PERSONAL DATA PROTECTION ACT, NO. 9 OF 2022

REGULATIONS made by the Minister of _____ under sections 53, read with section 24 of the Personal Data Protection Act, No. 9 of 2022.

Minister of _____

Colombo,

2024.

REGULATIONS

1. These Regulations may be cited as the Personal Data Protection (Personal Data Protection Impact Assessments) Regulations No. of 2024.

2. (1) Where a controller intends to carry out processing which involves-

(a) a systematic and extensive evaluation of personal data or special categories of personal data including profiling;

(b) a systematic monitoring of publicly accessible areas or telecommunication networks; or

(c) a processing activity as may be determined by way of rules taking into consideration the scope and associated risks of that processing,

such controller shall carry out a Personal Data protection Impact Assessment (hereinafter referred to as the "PDPIA"), which shall be substantially in the form set out in SCHEDULE I hereto.

(2) For the purpose of this regulation-

"systematic" includes, but not limited to, occurring according to a system, pre-arranged, organized or methodical, taking place as part of a general plan for data collection or carried out as part of a strategy; and

"extensive" means evaluation involving large numbers of data subjects, large volumes of data or high levels of detail in the evaluation.

3. The PDPIA shall set out the following information:-

(a) the name and contact information of the responsible person of the controller with whom the Authority shall communicate about the PDPIA;

(b) the name and contact information of the Data Protection Officer (if applicable) if different from that provided under paragraph (a);

(c) an overview of the processing which is intended to be carried out;

(d) the purpose of the processing, including-

(i) the intended outcome for data subjects; and

(ii) the expected benefits for the controller, any other parties or society as a whole;

(e) the department or other unit of the controller responsible for the relevant processing, to the extent as may be applicable;

(f) the relevant departments or individuals within the controller who were consulted when carrying out the PDPIA, to the extent as may be applicable;

(g) a description of the role of any processors or sub processors involved in the processing and contact information of each;

(h) any relevant processors or sub processors that were consulted when carrying out the PDPIA; and

(i) external experts who were consulted when carrying out the PDPIA.

4. The controller shall assess and describe the intended processing in the PDPIA which shall include the following:-

(a) the nature and scope of the personal data to be processed, including—

(i) the types of personal data, including any special categories of personal data or personal data pertaining to data subjects with limited capacity to consent or otherwise;

(ii) the number of data subjects involved;

(iii) the volume and types of the personal data; and

(iv) an assessment of the sensitivity of the personal data and the potential harm to data subjects in the event of a personal data breach.

(b) the nature and scope of the processing, including the following information and particulars:-

(i) the manner of collection, storage and usage of personal data;

(ii) the nature, extent and frequency of the processing;

(iii) the individuals or staff positions who shall have access to the personal data within the controller or any processors or sub processors;

(iv) any third parties with whom the personal data shall be shared or by whom the personal data shall otherwise be accessed, and the legal basis, restrictions on use, retention and onward sharing or access, and other terms and conditions applicable to such sharing or access;

(v) whether personal data shall be processed outside Sri Lanka and the manner in which the requirements of section 26 of the Act are complied with;

(vi) the duration of the processing, including the duration of the period for which data shall be retained and the manner in which the data shall be dealt with at the end of the data retention period; and

(vii) the technical and organizational measures in place to ensure integrity and confidentiality of the personal data as required by section 10 of the Act.

5. The controller shall ascertain the impact of the intended processing and describe in the PDPIA any barrier or limitation to compliance, or any risk of noncompliance, and any measures and safeguards the controller shall take to comply, with the obligations of the controller under Part I of the Act to-

(a) process personal data in a lawful manner under section 5 of the Act;

(b) define a purpose for personal data processing under section 6 of the Act;

(c) confine personal data processing to a defined purpose under section 7 of the Act;

(d) ensure accuracy under section 8 of the Act;

(e) limit the period of retention of personal data under section 9 of the Act;

(f) maintain integrity and confidentiality of personal data under section 10 of the Act;

(g) process personal data in a transparent manner under section 11 of the Act; and

(h) implement a Data Protection Management Programme that is consistent with the requirements of section 12 of the Act.

6. The controller shall ascertain the impact of the intended processing and describe in the PDPIA any likely barrier, limitation or risk of harm in the exercise of the rights of the data subjects, and any measures and safeguards the controller shall take to enable data subjects to exercise their rights, under Part II of the Act to-

(a) access to personal data under section 13 of the Act;

(b) withdraw consent to process personal data under subsection (1) of section 14 of the Act;

(c) object to processing of personal data under subsection (2) of section 14 of the Act;

(d) rectify or complete personal data under section 15 of the Act;

(e) have the right to erase personal data under section 16 of the Act;

(f) request a review of a decision based solely on automated processing under section 18 of the Act; and

(g) have the right of appeal under section 19 of the Act.

7. The controller shall ascertain the impact of the intended processing and describe in the PDPIA**,** the likelihood of the intended processing resulting in a risk of harm to the rights of the data subjects guaranteed by any written law, and the particulars relating to measures and safeguards the controller shall take to mitigate such risk.

8. For the purposes of regulation 7, rights of data subjects guaranteed by written laws that may be relevant may include, but not limited to, in relation to-

(a) control over personal data;

(b) limitation of rights and freedoms;

(c) discrimination;

(d) identity theft or fraud;

(e) financial loss;

(f) unauthorised reversal of pseudonymisation;

(g) damage to reputation;

(h) loss of confidentiality of personal data protected by professional secrecy; or

(i) any other economic, social or emotional harm or disadvantage to data subjects.

9. In ascertaining the impact of the processing and risks relating to the obligations of the controller and rights of data subjects under regulations 5, 6 and 7, the controller shall consider the origin, nature, potential impact, particularity and severity of risks, in each case from the perspective of the affected data subjects.

10. Measures and safeguards that the controller shall take for purposes of mitigating risks identified pursuant to regulations 5, 6 and 7 may include, but not limited to-

(a) refraining from collecting or further processing of certain types of

personal of data;

(b) reducing the scope of the processing;

(c) reducing the period of retention of personal data;

(d) taking additional security measures;

(e) training staff to ensure risks are anticipated and managed;

(f) anonymising or pseudonymising data where possible;

(g) using alternative technologies in the processing;

(h) putting clear data-sharing agreements into place;

(i) making changes to the information provided to data subjects under section 11 of the Act to inform them of identified risks;

(j) providing to data subjects the ability to opt out of processing where appropriate; or

(k) implementing new systems to help data subjects exercise their rights.

11. The controller shall provide such information and particulars including a conclusion in the PDPIA relating to the measures and safeguards taken by the controller to mitigate each of the risks of harm caused to the data subject by such processing of personal data.

12. (1) In assessing the risk of harm caused to any data subject by processing the personal data, the controller may consider the risk matrix specified in Schedule II, which may be attached to the PDPIA.

(2) In the event that the numeric value found by multiplying the numeric values assigned to probability and impact is 10 or above, the controller shall carry out a PDPIA.

(3) Notwithstanding the above, a controller may conduct a PDPIA as specified in Schedule I, at any time without having regard to the risk matrix specified in Schedule II.

13. The controller shall deliver an electronic copy of the PDPIA to the Authority.

14. Where-

(a) notwithstanding any planned measures and safeguards, the controller is

not able to mitigate likely risks of harm to data subjects; or

(b) the processing relates to national security, public order or public health,

then, after any consultation with the Authority, the controller shall implement any written instructions of the Authority and shall revise the PDPIA accordingly and submit the same to the Authority.

15. In these Regulations unless the context otherwise requires— "Act" means the Personal Data Protection Act, No. 9 of 2022;

"Authority" means the Data Protection Authority of Sri Lanka;

"Personal Data Protection Impact Assessment" means a personal data protection impact assessment, as described in section 24 of the Act; and

"sub processor" means a processor engaged by another processor for carrying out specific processing activities.

SCHEDULE I

(regulations 2 and 12)

Personal Data Protection Assessment

Regulation	Information and particulars
	Background and contact information
3(a)	Controller name: Name and contact information of person responsible for the PDPIA:

3(b)	Name and contact information of the Data Protection Officer (if applicable):

Regulation	Information and particulars
3(c)	Overview of the processing activity:
3(d)	Purpose of the processing- Intended outcome for data subjects: Expected benefits for the controller, any other parties or society as a whole:
3(e)	Department or other unit of the controller responsible for the relevant processing:
3(f)	Department or individuals in the controller consulted when carrying out the PDPIA:
3(g)	Describe the role of any processors or sub processors involved in the processing and contact information for each:
3(h)	Names and contact information of any relevant processors or sub processors that were consulted when carrying out the PDPIA (if applicable):
3(i)	Names and contact information of external experts who were consulted when carrying out the PDPIA (if applicable):
	Intended processing

4(a)(i)	Describe the types of personal data, including any special categories of personal data or personal data pertaining to people with limited capacity to consent or otherwise vulnerable populations:
4(a)(ii)	Estimate the number of data subjects involved:
4(a)(iii)	Describe the volume and variety of the personal data:
4(a)(iv)	What is the potential harm to data subjects in the event of a personal data breach? How does this assessment change depending on the level of sensitivity of the personal data?

Regulation	**Information and particulars**
4(b)(i)	The manner of collecting, storage and usage of personal data:
4(b)(ii)	Describe the nature, extent and frequency of the processing:
4(b)(iii)	Names of the individuals or staff positions who shall have access to the personal data within the controller or any processors or downstream sub processors:

4(b)(iv)	Identify any third parties with whom the personal data shall be shared or by whom the personal data could otherwise be accessed: Please include the following information with respect to such sharing or access: • the legal basis on which the sharing or access shall occur (e.g., contract details if contractual, section reference if statutory, etc.): • any restrictions on use: • any restrictions on retention: • any restrictions on onward sharing: • restrictions on access: • any other terms and conditions applicable to such sharing or access:
4(b)(v)	Whether personal data shall be processed outside Sri Lanka? If so, how are the requirements of section 26 of the Act satisfied?
4(b)(vi)	The duration of processing? The duration of the period for which data shall be retained? The manner in which the data shall be dealt with at the end of the data retention period?
4(b)(vii)	What technical and organizational measures are implemented to ensure integrity and confidentiality of the personal data as required by section 10 of the Act?
Regulation	**Information and particulars**
	Impact on the controller's obligations[1]

[1] The controller shall consider the origin, nature, potential impact, particularity and severity of each risk from the perspective of the affected data subjects.

5(a)	Describe any barrier or limitation to compliance, or any risk of noncompliance, with the obligations of the controller to process personal data in a lawful manner under section 5 of the Act: Describe any measures and safeguards the controller will take to comply:
5(b)	Describe any barrier or limitation to compliance, or any risk of noncompliance, with the obligations of the controller to define a purpose for personal data processing under section 6 of the Act: Describe any measures and safeguards the controller will take to comply:
5(c)	Describe any barrier or limitation to compliance, or any risk of noncompliance, with the obligations of the controller to confine personal data processing to a defined purpose under section 7 of the Act: Describe any measures and safeguards the controller will take to comply:
5(d)	Describe any barrier or limitation to compliance, or any risk of noncompliance, with the obligations of the controller to ensure accuracy in accordance with section 8 of the Act: Describe any measures and safeguards the controller will take to comply:
5(e)	Describe any barrier or limitation to compliance, or any risk of noncompliance, with the obligations of the controller to limit the period of retention of personal data in accordance with section 9 of the Act: Describe any measures and safeguards the controller will take to comply:
5(f)	Describe any barrier or limitation to compliance, or any risk of noncompliance, with the obligations of the controller to maintain integrity and confidentiality of personal data in accordance with section 10 of the Act:

Regulation	**Information and particulars**

	Describe any measures and safeguards the controller will take to comply:
5(g)	Describe any barrier or limitation to compliance, or any risk of noncompliance, with the obligations of the controller to process personal data in a transparent manner in accordance with section 11 of the Act: Describe any measures and safeguards the controller will take to comply:
5(h)	Describe any barrier or limitation to compliance, or any risk of noncompliance, with the obligations of the controller to implement a Data Protection Management Programme that is consistent with the requirements of section 12 of the Act: Describe any measures and safeguards the controller will take to comply:
	Impact on the rights of data subjects[2]
6(a)	Describe any barrier, limitation or risk to data subjects being able to exercise their rights to access to personal data under section 13 of the Act: Describe any measures and safeguards the controller will take to enable data subjects to exercise such rights:
6(b)	Describe any barrier, limitation or risk to data subjects being able to exercise their rights to withdraw consent under section 14(1) of the Act: Describe any measures and safeguards the controller will take to enable data subjects to exercise such rights:
6(c)	Describe any barrier, limitation or risk to data subjects being able to exercise their rights to object to processing under section 14(2) of the Act: Describe any measures and safeguards the controller will take to enable data subjects to exercise such rights:

Regulation	**Information and particulars**

[2] The controller shall consider the origin, nature, potential impact, particularity and severity of each risk from the perspective of the affected data subjects.

6(d)	Describe any barrier, limitation or risk to data subjects being able to exercise their rights to rectification or completion under section 15 of the Act: Describe any measures and safeguards the controller will take to enable data subjects to exercise such rights:
6(e)	Describe any barrier, limitation or risk to data subjects being able to exercise their rights to erasure under section 16 of the Act: Describe any measures and safeguards the controller will take to enable data subjects to exercise such rights:
6(f)	Describe any barrier, limitation or risk to data subjects being able to exercise their rights to request a review of a decision based solely on automated processing under section 18 of the Act: Describe any measures and safeguards the controller shall take to enable data subjects to exercise such rights:
6(g)	Describe any barrier, limitation or risk to data subjects being able to exercise their rights to appeal under section 19 of the Act: Describe any measures and safeguards the controller shall take to enable data subjects to exercise such rights:
7	Describe the likelihood of the intended processing resulting in a risk of harm to the rights of the data subjects guaranteed by any written law, such as (without limitation)- • control over personal data: • limitation of rights and freedoms: • discrimination: • identity theft or fraud: • financial loss: • unauthorised reversal of pseudonymisation: • damage to reputation:

Regulation	Information and particulars
	• loss of confidentiality of personal data protected by professional secrecy: • any other economic, social or emotional harm or disadvantage to data subjects: Describe any measures and safeguards the controller shall take to mitigate such risk:
	Conclusion
11	Describe the measures and safeguards the controller shall take to mitigate each of the risks of harm caused to data subjects:

Name of the officer:

Date:

Signature:

Attach supportive documents and add links, as may be necessary.

SCHEDULE II

(regulation 12)

Risk Matrix

		Impact How severe would the outcomes be if the risk occurred?				
		Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
Probability What is the probability the risk will happen?	Almost certain 5	Medium 5	High 10	Very high 15	Extreme 20	Extreme 25
	Likely 4	Medium 4	Medium 8	High 12	Very high 16	Extreme 20
	Moderate 3	Low 3	Medium 6	Medium 9	High 12	Very high 15
	Unlikely 2	Very low 2	Low 4	Medium 6	Medium 8	High 10
	Rare 1	Very low 1	Very low 2	Low 3	Medium 4	Medium 5