

# REPUBLIQUE DE VANUATU

## PROJET DE LOI N° DE 2024 RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

### Exposé des motifs

Le présent projet de loi dispose de la protection des données à caractère personnel (“la Loi”).

Le gouvernement de Vanuatu a reconnu l’importance d’élaborer une législation détaillée pour empêcher l’emploi abusif de données personnelles à des fins de surveillance et d’autres pratiques d’intrusion qui pourraient empiéter sur les droits de tout un chacun. Le gouvernement reconnaît aussi la nécessité de régir le système et les agences d’identification et, à l’échelon international, de positionner le Vanuatu parmi les juridictions qui assurent un environnement sûr pour des données personnelles dans le contexte d’une économie numérique en plein essor.

La présente loi dispose de mesures de conduite, de protection et de respect relativement à des données à caractère personnel et garantit la confiance publique dans l’emploi de données personnelles.

Le projet de loi a pour objectifs :

- a) de contribuer au respect et à la protection des droits et libertés fondamentaux des personnes physiques et, tout particulièrement, leur droit au secret eu égard au traitement de leurs données personnelles ;
- b) de veiller à ce que le traitement de données personnelles au Vanuatu soit soumis aux lois et aux structures de gouvernance du Vanuatu et contribue à la protection des personnes physiques au Vanuatu ;
- c) de mettre en place un cadre institutionnel et juridique adapté pour garantir l’application et la supervision efficaces d’une loi nationale pour la protection de données à caractère personnel, comprenant des délits et des peines en conséquence ;
- d) d’établir des meilleures pratiques en matière de législation pour la protection des données à caractère personnel reconnues internationalement ; et
- e) d’assurer une protection pour ce qui est de recueillir, de partager et de traiter des données personnelles en conformité avec les conventions onusiennes et d’autres lois internationales.

**Le Premier Ministre**



## REPUBLIQUE DE VANUATU

# PROJET DE LOI NO.        DE 2024 RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

### Sommaire

<b>TITRE 1</b>	<b>DISPOSITIONS PRELIMINAIRES .....</b>	<b>3</b>
1	Définition .....	3
2	Application de la loi.....	6
3	Loi dominante .....	7
<b>TITRE 2</b>	<b>REGLES RELATIVES AU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL .....</b>	<b>8</b>
4	Règles générales relatives au traitement de données à caractère personnel.....	8
5	Fins légales pour un traitement de données à caractère personnel .....	10
6	Traitement de catégories particulières de données à caractère personnel.....	10
7	Traitement de données à caractère personnel d'un enfant ou autre personne vulnérable .....	12
8	Consentement.....	13
<b>TITRE 3</b>	<b>DROITS DU SUJET DE DONNEES.....</b>	<b>15</b>
9	Accès à des informations et à des données personnelles .....	15
10	Restriction sur le traitement de données personnelles .....	16
11	Rectification et effacement de données personnelles .....	17
12	Opposition au traitement de données personnelles.....	18
13	Droit d'un sujet de données à ne pas être soumis à un processus de prise de décision automatisé .....	18
14	Représentation du sujet de données .....	19

<b>TITRE 4</b>	<b>FLOTS DE DONNÉES TRANSFRONTALIERS.....</b>	<b>20</b>
15	Conditions applicables au transfert hors de la juridiction du Vanuatu .....	20
16	Protections préalablement au transfert hors de la juridiction du Vanuatu .....	20
17	Transfert transfrontalier dans des situations spécifiques .....	21
<b>TITRE 5</b>	<b>EXECUTION .....</b>	<b>22</b>
18	Communication de documents ou d'informations .....	22
19	Requête pour mandat .....	22
20	Octroi de mandat.....	23
21	Contenu d'un mandat.....	23
22	Prorogation d'un mandat .....	24
23	Effets d'un mandat.....	24
<b>TITRE 6</b>	<b>DELITS.....</b>	<b>26</b>
24	Non respect d'une disposition de la présente loi .....	26
25	Obtention et divulgation illicites de données à caractère personnel .....	26
26	Modification de données personnelles pour empêcher la divulgation à un sujet de données .....	26
27	Entrave aux pouvoirs d'entrée dans des locaux.....	26
28	Destruction ou falsification d'informations demandées par le Commissaire .....	26
29	Entrave ou obstruction dans l'exercice légal de pouvoirs .....	27
30	Défense de communiquer des informations, des registres et des données .....	27
<b>TITRE 7</b>	<b>DISPOSITIONS DIVERSES.....</b>	<b>28</b>
31	Règlements.....	28
32	Entrée en vigueur .....	28

# REPUBLIQUE DE VANUATU

## PROJET DE LOI NO. DE 2024 RELATIVE A LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Disposant de la protection des données à caractère personnel et de questions connexes.

Le Président de la République et le Parlement promulguent le texte qui suit.

### TITRE 1 DISPOSITIONS PRELIMINAIRES

#### 1 Définition

Dans la présente loi, sous réserve du contexte :

**anonymisation** désigne le processus de supprimer des informations identificatoires dans des données personnelles de façon à ce que le sujet des données ne puisse être identifié, que ce soit directement ou indirectement ;

**données biométriques** désigne des données personnelles obtenues à partir d'un traitement technique spécifique qui se rapportent aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique. Ces données peuvent servir à permettre ou à confirmer l'identification unique de cette personne physique, telles des images faciales ou des données dactyloscopiques ;

**enfant** désigne une personne de moins de 18 ans ;

**Commissaire** désigne le commissaire de la protection des données à caractère personnel nommé en vertu de l'article 22 de la loi No. de 2024 sur l'Autorité de la sécurité numérique ;

**violation de données** désigne une violation de la sécurité par n'importe quelle personne qui conduit, accidentellement ou illégalement, à la destruction, la perte, la modification, la communication non autorisée ou l'accès à des données personnelles qui sont transmises, mémorisées ou traitées autrement ;

**centre de données** désigne un dispositif (y compris un cloud) qui fournit un accès commun à des applications et des données à l'aide d'une infrastructure complexe de réseau, d'ordinateurs et de mémorisation ;

**contrôleur des données** désigne la personne physique ou morale, l'administration publique ou une autre organisation qui a, seule ou conjointement avec d'autres, un pouvoir décisionnel eu égard au traitement de données ;

**traitement de données** désigne n'importe quelle opération ou ensemble d'opérations effectuée(s) sur des données personnelles, telle(s) que la collecte, la mémorisation, la préservation, la modification, l'extraction, la communication, la mise à disposition, l'effacement ou la destruction de données personnelles ou l'exécution d'opérations logiques ou arithmétiques sur de telles données. Traitement de données inclut le traitement de données personnelles dans un système de classement ;

**processeur de données** désigne une personne physique ou morale, une administration publique ou une autre organisation qui traite des données personnelles pour le compte du contrôleur des données ;

**serveur de données** désigne un ordinateur ou une plateforme qui sert à mémoriser, sécuriser, gérer et traiter des données ;

**sujet de données** désigne la personne qui peut être identifiée, directement ou indirectement, via un identifiant tel qu'un nom, un numéro d'identification, des données de localisation ou d'autres données biométriques ;

**interlocuteur désigné** désigne un employé ou autre personne physique ou une personne morale désignée par le contrôleur des données ou un processeur ;

**cryptage** désigne le processus de convertir le contenu de données lisibles en une forme codée à l'aide de moyens techniques. Le contenu ne redevient lisible qu'en utilisant la bonne clé ;

**système de classement** désigne n'importe quel ensemble structuré de données qui sont accessibles ou récupérables suivant des critères spécifiques ;

**droits et libertés fondamentaux** désigne les droits et libertés fondamentaux prévus par le sous-article 5.1) de la Constitution de la République of Vanuatu;

**données génétiques** désigne toutes les données se rapportant aux caractéristiques génétiques d'une personne physique obtenues à partir de l'analyse ;

- a) d'un échantillon biologique de la personne concernée, en particulier analyse chromosomique, de l'ADN ou de l'ARN ; ou
- b) de tout autre élément permettant d'obtenir des informations équivalentes ;

**intérêt légitime** inclut, sans s'y limiter, n'importe quel intérêt d'ordre commercial, individuel ou sociétal d'un sujet de données, d'un processeur de données, d'un contrôleur de données ou d'une tierce partie ;

**données personnelles ou à caractère personnel** désigne toute information ou donnée, qu'elle soit portée dans un registre ou non, laquelle :

- a) se rapporte à un sujet de données ; ou
- b) permet de sélectionner un sujet de données ou d'interagir avec lui ;

**profilage** désigne n'importe quelle forme de traitement automatisé de données personnelles pour évaluer certains aspects personnels en rapport avec une personne physique de façon à analyser ou prédire des aspects concernant son rendement au travail, sa situation économique, son état de santé, ses préférences personnelles, ses intérêts, sa fiabilité, son comportement, sa localisation ou ses mouvements ;

**pseudonymisation** désigne le traitement de données personnelles de telle manière que ces données ne puissent plus être attribuées à un sujet de données spécifique sans avoir recours à des informations supplémentaires, si ces informations supplémentaires sont tenues à part et sujettes à des mesures techniques et organisationnelles pour s'assurer que les données personnelles ne sont pas attribuées à un sujet de données ;

**destinataire** désigne une personne physique ou morale, une administration publique, agence ou autre organisation à laquelle des données personnelles sont communiquées, et inclut une tierce partie ;

**catégories particulières de données personnelles** inclut ce qui suit :

- a) des données génétiques ou des données personnelles en rapport avec des délits, des poursuites pénales et des condamnations ;
- b) des données biométriques identifiant de manière unique une personne ; et

- c) des données personnelles se rapportant à l'origine raciale ou ethnique, à des opinions politiques, à l'adhésion à un syndicat, à des croyances religieuses ou autres, à la santé ou à la vie sexuelle ;

**tierce partie** désigne une personne physique ou morale, une administration publique, agence ou organisation distincte du sujet de données, du contrôleur de données, du processeur de données, de l'interlocuteur désigné et d'autres personnes qui :

- a) relèvent directement de l'autorité du contrôleur ou du processeur de données ; et
- b) sont autorisées à traiter des données à caractère personnel ;

**personne vulnérable** désigne une personne qui :

- a) pourrait avoir besoin de services d'aide sociale en raison de maladie mentale, d'un handicap ou retard de développement, d'un autre handicap, de son âge, d'une maladie ou de troubles émotifs ; et
- b) n'est pas ou pourrait ne pas être en mesure de s'occuper d'elle-même ou de se protéger contre un mal significatif ou une exploitation grave.

## 2 Application de la loi

- 1) La présente loi s'applique à ce qui suit :
  - a) au traitement de données personnelles dans les secteurs privé et public, que ce soit par des moyens automatisés ou non, indépendamment de la nationalité ou du lieu de domicile de la personne physique qui est l'objet du traitement de données à caractère personnel ;
  - b) au traitement de données personnelles ou de catégories particulières de telles données concernant des personnes vivantes et non pas des personnes décédées ;
  - c) au traitement de données personnelles dans la juridiction du Vanuatu ;
  - d) au traitement de données personnelles générées ou recueillies au Vanuatu, indépendamment du lieu où le traitement est effectué ; et

- e) au traitement de données personnelles de personnes physiques qui sont au Vanuatu par un contrôleur ou un processeur de données qui n'est pas établi au Vanuatu lorsque les activités de traitement se rapportent à :
  - i) l'offre de biens ou de services à ces personnes au Vanuatu, indépendamment de savoir si un paiement est exigé du sujet des données ; ou
  - ii) la surveillance du comportement de ces personnes au Vanuatu dans la mesure où leur comportement se déroule au Vanuatu.
- 2) La présente loi ne s'applique pas au traitement de données à caractère personnel effectué tout simplement pour des activités personnelles ou domestiques.

### **3 Loi dominante**

Si une disposition de la présente loi est incompatible avec une disposition de n'importe quelle autre loi, ce sont les dispositions de la présente loi qui l'emportent.



## **TITRE 2 REGLES RELATIVES AU TRAITEMENT DE DONNEES A CARACTERE PERSONNEL**

### **4 Règles générales relatives au traitement de données à caractère personnel**

- 1) Les contrôleurs et les processeurs de données doivent traiter des données à caractère personnel conformément aux règles suivantes :
  - a) des données à caractère personnel doivent être traitées :
    - i) en conformité avec les conditions requises de la présente loi; et
    - ii) de manière juste et transparente eu égard au sujet des données ;
  - b) des données à caractère personnel doivent être traitées à des fins explicites, spécifiées et légitimes et le traitement desdites données devrait servir à de telles fins et ne pas être incompatibles avec ces fins ;
  - c) des données à caractère personnel doivent être suffisantes, pertinentes, proportionnelles et non pas excessives par rapport aux fins auxquelles elles sont traitées, en tenant compte à la fois de la quantité et de la qualité des données personnelles en train d'être traitées ;
  - d) des données à caractère personnel doivent être exactes et, dans la mesure où tel est nécessaire, tenues à jour et toute mesure raisonnable doit être prise pour s'assurer que des données personnelles qui ne sont pas exactes compte tenu des fins auxquelles elles sont traitées, sont corrigées ou effacées sans tarder;
  - e) des données à caractère personnel doivent être conservées sous une forme qui permet l'identification des sujets de données pour la durée nécessaire, sans plus, pour les besoins pour lesquels les données en question sont traitées ; et
  - f) des données à caractère personnel doivent être traitées d'une manière qui garantit que des mesures de sécurité raisonnables et

appropriées sont prises contre tout traitement non autorisé ou illicite et contre tout accès, destruction, perte, utilisation, modification ou divulgation, accidentellement ou de façon non autorisée.

- 2) Aux fins d'application du sous-alinéa 1)a)ii), une donnée personnelle est traitée de manière juste si elle :
  - a) est traitée d'une manière à laquelle le sujet de données pourrait raisonnablement s'attendre ; et
  - b) n'est pas traitée d'une manière qui pourrait avoir un effet défavorable infondé sur le sujet de données.
- 3) Aux fins d'application de l'alinéa 1)a)ii), une donnée personnelle est traitée de manière transparente si :
  - a) le sujet de données est informé de la façon dont les données personnelles vont être recueillies, utilisées ou traitées autrement ;
  - b) le sujet de données est informé du degré auquel les données personnelles seront traitées ; et
  - c) toute information ou communication en rapport avec le traitement des données personnelles est aisément accessible et compréhensible pour le sujet des données.
- 4) Des contrôleurs et des processeurs de données doivent s'assurer que le traitement de données personnelles à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques se déroule en conformité avec les protections appropriées prescrites par règlement.
- 5) Des contrôleurs et des processeurs de données doivent supprimer les données personnelles dès lors que les fins auxquelles elles ont été traitées ont été réalisées ou elles ne devraient être conservées que sous une forme qui empêche toute identification, directement ou indirectement, du sujet des données.
- 6) Une personne qui manque de se conformer aux conditions requises prévues au présent article commet un délit passible sur condamnation à une amende ne dépassant pas VT 10.000.000.

## **5 Fins légales pour un traitement de données à caractère personnel**

- 1) Un processeur ou un contrôleur de données ne peut traiter des données personnelles que si le traitement est :
  - a) basé sur le consentement du sujet des données à une ou plusieurs fins spécifiques ;
  - b) nécessaire pour conclure ou mener à bien un contrat auquel le sujet de données est partie ;
  - c) nécessaire pour protéger les droits ou les intérêts vitaux du sujet de données ou d'une autre personne physique ;
  - d) nécessaire pour être en conformité avec une obligation légale à laquelle le contrôleur de données est soumis ou dans l'exercice d'une autorité officielle dont il est investi ;
  - e) nécessaire pour une tâche menée dans l'intérêt public ou dans l'exercice d'une autorité officielle ;
  - f) nécessaire pour les besoins des intérêts légitimes du contrôleur de données ou d'une tierce partie, sauf si les intérêts ou les droits et libertés fondamentaux du sujet de données, surtout s'agissant d'un enfant, l'emportent sur de tels intérêts.
- 2) Une personne qui manque de se conformer aux conditions requises prévues au présent article commet un délit passible sur condamnation à une amende ne dépassant pas VT 10.000.000.

## **6 Traitement de catégories particulières de données à caractère personnel**

- 1) Il est interdit de procéder au traitement de catégories particulières de données personnelles.
- 2) Nonobstant le paragraphe 1), un contrôleur ou un processeur de données peut traiter des catégories particulières de données personnelles si le traitement est :
  - a) basé, sous réserve du paragraphe 3), sur le consentement du sujet des données à une ou plusieurs fins spécifiques ;

- b) nécessaire dans l'accomplissement d'obligations ou l'exercice de droits spécifiques du contrôleur de données ou du sujet des données tels qu'énoncés dans la présente ou toute autre loi ;
- c) nécessaire, sous réserve de conditions prévues par la présente ou toute autre loi, pour :
  - i) évaluer la capacité de travail d'un employé ; ou
  - ii) remplir des obligations ou exercer des droits spécifiques du contrôleur de données ou du sujet de données dans le domaine de l'emploi, de la sécurité sociale ou de la protection sociale ;
- d) nécessaire à des fins de prévention et de diagnostic médicaux, d'administration de soins ou de traitement, de gestion de services de santé ou en vertu d'un contrat avec un professionnel de la santé, sous réserve du secret professionnel et de conditions prévues par la présente loi ;
- e) nécessaire pour des raisons d'intérêt substantiel dans le domaine de la santé publique, telles que la surveillance et la protection contre une épidémie fatale et sa propagation ou à des fins d'actions humanitaires ;
- f) nécessaire pour protéger les intérêts vitaux du sujet de données ou d'une autre personne physique dans le cas où le sujet de données est physiquement ou légalement incapable de donner son consentement ;
- g) nécessaire pour des raisons de sécurité et de défense nationales, de sûreté publique ou pour la prévention, l'investigation ou des poursuites pénales de délits criminels ou l'exécution de peines pénales ;
- h) mené au cours d'activités légitimes assorties de protections appropriées par une fondation, une association ou autre organisation à but non lucratif ayant un objet politique, philosophique, religieux ou syndical et à condition que :
  - i) le traitement se rapporte uniquement aux membres ou anciens membres de l'organisation ou à des personnes

physiques qui sont régulièrement en contact avec elle dans le cadre de ses objectifs ; et

- ii) les données personnelles ne soient pas divulguées en dehors de l'organisation en question sans le consentement des sujets de données ;
  - i) nécessaire pour l'introduction, la poursuite ou la défense d'actions en justice ou chaque fois que les tribunaux agissent en leur capacité judiciaire ; ou
  - j) nécessaire à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou des fins statistiques, sous réserve de conditions prévues par la présente ou toute autre loi.
- 3) L'alinéa 2)a) ne s'applique pas si les règlements disposent que l'interdiction ne peut être levée, même avec le consentement écrit du sujet de données.
- 4) Aux fins d'application des alinéas 2)b), e) et g), le contrôleur de données ou le processeur de données doit s'assurer que des mesures appropriées sont en place pour protéger les droits et libertés fondamentaux de sujets de données.
- 5) Une personne qui manque de se conformer aux conditions requises prévues au présent article commet un délit passible sur condamnation à une amende ne dépassant pas VT 10.000.000.

## **7 Traitement de données à caractère personnel d'un enfant ou autre personne vulnérable**

- 1) Il est interdit de procéder au traitement de données personnelles d'un enfant.
- 2) Nonobstant le paragraphe 1), un contrôleur ou un processeur de données peut traiter des données personnelles d'un enfant si le traitement est :
  - a) basé sur le consentement ou autorisé par les parents de l'enfant, ses tuteurs ou représentants légaux, sauf si une loi dispose que l'enfant peut agir de son propre chef sans être représenté par ses parents ou son tuteur légal ;

- b) dans l'intérêt vital de l'enfant ;
  - c) nécessaire pour remplir une obligation légale à laquelle le contrôleur de données est soumis ;
  - d) nécessaire pour l'exécution d'une tâche menée par le contrôleur de données dans l'intérêt public comme prévu par une loi ; ou
  - e) nécessaire dans le contexte de services préventifs ou de soutien psychosocial proposés directement à un enfant.
- 3) Si une information et une communication en rapport avec le traitement sont adressées à un enfant, elles doivent être dans un langage clair et simple de sorte que l'enfant puisse facilement les comprendre et des mécanismes appropriés doivent être en place pour en vérifier l'âge.
- 4) S'agissant de traiter des données personnelles relativement à des personnes vulnérables, les contrôleurs et processeurs de données doivent :
- a) prendre en considération les besoins particuliers de telles personnes et les normes pertinentes en termes d'accessibilité ; et
  - b) s'assurer que les informations et les communications sur le traitement de données sont dans un langage clair et simple et aisément accessibles pour tous les sujets de données, quels que soient leur âge, leur sexe, leurs aptitudes ou leurs caractéristiques.
- 5) Une personne qui manque de se conformer aux conditions requises prévues au présent article commet un délit passible sur condamnation à une amende ne dépassant pas VT 10.000.000.

## **8 Consentement**

- 1) Si le traitement de données personnelles est basé sur le consentement d'un sujet de données, le contrôleur de données doit pouvoir montrer la preuve d'un tel consentement.
- 2) Un consentement est réputé ne pas avoir été donné librement si :

- a) ledit consentement est donné par abus d'autorité ou sous pression d'ordre économique ou autre, que ce soit directement ou indirectement ; ou
  - b) le sujet des données n'a pas vraiment le choix ou n'est pas libre de choisir ou n'est pas en mesure de refuser ou de retirer son consentement sans préjudice.
- 3) Une demande de consentement doit être présentée d'une manière qui :
- a) se distingue clairement d'autres affaires ; et
  - b) est exprimée dans un langage clair et simple.
- 4) Un processeur de données doit s'assurer :
- a) qu'un sujet de données a la possibilité de retirer un consentement donné à n'importe quel moment, et à titre gratuit ;
  - b) que, dans le cas de fins multiples, le consentement est donné par chaque personne et pour chaque fin spécifique ; et
  - c) que le sujet des données est informé qu'il peut rétracter son consentement et comment le faire.
- 5) Le retrait d'un consentement n'affecte pas la légalité du traitement de données qui a été effectué avant que le contrôleur de données ne le reçoive.

## TITRE 3 DROITS DU SUJET DE DONNEES

### 9 Accès à des informations et à des données personnelles

- 1) Un contrôleur de données doit s'assurer qu'un sujet de données peut obtenir, sur demande et à des intervalles acceptables :
  - a) une confirmation quant à la question de savoir si ses données personnelles sont en train d'être traitées ;
  - b) une copie des données personnelles sous traitement ; et
  - c) les informations suivantes :
    - i) les buts du traitement ;
    - ii) la source des données personnelles sous traitement ;
    - iii) les destinataires ou les catégories de destinataires auxquels les données personnelles sont communiquées ;
    - iv) si, le cas échéant, le contrôleur de données a l'intention de transférer les données personnelles en dehors de la juridiction du Vanuatu, et si oui, à quels destinataires et dans quelles juridictions ;
    - v) la durée de temps pendant laquelle les données personnelles seront conservées par le contrôleur ou le processeur de données ; et
    - vi) toute autre information que le contrôleur de données est tenu de fournir afin d'assurer la transparence du traitement en conformité avec la présente loi.
- 2) Le contrôleur de données doit fournir les informations prévues au paragraphe 1) de la manière suivante :
  - a) par écrit ;
  - b) dans un langage simple ;



- c) à titre gratuit ; et
  - d) dans le mois qui suit la date de réception d'une telle demande.
- 3) Si une demande selon le paragraphe 1) est trop excessive ou déraisonnable, le contrôleur de données peut :
- a) imposer un droit raisonnable sur la base des frais administratifs encourus ; ou
  - b) refuser de donner suite à la demande.
- 4) Si le contrôleur de données impose un droit en application de l'alinéa 3)a) ou refuse de donner suite à une demande en application de l'alinéa 3)b), à charge pour lui d'apporter la preuve de la nature excessive ou déraisonnable de la demande.

#### **10 Restriction sur le traitement de données personnelles**

- 1) Un contrôleur de données doit s'assurer, à la demande du sujet des données, que le traitement des données personnelles est l'objet de restriction dans l'une quelconque des circonstances suivantes :
- a) lorsque l'exactitude des données personnelle est contestée par le sujet de données, pour la période nécessaire pour permettre au contrôleur de vérifier l'exactitude des données personnelles ;
  - b) lorsque le traitement est contraire à la loi mais que le sujet des données s'oppose à l'effacement des données personnelles et demande à ce que leur utilisation soit l'objet de restriction ;
  - c) lorsque le contrôleur n'a plus besoin des données personnelles aux fins du traitement ;
  - d) lorsque le sujet de données s'est opposé au traitement en vertu de l'article 13 en attendant que soit vérifiée la question de savoir si les motifs légitimes du contrôleur l'emportent sur ceux du sujet de données.
- 2) Si un sujet de données a restreint le traitement de données personnelles en application du paragraphe 1), les données personnelles ne peuvent être traitées que dans l'une des circonstances suivantes :

- a) avec le consentement du sujet des données ;
  - b) pour l'introduction, la poursuite ou la défense d'une action en justice ou pour la protection des droits d'une autre personne physique ou morale ou pour des raisons d'intérêt public.
- 3) Le sujet de données qui a restreint le traitement de données personnelles en application du paragraphe 1) doit être informé par le contrôleur de données avant le traitement des données personnelles en application de l'alinéa 2)b).

### **11 Rectification et effacement de données personnelles**

- 1) Un contrôleur de données doit s'assurer que, sur demande d'un sujet de données, celui-ci peut obtenir la rectification de données personnelles inexactes ou incomplètes sans tarder et à titre gratuit.
- 2) Un contrôleur de données doit s'assurer que, sur demande d'un sujet de données, celui-ci obtient l'effacement de données personnelles sans tarder et à titre gratuit si :
- a) les données personnelles ne sont plus nécessaires aux fins auxquelles elles ont été recueillies ou traitées par ailleurs ;
  - b) le sujet des données retire le consentement sur lequel le traitement est basé ;
  - c) le sujet des données s'oppose au traitement en vertu de l'article 12 et le contrôleur ne peut pas démontrer qu'il existe un fondement légitime prépondérant pour le traitement ;
  - d) les données personnelles sont traitées contrairement à la loi ;
  - e) les données personnelles doivent être effacées pour remplir une obligation légale à laquelle le contrôleur est soumis.
- 3) Le contrôleur des données doit communiquer la demande d'un sujet de données en application du paragraphe 1) ou 2) à tous les destinataires auxquels les données personnelles concernées ont été communiquées, à moins qu'il ne puisse démontrer que c'est impossible ou nécessiterait des efforts disproportionnés.

## **12 Opposition au traitement de données personnelles**

Un contrôleur de données doit s'assurer qu'à la demande d'un sujet de données, celui-ci peut s'opposer au traitement de ses données personnelles à tout moment et à titre gratuit, sauf si le contrôleur de données peut démontrer :

- a) des motifs légitimes pour le traitement qui l'emportent sur les intérêts ou les droits et libertés fondamentaux du sujet des données ; ou
- b) l'introduction, la poursuite ou la défense d'une action en justice.

## **13 Droit d'un sujet de données à ne pas être soumis à un processus de prise de décision automatisé**

- 1) Un contrôleur de données doit s'assurer qu'à la demande d'un sujet de données, celui-ci n'est pas soumis à une décision qui le touche significativement ou est basée uniquement sur un traitement automatisé de données personnelles, y compris profilage, sans prendre en considération son avis.
- 2) Le paragraphe 1) ne s'applique pas si une décision :
  - a) est autorisée par une loi à laquelle le contrôleur de données est soumis et qui prévoit des mesures adaptées pour protéger les intérêts légitimes, les droits et libertés fondamentaux des sujets de données ;
  - b) est nécessaire pour conclure ou mener à bien un contrat entre le sujet de données et le contrôleur de données ; ou
  - c) est basée sur le consentement du sujet de données et que des garanties appropriées ont été mises en place.
- 3) Lorsque l'alinéa 2)b) ou c) s'applique, le contrôleur de données doit :
  - a) mettre en œuvre des mesures qui conviennent pour protéger les droits et libertés fondamentaux du sujet de données et ses intérêts légitimes ;
  - b) donner au sujet des données la possibilité d'obtenir une intervention humaine de la part du contrôleur ; et

- c) permettre au sujet des données d'apporter son point de vue et de contester la décision.
  
- 4) Si une décision selon le paragraphe 1) porte sur des catégories particulières de données personnelles ou des données personnelles d'enfants ou des données personnelles relatives à des personnes vulnérables, le traitement ne doit être effectué que si :
  - a) les conditions énoncées aux articles 6 et 7 pour le traitement sont remplies ;
  
  - b) le traitement est exigé par une loi ; et
  
  - c) le traitement est nécessaire pour des raisons impératives d'intérêt public.

#### **14 Représentation du sujet de données**

Un contrôleur de données doit s'assurer qu'un sujet de données peut autoriser un organisme, une organisation ou une association à but non lucratif qui a été dûment constitué(e) conformément à une loi à :

- a) déposer et poursuivre une plainte auprès du Commissaire pour le compte du sujet de données ;
  
- b) poursuivre un recours judiciaire efficace pour le compte du sujet de données en faisant appel d'une décision légalement obligatoire du Commissaire ; ou
  
- c) poursuivre un recours judiciaire efficace pour le compte du sujet de données contre un contrôleur ou un processeur de données.

## **TITRE 4 FLOTS DE DONNÉES TRANSFRONTALIERS**

### **15 Conditions applicables au transfert hors de la juridiction du Vanuatu**

- 1) Des données personnelles générées ou recueillies au Vanuatu ne doivent pas être utilisées ailleurs sans l'autorisation préalable du Ministre sur recommandation du Commissaire.
- 2) Nonobstant le paragraphe 1), des données personnelles générées ou recueillies au Vanuatu peuvent être transférées dans un autre pays ou à une organisation internationale sans l'autorisation préalable du Ministre si le pays ou l'organisation internationale en question a été prescrit(e) par le Ministre conformément au paragraphe 3).
- 3) Le Ministre peut, après avis du Commissaire, prescrire par règlement pour les pays et les organisations internationales :
  - a) qu'elles apportent un niveau approprié de protection de données personnelles ; et
  - b) qu'une autorisation préalable du Ministre n'est pas nécessaire s'agissant de transférer des données personnelles générées ou recueillies au Vanuatu à de tels pays ou organisations internationales prescrits.

### **16 Protections préalablement au transfert hors de la juridiction du Vanuatu**

En sus de l'article 15, le Ministre peut, sur avis de la Commission, prescrire des procédures de protection à appliquer s'agissant de transférer des données personnelles en dehors du Vanuatu si :

- a) l'information demandée est réputée de nature urgente et sensible par le Commissaire ; et
- b) le pays ou l'organisation internationale auquel ou à laquelle les données personnelles seront transférées a été prescrit(e) par le Ministre en application du paragraphe 15.3).

**17 Transfert transfrontalier dans des situations spécifiques**

Nonobstant l'article 15, le Commissaire pourra autoriser des transferts transfrontaliers de données personnelles à des pays ou des organisations internationales qui ne garantissent pas un degré de protection adapté si :

- a) le sujet des données a donné son consentement librement et de façon explicite et spécifique, après avoir été informé de tous les risques résultant du transfert en l'absence de protections suffisantes;
- b) les intérêts spécifiques du sujet de données nécessitent le transfert dans un cas particulier ;
- c) le transfert est effectué en vue de faire valoir un intérêt légitime, notamment un intérêt public de grande importance, qui est prévu par loi et qu'un tel transfert constitue une mesure nécessaire et proportionnée dans une société démocratique ;
- d) le transfert constitue une mesure nécessaire et proportionnée dans une société démocratique pour la liberté d'expression ; ou
- e) le transfert est nécessaire pour protéger les intérêts vitaux du sujet des données ou d'autres personnes dans le cas où le sujet des données est incapable physiquement ou légalement de donner son consentement.

## TITRE 5 EXECUTION

### 18 Communication de documents ou d'informations

- 1) Si le Commissaire est convaincu qu'un contrôleur de données détient en sa possession un document ou une information qui l'aidera à établir s'il y a eu une violation de la présente loi, il peut, par écrit, exiger que ledit contrôleur de données lui fournisse le document ou l'information en question.
- 2) Le contrôleur de données doit se conformer à la demande visée au paragraphe 1) sous les 14 jours de sa réception.
- 3) Le Commissaire ne doit pas communiquer un document ou une information quelconque obtenu en vertu du présent article à moins :
  - a) d'y être autorisé par le contrôleur de données ;
  - b) d'y être tenu par une ordonnance d'un tribunal ;
  - c) d'être convaincu que le document ou l'information n'identifie pas de contrôleur de données ou de sujet de données en particulier ; ou
  - d) que la communication ne soit exigée par la présente ou toute autre loi.

### 19 Requête pour mandat

- 1) Si le Commissaire est raisonnablement convaincu qu'un délit a été commis aux termes de la présente loi, il peut demander au Commissaire de Police de l'assister pour former une requête pour un mandat.
- 2) Une requête pour un mandat doit être formée par écrit et sous serment par le Commissaire de Police, et doit exposer :
  - a) le délit auquel se rapporte la requête ;
  - b) une description du centre de données ou d'un serveur de données ;
  - c) l'information à l'appui du soupçon raisonnable de la perpétration du délit ; et

- d) la durée pour laquelle le mandat est nécessaire.

## **20 Octroi de mandat**

- 1) La Court peut octroyer un mandat si elle est satisfaite de la requête du Commissaire de Police.
- 2) Sans limiter la portée du paragraphe 1), avant d'accorder un mandat, la Cour doit prendre en considération ce qui suit :
  - a) la gravité du délit auquel se rapporte la requête ;
  - b) la fiabilité de l'information à l'appui de la requête, y compris la nature de la source de l'information ;
  - c) si l'intérêt public pour la production de données du centre de données ou d'un serveur de données l'emporte sur le droit au secret d'une personne dont la vie personnelle pourrait être affectée par suite de la production des données ;
  - d) s'il y a un lien suffisant entre les preuves recherchées et le délit auquel se rapporte la requête ;
  - e) si le mandat doit être assorti d'une condition quelconque ;
  - f) la durée du mandat telle que proposée ; et
  - g) toutes autres affaires que la Cour estime pertinentes.

## **21 Contenu d'un mandat**

Un mandat doit contenir les informations suivantes :

- a) une description du centre de données et du serveur de données qui doivent être perquisitionnés ;
- b) le délit auquel la requête se rapporte ;
- c) les types de preuves pertinentes qui peuvent être recherchés ;



- d) le pouvoir du Commissaire de sécuriser un centre de données ou un serveur de données ou de le rendre inaccessible ;
- e) la date et l'heure d'expiration du mandat ; et
- f) toutes conditions imposées eu égard à l'exécution du mandat.

## **22 Prorogation d'un mandat**

- 1) La Cour doit préciser la date et l'heure d'expiration du mandat dans le mandat.
- 2) La Cour peut proroger la date et l'heure d'expiration d'un mandat si elle est satisfaite que l'objet pour lequel le mandat a été accordé ne peut être rempli avant son expiration.

## **23 Effets d'un mandat**

- 1) Aux termes d'un mandat accordé en vertu de l'article 20, le Commissaire de Police est autorisé à :
  - a) saisir un article qu'il est fondé à croire être :
    - i) une preuve pertinente en rapport avec un délit objet du mandat ; ou
    - ii) une preuve pertinente pour un autre délit à la présente ou toute autre loi ;
  - b) avoir accès à un centre de données ou un serveur de données aux fins d'obtenir des informations et des registres ;
  - c) saisir ou sécuriser un serveur de données ;
  - d) exiger qu'une personne ayant une connaissance du centre de données ou du serveur de données l'aide à y accéder ;
  - e) déplacer le serveur de données de l'endroit perquisitionné à un autre endroit pour l'examiner dans le but de constater s'il comporte des données auxquelles il pourrait accéder ou qu'il pourrait collationner ou saisir en vertu du mandat si :

- i) le contrôleur de données y consent ; ou
    - ii) ce serait beaucoup plus pratique d'agir ainsi compte tenu du temps qu'il faudrait pour copier les données et qu'il y a des motifs acceptables de soupçonner qu'il serait possible d'accéder aux données, de les collationner ou de les saisir en vertu du mandat ; et
  - f) se faire aider par le Commissaire ou une autre personne selon que raisonnablement nécessaire pour exécuter le mandat.
- 2) Si le Commissaire de Police saisit le serveur de données en application du paragraphe 1), il peut :
- a) en prendre possession ; et
  - b) le garder pour la durée qu'il considère nécessaire aux fins d'application de la présente loi.
- 3) Le Commissaire de Police doit rendre le serveur de données en sa possession en application du paragraphe 2) au contrôleur de données :
- a) s'il n'est plus nécessaire de le saisir ; ou
  - b) s'il ne va pas servir au titre de preuve, à moins que le Commissaire de Police ne soit raisonnablement fondé à croire que les données contenues dans le serveur de données pourraient servir au titre de preuve en rapport avec un délit.

## **TITRE 6 DELITS**

### **24 Non respect d'une disposition de la présente loi**

Quiconque manque de respecter une disposition de la présente loi commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

### **25 Obtention et divulgation illicites de données à caractère personnel**

1) Une personne autre que le contrôleur de données ne doit pas, sciemment ou imprudemment, obtenir, retenir ou divulguer ou faire divulguer des données personnelles :

a) sans l'autorisation du contrôleur de données ; et

b) dans l'intention d'obtenir un gain financier ou de causer du mal au sujet des données.

2) Une personne qui enfreint le paragraphe 1) commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

### **26 Modification de données personnelles pour empêcher la divulgation à un sujet de données**

Un contrôleur de données ou un processeur de données, ou une personne employée par l'un ou par l'autre, qui modifie, dégrade, bloque, efface, détruit ou dissimule des informations dans l'intention d'en empêcher la divulgation, totalement ou partiellement, à un sujet de données qui en a fait la demande, commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

### **27 Entrave aux pouvoirs d'entrée dans des locaux**

Quiconque entrave délibérément une personne dans l'exécution d'un mandat délivré en application de la présente loi commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

### **28 Destruction ou falsification d'informations demandées par le Commissaire**

Une personne qui détruit, dissimule ou falsifie, entièrement ou partiellement, une information, un document, un équipement ou un matériel, dans l'intention d'empêcher la communication d'informations au Commissaire en application de

l'article 18, commet un délit passible sur condamnation d'une amende ne dépassant pas VT 10.000.000.

**29 Entrave ou obstruction dans l'exercice légal de pouvoirs**

- 1) Une personne ne doit pas gêner ou entraver le Commissaire, un policier ou une personne assistant un policier dans l'exercice de ses fonctions en application de la présente loi.
- 2) Une personne qui manque de se conformer au paragraphe 1) commet un délit passible sur condamnation d'une amende ne dépassant pas VT 1.000.000.

**30 Défense de communiquer des informations, des registres et des données**

- 1) Une personne qui obtient des informations, des extraits, des registres ou des données en vertu d'une demande ou d'un mandat en application de la présente loi ne doit pas sciemment les communiquer, entièrement ou partiellement, autrement que dans l'accomplissement de ses devoirs.
- 2) Une personne qui manque de se conformer au paragraphe 1) commet un délit passible sur condamnation d'une amende ne dépassant pas VT 2.000.000.

## **TITRE 7 DISPOSITIONS DIVERSES**

### **31 Règlements**

- 1) Le Ministre peut, après avis du Commissaire, établir des règlements qui ne soient pas incompatibles avec la présente loi dans le but de mieux appliquer ou donner effet aux dispositions de la présente loi.
- 2) Sans limiter la portée générale du paragraphe 1), les règlements peuvent disposer de ce qui suit :
  - a) comment des données personnelles doivent être traitées en toute transparence ;
  - b) comment des contrôleurs de données conjoints doivent travailler ensemble et les obligations qui doivent incomber à chacun d'entre eux ou aux deux ;
  - c) les obligations des processeurs de données ;
  - d) la sécurité du traitement ;
  - e) l'enregistrement des opérations de traitement ;
  - f) les obligations relativement à des violations de données personnelles ; et
  - g) la notification de violation de données personnelles à des sujets de données.

### **32 Entrée en vigueur**

La présente loi entre en vigueur le jour de sa publication au Journal Officiel.