REPUBLIC OF VANUATU

DATA PROTECTION AND PRIVACY ACT NO. 13 OF 2024

Arrangement of Sections

REPUBLIC OF VANUATU

Assent: **05/12/2024**
Commencement: **02/01/2025**

DATA PROTECTION AND PRIVACY ACT NO. 13 OF 2024

An Act to provide for data protection and privacy and for related matters.

Be it enacted by the President and Parliament as follows-

PART 1 PRELIMINARY MATTERS

1 Interpretation

In this Act, unless the contrary intention appears:

biometric data means personal data resulting from specific technical processing, which relates to the physical, physiological or behavioural characteristics of a natural person. This data can be used to allow or confirm the unique identification of that natural person, such as facial images or dactyloscopic data;

child means an individual below the age of 18 years;

data centre means a facility (including a cloud) that provides shared access to applications and data using a complex network, computers, and storage infrastructure;

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

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, destruction of, or the carrying out of logical or arithmetical operations on such data. Data processing includes processing of personal data in a filing system;

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

data server means a computer or platform used for storing, securing, managing, and processing data;

data subject means the person who can be identified, directly or indirectly, via an identifier such as a name, ID number, location data or other biometric data;

Deputy Commissioner means the Deputy Commissioner of Data Protection and Privacy appointed under the Digital Safety Authority Act No. 15 of 2024;

designated contact person means an employee or other natural or legal person designated by the data controller or data processor;

filing system means any structured set of data which are accessible or retrievable according to specific criteria;

fundamental rights and freedoms mean the fundamental rights and freedoms provided under subarticle 5(1) of the Constitution of the Republic of Vanuatu;

genetic data means all data relating to the genetic characteristics of an individual which have been obtained as a result from an analysis of:

(a) a biological sample from the individual concerned, in particular chromosomal, Deoxyribonucleic acid (DNA) or Ribonucleic acid (RNA) analysis; or

(b) any other element enabling equivalent information to be obtained;

legitimate interest includes but is not limited to any commercial, individual or societal interest of a data subject, data processor, data controller or a third party;

personal data means any information or data, whether included in a record or not, which:

(a) relates to a data subject; or

(b) enables singling out or enables interaction with the data subject;

recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed and includes a third party;

special categories of personal data include the following:

(a) genetic data or personal data relating to offences, criminal proceedings and convictions; and

(b) biometric data uniquely identifying a person; and

(c) personal data relating to racial or ethnic origin, political opinions, trade-union membership, religious or other beliefs, health or sexual life;

third party means a natural or legal person, public authority, agency or body other than the data subject, data controller, data processor, designated contact person and other persons who:

(a) are under the direct authority of the data controller or processor; and

(b) are authorised to process personal data;

vulnerable individual means a person who:

(a) may be in need of community care services due to mental illness, developmental disability or delay, other disability, age, illness or emotional disturbance; and

(b) is unable to take care of himself or herself or unable to protect himself or herself against significant harm or serious exploitation.

2 Application of the Act

(1) This Act applies to the following:

(a) 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; and

(b) processing of personal data or special categories of personal data about living individuals and not about deceased persons; and

(c) processing of personal data done within the jurisdiction of Vanuatu; and

(d) processing of personal data generated or collected in Vanuatu, irrespective of where the processing is done; and

(e) processing of personal data of individuals who are in Vanuatu by a data controller or data processor not established in Vanuatu, where the processing activities are related to:

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

(ii) the monitoring of the behaviour of such individuals in Vanuatu subject to their behaviour taking place within Vanuatu.

(2) This Act does not apply to the processing of personal data done purely for personal or household activities.

3 Act to prevail

If a provision of this Act conflicts with a provision of any other Act, the provisions of this Act prevail.

PART 2 RULES RELATING TO PROCESSING OF PERSONAL DATA

4 General rules relating to processing of personal data

(1) Data controllers and data processors must process personal data in accordance with the following rules:

(a) personal data must be processed:

(i) under the requirements of this Act; and

(ii) fairly and in a transparent manner in relation to the data subject; and

(b) personal data must be processed for explicit, specified, and legitimate purposes and the processing of these data must be done for those purposes and must not be incompatible with them; and

(c) personal data must be adequate, relevant, proportional, and not excessive in relation to the purposes for which they are processed, taking into account both the quantity and the quality of personal data being processed; and

(d) personal data must be accurate and, to the extent necessary, be kept up to date and every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are rectified or erased without delay; and

(e) personal data must 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; and

(f) personal data must be processed in a manner that ensures reasonable and appropriate security measures against unauthorised or unlawful processing and against accidental or unauthorised access, destruction, loss, use, modification, or disclosure.

(2) For the purposes of subparagraph (1)(a)(i), personal data is being processed fairly if the personal data is:

(a) being processed in a manner that the data subject would reasonably expect; and

(b) not processed in a manner that may have unjustified adverse effect on the data subject.

(3) For the purposes of subparagraph (1)(a)(ii), personal data is being processed in a transparent manner if:

(a) the data subject is made aware of how the personal data is to be collected, used, or otherwise processed; and

(b) the data subject is made aware as to the extent the personal data will be processed; and

(c) any information or communication relating to the processing of the personal data is easily accessible by the data subject and that information is easy to understand.

(4) Data controllers and data processors must ensure that personal data for archiving purposes must be processed in the public interest, scientific or historical research purposes or statistical purposes and must be processed subject to appropriate safeguards prescribed by Regulations.

(5) Data controllers and data processors must delete personal data once the purpose for which it was processed has been achieved or must only be kept in a form that prevents any direct or indirect identification of the data subject.

5 Lawful purposes for processing personal data

A data controller or data processor may only process personal data for any of the following purposes:

(a) the processing is based on the data subject's consent to the processing for one or more specific purpose; or

(b) the processing is necessary for entering into or for the performance of a contract to which the data subject is a party; or

(c) the processing is necessary to protect the rights or legitimate interests of the data subject or of another natural person; or

(d) the processing is necessary for compliance with a legal obligation to which the data controller is subject to or is necessary for the performance of the function set out under any Act; or

(e) the processing is necessary for a task carried out in the public interest; or

(f) the processing is necessary for the purposes of the legitimate interests of the data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject, especially where the data subject is a child.

6 Prohibition of processing of special categories of personal data

(1) The processing of special categories of personal data is prohibited.

(2) Despite subsection (1), a data controller or data processor may process special categories of personal data if the special categories of personal data are processed for any of the following purposes:

(a) subject to subsection (3), processing is based on the data subject's consent to the processing for one or more specific purpose; or

(b) processing is necessary for the purpose of carrying out obligations or exercising specific rights of the data controller or of the data subject as set out under this Act or any other Act; or

(c) subject to conditions provided for by this Act or any other Act, processing is necessary for:

(i) the assessment of the working capacity of an employee; or

(ii) for carrying out the obligations and exercising specific rights of the data controller or of the data subject in the field of employment, social security or social protection; or

(d) subject to professional secrecy and conditions provided for by this Act, processing is necessary for preventive medical purposes and purposes of medical diagnosis, administration of care or treatment, management of health services or under a contract with a health professional; or

(e) processing is necessary for reasons of public health, such as monitoring and protecting the public against a life-threatening epidemic or pandemic and its spread or for the purposes of humanitarian actions; or

(f) processing is necessary to protect the legitimate interests of the data subject or of another individual where the data subject is physically or legally incapable of giving consent; or

(g) processing is necessary for the protection of national security, defence, public safety, or the prevention, investigation or prosecution of criminal offences or the execution of criminal penalties; or

(h) processing is carried out in the course of its activities with appropriate safeguards by a foundation, association or any other charitable bodies with a political, philosophical, religious or trade union purpose and on the condition that:

(i) the processing relates solely to the members or to former members of the body (a foundation, association or any other charitable bodies) or to individuals who have regular contact with it in connection with its purposes; and

(ii) the personal data are not disclosed outside that body (a foundation, association or any other charitable bodies) without the consent of the data subjects; or

(i) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity; or

(j) subject to conditions provided for by this Act or any other Act, processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

(3) For the purposes of paragraphs (2)(b), (e) and (g), the data controller or the data processor must ensure that appropriate measures are in place to safeguard the fundamental rights and freedoms of data subjects.

7 Processing personal data of a child or other vulnerable individual

(1) The processing of the personal data of a child is prohibited.

(2) Despite subsection (1), a data controller or data processor may process personal data of a child for any of the following purposes:

(a) processing is based on the consent given or authorised by the child's parents, carers, or legal representatives unless an Act provides that the child may act by himself or herself without being represented by his or her parents or legal guardian; or

(b) processing is in the legitimate interests of the child; or

(c) processing is necessary to meet a legal obligation to which the data controller is subject to; or

(d) processing is in the public interest as provided by an Act; or

(e) processing is necessary in the context of preventive or counselling services offered directly to the child.

(3) If information and communication relating to processing is addressed to a child, the information and communication must be in a clear and plain language so that the child can easily understand and appropriate mechanisms for age verification must be in place.

(4) When processing personal data relating to vulnerable individuals, data controllers and data processors must:

(a) consider the specific needs of those individuals and relevant accessibility standards; and

(b) ensure that information and communication about data processing must be in a clear and plain language and is accessible to all data subjects regardless of their age, gender, abilities or characteristics.

8 Consent

(1) If the processing of personal data is based on the consent of a data subject, the data controller must be able to demonstrate evidence of such consent.

(2) A consent is deemed not to have been freely given if:

(a) that consent is given under undue influence or pressure of an economic or other nature, whether direct or indirect; or

(b) the data subject has no genuine or free choice or is unable to refuse or withdraw consent without prejudice.

(3) A request for consent must be presented in a manner that:

(a) is clearly distinguishable from other matters; and

(b) uses a clear and plain language.

(4) A data processor must ensure:

(a) that a data subject is able to withdraw any consent given at any time, free of charge; and

(b) in the case of multiple purposes – that consent must be given for each individual and specific purpose; and

(c) that the data subject is informed that he or she may withdraw consent and how he or she may do so.

(5) The withdrawal of consent does not affect the lawfulness of the data processing that occurred before the data controller received the withdrawal of consent.

PART 3 RIGHTS OF THE DATA SUBJECT

9 Access to information and personal data

(1) A data controller must ensure that a data subject is able to obtain, on the data subject's request and within a reasonable time:

(a) confirmation as to whether personal data about the data subject is being processed; and

(b) a copy of the personal data undergoing processing; and

(c) the following information:

(i) the purposes of the processing; and

(ii) the source of the personal data undergoing processing; and

(iii) the recipients or categories of recipients whom the personal data are disclosed; and

(iv) where applicable, the fact that the data controller intends to transfer personal data to another jurisdiction, and if so, to which recipients and in which jurisdiction; and

(v) the period for which personal data will be retained by the data controller or data processor; and

(vi) any other information that the data controller is required to under this Act or any other Act.

(2) The data controller must provide information under subsection (1) in the following manner:

(a) in writing; and

(b) in plain language; and

(c) free of charge; and

(d) within one month after the date of the receipt of a request.

(3) If a request under subsection (1) is too excessive or unreasonable, the data controller may:

(a) charge a reasonable fee based on the administrative costs incurred; or

(b) refuse to act on the request.

(4) If the data controller charges a fee under paragraph (3)(a) or refuses a request under paragraph (3)(b), the data controller bears the burden of proving the excessive or unreasonable nature of the request.

10 Restriction of processing of personal data

(1) A data controller may restrict the processing of personal data upon the request of a data subject in any of the following circumstances:

(a) where the accuracy of the personal data is contested by the data subject, for such period necessary to enable the controller to verify the accuracy of the personal data; or

(b) where the processing is unlawful, but the data subject opposes erasing the personal data and requests the restriction of their use instead; or

(c) where the data controller no longer needs the personal data for the purposes of the processing; or

(d) where the data subject has objected to processing under section 12 pending the verification whether the legitimate grounds of the data controller override those of the data subject.

(2) If the data controller has restricted the processing of personal data under subsection (1), the personal data can only be processed in any of the following circumstances:

(a) with the data subject’s consent; or

(b) for the establishment, exercise or defence of legal claims; or

(c) for the protection of the rights of another natural or legal person; or

(d) for reasons of public interest.

(3) The data controller who has restricted processing of personal data under subsection (1) must inform the data subject before personal data is processed for the purpose under paragraph (2)(b),(c) or (d).

11 Rectifying and erasing personal data

(1) A data controller must ensure that, on a data subject's request, the data subject receives any rectification of inaccurate or incomplete personal data, without delay and free of charge.

(2) A data controller must ensure that, on a data subject's request, the data subject's personal data is erased, without delay and free of charge, if:

(a) the personal data is no longer necessary for the purposes for which it was collected or otherwise processed; or

(b) the data subject withdraws his or her consent on which the processing is based; or

(c) the data subject objects to the processing, under section 12, and the data controller cannot demonstrate an overriding legitimate basis for the processing; or

(d) the personal data is being processed unlawfully; or

(e) the personal data must be erased to comply with a legal obligation to which the data controller is subject to.

(3) The data controller must communicate the data subject's request under subsection (1) or (2) to all recipients to whom the personal data concerned have been disclosed.

(4) Subsection (3) does not apply where the data controller can demonstrate that this is impossible or will involve disproportionate efforts to communicate the data subject's request.

12 Objection to the processing of personal data

A data controller must ensure that the data subject is able to object to the processing of his or her personal data, at any time and free of charge, unless the data controller can demonstrate:

(a) legitimate grounds for the processing which override the interests or fundamental rights and freedoms of the data subject; or

(b) the establishment, exercise, or defence of a legal claim.

13 Data subject's right not to be subject to automated decision making

(1) A data controller must ensure that, on a data subject's request, the data subject must not be subject to a decision significantly affecting him or her

based solely on the automated processing of personal data, including profiling, without having his or her views taken into consideration.

(2) For the purposes of subsection (1), **profiling** means any form of automated processing of personal data to assess certain personal aspects relating to a natural person.

(3) Subsection (1) does not apply if a decision:

(a) is authorized by law to which the data controller is subject; or

(b) is necessary for entering or for the performance of a contract between the data subject and the data controller; or

(c) is based on the data subject's consent and where appropriate guarantees have been put in place.

(4) Where paragraph (3)(b) or (c) applies, the data controller must:

(a) implement suitable measures to safeguard the data subject's fundamental rights and freedoms and legitimate interests; and

(b) provide the data subject the possibility to obtain human intervention on the part of the controller.

(5) Where a decision under subsection (1) is based on special categories of personal data, or personal data of children or personal data concerning vulnerable individuals, the processing must only be carried out if:

(a) conditions for the processing as set out in sections 6 and 7 are met; and

(b) the processing is necessary for reasons of public interest; and

(c) the processing is required by any other Act.

14 Representation of the data subject

A data controller must ensure that a data subject is able to authorise a person, non-profit body, organisation or association to lodge and pursue a complaint, on behalf of the data subject, with the Deputy Commissioner or the Court.

PART 4 TRANSBORDER DATA FLOWS

15 Conditions for transfer outside of Vanuatu

(1) Personal data generated or collected in Vanuatu must not be used elsewhere without prior authorisation of the Minister, on the recommendation of the Deputy Commissioner.

(2) Despite subsection (1), personal data generated or collected in Vanuatu may be transferred to another country or international organisation without the prior authorisation of the Minister if that country or that international organisation has been prescribed by the Minister under subsection (3).

(3) The Minister may, on the recommendation of Deputy Commissioner, by Order, list the countries and international organisations which provide an appropriate level of protection of personal data.

16 Safeguards prior to transfer outside of Vanuatu

In addition to section 15, the Minister may, on the advice of the Deputy Commissioner, prescribe safeguard procedures to be used when transferring personal data outside of Vanuatu if:

(a) the information being request is considered by the Deputy Commissioner to be urgent and sensitive in nature; and

(b) the country or international organisation to which the personal data will be transferred to has been prescribed under subsection 15(3).

17 Cross-border transfer for specific situations

Despite section 15, the Minister on the recommendation of the Deputy Commissioner may authorise the cross-border transfer of personal data to other countries or international organisations which do not ensure an appropriate level of protection may take place if:

(a) the data subject has given explicit, specific and free consent, after being informed of all risks arising with the transfer in the absence of appropriate safeguards; or

(b) the specific interests of the data subject require the transfer in a particular case; or

(c) the transfer is necessary for any purpose approved by the Commission.

PART 5 ENFORCEMENT

18 Disclosure of document or information

(1) If the Deputy Commissioner is satisfied that a data controller is in possession of a document or information that will assist the Deputy Commissioner in determining whether there has been a breach of this Act, the Deputy Commissioner may, in writing, require that data controller to provide such document or information.

(2) The data controller under subsection (1) must comply with the request within 14 days after receiving the request.

(3) The Deputy Commissioner must not disclose any document or information received under this section unless:

(a) authorised by the data controller; or

(b) required by a court order to disclose such document or information; or

(c) the Deputy Commissioner is satisfied that the document or information does not identify any particular data controller or data subject; or

(d) disclosure is required under this Act or any other Act.

19 Application for a search warrant

(1) If the Deputy Commissioner is reasonably satisfied that an offence has been committed under this Act, he or she may request the Commissioner of Police for assistance in making an application for a search warrant.

(2) An application for a search warrant must be in writing and made on oath by the Commissioner of Police, and must set out:

(a) the offence to which the application relates; and

(b) a description of the data centre or a data server; and

(c) the information relied on to support the reasonable suspicion of the commission of the offence; and

(d) the period the search warrant is required.

20 Granting of search warrant

(1) The Court may grant a search warrant if the Court is satisfied with the application of the Commissioner of Police.

(2) Without limiting subsection (1), prior to granting a search warrant, the Court must consider the following:

(a) the seriousness of the offence to which the application relates; and

(b) the reliability of the information on which the application is based, including the nature of the source of the information; and

(c) whether the public interest in the production of data from the data centre or a data server outweighs the right to privacy of a person whose privacy may be affected as a result of the production; and

(d) whether there is sufficient connection between the evidence sought and the offence to which the application relates; and

(e) whether any condition must be included in the search warrant; and

(f) the proposed duration of the search warrant; and

(g) any other matters that the Court considers relevant.

21 Contents of search warrant

A search warrant must state the following information:

(a) a description of the data centre and data server to be searched; and

(b) the offence to which the application relates; and

(c) the types of evidential material that may be searched for; and

(d) the power of the Deputy Commissioner to secure or render inaccessible a data centre or a data server; and

(e) the date and time the search warrant expires; and

(f) any conditions imposed in relation to executing the search warrant.

22 Extension of a search warrant

(1) The Court must specify in the search warrant the date and time the search warrant expires.

(2) The Court may, upon application of the Commissioner of Police, extend the date and time, when a search warrant expires, if it is satisfied that the purpose for which the search warrant was granted cannot be satisfied before the search warrant is expired.

23 Effects of a search warrant

(1) The Commissioner of Police is authorised, under a search warrant granted under section 20, to:

(a) seize an item that the Commissioner of Police believes on reasonable grounds to be:

(i) evidential material in relation to an offence to which the search warrant relates; or

(ii) evidential material that is relevant to another offence under this Act or any other Act; and

(b) access, a data centre or a data server for the purposes of obtaining information and records; and

(c) seize or secure a data server; and

(d) require a person with a knowledge of the data centre or data server to assist the Commissioner of Police in accessing the data centre or a data server; and

(e) move the data server at the place searched to another place for examination in order to determine whether it contains data that could be accessed, collated or seized under the search warrant; and

(f) use the assistance of the Deputy Commissioner or any other person as reasonably necessary for the execution of the search warrant.

(2) If the Commissioner of Police seizes the data server under subsection (1), the Commissioner of Police:

(a) may take possession of it; and

(b) may retain it for such period as he or she considers necessary for the purposes of this Act.

(3) The Commissioner of Police must return the data server under subsection (2) to the data controller if:

(a) it is no longer necessary to seize the data server; or

(b) it is not to be used in evidence.

PART 6 OFFENCES

24 Non-compliance with a provision of this Act

A person who contravenes a provision of this Act commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

25 Unlawful obtaining and disclosing of personal data

(1) A person other than the data controller, must not knowingly or recklessly obtain, retain or disclose or procure the disclosure of personal data:

(a) without the authorisation of the data controller; and

(b) with the intention of financial gain or causing harm to the data subject.

(2) A person who contravenes subsection (1) commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

26 Alteration of personal data to prevent disclosure to a data subject

A data controller or a data processor, or an employee of a data controller, or data processor, who alters, defaces, blocks, erases, destroys or conceals personal information with the intention of preventing disclosure of all or part of the personal information to a data subject commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

27 Obstruction of powers of entry to premises

A person who intentionally obstructs a person in the execution of a search warrant issued under this Act commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

28 Destruction, concealment or falsification of information requested by the Deputy Commissioner

A person who destroys, conceals or falsifies all or part of any personal information, document, equipment or material, with the intention of preventing disclosure of personal information to the Deputy Commissioner under section 18 commits an offence, punishable on conviction, by a fine not exceeding VT10,000,000.

29 Hindering or obstructing the lawful exercise of powers

(1) A person must not hinder or obstruct, the Deputy Commissioner, a police officer, or a person assisting a police officer, in exercising out his or her powers under this Act.

(2) A person who contravenes subsection (1) commits an offence, punishable on conviction, by a fine not exceeding VT1,000,000.

30 Prohibition on disclosure of information, records and data

(1) A person who obtains information, extracts, records or data under a request, or search warrant under this Act must not knowingly disclose in whole or in part the information, records or data.

(2) A person who contravenes subsection (1), commits an offence, punishable on conviction, by a fine not exceeding VT2,000,000.

PART 7 MISCELLANEOUS PROVISIONS

31 Regulations

(1) The Minister may, on the advice of the Deputy Commissioner, make Regulations not inconsistent with this Act for the better carrying out or giving effect to the provisions of this Act.

(2) Without limiting the generality of subsection (1), the Regulations may provide for any or all of the following:

(a) how personal data must be processed transparently;

(b) how joint-data controllers are to work together and the obligations that are to be imposed on each or both of the data controllers;

(c) the obligations of the data processors;

(d) security of processing;

(e) record of processing operations;

(f) obligations relating to personal data breaches;

(g) personal data breach notification to data subjects.

32 Commencement

This Act commences on the day on which it is published in the Gazette.