LONG GOD YUMI STANAP

République de Vanuatu

Nationale du Vanuatu
Politique de Protection des Données et de la Vie privée

Avant-propos du Premier ministre

Hon. Alatoi Ishmael KALSAKAU

J'ai le plaisir de vous présenter la Politique nationale de Vanuatu sur la protection des données et de la vie privée de 2023, une politique qui complète et renforce nos efforts tels qu'énoncés dans la stratégie nationale sur la cybersécurité de 2030. Elle établit le fondement de la loi de Vanuatu sur la protection des données privées qui donnera effet aux droits afférents entérinés dans la Constitution et les instruments internationaux auxquels le Vanuatu est partie et marque ainsi l'engagement de l'Etat à veiller au respect et à la protection des données personnelles et des droits afférents des personnes physiques, dont le droit au secret.

La Constitution de la République de Vanuatu (2006) (la «Constitution») reconnaît que «sont accordés à toute personne" un certain nombre de «droits fondamentaux et de libertés individuelles.» Ces droits fondamentaux et libertés peuvent être impactés défavorablement par l'exploitation de données personnelles. Aussi le gouvernement de la République de Vanuatu souhaite adopter des mesures législatives pour aider à guider, protéger et respecter les données personnelles, les droits fondamentaux et les libertés y relatifs et garantir que le public puisse avoir confiance dans l'utilisation de données personnelles..

De plus, il est crucial que les citoyens, les entreprises et les plate-formes en ligne au Vanuatu fonctionnent dans le respect des fondements énoncés dans la Constitution de Vanuatu (Titre II, Chapitre 1, Article 5) – qui reconnaissent que sont accordés à toute personne plusieurs "Droits fondamentaux et Libertés individuelles" et disposent de "garanties contre la violation du domicile". Cela signifie que "le respect et le sens de la responsabilité" doivent prédominer dans la communication en ligne, surtout s'agissant de communications par courriel, texte, image, contenu de sites internet, affichage de blogs, commentaires, forums en ligne, réseaux sociaux et applications sur les téléphones.

J'invite toutes les parties prenantes, les citoyens et les touristes en visite au Vanuatu à accorder la priorité à collaborer diligemment avec le gouvernement de Vanuatu et les autorités concernées dans le cadre de cette politique nationale – il s'agit de veiller à ce que toutes les données engendrées et/ou recueillies au Vanuatu soient toujours en conformité avec la législation et les structures d'administration du Vanuatu et ne soient pas utilisées ailleurs sans l'autorisation préalable des autorités compétentes, qu'il s'agisse d'une catégorie de transferts ou d'un transfert particulier, ou en vertu de la loi.

Hon. MAAU'KORO, MOLI TAMBE,

URE VIRA TAMBE, LAVISE VAHE

ALATOI ISHMAEL KALSAKAU (MP), Prime Minister

Remerciements

L'élaboration de la politique nationale sur la protection des données personnelles n'aurait pas pu voir le jour sans les efforts et les contributions résolus du Conseil de l'Europe, des membres du groupe spécial œuvrant pour la protection des données personnelles et d'autres personnes, y compris le soutien financier et technique de la part de parties prenantes et d'institutions.

Tankio tumas au gouvernement, en passant par le Premier ministre et le Directeur Général, l'agent principal de l'information et son adjoint au bureau du Premier ministre, pour leur concours et leur enthousiasme dans l'élaboration de cette grande politique nationale.

Tankio tumas au Conseil de l'Europe qui a aidé à fournir des experts techniques et un soutien financier pour l'élaboration de la présente politique.

Tankio tumas aux diverses institutions qui ont aidé à fournir un soutien technique et financier pour l'élaboration de cette politique, et en particulier le Haut Commissariat australien au Vanuatu, l'équipe d'intervention d'urgence en informatique, la cellule du droit à l'information, le bureau du régulateur des télécommunications, des communications radio et de la radio-diffusion, la Banque de Réserve de Vanuatu, le Bureau des Statistiques de Vanuatu, le Service de l'Etat civil, la cellule du renseignement financier, le Parquet, la Commission de la Fonction publique et le Ministère de la Justice et des Services d'intérêt général de Vanuatu.

Tankio tumas à tous les groupes consultatifs techniques provinciaux, les agences consciencieuses et leurs représentants qui ont participé et contribué aux ateliers de consultation menés dans l'ensemble du pays, et aussi le comité d'examen de la politique.

Enfin, tankio tumas à toutes les agences gouvernementales, aux entreprises d'Etat, aux organisations du secteur privé, aux organisations non gouvernementales, aux écoles, aux communautés et aux usagers de l'internet qui ont accepté nos invitations de consultation et séances de sensibilisation en ligne, dont les causeries, et y ont répondu. Vos contributions ont modelé cette politique en un instrument des pouvoirs publics centré sur l'usager qui va rehausser les efforts nationaux pour sauvegarder la confiance du public dans l'utilisation de données personnelles.

Abréviations

CE	Conseil de l'Europe
LPD	Loi sur la protection des données
RGPD	Règlement général sur la protection des données
UE	Union Européenne
TIC	Technologie de l'Information et de la Communication
ASN	Autorité de la sécurité numérique
ONU :	Organisation des Nations Unies

Définitions

Anonymisation désigne le processus appliqué aux données personnelles pour faire en sorte que les sujets de données ne puissent pas être identifiés, que ce soit directement ou indirectement, sans y consacrer trop de temps, d'effort ou de ressources;

Données biométriques désigne les données personnelles issues d'un traitement technique spécifique se rapportant aux caractéristiques physiques, physiologiques ou comportementales d'une personne physique, lesquelles permettent ou confirment l'identification unique de cette personne, telles que représentations faciales ou données dactyloscopiques;

Consentement désigne n'importe quelle indication spécifique, renseignée donnée librement et sans ambiguité des souhaits du sujet des données par laquelle il ou elle signifie son accord, par une déclaration ou par une action affirmative claire, au traitement spécifié de données personnelles le ou la concernant;

Entreposage dans le Cloud désigne un modèle de dépôt de données où des données sont entreposées dans des serveurs virtuels tenus par des tiers;

Contrôleur de données désigne la personne physique ou morale, autorité publique, service ou agence ou autre organisme qui, seul ou conjointement avec d'autres, dispose du pouvoir de prise de décision eu égard au traitement de données;

Violation de données désigne une violation de la sécurité par une personne quelle qu'elle soit entraînant, accidentellement ou illégalement, la destruction, la perte, la modification, la communication non autorisée de données personnelles ou l'accès à des données personnelles transmises, entreposées ou traitées autrement;

Traitement de données désigne n'importe quelle opération ou suite d'opérations menée sur des données personnelles, telle que la collecte, l'entreposage, la sauvegarde, la modification, l'extraction de telles données ou des opérations logiques et/ou arithmétiques sur de telles données. Lorsqu'un traitement automatique n'est pas utilisé, "traitement de données" désigne une opération ou suite d'opérations effectuée sur des données personnelles dans le cadre d'un ensemble structuré de telles données qui sont accessibles ou peuvent être extraites suivant des critères spécifiques;

Données génétiques désigne toutes les données se rapportant aux caractéristiques génétiques d'une personne qui ont été soit héritées soit acquises pendant le développement prénatal telles qu'elles résultent d'une analyse d'un échantillon biologique de la personne concernée, en particulier une analyse des chromosomes, de l'ADN ou de l'ARN ou une analyse de tout autre élément permettant d'obtenir une information équivalente;

Données médicales désigne toutes les données personnelles concernant la santé physique ou mentale d'une personne, y compris des services de soin, lesquelles révèlent des informations sur sa santé antérieure, actuelle et future;

Personne identifiable désigne une personne qui peut identifiée, directement ou indirectement, en particulier par renvoi à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, une image, un identifiant en ligne ou à un ou plusieurs facteurs spécifiques de son identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale;

Données personnelles désigne n'importe quelle information ou donnée, qu'elle soit enregistrée ou non dans un dossier, se rapportant à une personne identifiée ou identifiable ("sujet de données") ou permettant de distinguer ou d'interagir avec une personne individuellement;

Informaticien désigne une personne physique ou ayant la personnalité juridique, une autorité publique, un service, une agence ou tout autre organisme qui traite des données personnelles pour le compte du contrôleur;

Pseudonymisation désigne le traitement de données personnelles d'une telle manière que ces données ne peuvent plus être attribuée à un sujet de données particulier sans avoir des informations supplémentaires, à condition que celles-ci soient gardées à part et soumises à des mesures techniques et organisationnelles de façon à garantir que les données personnelles ne soient pas attribuées à une personne identifiée ou identifiable;

Catégories particulières de données personnelles désigne des données génétiques ; des données personnelles se rapportant à des délits, des poursuites et des condamnations pénales ; des données biométriques identifiant une personne de façon unique ; des données personnelles se rapportant à une origine raciale ou ethnique, des opinions politiques, une affiliation à un syndicat, des croyances religieuses ou autres, la santé ou la vie sexuelle.

Table des matières

1 Introduction

Le développement de la technologie de l'information et de la communication (TIC) et la mondialisation croissante des services font intervenir la collecte et l'exploitation de données personnelles et sensibles extrêmement détaillées sur des personnes individuelles d'une ampleur plus grande que jamais auparant sur l'ensemble des secteurs privé et public.

Certes, des solutions entraînées par les données et la numérisation ont le potentiel d'accélérer la croissance économique, les avantages sociétaux, l'inclusion et l'accès à des services, mais elles présentent aussi de nouveaux risques pour les droits fondamentaux et les libertés individuelles des personnes qui nécessitent une réponse tant juridique que politique. Les cadres et écosystèmes juridiques nationaux et mondiaux sur la protection des données en pleine évolution requièrent un effort conjoint pour répondre aux préoccupations du public, mener une lutte efficace contre la propagation de la cybercriminalité et mettre en place des cadres législatifs et règlementaires solides.

La Constitution de la République de Vanuatu (2006) (la «Constitution»)[1] reconnaît que «sont accordés à toute personne « un certain nombre de «droits fonndamentaux et libertés individuelles.» Ceux-ci peuvent être impactés défavorablement par l'exploitation de données personnelles. Le Titre II, Chapitre I, Article 5 de la Constitution reconnaît et dispose expressément de garanties contre la violation du domicile et de la garantie de la loi eu égard à d'autres droits fondamentaux et libertés individuelles qui impliquent la nécessité de protéger la vie privée. Pour ce faire, le gouvernement de la République de Vanuatu souhaite adopter des mesures législatives pour aider à respecter et protéger les données personnelles, les droits fondamentaux et les libertés y relatifs et garantir que le public puisse avoir confiance dans l'utilisation de données personnelles.

Le gouvernement de la République de Vanuatu souahaite s'appuyer sur le droit à la vie privée et aux droits afférents entérinés dans la Constitution et dans des instruments internationaux auxquels le Vanuatu est partie, tels que le Pacte international relatif aux droits civils et politiques des Nations Unies (ONU) (Article 17)[2], la Convention sur les droits de l'enfance (Article 16)[3], la Convention sur les droits des personnes handicapées (Article 22)[4] et la Convention du Conseil de l'Europe sur la cybercriminalité (Article 15)[5]. Il tient aussi à se conformer aux meilleures pratiques internationales et, tout particulièrement, celles qui sont énoncées dans le seul traité international qui soit obligatoire dans ce domaine – la Convention du CE pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (STE No. 108 de 1981, «Convention 108»)[6] et le protocole y portant modification (STCE No. 223 de 2018, «Convention 108+»)[7].

---

1 Edition 2006, https://www.gov.vu/images/legislation/constitution-en.pdf

2 Pacte international relatif aux droits civils et politiques, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

3 Convention sur les droits de l'enfance, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

4 Convention sur les droits des personnes handicapées, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities

5 La Convention de Budapest Convention et ses Protocoles, https://www.coe.int/en/web/cybercrime/the-budapest-convention

6 Convention 108 https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=108

7 Convention 108+ https://www.coe.int/en/web/data-protection/convention108/modernised

La présente politique nationale sur la protection des données cadre parfaitement avec Vanuatu 2030 - Le Plan du Peuple[8], la stratégie nationale sur la cyber-sécurité 2030[9] et d'autres politiques nationales. En outre, elle a été renseignée par la décision n° 171 de 2021 du Conseil des Ministres[10]. La politique reflète la prise de conscience croissante quant à la nécessité de définir des politiques gouvernementales liées à une société de l'information de manière intégrée et holisitique et d'entériner la protection des données personnelles dans le droit du pays, dans le sens de la meilleure pratique internationale et tout particulièrement, la Convention modernisée 108+ et le Règlement général de UE sur la protection des données à caractère personnel (RGPD)[11].

Cette politique a été élaborée avec l'assistance technique apportée par le projet d'action globale sur la cybercriminalité élargie (GLACY+), une initiative conjointe du CE et de l'UE.

---

8 Plan National de Développement Durable 2016 à 2030 - Vanuatu 2030

9 Stratégie nationale sur la cybersécurité 2030 <Vanuatu_National_CyberSecurity_Strategy2030_Booklet.pdf (gov.vu)>

10 Décision No. 171 du Conseil des Ministres du gouvernement de Vanuatu en date du 5 août 2021.

11 Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, et abrogeant la Directive 95/46/EC (Règlement général sur la protection des données)

2 Objet de la politique

Cette politique a pour objet de créer les fondations d'une loi sur la protection des données et de la vie privée qui donnera effet aux droits afférents entérinés dans la Constitution et les instruments internatioaux auxquels le Vanuatu est partie et de montrer l'engagement de l'Etat à veiller au respect et à la protection des données à caractère personnel et des droits afférents de la personne, et notamment le droit à la vie privée. La protection des données est un aspect de la protection de la vie privée, mais il y en a d'autres, tels que les ingérences physiques, qui ne sont pas couvertes par cette politique.

Certes, cette politique traite uniquement, dans le détail, des données à caractère personnel, mais elle reconnaît la nécessité et l'importance d'avoir des politiques traitant d'autres formes de données, qui ne sont pas à caractère personnel, notamment en ce qui concerne leur importance pour la souveraineté du Vanuatu en matière de données. Cette souveraineté requiert que des politiques soient élaborées au sujet de la propriété des données, 'les données en tant que produit de base' exploitées par l'intermédiaire d'une infracture transparente protégée et sécurisée et, de manière générale, la nécessité d'avoir un modèle de définition et de gouvernance clair pour des données créées, sauvegardées et réutilisées.

La présente politique énonce la base pour réaliser ces objectifs en ce qui concerne des données personnelles et d'autres politiques et lois serviront aux données qui ne sont pas à caractère personnel.

3 Objectif

La politique a pour objectif de renseigner la rédaction d'une loi sur la protection des données destinée à réaliser ce qui suit :

3.1. contribuer au respect et à la protection des droits fondamentaux et des libertés individuelles des personnes physiques et, en particulier, de leur droit au respect de leur vie privée en ce qui concerne le traitement de leurs données à caractère personnel ;

3.2. veiller à l'harmonisation des politiques gouvernementales en matière de cybersécurité, de lutte contre la cybercriminalité et de protection de la vie privée des personnes, y compris leur mise en œuvre et leur évaluation en continu relativement à la résilience des équipements et services nationaux d'importance cruciale ;

3.3. aider à mettre en place un cadre institutionnel approprié pour garantir une mise en œuvre et une surveillance efficaces d'une loi nationale sur la protection des données et de la vie privée, comportant aussi bien des pénalités que des mécanismes de réparation appropriés (y compris dédommagement) ;

3.4. établir et partager des meilleures pratiques reconnues internationalement en matière de loi sur la protection des données et de la vie privée ;

3.5. prévoir comme condition requise la création d'une Autorité de sécurité numérique (ASN) indépendante et impartiale dotée des pouvoirs, des ressources et des moyens appropriés pour bien surveiller, suivre et faire respecter la conformité et la sauvegarde des droits de protection des données et de la vie privée des personnes ;

3.6. garantir une protection supplémentaire à l'égard du traitement de données à caractère personnel relatives à des enfants, conformément à l'article 16 de la Convention de l'ONU relative aux droits de l'enfant ;

3.7. veiller à avoir des sauvegardes appropriées pour le traitement de catégories particulières de données personnelles afin d'empêcher des effets défavorables pour les personnes ;

3.8. s'assurer que les données à caractère personnel traitées au Vanuatu sont soumises aux lois et structures d'administration du Vanuatu et restent toujours protégées par les cadres nationaux juridiques et administratifs concernés, rehaussant ainsi l'intégrité des données personnelles au Vanuatu et contribuant à la protection des personnes physiques au Vanuatu ;

3.9. promouvoir l'harmonisation du cadre juridique du Vanuatu pour la protection des données avec d'autres juridictions régionales et internationales garantissant la circulation de données personnelles dans des conditions d'assurance et de confiance ;

3.10. veiller à la compatibilité avec la culture, les traditions et valeurs du Vanuatu et les faire progresser.

4 Portée

4.1. La politique devrait couvrir, dans le détail, des composants cruciaux qui permettront d'élaborer la loi sur la protection des données, de même que des mandats spécifiques pour garantir non seulement que le Vanuatu réalise l'élaboration et l'exécution de la loi sur la protection des données, mais aussi que des mécanismes soient mis en place comportant des procédures et des processus de protection d'informations personnelles identifiables.

Par conséquent, la portée de la présente politique couvre la protection d'informations personnelles identifiables, des procédures et des processus pertinents inclus dans d'autres cadres législatifs du Vanuatu et, à l'échelon du contexte international, la mise en œuvre de règlements nationaux et, finalement, l'établissement de la loi de Vanuatu relative à la protection des données (LPD).

4.2. La LPD devrait s'appliquer à ce qui suit:

4.2.1. au traitement de données à caractère personnel dans les secteurs privé et public, que ce soit par des moyens automatisés ou non, indépendamment de la nationalité ou du lieu de séjour de la personne physique qui est l'objet du traitement de données personnelles;

4.2.2. au traitement de données personnelles ou de catégories particulières de données personnelles concernant des personnes vivantes et non pas des personnes décédées;

4.2.3. au traitement de données personnelles entrepris à l'intérieur de la juridiction du Vanuatu ;

4.2.4. au traitement de données personnelles générées ou recueillies au Vanuatu, indépendamment du lieu où le traitement est entrepris[12];

12 La Décision nº 171 de 2021 du Conseil des Ministres du gouvernement de Vanuatu relative à la protection des données et de la vie privée (réunion nº 016 , jeudi 5 août 2021) dispose que toutes les données générées et/ou recueillies au Vanuatu doivent toujours être sujettes aux lois et structures d'administration du Vanuatu et ne doivent pas être utilisées ailleurs sans l'autorisation préalable des autorités compétentes. Se reporter aussi à l'article 13 de la présente politique.

4.2.5. au traitement des données personnelles de personnes qui sont au Vanuatu par un contrôleur ou un informaticien qui n'est pas établi au Vanuatu, dès lors que les activités de traitement se rapportent à ce qui suit :

(a) à l'offre de biens ou de services à ces personnes au Vanuatu, indépendamment de la question de savoir si un paiement du sujet des données est exigé; ou

(b) au suivi de leur comportement dans la mesure où leur comportement a lieu au Vanuatu.

4.3. La LPD ne devrait pas s'appliquer au traitement de données personnelles servant purement à des activités personnelles ou ménagères.

4.4. La LPD devrait définir et promouvoir la souveraineté des données à l'égard de données à caractère personnel et créer des mécanismes de protection des données qui établissent clairement la souveraineté et la propriété de données relativement à des données personnelles.

5 Principes de base pour la protection de données personnelles

Les données personnelles et les catégories particulières de données personnelles doivent être traitées de façon juste, légale, transparente et de manière proportionnelle aux fins légitimes poursuivies. A toutes les étapes du traitement, il s'agit de trouver le juste milieu entre tous les intérêts concernés, qu'ils soient publics ou privés, et les droits et libertés des personnes. A partir de la Convention 108+ et des meilleures pratiques internationales, la LPD devrait énoncer les principes de base suivants qui doivent être respectés et appliqués à toutes les étapes du traitement de données:

5.1. Traitement juste, transparent et légal

5.1.1. Des données personnelles doivent être traitées de façon **juste**.

5.1.2. Des données personnelles doivent être traitées d'une manière **transparente**. Les sujets de données ont le droit de connaître le traitement de leurs données personnelles. Les contrôleurs devraient être tenus d'agir de manière transparente pour garantir un traitement juste et d'informer les sujets de données de leur identité sous une forme appropriée et fournir d'autres informations essentielles sur le traitement et leurs droits afin de garantir un traitement juste et légitime.

5.1.3. Des données personnelles doivent être traitées de façon **l**égale sur une base légitime comme indiqué au paragraphe 6.

5.2. Objet légitime spécifique et limitations

5.2.1. Des données personnelles doivent être traitées à des **fins explicites, spécifiées et légitimes** et le traitement des données en question doit servir aux fins citées sans être incompatible avec.

5.2.2. Un nouveau traitement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou des fins statistiques pourrait être considéré comme compatible avec lesdites fins, sous réserve de mettre en place des sauvegardes appropriées.

5.3. Minimisation des données

5.3.1. Les données personnelles soumises à un traitement doivent être **suffisantes, pertinentes sans être excessives** par rapport à l'objet de leur traitement.

5.3.2. Cette exigence renvoie non seulement à la quantité mais aussi à la qualité des données personnelles.

5.4. Exactitude

5.4.1. Des données personnelles objet d'un traitement doivent être **exactes** et, dans la mesure où c'est nécessaire, tenues à jour.

5.5. Limite quant à la durée de conservation

5.5.1. Des données personnelles objet d'un traitement ne doivent être conservées sous une forme permettant d'identifier les sujets des données que pour la durée nécessaire aux fins mêmes auxquelles elles sont traitées.

5.5.2. Les données personnelles doivent être supprimées une fois que l'objet de leur traitement a été réalisé ou ne doivent être conservées que sous une forme qui ne permet pas d'identifier directement ou indirectement le sujet de ces données ('anonymisées').

5.6. Sécurité des données et notification de violation

5.6.1. Le contrôleur et, le cas échéant, l'informaticien doivent prendre des mesures de sécurité raisonnables et appropriées pour protéger les données personnelles contre des risques tels qu'accès accidentel ou non autorisé, destruction, perte, utilisation, modification ou divulgation.

5.6.2. Le contrôleur doit notifier sans délai l'ASD, au moins, de violations de données personnelles qui pourraient porter gravement atteinte aux droits fondamentaux et libertés individuelles des sujets des données.

5.7. Responsabilité démontrable

5.7.1. Les contrôleurs (et, le cas échéant, les informaticiens) doivent prendre toutes les mesures appropriées pour respecter les principes énoncés dans la LPD et être en mesure de démontrer que le traitement de données sous leur contrôle y est conforme.

6 Base légitime

La LPD doit s'attacher à garantir la légalité d'un traitement de données en exigeant que le traitement de données personnelles ne soit entrepris que sur la base du consentement du sujet des données ou sur une autre base légitime stipulée par la LPD ou par un texte de loi, c'est-à-dire lorsque le traitement de données personnelles est nécessaire pour l'exécution d'un contrat avec le sujet des données, pour l'exécution d'une tâche dans l'exercice de l'autorité publique, pour le respect d'une obligation légale à laquelle le contrôleur est soumis, pour les besoins des intérêts légitimes poursuivis par le contrôleur ou un tiers, sauf dans le cas où les intérêts ou les droits fondamentaux et libertés du sujet des données (notamment des enfants) l'emportent sur ces intérêts légitimes ou qu'il est nécessaire de protéger les intérêts vitaux du sujet des données.

Un traitement sur une base légitime nécessite aussi que les données personnelles soient traitées de manière transparente (voir art. 5.2).

7 Catégories particulières de données

Le traitement de certains types de données personnelles ou le traitement de certaines données personnelles qui révèle des informations de nature sensible pourrait conduire à des empiètements sur les intérêts, droits et libertés des personnes. Ce peut, par exemple, être le cas où il existe un risque éventuel de discrimination ou d'atteinte à la dignité ou l'intégrité physique d'une personne, ou que le traitement de données personnelles puisse porter atteinte à la présomption d'innocence ouou d'autres droits et libertés importants.

7.1. Le traitement de catégories particulières de données ne doit être autorisé que dans le cas où des sauvegardes appropriées sont prévues par la loi.

7.2. Les sauvegardes doivent garantir une protection contre des risques que le traitement pose pour les intérêts et les droits et libertés du sujet des données, notamment le risque de discrimination.

8 Traitement en rapport avec un enfant et d'autres personnes vulnérables

8.1. L'intérêt d'un enfant doit être une considération première dans tout traitement de données concernant des enfants et des sauvegardes spécifiques doivent s'appliquer pour garantir que des enfants ne sont pas l'objet d'ingérence arbitraire ou illicite à l'égard de leurs droits dans un environnement numérique.

8.2. Les contrôleurs (et, le cas échéant, les informaticiens) et la LPD doivent être tenus d'apporter une attention particulière aux droits de protection des données des enfants et d'autres personnes vulnérables et, s'il y a lieu, de modifier les protections pour garantir leur efficacité à l'égard de telles personnes.

9 Protection des données et de la vie privée à dessein et par défaut

9.1. 9.1 Pour s'assurer que des conditions de protection des données sont intégrées le plus tôt possible, les contrôleurs (et, le cas échéant, les informaticiens) doivent examiner l'impact potentiel du traitement envisagé sur les droits fondamentaux et libertés individuelles des sujets des données avant de commencer le traitement et concevoir le traitement des données de manière à empêcher ou minimiser le risque d'ingérence dans lesdits droits et libertés.

9.2. Au moment de mettre en place les conditions techniques requises pour des réglages par défaut, les contrôleurs et les informaticiens doivent sélectionner les configurations types les plus favorables au respect de la vie privée pour faire en sorte que l'utilisation d'applications et de logiciels ne viole pas les droits des sujets de données (protection des données par défaut) et pour éviter de traiter davantage de données personnelles qu'il n'est nécessaire pour réaliser l'objectif légitime.

10 Evaluation des impacts de la protection des données

10.1. Lorsque le traitement de données à caractère personnel est susceptible d'aboutir à risque élevé d'atteinte aux droits fondamentaux et libertés individuelles de sujets de données, les contrôleurs (et, le cas échéant, les informaticiens) doivent mener, avant de lancer le traitement, une évaluation de l'impact des opérations de traitement envisagées sur la protection des données personnelles et concevoir le traitement de manière à empêcher ou minimiser de tels risques.

10.2. Une évaluation d'impact sur la protection de données doit être obligatoire en particulier dans le cas:

(a) d'une évaluation systématique et approfondie d'aspects personnels concernant des personnes qui est basée sur un traitement automatisé, y compris de l'établissement d'un profil;

(b) d'un traitement d'une grande échelle de catégories particulières de données personnelles; et

(c) de la surveillance systématique à grande échelle d'une zone accessible au public.

10.3. La Commission de sécurité numérique doit aussi pour établir et rendre publique une liste d'autres opérations de traitement qui nécessitent une évaluation d'impact sur la protection de données.

11 Sécurité des données

11.1. La sécurité des données personnelles est essentielles pour éviter des effets défavorables pour le sujet des données. C'est pourquoi la LPD doit exiger que des mesures techniques et organisationnelles appropriées soient mises en œuvre pour chaque traitement en vue de protéger les données contre tout accès, contre leur destruction, leur perte, leur utilisation, leur modification ou leur divulgation, que ce soit accidentellement ou sans autorisation. En déterminant de telles mesures, les contrôleurs (et, le cas échéant, les informaticiens) doivent tenir compte des conséquences potentiellement nuisisibles pour la personne, de la nature des données personnelles, du volume de données personnelles traité, du degré de vulnérabilité de l'architecture technique utilisée pour le traitement, de la nécessité d'interdire l'accès aux données, des conditions requises concernant la conservation à long terme, et ainsi de suite.

11.2. Les mesures de sécurité doivent également tenir compte de l'état actuel des méthodes et techniques de sécurisation de données (telles que pseudonymisation, encryptage, confidentialité, integrité, disponibilité et résilience des systèmes et services de traitement en permanence, mise à l'épreuve, appréciation et évaluation de l'efficacité des mesures techniques et organisationnelles à des intervalles réguliers) dans le domaine du traitement de données. Le coût des mesures de sécurité doit être proportionné à la gravité et la probabilité des risques potentiels.

12 Notification de violation de données

12.1. Notification à l'ASD

12.1.1. Sachant que les violations de données peuvent nuire gravement à la protection de la vie privée et des données des personnes, dans le cas d'une violation de données qui est susceptible d'entraîner un risque élevé d'atteinte aux droits et libertés des sujets de données, les contrôleurs (et, le cas échéant, les informaticiens) doivent être tenus de documenter tous les faits se rapportant à la violation des données, aux conséquences éventuelles et aux mesures prises et/ou envisagées pour régler la question de la violation et de notifier l'ASD, dans les plus brefs délais et au plus tard dans les 72 heures après s'en être rendus compte.

12.1.2. Dans le cas où l'ASD n'est pas notifiée dans les 72 heures, la notification doit être accompagnée de justifications du retard.

12.1.3. Dans le cas et dans la mesure où il n'est pas possible de fournir les informations dans un même temps, il faut les fournir progressivement par étapes sans plus de retard indû.

12.2. Notification au(x) sujet(s) des données

12.2.1. Dans le cas où une violation de données personnelles est susceptible d'entraîner un risque élevé d'atteinte aux droits et libertés des sujets de données, tel que discrimination, vol ou usurpation d'identité, perte financière, atteinte à la réputation, perte de confidentialité de données protégées par le secret professionnel ou tout autre préjudice économique ou social significatif, les contrôleurs (et, le cas échéant, les informaticiens) doivent également notifier la violation des données personnelles au sujet des données dans les plus brefs délais.

12.2.2. La communication au sujet des données doit décrire, dans un langage simple et clair, la nature de la violation des données, indiquer des points de contact et recommander des mesures pour régler la violation et/ou en atténuer les effets nuisibles éventuels.

12.2.3. Dans les cas où le contrôleur (et, le cas échéant, l'informaticien) n'informe pas de son propre chef le(s) sujet(s) de données de la violation des données, l'ASD, après avoir pris en considération les effets nuisibles probables de la violation, doit être autorisée à exiger du contrôleur (et, le cas échéant, de l'informaticien) qu'il le fasse.

13 Circulation transfrontalière de données personnelles

13.1. La libre circulation de données personnelles peut favoriser de multiples objectifs nationaux, y compris l'expansion de l'économie numérique, et ne doit pas être entravées par la LPD, sauf pour ce qui des fondements énoncés dans la présente politique. Il devrait être impératif de s'assurer qu'un niveau de protection au moins équivalent est accordé aux données personnelles quand elles sont transférées au-delà des frontières tel que c'est prévu dans la juridiction du Vanuatu. Un transfert transfrontalier de données personnelles ne doit donc avoir lieu que si un niveau de protection approprié, basé sur celui prévu au Vanuatu, est garanti. La politique du gouvernement de Vanuatu part du principe que toutes les données générées et/ou recueillies au Vanuatu doivent toujours être soumises aux lois et structures d'administration du Vanuatu et ne doivent pas être utilisées ailleurs sans l'autorisation préalable des autorités compétentes, que ce soit pour une catégorie de transferts ou un transfert en particulier, ou par loi. Cette 'autorisation préalable' est obligatoire pour tout le trafic transfrontalier de données personnelles[13] (voir aussi art. 4 de cette politique).

13.2. Un niveau de protection approprié doit pouvoir être garanti par :

(a) la loi du pays ou l'organisation internationale destinataire, y compris des traités ou accords internationaux applicables, avec un niveau de protection au moins équivalent à celui prévu dans la juridiction du Vanuatu ; ou

(b) des sauvegardes type, ponctuelles ou approuvées, prévues par des instruments obligatoires et exécutoires, adoptées et appliquées par les contrôleurs ou les informaticiens intervenant dans le transfert et le nouveau traitement.

13.3. Pour la coopération internationale en matière d'exécution de la loi, une base juridique appropriée concernant le transfert doit être vérifiée et constatée et un niveau de protection approprié des données garanti.

13.4. Cette politique reconnaît les avantages économiques et sociétaux que la circulation transfrontalières de données peut apporter, notamment par des solutions technologiques efficaces et d'avant-garde comme les services de conservation du 'cloud', à condition qu'elles comportent des sauvegardes et des garanties appropriées pour la protection des données personnelles et soient en conformité avec la classification nationale de sécurité des informations du Vanuatu.

---

13 Décision nº 171 de 2021 du Conseil des Ministres du gouvernement de Vanuatu relative à la protection des données et de la vie privée (réunion nº 016 , jeudi 5 août 2021).

14 Droits des personnes (sujets de données)

14.1. La présente politique stipule les droits que chaque personne doit pouvoir exercer concernant le traitement de données à caractère personnel la concernant, lesquels seront ensuite intégrés à la législation. Chaque personne doit avoir le droit:

(a) de ne pas faire l'objet d'une décision qui la touche de façon significative basée uniquement sur un traitement automatisé de ses données personnelles sans que ses points de vue n'aient été pris en considération;

(b) d'obtenir, sur demande, à des intervalles acceptables et sans retard ou coût excessif, confirmation du traitement de données personnelles la concernant; communication, sous une forme intelligible, des données traitées; toutes les informations sur leur origine, sur la durée de leur conservation de même que toute autre information que le contrôleur est tenu de fournir afin de garantir la transparence du traitement;

(c) d'obtenir, sur demande, les raisons du traitement de données personnelles la concernant;

(d) de s'opposer à tout moment au traitement de données personnelles la concernant sauf si le contrôleur montre qu'il y a des motifs légitimes de procéder au traitement lesquels l'emportent sur ses intérêts ou droits fondamentaux et libertés individuelles;

(e) d'obtenir, sur demande, gratuitement et sans délai excessif, la rectification ou la suppression des données traitées contrairement aux dispositions de la LPD;

(f) d'avoir recours, judiciairement ou autrement, pour violation de la LPD; et

(g) de bénéficier, indépendamment de sa nationalité ou de son lieu de séjour, de l'assistance de l'ASD dans l'exercice de ses droits.

14.2. L'alinéa 14.1a) ne s'applique pas en cas de décision autorisée par la loi à laquelle le contrôleur est soumis et laquelle impose aussi des mesures pertinentes pour préserver les droits, libertés et les intérêts légitimes du sujet des données.

15 Exceptions

15.1. Les droits à la protection de la vie privée et des données à caractère personnel ne doivent pas être considérés comme des droits absolus. Ils doivent être conciliés avec d'autres droits humains et libertés individuelles, dont la liberté d'expression, et peuvent être sujets à des exceptions spécifiques pour le traitement légal de données personnelles entrepris pour des intérêts publics ou privés importants.

15.2. La LPD pourra aménager des exceptions et des restrictions à un nombre limité de dispositions (ex. en lien avec le principe de transparence et les droits du sujet des données) à la condition que de telles exceptions soient prévues par la loi, respectent l'esprit des droits fondamentaux et libertés individuelles et constituent des mesures nécessaires et proportionnées dans une société démocratique pour la protection de la sécurité nationale, la défense, la sécurité publique, d'importants intérêts économiques et financiers de l'Etat, l'impartialité et l'indépendance du judiciaire ou la prévention, l'investigation et la poursuite de délits criminels et l'exécution de peines criminelles et d'autres objectifs essentiels d'intérêt public général ou la protection du sujet des données ou des droits fondamentaux et libertés individuelles de tiers, et notamment la liberté d'expression.

15.3. La portée et le contenu des exceptions doivent être limités au minimum nécessaire pour parvenir à l'objectif légitime poursuivi et l'utilisation d'exception et de restrictions sera soumise à des sauvegardes objectives et adéquates contre toute application globale ou arbitraire, telles qu'une supervision efficace et indépendante.

15.4. Des exceptions applicables à des activités de traitement à des fins de sécurité et de défense nationales doivent faire l'objet d'un examen indépendant et efficace prévu par la législation.

16 Création d'une Commission de sécurité numérique

16.1. Il est indispensable d'avoir une Commission de supervision totalement indépendante et impartiale dotée des pouvoirs et des ressources nécessaires pour superviser, surveiller et veiller au respect de la LPD en vue de sauvegarder la protection des données et les droits à la vie privée des personnes. La CSN/ASN??? doit avoir quatre attributs essentiels: i) indépendance; ii) attributions pertinentes; iii) ressources nécessaires pour s'acquitter de ses fonctions; et iv) transparence maximum dans l'exécution de ses fonctions de règlementation.

16.2. La CSN/ASN devra être créée par la LPD en tant qu'organisme administratif indépendant. La LPD doit stipuler que cet organisme agira en toute indépendance et impartialité dans l'accomplissement de ses devoirs et l'exercice de ses pouvoirs et, ce faisant, ne sollicitera ni n'acceptera des instructions. La LPD disposera de la méthode de nomination de ses membres et les conditions de leur mandat, de la portée de sa mission, de ses tâches et pouvoirs, de sa faculté d'acquérir des biens immobilier et d'ester en justice[14].

16.3. La CSN/ASN pourra être structurée sous diverses formes pour satisfaire à ces conditions, notamment : i) un Commissaire unique, chargé de la protection des données uniquement ; ou ii) une Commission (composée de plusieurs commissaires), chargée de la protection des données uniquement ; ou iii) un Commissaire ou une Commission chargée d'autres responsabilités (ex. droit à l'information ; médiateur ; lutte contre la discrimination).

16.4. Conformément à la reconnaissance du droit à la vie privée comme droit fondamental humain par le gouvernement de Vanuatu et du fait que le Vanuatu est partie à des conventions internationales sur les droits humains qui incluent cette reconnaissance[15], la LPD doit confirmer expressément que la CSN/ASN traitera la vie privée d'une personne comme un droit fondamental humain. La CSN/ASN doit exercer ses pouvoirs et s'acquitter de ses fonctions en conformité avec la culture, les traditions et les valeurs du Vanuatu[16].

16.5. La CSN/ASN doit être habilitée à s'acquitter des fonctions suivantes:

(a) de surveiller et faire respecter l'application de la LPD;

(b) de détenir et d'exercer des pouvoirs d'investigation et d'intervention en réponse à la fois à des réclamations et à des investigations menées à l'initiative de la CSN/ASN (de son propre chef);

(c) de s'occuper de réclamations déposées par des sujets de données concernant leurs droits à la protection des données et de les tenir informés de la suite qui y est donnée;

---

14 Vanuatu's *Right to Information Act* Part 6 ('Information Commissioner'), particularly s. 58, is an example of such provisions.

15 An example is Vanuatu's recognition of the right to privacy as a fundamental human right (by virtue of Chapter 2, Part 1, Section 5 of the Constitution) and by it being party to international human rights conventions,

16 An example is the reference to Ni-Vanuatu culture and traditions in its RTI Act s. 52(5)(a).

(d) d'autoriser et de valider des sauvegardes type à l'égard de la circulation transfrontalière de données;

(e) de prendre des décisions concernant des infractions à la LPD et imposer les sanctions administratives nécessaires, que ce soit à la suite d'une réclamation ou d'une investigation de son propre chef ; de telles décisions doivent être sujettes à un droit d'appel par devant les tribunaux;

(f) d'introduire ou d'être partie à des poursuites judiciaires comme prévu par la LPD et d'avoir le pouvoir de porter des infractions aux dispositions de la LDP à l'attention d'autres autorités;

(g) d'émettre des opinions et d'approuver des codes de conduite règlementaires ou des lignes directrices concernant le traitement de données personnelles, comme prévu par la LPD;

(h) de publier des rapports de ses activités; et

(i) d'aider des personnes à exercer leurs droits aux termes de la LPD.

16.6. La mission de la CSN/ASN doit inclure une obligation de coopération internationale, de promouvoir la sensibilisation du public au sujet de ses attributions, de ses pouvoirs et de ses activités ; des droits des sujets de données et de l'exercice de tels droits ; et de sensibiliser les contrôleurs et les informaticiens quant à leurs obligations légales aux termes de la LPD, surtout s'agissant du traitement de catégories particulières de données telles que celles des enfants et d'autres personnes vulnérables.

16.7. La CSN/ASN doit être consultée au sujet de propositions de mesures législatives ou administratives impliquant le traitement de données personnelles et au sujet de demandes et de réclamations de la part de sujets de données.

16.8. Afin de garantir l'indépendance financière de la CSN/ASN, celle-ci doit être dotée de ressources techniques et financières suffisantes, de même que des locaux et des équipements nécessaires pour qu'elle puisse s'acquitter efficacement de ses tâches et exercer ses pouvoirs, y compris les tâches qui doivent être menées dans le contexte de la coopération internationale. La LPD doit préciser les sources de financement pour la CSN/ASN, y compris sous forme de subventions d'aide.

16.9. La CSN/ASN doit être dotées des moyens nécessaires pour pouvoir nommer des employés compétents et développer sa capacité interne en vue de s'acquitter efficacement de ses fonctions.

16.10. Les employés de la CSN/ASN doivent être tenus au secret dans l'accomplissement de leurs devoirs et l'exercice de leurs pouvoirs.

16.11. La CSN/ASN doit être habilitée à s'engager dans la coopération internationale et à s'acquitter des fonctions de protection des données qui sont nécessaires pour remplir des obligations éventuelles découlant de conventions internationales auxquelles le Vanuatu pourrait devenir partie, y compris d'apporter concours à des sujets de données.

16.12. La CSN/ASN doit s'attacher à faire preuve de transparence maximum dans ses fonctions de règlementation (sanctions, compensation, incitations à la conformité, etc). En plus d'un rapport annuel qui doit être présenté au Parlement, elle doit régulièrement publier sur son site internet les résultats de ses investigations (que ce soit suite à des réclamations ou de sa propre initiative) sélectionnées sur la base de critères d'importance objectifs. Une telle publication d'investigations doit citer le nom du contrôleur ou de l'informaticien concerné si tel est justifié en guise de dissuasion.

17 Délits, pénalités administratives et recours

En plus d'ordres de se conformer à la LPD, diverses dispositions doivent être employées pour garantir l'exécution réelle de la LPD, y compris concernant i) des délits qui doivent faire l'objet de poursuites judiciaires; ii) des pénalités administratives (amendes) pour infractions à la LPD qui peuvent être infligées par la CSN/ASN; et iii) des actions intentées par des sujets de données pour obtenir l'exécution de jugements à l'encontre d'un contrôleur ou d'un informaticien. Deux autres moyens de veiller à la conformité sont: iv) réparations pour les sujets de données; et v) renforcement de la conformité volontaire.

Le résultat recherché est un système de 'règlementation réactive' : une pyramide de sanctions de plus en plus sévères ; leur application est transparente pour toutes les parties et le public ; la visibilité de sanctions moins sévères réduit la nécessité d'en infliger de plus sévères; et une conformité accrue réduit la nécessité d'imposer des sanctions.

17.1. La liste des délits, des peines et des défenses d'une personne accusée de ces délits sera définie suivant le système de la justice pénale nationale, y compris la législation sur la cybercriminalité telle qu'applicable. Les délit doivent inclure : l'obtention et la divulgation de données personnelles contrairement à la loi ; la modification de données personnelles pour empêcher la divulgation à des sujets de données ; le fait d'entraver l'exercice de pouvoirs d'entrée dans des locaux ; fausse déclaration faite en réponse à un avis lancé par la CSN/ASN; et la destruction ou la falsification d'informations demandées par la CSN/ASN.

17.2. Les amendes administratives prévues par la LPD doivent être efficaces, proportionnelles et dissuasives. Elles doivent pouvoir être appliquées efficacement aussi bien à l'égard de petites ou moyennes entreprises que de grosses sociétés multinationales.

17.3. Les sujets de données doivent avoir le droit de saisir directement le tribunal compétent au Vanuatu pour faire respecter la LPD sans avoir à passer d'abord par la CSN/ASN. Ils doivent pouvoir nommer une organisation à but non lucratif pour exercer tous les droits des sujets de données par devant la CSN/ASN ou les tribunaux du Vanuatu.

17.4. La LPD doit disposer de réparations dans le cas où un sujet de données subit ou pourrait subir des dommages matériels ou immatériels à cause d'infractions réelles ou anticipées à la LPD commises par un contrôleur ou un informaticien.

17.5. La CSN/ASN doit être habilitée à ordonner l'attribution d'un dédommagement à l'encontre d'un contrôleur ou d'un informaticien pour dommage matériel (tel que perte d'emploi ou atteinte au degré de solvabilité) ou dommage immatériel (tel qu'affliction) résultant d'une infraction à la LPD.

17.6. Tous les ordres rendus par la CSN/ASN doivent faire l'objet d'un droit d'appel par l'une ou l'autre des parties auprès du tribunal compétent. Pour l'attribution d'un dédommagement, les motifs de l'appel peuvent inclure un montant de dommages-intérêts.

18 Renforcement de la conformité – Education et soutien à la communauté

Une fois en établie, la CSN/ASN doit se charger en permanence de veiller à ce que la communauté, parmi tous les groupes de parties prenantes concernées, comprenne l'objet et les fonctions de la CSN/ASN et que la mise en conformité avec la LPD bénéficie d'un renforcement positif.

Pour que la règlementation réactive soit vraiment efficace, elle doit inclure le développement de mesures de renforcement positives pour assurer la conformité avec la LPD, y compris des encouragements tels que éloges informels et publicité pour bonnes pratiques, éloges formels dans les rapports annuels, concours et prix.

19 Suivi et évaluation

L'Autorité de sécurité numérique (ASN) est une autorité de supervision indépendante et impartiale, dotée des pouvoirs et des ressources nécessaires pour superviser, surveiller et faire respecter la conformité avec la LPD. Ceci est crucial pour la protection des données et les droits à la vie privée des personnes. Il est impératif que l'ASN surveille et assure proactivement l'élaboration et l'application de la LPD et de ses plans d'action, en identifiant des lacunes éventuelles dans le processus, des aspects qu'il faudrait améliorer et tiennent les contrevenants responsables de leurs actions.

Un plan directeur de mise en œuvre de la politique de protection des données et de la vie privée doit être élaboré en vue de prévoir des plans d'action et des activités qui seront guidés par cette politique. Le plan directeur de mise en œuvre permettra d'en assurer proactivement le suivi et l'évaluation et l'exécution.

19.1. Suivi : le Commissaire de la protection des données et de la vie privée coordonne, surveille et rend compte de l'avancement de la mise en œuvre de la LPD à l'Autorité de sécurité numérique et produit les deux rapports importants suivants:

(a) Rapport trimestriel : rendant compte de la mise en œuvre de la LPD;

(b) Rapport annuel : rendant compte des progrès réalisés au cours de l'année vers les cibles de la LPD comme indiqué dans le plan directeur de mise en œuvre. Il sera produit durant le premier trimestre de l'année et doit être utilisé par les preneurs de décisions pour renseigner les décisions de programmation du gouvernement en vue de parvenir aux cibles nationales dans 'Vanuatu 2030'.

19.2. Evaluation : La mise en œuvre de la LPD permettra de détecter ce qu'il y a lieu de réexaminer.

Nationale du Vanuatu Politique de Protection des Données et de la Vie privée