PERSONAL DATA PROTECTION ACT, NO. 9 OF 2022

RULES made by the Data Protection Authority of Sri Lanka, under sections 52, read with section 23 of the Personal Data Protection Act, No. 9 of 2022.

Data Protection Authority of Sri Lanka

Colombo, 2024.

RULES

1. These Rules may be cited as the Personal Data Protection (Personal Data Breach Notification) Rules No. of 2024.

2. (1) These Rules shall apply to controllers.

(2) A personal data breach with respect to a controller shall include any such breach that occurs with respect to processing of personal data by a processor or any downstream sub processor on behalf of such controller.

3. A controller shall notify the Authority of any personal data breach that has occurred or is reasonably likely to have occurred in such form as specified in Schedule I hereto, unless the personal data breach is unlikely to result in a risk, or is likely to result in a low risk, to the rights and freedoms of data subjects.

4. A controller shall notify the data subjects where the controller is of the opinion that the data subjects are affected or likely to be affected by a personal data breach that is likely to result in a high risk to rights and freedoms, in such form as may be specified in Schedule II hereto.

5. (1) A controller shall notify the Authority of any personal data breach under rule 3, to the extent feasible, within seventy two hours after-

(a) the controller (or the relevant processor or sub processor) becomes aware that a personal data breach has occurred; or

(b) the controller has determined, or shall have reasonably determined, based on the information available to it (or the relevant processor or sub processor) at the time that a personal data breach is reasonably likely to have occurred.

(2) Where it is not feasible to notify the Authority as specified in paragraph (1) within seventy two hours, such notification shall be accompanied by reasons for the delay.

6. A notification to the Authority made under rule 3 shall include the following information to the extent known at the time of the notification— (a) the timing and nature of the personal data breach;

(b) the categories of data subjects and personal data affected by the personal data breach;

(c) the approximate number of data subjects affected by the personal data breach;

(d) the name and contact details of the Data Protection Officer, or if not designated, another point of contact of the controller;

(e) the likely consequences of the personal data breach for ongoing security of the controller's processing of personal data and the rights and freedoms of the concerned data subjects, and any other material consequences;

(f) a summary of the risk assessment conducted in accordance with rules 3 and 4;

(g) a description of the manner in which the controller shall make a notification to data subjects, if required under rule 4;

(h) a description of the measures taken or proposed to be taken by the controller or its processors or sub processors to address the personal data breach, including measures to mitigate its possible adverse effects on the affected data subjects; and

(i) a certification by the controller or in the case of a controller that is an entity, the Data Protection Officer or, if there is no Data Protection Officer designated, then the secretary, chief executive officer or the head of such entity, that all the information in the notification is true and complete to the best of the knowledge of such controller**'s** or in the case of a controller that is an entity, such person's knowledge).

7. Where the controller is not aware of the information required under rule 6 with a reasonable level of confidence at the time of making a notification, it shall indicate so in the notification and shall continue to investigate the matter.

8. After notifying the Authority under rule 4, if the controller becomes aware of additional information that would materially alter, amend, supplement or enhance such notification, it shall promptly submit an amended notification to the Authority.

9. A controller shall make the notification to data subjects required by rule 4 at the same time as making the notification to the Authority under rule 3 with respect to the same personal data breach.

10. A notification to data subjects under rule 4 shall include the following information, to the extent known:-

(a) the nature the timing of the personal data breach;

(b) the categories of data subjects and personal data affected by the personal data breach;

(c) the approximate numbers of data subjects affected by the personal data breach;

(d) the name and contact details of the Data Protection Officer, or if not designated, another point of contact of the controller to address inquiries regarding the personal data breach;

(e) the likely consequences of the personal data breach for affected data subjects;

(f) a description of measures taken or proposed to be taken by the controller to address the breach, including measures to mitigate its possible adverse effects on the affected data subjects;

(g) proposed measures an affected data subjects shall take to mitigate the possible risks of harm from the personal data breach that are appropriate to the nature of the personal data breach and the potential adverse consequences to the data subject, such as:-

(i) resetting passwords;

(ii) monitoring activity in financial accounts;

(iii) contacting service providers or counterparties to alert them to the breach and potential mitigating steps they could take; and

(iv) in cases of destruction, loss or alteration of personal data, a means of recovering the personal data from other sources; and

(h) a website address where further information is or shall be made available.

11. Subject to rule 12, a notification to data subjects under rule 4 shall use one or more reasonably effective and available means to notify all affected data subjects, which may include, without limitation-

(a) emails with a clear subject line indicating the personal data breach, if feasible using a "verified sender" technique to avoid the email being marked as spam;

(b) concise text messages using Short Message Service (SMS) within any applicable character limits, including links to official websites for more information (except to the extent limited by applicable law relating to unsolicited communications);

(c) phone calls, where automated voice messages or customer service representatives convey the essential information;

(d) social media and direct messaging applications or other applications with widespread usage;

(e) video messaging, webinars and informational sessions for large scale personal data breaches; and

(f) physical mail, where other means of notification are inefficient or other contact information is outdated or compromised.

12. If the methods of direct notification to data subjects under rule 11 involve disproportionate effort or expense or are otherwise not feasible, a controller may make a public notification in one or more widely used media sources by which affected data subjects are likely to be informed, including, without limitation, newspapers, magazines, websites, social media, online advertising, radio, television and billboards and any other media, electronic or otherwise.

13. A controller considering the proportionality of effort, expense, and feasibility of direct notification to data subjects for the purposes of rule 12 shall consider-

(a) the likelihood and severity of risks to the rights and freedoms of the data subjects, taking into account the results of the risk assessment conducted for purposes of rules 3 and 4;

(b) the relative advantages of direct notification compared with a public notification as a means of making the data subjects aware;

(c) the administrative effort and financial cost required to locate, obtain, organise and use the forms of contact information required to directly notify data subjects; and

(d) the administrative effort and financial cost of effective public notification.

14. For purposes of making a public notification under rule 12, the controller shall-

(a) make multiple attempts at using diverse media sources if necessary to ensure that data subjects are likely to be informed; and

(b) tailor the notification strategy to any special circumstances of the affected data subjects, including the types of media that are widely used in their region

or are popular within any relevant social, economic, religious or other group or organisation of which they are members.

15. If, after making a notification to data subjects under rule 11 or 12, the controller becomes aware of additional information that would materially alter, amend, supplement or enhance such notification, it shall promptly make an amended notification.

16. All notifications to data subjects under rules 11, 12 and 15 shall be in plain and clear language using a language or dialect that is understandable to any person and, in the case of written notifications, easily readable font styles and sizes.

17. A controller shall promptly submit to the Authority a copy (in the case of written notifications) or written summary (in the case of other formats) of any notification to data subjects made under rules 11, 12 and 15 when such notifications are made.

18. If the Authority determines that the content or means of a controller's notification to data subjects is insufficient under rules 11, 122 or 155, it may order the controller to make additional notifications, or make its own direct or public notifications about the personal data breach to inform the affected data subjects and may require the controller to reimburse the cost thereof.

19. A controller shall keep written records of all personal data breaches and its processors' and sub processors related obligations under the Act in a manner that would enable the Authority to verify compliance with the Act and these Rules, including, without limitation, the following:-

(a) details of the nature, likely causes and likely effects of confirmed or likely personal data breaches and related facts;

(b) all mitigating and remedial actions taken by the controller or any processor or sub processor;

(c) summaries of all risk assessments, investigations, evaluations, decisions and determinations that the controllers, processors downstream sub processors made with respect to confirmed or likely personal data breaches; and

(d) copies or summaries if the notifications were not in writing of any notifications made to the Authority and data subjects regarding confirmed or likely personal data breaches.

20. For purposes of assessing likelihood of risk of personal data breach for purposes of rules 3 and 4, the controller shall have regard to the following:-

(a) a risk to the rights and freedoms of a data subject may include, without limitation, the risk of—

(i) loss of control over personal data;

(ii) limitation of rights and freedoms;

(iii) discrimination;

(iv) identity theft or fraud;

(v) financial loss;

(vi) unauthorised reversal of pseudonymisation;

(vii) damage to reputation;

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

(ix) any other economic, social or emotional harm or disadvantage to the data subject concerned.

(b) the likelihood of risk to the rights and freedoms of a data subject resulting from a personal data breach may be affected by, without limitation—

(i) the likely effectiveness of any technical and administrative measures implemented to mitigate the likely harm resulting from the personal data breach, including any encryption or deidentification of the data;

(ii) any subsequent measures taken by the controller or on the controller's behalf to mitigate such risk; and

(iii) the nature, sensitivity, scale and scope of the personal data involved;

(c) the controller may, unless there is a reason to the contrary, consider a personal data breach as being likely to result in a low risk to the rights and freedoms of data subjects-

(i) personal data that was lost, altered or destroyed is likely to be quickly recovered from backup copies and other sources, and it is unlikely that any data subject will be affected by the temporary unavailability;

(ii) personal data that are disclosed or accessed without authority are already readily publicly available;

(iii) personal data that are disclosed or accessed without authority are encrypted, de-identified, tokenised or similarly protected using state of the art technology to make them inaccessible or unintelligible, and any decryption key, mechanism for reidentification, password or similar decoding mechanism has not been compromised; and

(iv) the controller has instituted mitigating measures that significantly lower the risk of unauthorised access to data such as by requiring password changes; and

(d) whether a personal data breach is likely to result in a high risk to the rights and freedoms of data subjects is a factor of the severity and the likelihood of the potential adverse consequences for data subjects, so that—

(i) the more severe the consequences are, the higher the risk shall be; and

(ii) the greater the likelihood of the consequences occurring are, the higher the risk shall be.

21. In these Rules 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; and

"sub processor" means, a processor engaged by another processor for carrying out specific processing activities under subsection (3) of section 22 of the Act.

SCHEDULE I

(rule 3)

Notification of Personal Data Breach to the Authority

Name and address of the controller:	
The name and contact details of the Data Protection Officer, or if not designated, another point of contact of the controller	
1. The timing and nature of the personal data breach	
2. Details of the categories of data subjects and personal data affected by the personal data breach	
3. The approximate number of data subjects affected by the personal data breach	
4. Details of the likely consequences of the personal data breach for ongoing security of the controller's processing of personal data and the rights and freedoms of the concerned data subjects, and any other material consequences	
5. The conclusion of the risk assessment conducted as per the requirements of rule 3 of these Regulations.	
6. A description of the manner in which the controller shall make a notification to data subjects, if required under rule 4 of these Regulations.	
7. A description of the measures taken or proposed to be taken by the controller or its processors or sub processors to address the personal data breach, including measures to mitigate its possible adverse effects on the affected data subjects	

Declaration by the Controller:

I, the undersigned, hereby certifies that I'm authorized to make this notification and the that all the information in this notification is true and complete to the best of the knowledge of my knowledge.

Signature:
Name:
Designation:
Date:

Note: Insert name of the controller if it is a natural person, or in the case of a controller that is a legal person, insert name of the Data Protection Officer or, if there is no Data Protection Officer designated, then the name of secretary, chief executive officer or the head of such legal person.

SCHEDULE II

(rule 4)

Notification of Personal Data Breach to the Affected Data Subjects

Name and address of the controller:	
The name and contact details of the Data Protection Officer, or if not designated, another point of contact of the controller	
1. The timing and nature of the personal data breach	
2. Details of the categories of data subjects and personal data affected by the personal data breach	
3. The approximate number of data subjects affected by the personal data breach	
4. Details of the likely consequences of the personal data breach for affected data subjects	
5. A description of any measures taken or proposed to be taken by the controller to address the breach, including measures to mitigate its possible adverse effects on the affected data subjects	
6. Proposed measures an affected data subjects shall take to mitigate the possible risks of harm from the personal data breach that are appropriate to the nature of the personal data breach and the potential adverse consequences to the data subject (i.e. resetting passwords, monitoring activity in financial accounts, contacting service providers or counterparties to alert them to the breach and potential mitigating steps they could take; and in cases of destruction, loss or alteration of personal data, a means of recovering the personal data from other sources)	
7. A website address where further information is or shall be made available.	