Republic of Vanuatu

Vanuatu National Data Protection & Privacy Policy

The Prime Minister's Foreword

Hon. Alatoi Ishmael KALSAKAU

I am pleased to present to you Vanuatu's National Data Protection and Privacy Policy 2023, a Policy that complements and strengthens our efforts outlined in the National Cyber Security Strategy of 2030. It creates the foundation of Vanuatu's data protection and privacy law that will give effect to associated rights enshrined in the Constitution and international instruments to which Vanuatu is a party thus, express the commitment of the State to ensure respect for, and the protection of, personal data and associated rights of individuals including the right to privacy.

The Constitution of the Republic of Vanuatu (2006) (the "Constitution"), recognizes that "all persons are entitled" to a number of "fundamental rights and freedoms." Such fundamental rights and freedoms can be adversely impacted by the use of personal data. Thus, the Government of the Republic of Vanuatu wishes to adopt legislative measures to help guide, protect and respect personal data, associated fundamental rights and freedoms and to ensure public trust in the use of personal data.

Moreover, it is crucial for citizens, businesses, and online platforms in Vanuatu operate and respect the basis set out in the Constitution" of Vanuatu (Chapter 2, Part 1 Section 5) – which recognizes that all persons are entitled to several "Fundamental Rights and Freedoms" as well as provides for the "Protection of the Privacy of the Home." It means "Respect and Responsibility" must predominate online communication, mainly when communicating via emails, texts, pictures, website content, blog posts, comments, online forums, social media, and phone-based apps.

I am calling on all stakeholders and citizens, including tourists traveling into Vanuatu, to prioritize and effectively collaborate with the Government of Vanuatu and respective authorities on this national Policy – a task and effort to make sure that all data generated and/or collected in Vanuatu must always be subjected to the laws and governance structures of Vanuatu and must not be used elsewhere without prior authorization from relevant authorities, for either a class of transfers or a particular transfer, or by law.

Hon. MAAU'KORO, MOLI TAMBE,

URE VIRA TAMBE, LAVISE VAHE

ALATOI ISHMAEL KALSAKAU (MP), Prime Minister

Acknowledgement

The development of the National Data Protection & Privacy Policy would not have been successful without the determined efforts and contributions of the Council of Europe, the National Data Protection and Privacy Taskforce members and individuals. This includes the financial and technical support from stakeholders and institutions.

Tankio tumas to the Government through the Prime Minister and the Director General, the Chief Information Officer (CIO), and the Deputy CIO of the Prime Minister's Office for their assistance and enthusiasm in developing this significant National Policy.

Tankio tumas to the Council of Europe who helped provide technical experts and financial support to the development of this policy.

Tankio tumas to various institutions who helped provide technical and financial support towards the development of this Policy, particularly the Australian High Commission in Vanuatu, the Computer Emergency Response Team (CERTVU), the Right to Information unit (RTI), the Telecommunications Radiocommunications and Broadcasting Regulator's (TRBR) Office, the Reserve Bank of Vanuatu (RBV), the Vanuatu Bureau of Statistics (VBoS), the department of Civil Registry and Vital Statistics (VRVS), the Financial Intelligence Unit (FIU), the Office of the Public Prosecution (OPP) of Vanuatu, the Public Service Commission (PSC), and the Ministry of Justice and Community Services (MJCS) of Vanuatu.

Tankio tumas to all the Provincial Technical Advisory Groups (PTAG), the dedicated agencies, and their representatives who took part and contributed to the nationwide consultation workshops and also the Policy review committee.

Finally, tankio tumas to all government agencies, state-owned enterprises, private sector organizations, non-government organizations, schools, communities, and Internet users who have accepted and responded to our consultation invitations and online awareness sessions, including talkback shows. Your contributions have shaped this Policy into a user-centric government instrument that will empower national efforts to safeguard the public trust in the use of personal data.

Abbreviations

CoE:	Council of Europe
DPA:	Data Protection Act
GDPR:	General Data Protection Regulation
EU:	European Union
ICT:	Information, Communication and Technology
DSA:	Digital Safety Authority
UN:	United Nations

Definitions

Anonymisation means the process applied to personal data so that the data subjects can no longer be identified, either directly or indirectly, without expenditure of unreasonable time, effort or resources;

Biometric data means personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

Consent means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the specified processing of personal data relating to him or her;

Cloud Storage means data deposit model in which data are stored on virtual servers hosted by third parties;

Data Controller means the natural or legal person, public authority, service, agency or any other body which, alone or jointly with others, has decision-making power with respect to data processing;

Data Breach means a breach of security by any person leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

Data processing means any operation or set of operations performed on personal data, such as the collection, storage, preservation, alteration, retrieval, disclosure, making available, erasure, or destruction of, or the carrying out of logical and/or arithmetical operations on such data. Where automated processing is not used, "data processing" means an operation or set of operations performed upon personal data within a structured set of such data which are accessible or retrievable according to specific criteria;

Genetic data means all data relating to the genetic characteristics of an individual which have been either inherited or acquired during prenatal development, as they result from an analysis of a biological sample from the individual concerned, in particular chromosomal, DNA or RNA analysis or analysis of any other element enabling equivalent information to be obtained;

Health-related data means all personal data concerning the physical or mental health of an individual, including the provision of health-care services, which reveals information about this individual's past, current and future health;

Identifiable individual means an individual who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, image, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that individual;

Personal data means any information or data, whether included in a record or not, relating to an identified or identifiable individual ("data subject"), or which enables singling out or enables interaction with a person as an individual;

Data Processor means a natural or legal person, public authority, service, agency or any other body which processes personal data on behalf of the controller;

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable individual;

Special categories of personal data mean genetic data; personal data relating to offences, criminal proceedings and convictions; biometric data uniquely identifying a person; personal data relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life.

Table of Contents

1 Introduction

The development of information, communication, and technology (ICT) and the increasing globalisation of services involve the collection and use of richly detailed personal and sensitive data about individuals in greater volumes than ever before across the private and public sectors.

While data-driven solutions and digitalisation have great potential to accelerate economic growth, societal benefits, greater inclusion and access to services, they also pose new risks for the rights and fundamental freedoms of individuals that require a reciprocal legal and policy response. The changing national and global data protection legal frameworks and ecosystem call for a collaborative effort to respond to public concerns, an effective fight against the spread of cybercrime and solid legislative and regulatory frameworks.

The Constitution of the Republic of Vanuatu (2006) (the "Constitution")[1], recognises that "all persons are entitled" to a number of "fundamental rights and freedoms." Such fundamental rights and freedoms can be adversely impacted by the use of personal data. Chapter 2, Part 1, Section 5 of the Constitution expressly recognises and provides for protection of the privacy of the home, and for the protection of the law with regards to other fundamental rights and freedoms which imply the requirement to protect privacy. To this end, the Government of the Republic of Vanuatu wishes to adopt legislative measures to help respect and protect personal data and associated fundamental rights and freedoms and to ensure public trust in the use of personal data.

The Government of the Republic of Vanuatu wishes to build on the right to privacy and associated rights enshrined in the Constitution and in international instruments to which Vanuatu is a party such as the United Nations (UN) International Covenant on Civil and Political Rights (Article 17)[2], Convention on the Rights the Child (Article 16)[3], Convention the Rights of Persons with Disabilities (Article 22)[4] and Council of Europe (CoE) Convention on Cybercrime (Article 15)[5]. It also wishes to meet international best practices and, in particular those set out in the only legally binding international treaty in the field – the CoE Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108 of 1981, "Convention 108")[6] as well as its amending protocol (CETS No. 223 of 2018, "Convention108+")[7].

---

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

2 International Covenant on Civil and Political Rights, https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

3 Convention on the Rights the Child, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-child

4 Convention the Rights of Persons with Disabilities, https://www.ohchr.org/en/instruments-mechanisms/instruments/convention-rights-persons-disabilities

5 The Budapest Convention and its Protocols, 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

This National Data Protection Policy is fully aligned with Vanuatu 2030 - The People's Plan,[8] the National Cyber Security Strategy 2030[9] and other national policies. It is also informed by Vanuatu Government's Council of Minister Decision No. 171 of 2021.[10] The Policy reflects the increasing recognition of the need to define government policies related to information society in an integrated and holistic manner and to enshrine the protection of personal data and privacy in the domestic law of the Republic of Vanuatu in line with international best practice, in particular the modernised Convention 108+ and the EU's General Data Protection Regulation (GDPR).[11]

This Policy was developed with technical assistance provided by the Global Action on Cybercrime Extended (GLACY+) project, a joint initiative of the CoE and the EU.

---

8 National Sustainable Development Plan 2016 to 2030- Vanuatu 2030

9 National Cyber Security Strategy 2030 <Vanuatu_National_CyberSecurity_Strategy2030_Booklet.pdf (gov.vu)>

10 Vanuatu Government's Council of Minister Decision No. 171 of the 5th of August 2021.

11 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2 Purpose of the Policy

The purpose of this Policy is to create the foundations of a data protection and privacy law that will give effect to associated rights enshrined in the Constitution and international instruments to which Vanuatu is a party and to express the commitment of the State to ensure respect for, and the protection of, personal data and associated rights of individuals, and in particular the right to privacy. Data protection is one aspect of the protection of privacy, but there are other aspects of privacy protection, such as physical intrusions, not covered by this policy.

While this Policy only deals in detail with personal data, it recognises the need for and the importance of policies dealing with other (non-personal) data, particularly in relation to its importance to Vanuatu's data sovereignty. Vanuatu's data sovereignty is its right to determine which laws apply to the processing of data (both personal and non-personal) that is collected or generated in or about Vanuatu. This data sovereignty requires policies to be developed concerning data ownership, 'data as a commodity' operationalised through a secure protected transparent infrastructure, and overall, the need for a clear definition and governance model for data created, stored and re-used.

This Policy sets out the basis for achieving those objectives in relation to personal data, and other policies and laws will do so in relation to non-personal data.

3 Objective

The objective of the Policy is to inform the development of a Data Protection Act (DPA) which will achieve the following:

3.1. Contribute to respect for and the protection of the fundamental rights and freedoms of natural persons, and in particular, their right to privacy with respect to the processing of their personal data;

3.2. Ensure the harmonisation of government policies on cyber security, fight against cybercrime and the protection of individuals' privacy including their implementation and continuous assessment in relation of the resilience of critical national infrastructure and services;

3.3. Help establish an appropriate institutional framework to ensure the effective implementation and oversight of a national data protection and privacy law, including both appropriate penalties and redress mechanisms (including compensation);

3.4. Establish and share internationally recognised best practices in data protection and privacy law;

3.5. Establish the requirement for an independent and impartial Digital Safety Authority (DSA) appropriately empowered, resourced and equipped to sufficiently oversee, monitor and enforce compliance and safeguarding of the data protection and privacy rights of individuals;

3.6. Ensure additional protection with regards to the processing of personal data about children in accordance with Article 16 of the UN Convention on the Rights of the Child;

3.7. Ensure appropriate safeguards for the processing of special categories of personal data to prevent adverse effects for individuals;

3.8. Ensure that personal data processed in Vanuatu is subject to the laws and governance structures of Vanuatu and always remains protected by the relevant national legal and governance frameworks, thus increasing the integrity of personal data within Vanuatu and contributing to the protection of individuals in Vanuatu.

3.9. Promote the harmonization of Vanuatu's data protection legal framework with other regional and international jurisdictions ensuring the flow of personal data under conditions of assurance and trust.

3.10. ensure consistency with and advance Vanuatu's culture, traditions and values.

Note: 1. Add more objectives

4 Scope

4.1. The policy should elaborate and cover crucial components that will enable the development of the Data Protection Law as well as specific mandates to ensure Vanuatu not only achieve the development and enforcement of the Data Protection Act but also mechanisms which entails procedures and processes of protection Personal Identifiable Information.

Therefore, the scope of this policy covers the protection of Personal Identifiable Information, relevant procedures and processes included in other legislative frameworks of Vanuatu and at the international context, implementation of national regulations, and the finally establishment of the Data Protection Act (DPA) of Vanuatu.

4.2. The DPA should apply to:

4.2.1. The processing of personal data in the private and public sectors, whether by automated or non-automated means, irrespective of the nationality or place of residence of the natural person who is the subject of the processing of personal data;

4.2.2. Processing of personal data or special categories of personal data about living individuals and not about deceased persons;

4.2.3. Processing of personal data undertaken within the jurisdiction of Vanuatu;

4.2.4. Processing of personal data generated or collected in Vanuatu, irrespective of where the processing is undertaken.[12]

12 Vanuatu Government's Council of Ministers Decision No. 171 of 2021) on Data Protection & Privacy (meeting No. 016 , Thursday 5 August 2021) provides that all data generated and/or collected in Vanuatu must always be subjected to the laws and governance structures of Vanuatu and must not be used elsewhere without prior authorisation from relevant authorities. See also section 13 of this Policy.

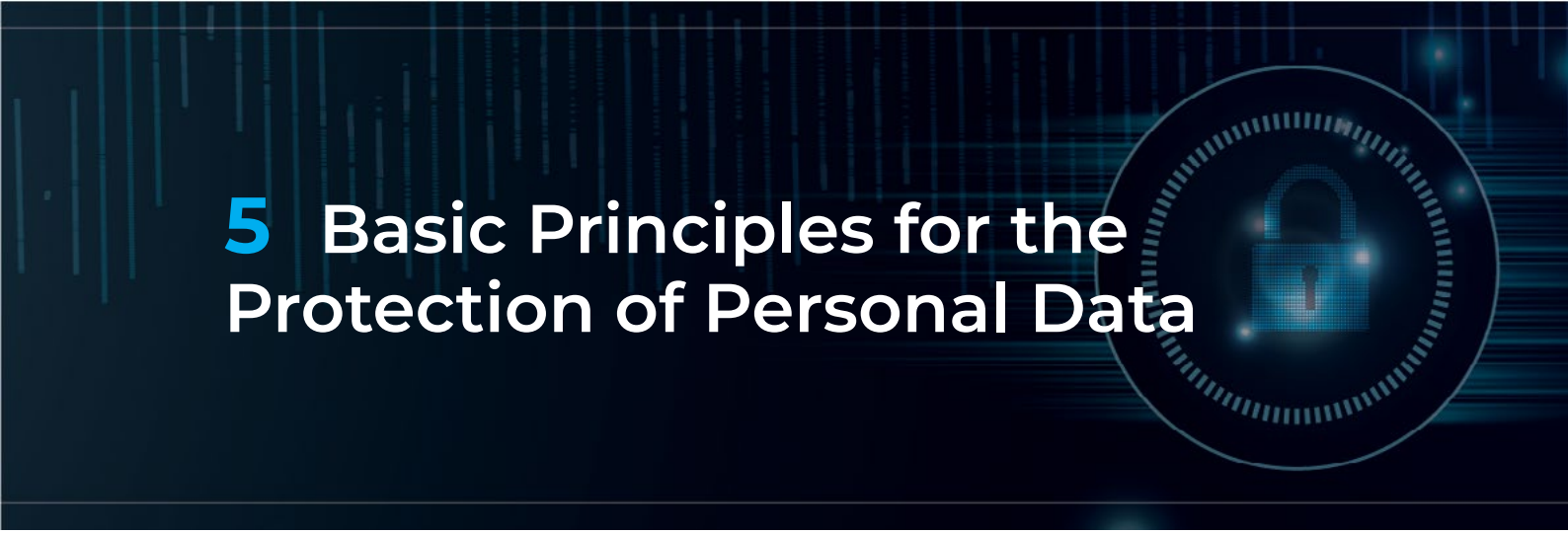
4.2.5. Processing of personal data of individuals who are in Vanuatu by a controller or processor not established in Vanuatu, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such individuals in Vanuatu; or

(b) the monitoring of their behaviour as far as their behaviour takes place within Vanuatu.

4.3. The DPA should not apply to the processing of personal data done purely for personal or household activities.

4.4. The DPA should define and promote data sovereignty in relation to personal data, and create data protection mechanisms which clarify data sovereignty and data ownership in relation to personal data.



5 Basic Principles for the Protection of Personal Data

Personal data and special categoris of personal data should be processed fairly, lawfully, transparently and in a manner that is proportionate in relation to the legitimate purpose pursued. At all stages of the processing, a fair balance should be struck between all interests concerned, whether public or private, and the rights and freedoms of individuals. Based on Convention 108+ and international best practices, the DPA should set out the following basic principles to be respected and applied at all stages of the data processing:

5.1. Fair, transparent and lawful processing

5.1.1. Personal data should be processed **fairly**.

5.1.2. Personal data should be processed in a **transparent** manner. Data subjects have the right to know about the processing of their personal data. Controllers should be required to act transparently to ensure fairness of processing and to inform data subjects in an appropriate form of the controller's identity and other key information about the processing and their rights in order to ensure fair and legitimate processing.

5.1.3. Personal data should be processed **lawfully** and should have a legitimate basis as set out in paragraph 6.

5.2. Specific Legitimate Purpose and Purpose Limitation

5.2.1. Personal data should be processed for **explicit, specified, and legitimate purposes** and the processing of these particular data should serve those purposes and should not be incompatible with them.

5.2.2. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes may be considered compatible with those purposes, subject to appropriate safeguards being put in place.

5.3. Data Minimisation

5.3.1. Personal data undergoing processing should be **adequate, relevant and not excessive** in relation to the purposes for which they are processed.

5.3.2. This requirement not only refers to the quantity, but also to the quality of personal data.

5.4. Accuracy

5.4.1. Personal data undergoing processing should be **accurate** and, to the extent necessary, should be kept up to date.

5.5. Storage Limitation

5.5.1. Personal data undergoing processing should be preserved in a form which permits identification of data subjects for no longer than is necessary for the purposes for which those data are processed.

5.5.2. Personal data should be deleted once the purpose for which it was processed has been achieved or should only be kept in a form that prevents any direct or indirect identification of the data subject ('anonymised').

5.6. Data Security and Security Breach Notification

5.6.1. The controller, and, where applicable the processor, should take reasonable and appropriate security measures to safeguard personal data against risks such as accidental or unauthorised access to, destruction, loss, use, modification or disclosure.

5.6.2. The controller should notify, without delay, at least the DSA of personal data breaches which may seriously interfere with the rights and fundamental freedoms of data subjects.

5.7. Demonstrable accountability

Controllers (and, where applicable, processors), should take all appropriate measures to comply with the principles set out in the DPA and be able to demonstrate that the data processing under their control complies with them.

6 Legitimate Basis

The DPA should strive to ensure the lawfulness of data processing by requiring that processing of personal data should only be carried out on the basis of the consent of the data subject or of some other legitimate basis laid down by the DPA or by law i.e., when processing personal data is necessary for the performance of a contract with the data subject, for the performance of a task carried out in the exercise of public authority, for compliance with a legal obligation to which the controller is subject, for the purpose of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject (particularly children), or if necessary to protect the vital interests of the data subject.

Processing on a legitimate basis also requires that personal data be processed in a transparent manner (see section 5.2).

7 Special Categories of Data

The processing of certain types of personal data, or the processing of certain personal data for the sensitive information it reveals, may lead to encroachments on the interests, rights and freedoms of individuals. This can, for instance, be the case where there is a potential risk of discrimination or injury to an individual's dignity or physical integrity or where the processing of personal data could affect the presumption of innocence or other important rights and freedoms.

7.1. The processing of the special categories of data should only be allowed where additional appropriate safeguards are established in law.

7.2. The safeguards should protect against risks that the processing presents for the interests and the rights and freedoms of the data subject, notably the risk of discrimination.

8 Processing relating to a child and other vulnerable individuals

8.1. The child's best interests shall be a primary consideration in all processing concerning children, and specific safeguards should apply to ensure that children are not subjected to arbitrary or unlawful interference with their rights in the digital environment.

8.2. Controllers (and, where applicable, processors) and the DSA should be required to give specific attention to the data protection rights of children and other vulnerable individuals and, where necessary, modify protections to ensure they are effective for these individuals.

9 Data Protection and Privacy by Design and by Default

9.1. To ensure that data protection requirements are integrated as early as possible, controllers (and, where applicable, processors) should examine the potential impact of the intended processing on the rights and fundamental freedoms of data subjects prior to the commencement of the processing and design the data processing in such a manner as to prevent or minimise the risk of interference with those rights and fundamental freedoms.

9.2. When setting up the technical requirements for default settings, controllers and processors should choose the most privacy-friendly standard configurations so that the usage of applications and software does not infringe the rights of the data subjects (data protection by default), and to avoid processing of more personal data than necessary to achieve the legitimate purpose.

10 Data Protection Impact Assessment

10.1. Where the processing of personal data is likely to result in a high risk to the rights and fundamental freedoms of data subjects, controllers (and, where applicable, processors) should -prior to the commencement of such processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data and should design the processing in such a manner to prevent or minimise such risks.

10.2. Data protection impact assessment should, in particular, be required in the case of:

(a) a systematic and extensive evaluation of personal aspects relating to individuals, which is based on automated processing, including profiling;

(b) processing on a large scale of special categories of personal data; and

(c) systematic monitoring of a publicly accessible area on a large scale.

10.3. 10.3 The Digital Safety Commission should also be able to establish and make public a list of other processing operations that require data protection impact assessment.

11 Data Security

11.1. The security of personal data is key to preventing adverse effects for the data subject. Thus, the DPA should require that appropriate technical and organisational measures are implemented for each processing to protect the data against accidental or unauthorised access to, destruction, loss, use, modification or disclosure. While determining appropriate technical and organisational measures, controllers (and, where applicable, processors), should take into account the potential adverse consequences for the individual, the nature of the personal data, the volume of personal data processed, the degree of vulnerability of the technical architecture used for the processing, the need to restrict access to the data, requirements concerning long-term storage, and so forth.

11.2. The security measures should also take into account the current state of the art of data-security methods and techniques (such as pseudonymisation, encryption, ongoing confidentiality, integrity, availability and resilience of processing systems and services, regular testing, assessing and evaluating the effectiveness of technical and organisational measures) in the field of data processing. The cost of security measures should be commensurate with the seriousness and probability of the potential risks.

12 Data Breach Notification

12.1. Notification to DSA

12.1.1. Recognising that data breaches can be very detrimental to the privacy and data protection rights of individuals, in case of a data breach that is likely to result in a high risk to the rights and freedoms of data subjects, controllers (and, where applicable, processors) should be required to document all facts relating to the data breach, its potential consequences and measures taken and/or proposed to address the breach and notify the DSA, without any undue delay, and not later than 72 hours after becoming aware of it.

12.1.2. Where the notification to the DSA is not made within 72 hours, it should be accompanied by reasons for the delay.

12.1.3. Where, and in so far as, it is not possible to provide the information at the same time, the information should be provided in phases without undue further delay.

12.2. Notification to the data subject(s)

12.2.1. Where a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects, such as discrimination, identity theft or fraud, financial loss, damage to reputation, loss of confidentiality of data protected by professional secrecy or any other significant economic or social disadvantage, controllers (and, where applicable, processors) should also communicate the personal data breach to the data subject without undue delay.

12.2.2. The communication to the data subject should describe in clear and plain language the nature of the data breach, provide contact points and recommend measures to address the data breach and/or mitigate its possible adverse effects.

12.2.3. In cases where the controller (and, where applicable, processor) does not on its own initiative inform the data subject(s) of the data breach, the DSA, having considered the likely adverse effects of the breach, should be allowed to require the controller (and, where applicable, processor) to do so.

13 Transborder Flows of Personal Data

13.1. The free flow of personal data can support multiple national objectives, including the expansion of the digital economy, and should not be impeded by the DPA except on the basis set out by this Policy. It should be essential to ensure that at least an equivalent level of protection is afforded to personal data when transferring it across borders as provided for within the jurisdiction of Vanuatu. The cross-border transfer of personal data therefore should only take place where an appropriate level of protection based on the level of protection provided in Vanuatu is secured. Vanuatu Government policy is that all data generated and/or collected in Vanuatu must always be subjected to the laws and governance structures of Vanuatu and must not be used elsewhere without prior authorisation from relevant authorities, for either a class of transfers or a particular transfer, or by law. Such 'prior authorisation' is required for all transborder flows of personal data [13] (See also section 4 of this Policy).

13.2. An appropriate level of protection should be able to be secured by:

(a) the law of the receiving country or international organisation, including applicable international treaties or agreements, ensuring at least an equivalent level of protection as is provided for within the jurisdiction of Vanuatu, or;

(a) ad hoc or approved standardised safeguards provided by legally binding and enforceable instruments adopted and implemented by controllers or processors involved in the transfer and further processing.

13.3. For international law enforcement co-operation an appropriate legal basis for the transfer should be ascertained and established and an appropriate level of protection of personal data ensured.

13.4. This policy recognised the economic and societal benefits that transborder flows of data can bring, notably through efficient and advanced technology solutions such as cloud storage services, provided they include appropriate safeguards and guarantees for the protection of personal data and are compliant with the National Information Security Classification of Vanuatu.

13 Vanuatu Government's Council of Ministers Decision No. 171 of 2021) on Data Protection & Privacy (meeting No. 016 , Thursday 5 August 2021).

14 Rights of Individuals (Data Subjects)

14.1. This Policy sets out the rights that every individual should be able to exercise concerning the processing of personal data relating to him or her, which will subsequently be incorporated in the legislation. Every individual should have the right:

(a) not to be subject to a decision significantly affecting him or her based solely on an automated processing of personal data without having his or her views taken into consideration;

(b) to obtain, on request, at reasonable intervals and without excessive delay or expense, confirmation of the processing of personal data relating to him or her; the communication in an intelligible form of the data processed; all available information on their origin; on the preservation period as well as any other information that the controller is required to provide in order to ensure the transparency of processing;

(c) to obtain, on request, knowledge of the reasoning underlying the processing of personal data about him or her;

(d) to object at any time to the processing of personal data concerning him or her unless the controller demonstrates legitimate grounds for the processing which override his or her interests or rights and fundamental freedoms;

(e) to obtain, on request, free of charge and without excessive delay, the rectification or erasure of such data processed contrary to the provisions of the DPA;

(f) to judicial and non-judicial remedies for violations of the DPA; and

(g) to benefit, whatever his or her nationality or residence, from the assistance of the DSA in exercising his or her rights.

14.2. Sub-paragraph 14.1(a) should not apply where the decision is authorised by law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

15 Exceptions

15.1. The rights to privacy and to the protection of personal data should not be viewed as absolute rights. They have to be reconciled with other human rights and fundamental freedoms, including freedom of expression and may be subject to specific exceptions for the lawful processing of personal data undertaken for important public or private interests.

15.2. The DPA may allow exceptions and restrictions to a limited number of provisions (e.g. related to the transparency principle and rights of the data subject) on condition that such exceptions are provided for by law, respect the essence of the fundamental rights and freedoms, and are necessary and proportionate measures in a democratic society for the protection of national security, defence, public safety, important economic and financial interests of the State, the impartiality and independence of the judiciary or the prevention, investigation and prosecution of criminal offences and the execution of criminal penalties, and other essential objectives of general public interest or the protection of the data subject or the rights and fundamental freedoms of others, notably freedom of expression.

15.3. The scope and content of the exceptions should be limited to the minimum necessary to achieve the legitimate objective pursued and the use of exceptions and restrictions shall be subject to objective and adequate safeguards against their blanket or arbitrary application, such as effective and independent supervision.

15.4. Exceptions for processing activities for national security and defence purposes should be subject to independent and effective review provided for by legislation.

16 Establishment of a Digital Safety Commission

16.1. A completely independent and impartial supervisory Commission appropriately empowered and equipped to oversee, monitor and enforce compliance with the DPA is crucial for safeguarding the data protection and privacy rights of individuals. The DSA should have four key attributes: (i) independence; (ii) sufficient functions; (iii) sufficient resources to carry out those functions; and (iv) maximum transparency in the operation of its regulatory functions.

16.2. The DSA should be established by the DPA as an independent administrative body, which should set out that it will act with complete independence and impartiality in performing its duties and exercising its powers, and in doing so shall neither seek nor accept instructions. The DPA should set out the mode of appointment of its members and the conditions regarding their term, the scope of its mandate, its tasks and powers, its ability to acquire property, sue and be sued.[14]

16.3. The structure of the DSA may take a number of forms that satisfy these conditions, including: (i) a single Commissioner, solely for data protection; or (ii) a Commission (multiple commissioners), solely for data protection; or (iii) a Commissioner or Commission also with other responsibilities (e.g., right to information; ombudsman; anti-discrimination).

16.4. Consistent with the Government of Vanuatu's recognition of the right to privacy as a fundamental human right and by being party to international human rights conventions involving such recognition,[15] the DPA should expressly confirm that the DSA will treat the privacy of an individual as a fundamental human right. The DSA should exercise its powers and functions consistent with Vanuatu's culture, traditions and values.[16]

16.5. The DSA should be empowered to carry out the following functions:

(a) to monitor and enforce the application of the DPA;

(b) to hold and exercise powers of investigation and intervention, in response to both complaints and 'DSA initiated' ('own motion') investigations;

(c) to handle complaints lodged by a data subject concerning their data protection rights and keep data subjects informed of progress;

(d) to perform the function of authorising and approving standardised safeguards relating to transborder data flows;

---

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).

(e) to make determinations relating to violations of the DPA and impose the necessary administrative sanctions, whether as a result of a complaint or an 'own motion' investigation; such decisions should be subject to a right of appeal through the courts;

(f) to institute or be a party to legal proceedings as provided for under the DPA, and to have the power to bring to the attention of other authorities' violations of the provisions of the DPA;

(g) to issue opinions and approve Statutory Codes of Conduct or Guidelines relating to the processing of personal data, as provided for under the DPA;

(h) to publish reports of its activities; and

(i) to assist individuals to exercise their rights under the DPA.

16.6. The DSA's mandate should include the responsibility to take part in international cooperation, to promote public awareness of its functions, powers and activities; the rights of data subject and exercise of such rights; and awareness of controllers, processors and their legal obligations under the DPA especially in processing special category of data such as that of children and other vulnerable individuals.

16.7. The DSA should be consulted on proposals for any legislative or administrative measures involving the processing of personal data, and requests and complaints from data subjects.

16.8. In order to ensure its financial independence, the DSA should be equipped with sufficient technical and financial resources as well as the premises and infrastructure necessary for the effective performance of its tasks and the exercise of its powers, including those to be carried out in the context of international cooperation. The DPA should set out the sources of funding for the DSA, including by way of grant-in-aid.

16.9. The DSA should be provided with the necessary resources to enable it to appoint skilled staff and build internal capacity to enable the effective performance of its functions.

16.10. The staff of the DSA should be bound by the obligations of confidentiality in the performance of their duties and the exercise of their powers.

16.11. DSA should be empowered to undertake international cooperation, and to perform the data protection functions that are necessary to give effect to any obligations arising from international agreements to which Vanuatu may become a party, including providing assistance to data subjects.

16.12. The DSA should aim to achieve maximum transparency in its regulatory functions (sanctions, compensation, compliance inducements etc). In addition to its annual report, tabled in the legislature, it should publish on its website, on a regular basis, the results of its investigations (either of complaints or self-initiated), selected on the basis of objective criteria of importance. Such publication of investigations should, where justifiable as a deterrent, name the controller or processor involved.

17 Offences, administrative penalties and remedies

In addition to orders to comply with the DPA, a number of means should be used to ensure effective enforcement of the DPA, including (i) offences, which require prosecution before the courts; (ii) administrative penalties (fines) for breaches of the DPA, which may be issued by the DSA; and (iii) actions by data subjects to obtain judicial enforcement against a controller or processor. Two further means of ensuring compliance are: (iv) remedies to data subjects; and (v) reinforcement for voluntary compliance.

The desired result is a system of 'responsive regulation': a pyramid of increasingly serious sanctions; their use is transparent to all parties and the public; the visibility of lesser sanctions reduces the need for higher ones; and increased compliance reduces the need for sanctions.

17.1. The list of offences, penalties and defences of a person charged with these offences will be determined in accordance with the national criminal justice order, including applicable cybercrime legislation. Offences should include: Unlawfully obtaining and disclosing of personal data; Alteration of personal data to prevent disclosure to data subject; Obstruction of powers of entry to premises; False statement made in response to a notice issued by the DSA; and Destruction or falsification of information requested by the DSA.

17.2. Administrative fines under the DPA should be effective, proportionate and dissuasive and able to be utilised effectively in relation to both a small or medium-size enterprise and a large multinational company.

17.3. Data subjects should have the right to proceed directly before the appropriate Vanuatuan court to enforce the DPA, without the necessity to first proceed before the DSA. They should be entitled to appoint a not-for-profit organisation to exercise all the rights of the data subject before the DSA or the courts of Vanuatu.

17.4. The DPA should provide remedies wherever a data subject has suffered or may suffer material or non-material damage because of actual or anticipated breaches of the DPA by a controller or processor.

17.5. The DSA should be empowered to order against a controller or processor the award of compensation for material damage (such as loss or employment, or damage to credit rating) or non-material damage (such as emotional distress) occurring as a result of a breach of the DPA.

17.6. All orders made by the DSA should be subject to a right of appeal by either party to the appropriate court. For an award of compensation, the grounds of appeal may include the quantum of damages.

18 Compliance reinforcement Community education and support

The DSA should have a continuing role, once the DPA is in force, in ensuring that there is community understanding, among all relevant stakeholder groups, of the purpose for and functions of the DPA, and that compliance with the DPA receives positive reinforcement.

For responsive regulation to be fully effective, it should include the development of positive reinforcements for compliance with the DPA, including such supports as informal praise and publicity for good practices, formal praise in annual reports, competitions and prizes.

19 Monitoring and Evaluation

The Digital Safety Authority (DSA) is an independent and impartial supervisory Authority appropriately empowered and equipped to oversee, monitor and enforce compliance with the DPA. This is crucial for safeguarding the data protection and privacy rights of individuals. It is vital that the DSA proactively monitor and enforce the development and implementation of the DPA and its action plans, identifying potential gaps in the process, outlining areas for improvement, and hold offenders accountable for their actions.

The Data Protection and Privacy Policy Implementation Matrix must be developed to provide action plans and activities that will be guided by this Policy. This Implementation Matrix will enable a proactive monitoring and evaluation phase and execution.

19.1. Monitoring: The Data Protection and Privacy Commissioner will coordinate, monitor, and report on the implementation progress of the DPA to the Digital Safety Authority and it will produce these two important reports;

(a) Quarterly Report : reports on the implementation of the DPA

(b) Annual Report: Reports on the progress made over the year towards the targets of the DPA as stated in the implementation matrix. This will be produced during the first quarter of the year and should be used by decision makers to inform Government programming decisions to achieve the national targets in 'Vanuatu 2030'.

19.1. Evaluation: The implementation of the DPA will determine the areas for review.

Vanuatu National Data Protection & Privacy Policy