PERSONAL DATA PROTECTION ACT, NO. 9 OF 2022

Directives made by the Data Protection Authority of Sri Lanka, under subsection (4) of section 26, read with paragraph (s) of section 32 and paragraph (c) of section 33 of the Personal Data Protection Act, No. 9 of 2022.

Data Protection Authority of Sri Lanka

Colombo,

, 2024

DIRECTIVES

1. These Directives may be cited as the Personal Data Protection (Specification of Instruments for Processing of Personal Data Outside Sri Lanka) Directives No. of 2024.

2. These Directives shall apply to controllers or processors other than public authorities

3. These Directives shall not apply to processing of personal data in a third country prescribed by the Minister pursuant to an adequacy decision made under subsection (2) of section 26 of the Act.

4. For the purpose of subsection (4) of section 26 of the Act, a controller or processor other than a public authority shall adopt the following instruments to ensure binding and enforceable commitments of the recipient in the third country to ensure appropriate safeguards to the rights of the data subjects and remedies protected by the Act:-

(a) binding corporate rules referred to in directive 6;

(b) an agreement referred to in directive 6;

(c) a code of conduct referred to in directive 6;

(d) a binding certification scheme referred to in directive 6;

(e) a cross border processing impact assessment referred to in directive 7; and

(f) a resolution of the board of directors or equivalent authority of a controller referred to in directive 9.

5. A controller, processor or sub processor shall transfer personal data to a controller, processor or sub processor who process such data in a country outside Sri Lanka only if—

(a) the controller, processor or sub processor as the case may be, who transfers such personal data and the recipient of such personal data-

(i) is subject to any binding corporate rules under directive 6; or

(ii) has entered into an agreement under directive 6;

(b) the recipient of such personal data-

(i) has undertaken to comply with a code of conduct under directive 6; or

(ii) is certified as compliant under a certification scheme under directive 6; or

(c) the transferring controller, processor or sub processor, as the case may be, has carried out a cross border processing impact assessment under directive 7.

6. (1) Binding corporate rules, an agreement, a code of conduct or a certification scheme shall qualify for the purposes of directive 5 with respect to the relevant processing if -

(a) the recipient is a controller, such binding corporate rules, agreement, code of conduct or certification scheme include written, binding and enforceable controller's processing obligations applying to the recipient;

(b) the recipient is a processor or sub processor, such binding corporate rules, agreement, code of conduct or certification scheme include written, binding and enforceable processor's processing obligations applying to the recipient; and

(c) such binding corporate rules, agreement, code of conduct or certification scheme expressly confer enforceable rights on data subjects with regard to the controller's processing obligations or processor's processing obligations, as the case may be, in so far as they apply to the processing of their personal data.

(2) For the purpose of directive 5 and this directive, a certification scheme includes any certification system specified in the Schedule hereto.

7. A cross border processing impact assessment shall qualify for the purposes of directive 5, if the transferring controller, processor or sub processor, as the case may be, has assessed—

(a) the relevant written law and enforcement mechanisms relating to the protection of personal data in the third country; and

(b) the binding and enforceable commitments of the recipient in the third country,

and such assessment reasonably concludes that the combination of such law, enforcement mechanisms and commitments ensure appropriate safeguards of the rights of data subjects and remedies protected by the Act, including controller's processing obligations and processor's processing obligations, as applicable.

8. Where a controller, processor or sub processor is engaged in direct processing of personal data in a third country, such processing shall comply with the controller's processing obligations or processor's processing obligations, as applicable.

9. Where a controller, processor or sub processor transfers personal data to a recipient in a third country to whom the Act may not apply by virtue of subsection (2) of section 2 of the Act, for further processing, the board of directors or equivalent authority of the controller, processor or sub processor, as the case may be, shall ensure that-

(a) the controller, processor or sub processor shall take all necessary steps to comply with:

(i) the controller's or processor's processing obligations, as may be applicable, with respect to such processing; and

(ii) the provisions of the Act and any regulation, rule or other instrument made thereunder applicable to further processing of personal data; and

(b) the board of directors or equivalent authority of the controller, processor or sub processor shall be provided annual reports on the implementation of and compliance with paragraph (a).

10. For the purposes of directives 6, 7, 8 and 9-

(a) "controller's processing obligations" means-

(i) obligation of a controller set out in Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of the Act with respect to any processing and any further processing of the personal data to be carried out by it or by any processor or sub processor on its behalf;

(ii) obligation of a controller to enter into a written, binding and enforceable agreement in relation to such cross border processing of personal data carried out by a processor;

(b) "processor's processing obligations" means-

(i) obligations of a processor or sub processor to designate or appoint a Data Protection Officer under section 20 of the Act, in the circumstances set out in paragraph (b) of subsection (1) of section 20 of the Act;

(ii) obligations of a processor or sub processor to comply with the provisions of subsection (1) of section 22 of the Act; and

(iii) obligations of a processor or sub processor to enter into a written, binding and enforceable agreement in relation to such cross border processing of personal data caried out by a processor.

11. A controller, processor or sub processor who processes personal data in a country outside Sri Lanka shall provide to the Authority a copy of-

(a) any binding corporate rules, agreement, code of conduct or certification scheme referred to in directive 5; and

(b) any resolution of the board of directors or equivalent authority of the controller referred to in directive 9,

if requested by the Authority in writing.

12. Directive 11 shall not come into force until three years from the date of coming into operation of section 26 of the Act.

13. Nothing in these directives shall be interpreted to limit the obligations of controllers and processors relating to the processing of personal data, including any transfers of personal data to third parties, under the Act and any regulation, rule or other instrument made thereunder.

14. In these directives, unless the context otherwise requires-

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

"Act" means the Personal Data Protection Act, No. 9 of 2022;

"binding corporate rules" means personal data protection policies and procedures adhered to by the members of a group of firms under common control with respect to the transfer of personal data among such members and containing the controller's processing obligations or processor's processing obligations, as applicable;

"certifying bodies" means the bodies local or foreign that provide certification services relating to the processing of personal data or qualifications of Data Protection Officers;

"certification scheme" means a scheme under which a certifying body having an appropriate level of expertise in relation to the subject-matter of the scheme certifies participants in the scheme as compliant with this Directive and any other criteria relating to the processing of personal data or qualifications under the scheme;

"code of conduct" means a code setting out personal data protection policies and procedures where compliance by the controllers or processors undertaking to apply it is subject to mandatory monitoring by a body having an appropriate level of expertise in relation to the subject-matter of the code;

"controller" means, any natural or legal person, public authority, nongovernmental organization, agency or any other body or entity which alone or jointly with others determines the purposes and means of the processing of personal data;

"cross border processing impact assessment" means an assessment referred to in directive 7;

"data subject" means, an identified or identifiable natural person, alive or deceased, to whom the personal data relates;

"Data Protection Officer" means, the person designated or appointed under section 20 of the Act;

"direct processing" means processing conducted directly by the relevant controller or processor, as opposed to any processing conducted by a processor acting on its behalf (in the case of a controller) or any sub processor;

"identifiable natural person" is a natural person who can be identified, directly or indirectly, by reference to any personal data;

"local authority" means, a Municipal Council, Urban Council or a Pradeshiya Sabha and includes any authority created or established by or under any law to exercise, perform and discharge powers, duties and functions corresponding or similar to the powers, duties and functions exercised, performed or discharged by any such Council or Sabha;

"personal data" means, any information that can identify a data subject directly or indirectly, by reference to-

(a) an identifier such as a name, an identification number, financial data, location data or an online identifier; or

(b) one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that individual or natural person;

"processing" means, any operation performed on personal data including but not limited to collection, storage, preservation, alteration, retrieval, disclosure, transmission, making available, erasure, destruction of, consultation, alignment, combination, or the carrying out of logical or arithmetical operations on personal data;

"processor" means, a natural or legal person, public authority or other entity established by or under any written law, which processes personal data on behalf of a controller;

"public authority" means, a Ministry, any Department or Provincial Council, local authority, statutory body or any institution established by any written law, or a Ministry, any Department or other authority or institution established or created by a Provincial Council;

"Sri Lanka" means, the territorial limits of Sri Lanka as stipulated by Article 5 of the Constitution and includes the territorial waters or air space of Sri Lanka, any ship or aircraft registered in Sri Lanka, any location within the premises of a Sri Lankan mission or the residence of the Head of such mission, diplomatic agent or any other member of such mission, situated outside Sri Lanka, or within any premises occupied on behalf of, or under the control of, the Government of Sri Lanka or any statutory body established in Sri Lanka and situated outside Sri Lanka; and

"sub processor" means, in accordance with subsection (2) of section 22 of the Act, a processor engaged by another processor for carrying out specific processing activities.

SCHEDULE

(Directive 6)

Certification systems

1. Cross-Border Privacy Rules (CBPR) System of the Asia-Pacific Economic Cooperation (APEC);

2. Europrivacy certification scheme of the European Centre for Certification and Privacy (ECCP);

3. any national or other certification scheme of any Member State of the European Union, Switzerland or the United Kingdom by which a duly certification body, duly accredited as such under authority of law, provides certification of an organisation's compliance with the European General Data Protection Regulations (GDPR) or the applicable national general data protection law of the relevant State; and

4. any other certification scheme by which a certification body, duly accredited as such under authority of law, provides certification of an organisation's compliance with a data protection law of any country, standard or code of practice in each case containing obligations of controllers and processors substantially similar to those in Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of the Act.