en question ne peut plus porter sur ces données;

ou

(b) d'être informée avant que les données à caractère personnel ne soient divulguées pour la première fois à des tierces parties ou avant qu'elles n'aient été utilisées pour leur compte aux fins du marketing direct, et qu'il leur soit expressément offert le droit de faire objection sans frais à cette divulgation ou utilisation.

(2) La renonciation au paiement de frais en vertu du paragraphe (1) peut être refusée par le contrôleur en cas d'utilisation indue de la demande par la personne concernée.

(3) La décision du contrôleur de données peut faire l'objet d'une plainte adressée à l'Autorité par la personne concernée conformément à l'Article 6.

Retards

34. Le contrôleur de données doit donner une réponse à la demande de la personne concernée dans un délai de 45 jours. Sinon, une plainte peut être adressée à l'Autorité.

Pouvoir d'édicter des règlements

35. L'Autorité peut spécifier d'autres règles relatives à l'exercice du droit visé aux Articles 31 à 33.

Décision prise exclusivement sur la base du traitement automatique des données

36. (1) Une décision ayant des effets juridiques sur une personne ou l'affectant de manière importante ne doit pas être prise sur la seule base du traitement automatique des données dans le but d'évaluer certains aspects de sa personnalité.

(2) L'interdiction visée au paragraphe (1) n'est pas applicable si la décision est prise dans le contexte d'un accord ou est basée sur une disposition établie par ou en vertu de la loi. Cet accord ou cette disposition doit contenir des mesures appropriées pour sauvegarder les intérêts légitimes de la personne concernée définie par sa loi nationale ou par une convention internationale. Il convient de donner à la personne concernée l'opportunité de défendre efficacement son point de vue.

Représentation de la personne concernée

37. (1) Si la personne concernée est un enfant, ses droits, en vertu de la présente loi type, peuvent être exercés par ses parents ou un tuteur légal, sauf si la loi prescrit que l'enfant peut agir par lui-même sans être représenté par ses parents ou son tuteur légal.

(2) Suivant son âge et sa capacité, il peut être associé à l'exercice de ses droits.

38. (1)

(a) d'être informée avant que les données à caractère personnel ne soient divulguées pour la première fois à des tierces parties ou avant qu'elles n'aient été utilisées pour leur compte aux fins du marketing direct, et qu'il leur soit expressément offert le droit de faire objection sans frais à cette divulgation ou utilisation.

(b) Si cette personne ne veut pas accepter les frais ou si elle est en défaut de paiement, les droits sont exercés, en séquence ultérieure, par un enfant qui est majeur, un parent, un frère ou une sœur de la personne concernée et qui sont majeurs.

(2)

(a) Si cette personne n'accepte pas les frais ou est en défaut de paiement, un tuteur spécifique désigné par le tribunal compétent exercera les droits de la personne concernée.

(b) Cela est valable aussi en cas de conflit entre deux ou plusieurs personnes mentionnées au paragraphe 1.

(3) Dans la mesure du possible, il convient de tenir compte de la capacité de la personne concernée pour l'associer à l'exercice de ses droits.

TITRE VIII: RECOURS À L'AUTORITÉ JUDICIAIRE

Recours à l'autorité judiciaire

39. Sous réserve de l'épuisement de l'appel offert par l'intermédiaire de l'Autorité au titre de la présente loi, la personne concernée sera habilitée à interjeter des appels légaux auprès des autorités judiciaires compétentes.

40. Le législateur mettra en place un système d'action de groupe (ou de recours collectif) pour aider la personne concernée dans l'exercice de ses droits établis au titre de la présente loi type.

Titre IX

TITRE IX: SANCTIONS

Sanctions

41. (1) Tout membre, permanent ou suppléant, collaborateur, conseiller, entrepreneur ou autre membre du personnel de l'Autorité ou tout expert qui a violé l'obligation du secret visé dans la présente loi type sera passible du paiement d'une amende de (…).

(2) Tout contrôleur de données, son représentant, mandataire ou cessionnaire qui ne se conforme pas aux obligations prescrites aux Articles 24 à 25, sera passible d'une amende de (…).

(3) Une amende de (….) à (…) sera imposée à:

(a) tout contrôleur, son représentant, mandataire ou cessionnaire traitant des données à caractère personnel en violation des conditions imposées par les Articles 11(1), 12 et 13;

(b) tout contrôleur, son représentant, mandataire ou cessionnaire traitant des données à caractère personnel dans des cas autres que ceux mentionnés à l'Article 14;

(c) tout contrôleur, son représentant, mandataire ou cessionnaire traitant des données à caractère personnel en violation des Articles 15 à 19;

(d) tout contrôleur, son représentant, mandataire ou cessionnaire n'ayant pas communiqué les informations visées à l'Article 31(1) dans les (…) jours à compter de la réception de la demande, ou qui, en connaissance de cause, communique des informations incorrectes ou incomplètes;

(e) toute personne qui recourt à des actes de violence, à la force, à des menaces, des dons ou des promesses aux fins d'obliger une autre personne à divulguer des informations qui sont obtenues par l'exercice du droit défini à l'Article 31(1), ou aux fins d'obtenir le consentement de l'autre personne pour le traitement de données à caractère personnel se rapportant à cette personne;

(f) tout contrôleur, son représentant, mandataire ou cessionnaire ayant commencé, géré, continué de gérer ou terminé le processus automatique de données à caractère personnel sans satisfaire aux exigences de l'Article 26;

(g) tout contrôleur, son représentant, mandataire ou cessionnaire ayant communiqué des informations incomplètes ou incorrectes dans les notifications imposées par l'Article 27;

(h) tout contrôleur, son représentant, mandataire ou cessionnaire qui, en violation de l'Article 29(2), refuse de communiquer à l'Autorité les informations demandées;

(i) toute personne qui transfère des données à caractère personnel ou pour laquelle des données à caractère personnel sont transférées vers un pays en dehors de la Communauté de développement d'Afrique australe (SADC) inclus dans la liste visée à l'Article 44(2), ou toute personne qui autorise ces transferts en dépit des dispositions de l'Article 45;

(j) toute personne qui empêche l'Autorité, ses membres ou ses experts de donner suite à l'enquête visée à l'Article 4.

(4) En cas de condamnation pour l'une quelconque des infractions décrites au présent article, le Tribunal ordonnera la publication entière ou partielle du jugement dans un ou plusieurs journaux de la manière qu'il déterminera et aux frais de la personne reconnue coupable.

Titre IX

(5)

(a) En cas de condamnation pour l'une quelconque des infractions décrites au présent article, le juge peut prononcer la saisie des supports contenant les données à caractère personnel auxquelles l'infraction a trait, tels que les systèmes de classement manuels, les disques magnétiques ou les rubans magnétiques, à l'exception des ordinateurs ou de tout autre équipement, ou il peut ordonner la radiation des données.

(b) La saisie ou la radiation peuvent aussi être ordonnés même si les supports contenant les données à caractère personnel n'appartiennent pas à la personne reconnue coupable.

(c) Les objets saisis devront être détruits lorsque le jugement deviendra définitif.

(6) Le présent article n'empêchera pas l'adoption de toute mesure d'indulgence établie par la loi, comme la suspension ou une peine avec sursis, sauf pour les décisions visées aux paragraphes (4) et (5) ci-dessus.

(7) Sans préjudice de la révocation des compétences stipulées dans des dispositions particulières, le Tribunal peut, dans le cadre d'une condamnation pour une infraction mentionnée au présent article, imposer une interdiction de gérer tout traitement de données à caractère personnel, directement ou par un intermédiaire, pour une durée maximale de [....] ans.

(8) Toute violation de l'interdiction présentée au paragraphe 7 ci-dessus ou toute récidive se rapportant aux infractions visées au présent article sera punie d'une peine d'emprisonnement de […] mois à [….] an et/ou d'une amende de […..] à […].

(9) Le contrôleur ou son représentant sera passible du paiement des amendes encourues par son mandataire ou son cessionnaire.

Titre X

TITRE X: LIMITATIONS

Limitations

42. (1) Les Etats Membres peuvent prendre des dispositions pour limiter les obligations et les droits visés aux Articles 11 (1), 12 et 13, aux Articles 21 et 22 et aux Articles 31, 32 et 33, lorsque cette limitation est nécessaire pour préserver:

(a) la sécurité de l'Etat;

(b) la défense;

(c) la sécurité publique (y compris le bien-être ou l'intérêt de l'Etat lorsque l'opération de traitement a trait aux questions de sécurité de l'Etat);

(d) la prévention, l'investigation ou la preuve d'infractions pénales, la poursuite de délinquants ou l'exécution de sentences pénales ou de mesures de sécurité ou la violation de codes de conduite professionnels dans le cas d'une profession réglementée.

(e) un suivi, un examen ou une tâche réglementaire lié, même occasionnellement, à l'exercice de l'autorité officielle dans les cas visés aux points (c) et (d).

(2)

(a) L'Article 11 (1) (c), les Articles 15, 18, 21, 22, 26, 31 et 32 et le Chapitre 11 ne s'appliquent pas au traitement de données à caractère personnel effectué à la seule fin:

- de l'expression littéraire et artistique;

et

- du journalisme professionnel, conformément aux règles éthiques de cette profession.

(b) Toutefois, s'agissant du traitement mentionné au paragraphe (2) ci-dessus, l'exonération de l'obligation de faire une déclaration prévue à l'Article 26 est subordonnée à la désignation, par un contrôleur de données, d'un responsable de la protection des données qui appartient à une entreprise de médias, qui tient un registre du traitement effectué par le contrôleur de données et qui assure de façon indépendante l'application correcte des dispositions de la présente loi type. Cette désignation doit être notifiée à l'Autorité conformément à l'Article 26.

(c) En cas de non-conformité avec les dispositions de la présente loi type qui s'appliquent au traitement prévu au présent article, l'Autorité ordonnera au contrôleur de données d'assurer la conformité de toutes ces questions avec la présente loi type. En cas de manquement à ses obligations, le responsable est démis de ses fonctions à la demande ou après consultation de l'Autorité.

(3) Les dispositions des paragraphes précédents n'empêcheront pas l'application des dispositions du [Code civil, par exemple], des lois relatives aux médias et du Code pénal qui prescrivent les conditions de l'exercice du droit de réponse et qui empêchent, limitent, réparent et, au besoin, sanctionnent les violations de la vie privée et les attaques contre la réputation des particuliers.

Titre XI

TITRE XI: FLUX TRANSFRONTALIER

A un Etat membre qui a transposé la présente loi type

43. (1) Sans préjudice des Articles 11, 12, 13 et 17, les données à caractère personnel doivent uniquement être transférées aux destinataires soumis à la loi nationale adoptée pour la mise en œuvre de la présente loi type,

(a)

(i.) si le destinataire établit que les données sont nécessaires à l'accomplissement d'une tâche exécutée dans l'intérêt public ou soumise à l'exercice d'un organisme public, ou

(b)

(i.) si le destinataire établit la nécessité de faire transférer les données et s'il n'y a pas de raison de supposer que les intérêts légitimes de la personne concernée pourraient être lésés.

(ii.) Le contrôleur est tenu de vérifier la compétence du destinataire et d'évaluer provisoirement la nécessité du transfert des données. Si des doutes apparaissent quant à cette nécessité, le contrôleur doit chercher à obtenir d'autres informations auprès du destinataire.

(iii.) Le destinataire doit s'assurer que la nécessité du transfert des données peut être ultérieurement vérifiée.

(c) Le destinataire ne peut traiter les données à caractère personnel qu'aux fins pour lesquelles elles ont été transmises

A un Etat membre qui n'a pas transposé la présente loi type ou à un Etat non-membre

44. (1)

(a) Les données à caractère personnel ne peuvent être transférées aux destinataires, à l'exception des Etats Membres de la SADC, qui ne sont pas soumis à la loi nationale adoptée en vertu de la présente loi type, que si un niveau de protection adéquat est assuré dans le pays du destinataire ou au sein de l'organisation internationale destinataire et si les données sont transférées exclusivement pour permettre l'exécution des tâches relevant de la compétence du contrôleur.

(b) Le caractère adéquat du niveau de protection offert par le pays tiers ou par l'organisation internationale en question doit être évalué à la lumière de toutes les circonstances entourant une opération de transfert de données ou un semble d'opérations de transfert de données. Une attention particulière doit être prêtée à la nature des données, à l'objectif et à la durée de l'opération ou des opérations de traitement proposées, au pays tiers destinataire ou à l'organisation internationale destinataire, aux règles de droit, tant générales que sectorielles, en vigueur dans le pays tiers ou l'organisation internationale en question, aux règles professionnelles et aux mesures de sécurité qui sont respectées dans ce pays tiers ou cette organisation internationale.

(2) L'Autorité stipulera les catégories d'opérations de traitement et les circonstances dans lesquelles le transfert de données à caractère personnel vers des pays en dehors de la SADC n'est pas autorisé.

45. (1) A titre de dérogation de l'Article 46, un transfert ou un ensemble de transferts de données à caractère personnel vers un pays en dehors de la SADC qui n'assure pas un niveau de protection adéquat peut avoir lieu dans l'un des cas suivants:

(a) la personne concernée a donné son consentement sans ambiguïté au transfert proposé;

(b) le transfert est nécessaire à l'exécution d'un contrat entre la personne concernée et le contrôleur ou à la mise en place de mesures précontractuelles prises en réponse à la demande de la personne concernée;

(c) le transfert est nécessaire à la conclusion ou à l'exécution d'un contrat conclu ou devant être conclu entre le contrôleur et une tierce partie dans l'intérêt de la personne concernée;

(d) le transfert est nécessaire ou légalement exigé pour des motifs d'intérêt public importants ou pour l'établissement, l'exercice ou la défense de réclamations légales;

(e) le transfert est nécessaire afin de protéger les intérêts vitaux de la personne concernée;

(f) le transfert est effectué à partir d'un registre qui, conformément aux lois ou aux règlements, est destiné à fournir des informations au public et qui peut être consulté soit par le public en général, soit par toute personne pouvant démontrer un intérêt légitime, dans la mesure où les conditions concernant la consultation, prévues par la loi, sont remplies dans le cas présent.

(2) Sans préjudice des dispositions du paragraphe précédent, l'Autorité peut autoriser un transfert ou un ensemble de transferts de données à caractère personnel vers un pays en dehors de la SADC qui n'assure pas un niveau de protection adéquat, si le contrôleur assure des sauvegardes adéquates eu égard à la protection de la vie privée, des droits fondamentaux et des libertés fondamentales des individus, et en ce qui concerne l'exercice des droits correspondants; ces sauvegardes peuvent notamment découler de clauses contractuelles appropriées.

TITRE XII: CODE DE CONDUITE

Code de conduite

46. (1) La présente loi type encourage l'élaboration de codes de conduite destinés à contribuer à la mise en œuvre correcte des dispositions nationales adoptées par les Etats Membres en vertu de la présente loi type, en tenant compte des caractéristiques spécifiques des divers secteurs.

(2) Les Etats Membres doivent prendre des dispositions relatives aux associations commerciales et autres organismes représentant d'autres catégories de contrôleurs qui ont élaboré des projets de codes nationaux ou qui ont l'intention de modifier ou d'étendre des codes nationaux existants pour pouvoir les soumettre à l'avis de l'Autorité.

(3) Les Etats Membres doivent prendre des dispositions pour que cette autorité vérifie, entre autres, si les projets de documents qui lui sont soumis sont conformes aux dispositions nationales adoptées en vertu de la présente loi type. Si elle le juge approprié, l'autorité cherchera à connaître les avis des personnes concernées ou de leurs représentants.

Titre XIII

TITRE XIII: DÉCLENCHEMENT D'ALERTE ÉTHIQUE

Déclenchement d'alerte éthique

47. (1)

(a) L'Autorité établira des règles donnant l'autorisation concernant et régissant le système de déclenchement d'alerte éthique (ou dénonciation).

(b) L'Autorité établira des règles donnant l'autorisation concernant et régissant le système de déclenchement d'alerte éthique (ou dénonciation).

(i.) les principes de justice et de légalité et l'objectif du traitement;

(ii.) les principes liés à la proportionnalité comme à la limitation du champ d'application, l'exactitude des données qui seront traitées;

(iii.) le principe d'ouverture à respecter lors de la communication d'informations collectives et individuelles adéquates sur:

- le champ d'application et l'objectif du déclenchement d'alerte éthique (ou de dénonciation);
- le traitement des comptes rendus;
- les conséquences des comptes rendus justifiés et non justifiés;
- la façon d'exercer les droits d'accès, de rectification, de radiation ainsi que l'autorité compétente à laquelle une demande peut être adressée;
- la tierce partie qui peut recevoir des données à caractère personnel concernant l'informant et la personne qui est impliquée dans le champ d'application du compte-rendu (par exemple le service d'audit interne si le "responsable du compte rendu" a besoin de vérifier certains points).

La personne qui est impliquée sera informée dès que possible par le "responsable du compte rendu" de l'existence du compte rendu et des faits dont elle est accusée afin d'exercer les droits établis dans la présente loi type.

L'information de la personne impliquée peut être reportée dans des cas exceptionnels (par ex: risque de destruction des preuves).

(iv.) les règles techniques et organisationnelles;

(v.) les règles concernant les droits de la personne concernée, en spécifiant que le droit d'accès ne permet pas d'accéder aux données à caractère personnel liées à un tiers sans son consentement exprès et écrit;

(vi.) les règles de notification à l'Autorité.

Bureau de développement des télécommunications (BDT)
Union internationale des télécommunications
Place des Nations
CH-1211 Genève

E-mail: bdtmail@itu.int
www.itu.int/ITU-D/projects/ITU_EC_ACP/

Genève, 2013