Evaluating Policy Influence with Process Tracing

LIRNEasia inputs for

PERSONAL DATA PROTECTION ACT, No. 9 OF 2022

Isuru Samaratunga and Milindu Tissera

September 2022

This report is to..

1. Evaluate the impact of interventions by LIRNEasia on the Personal Data Protection Act, No. 9 of 2022. The three interventions are written comments (see Annex 1) submitted and nine Op-Eds by Rohan Samarajiva on;
   - the proposals for the proposed Data protection legislation on 16 June 2019
   - the Personal Data Protection Draft Bill on 5 October 2019
2. Provide details of media coverage of above comments and on the Act in general

The most significant impacts of LIRNEasia comments are;

1. Cost of compliance is reduced

June 2019 Draft stated that 'subjected to exemptions provided under this Act, no person shall act as a controller unless registered with the Authority..' Commenting on that LIRNEasia pointed out the vast scope of those who are required to register, high transaction cost, annual workload adds for regulators and unnecessary administrative burdens on SMEs due to registration requirement.

The registration requirement has been removed from the Act. It reduces the costs of compliance for the many thousands of micro, small and medium enterprises. (See slide 4 for more details)

2. Cross border flow of personal data is rationalized

June 2019 Draft stated that 1) 'any processing of personal data by a controller which is a government Ministry, Department or statutory body shall be proceed only in Sri Lanka. 2) 'A controller or processor shall not be subject to any specific authorisation from the Authority if the Minister by Regulation prescribes a third country, a territory or one or more specified sectors within that third country, or the international organisation, where processing takes place, ensures an adequate level of protection in accordance with the provisions of this Act'.

LIRNEasia pointed out that this deprives Sri Lanka entities from use of low-cost and high quality cloud services, creates price-gouging opportunities for local data centers, and prevents taking rational decisions in dynamic market.

The Act allows public authority to process personal data as a controller or processor in a third country after a consultation with the Authority and a controller or processor other than a public authority can process personal data in a third country. (See slide 5 for more details)

Back to slide # 3

Cost of compliance is reduced by removing registration requirement of controllers and processors

Shedule in the Draft	LIRNEasia comments	Impact: Schedule in the Act
16. REGISTRATION OF CONTROLLERS AND PROCESSORS 1.1) Subject to exemptions provided under this Act, no person shall act as a controller unless registered with the Authority in accordance with the provisions of this Section and by paying such annual fee as prescribed. 2.2) Controllers that are Public Authorities who are deemed controllers shall be excluded from the payment of the registration fee under section 16(1). 17. APPLICATION FOR REGISTRATION 1.1) Every person who intends to act as a controller shall apply to the Authority in the prescribed form within such time period as prescribed. 2.2) An application under subsection (1) shall provide the following particulars – 1. A description of the personal data to be processed by the applicant , and of 2. the category of data subjects, to which the personal data relates; 3. a statement as to whether the applicant is likely to hold any special 4. categories of personal data; 5. a description of the purpose for which the personal data is to be processed; 6. a description of any recipient to whom the applicant intends or may intend 7. to disclose the personal data; 8. the name, or a description of, any country to which the applicant intends or 9. may wish, directly or indirectly, to transfer the personal data; 10. statement as to a representative for the purposes of this Act and details of 11. such representative; 12. a general description of the risks, safeguards, security measures and 13. mechanisms to ensure the protection of personal data; and 14. any other details as may be prescribed by the Authority. 3.3) A controller who knowingly supplies any false or misleading detail under subsection 17(2) commits an offence under this Act. 4.4) The Authority shall issue a certificate of registration to an applicant who satisfies the prescribed criteria to be registered as a controller. 5.5) Where there is a change in any particular outlined under subsection (2), the controller shall notify the Authority of such change in prescribed period. On receipt of such notification the Authority shall amend the respective entry in such Register maintained by the Authority.	…There are likely to be thousands of data controllers. Annual registration adds workload to both the regulator and the controllers. May be useful to leave room for multi-year registrations to reduce costs on both sides. …The first operative part “subject to exemptions provided under this Act” is of grave importance, to ensure that small organizations (deemed small on the basis of number of employees and/or the amount of personal data they process) are not burdened with unnecessary administrative burdens, especially since the current process (Section 17 and 19) are quite cumbersome. As such the ministry might consider different categories of requirements in relation to registration and in some case exclude smaller organizations all together from registration even if they would still be subject to this act. …The first operative part “subject to exemptions provided under this Act” is of grave importance, to ensure that small organizations (deemed small on the basis of number of employees and/or the amount of personal data they process) are not burdened with unnecessary administrative burdens, especially since the current process (Section 17 and 19) are quite cumbersome. As such the ministry might consider different categories of requirements in relation to registration and in some case exclude smaller organizations all together from registration even if they would still be subject to this act. Op-ed’s- Increasingly, individuals maintain databases in computerised form. A family’s invitee list for a wedding is an example. Section 2(3) of the bill excludes “personal data processed purely for private, domestic or household purposes by an individual”. If the invitee list is maintained by an event organiser, it is subject to the provisions of the Bill. Citizens need not concern themselves about the obligations imposed on data controllers by the proposed law. The scope of those who are required to register is so vast and the transactions costs are so high that many small businesses and organisations do not register. Even in Europe, data protection authorities do not have the personnel to actively compel registration and compliance.	Registration requirement has been removed from the Act

LIRNEasia
Pro-poor. Pro-market.

Back to slide # 3

Cross boarder flow of personal data is rationalized

Section in the Draft	LIRNEasia comments	Impact: Schedule in the Act
1.PART VI – CROSS-BORDER FLOW OF PERSONAL DATA 28.Any processing of personal data by a controller which is a government Ministry, Department or statutory body shall be processed only in Sri Lanka and shall not be processed outside the territory of Sri Lanka unless the Authority in concurrence with such controller and relevant regulatory body classify categories of personal data that should be localised. 28.A controller or processor shall not be subject to any specific authorisation from the Authority if the Minister by Regulation prescribes a third country, a territory or one or more specified sectors within that third country, or the international organisation, where processing takes place, ensures an adequate level of protection in accordance with the provisions of this Act. 29. However,wheresuchdecisionunderSection30hasnotbeenmade,acontroller or processor may process data at a location outside Sri Lanka only if the controller or processor has provided appropriate safeguards, and on condition that enforceable data subject rights and effective legal remedies for data subjects are available.	… S. 29. This will deprive Sri Lanka entities from use of low-cost and high-quality cloud services and create price-gouging opportunities for local data centers. There should be a strong justification for such a blanket prohibition. …Why not leave room for CLOUD Act provisions, which would at least allow for reasonable legal access? S. 33 seems to miss the whole point of cloud services. Prior approval makes no sense in a dynamic market. ..Ambiguities exist in section 25, where (1) applies only to public authorities, and the other subsections may apply more broadly. Why constrain options for data storage in a small economy? Cannot the legitimate law enforcement objectives be better achieved by CLOUD act like provisions, without driving up costs and compromising security of data storage by public authorities? …Section 30 provides for the Minister in charge to prescribe foreign jurisdictions for which controllers located in those said locations do not require authorization from the Authority. In order to give certainty to businesses and foreign entities that currently provide important services to Sri Lankan citizens and business, it is strongly recommended a non-exhaustive list of foreign territories which have recognized data protection legislation be included as a guideline/regulation at the time of finalizing this act. …Somewhat peculiarly, adequacy provisions have also been extended to private entities that are not public authorities. The difference appears to be that public authorities may process only specified subsets of data even in countries that pass the adequacy test, while the entirety of the data held by private entities may be so processed. It is unlikely that the powerful cloud-based processing capacities of companies such as Google will be fragmented and located in national territories to satisfy data localisation rules.	26. (1) Where a public authority process personal data as a controller or processor, such personal data shall be processed only in Sri Lanka and shall not be processed in a third country, unless the Authority in consultation with, that controller or processor as the case may be and the relevant regulatory or statutory body, classifies the categories of personal data which may be permitted to be processed in a third country, prescribed by the Minister pursuant to an adequacy decision made under subsection (2). (2) (*a*) For the purpose of making an “adequacy decision”, the Minister shall, in consultation with the Authority take into consideration the relevant written law and enforcement mechanisms relating to the protection of personal data in a third country and the application of the provisions of Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of this Act, and such other prescribed criteria relating to the processing of personal data, in a third country for the purpose of cross border data flow. (3) A controller or processor other than a public authority may process personal data– 1.(*a*) in a third country prescribed pursuant to an adequacy decision; or 2.(*b*) in a country, not being a third country prescribed pursuant to an adequacy decision, only where such controller or processor as the case may be, ensures compliance with the respective obligations imposed under Part I, Part II and sections 20, 21, 22, 23, 24 and 25 of Part III of this Act.

LIRNEasia
Pro-poor. Pro-market.

In summary

Out of LIRNEasia comments:

1. Nineteen comments have been accepted
2. Five comments have been partially accepted
3. Thirteen comments have not been accepted

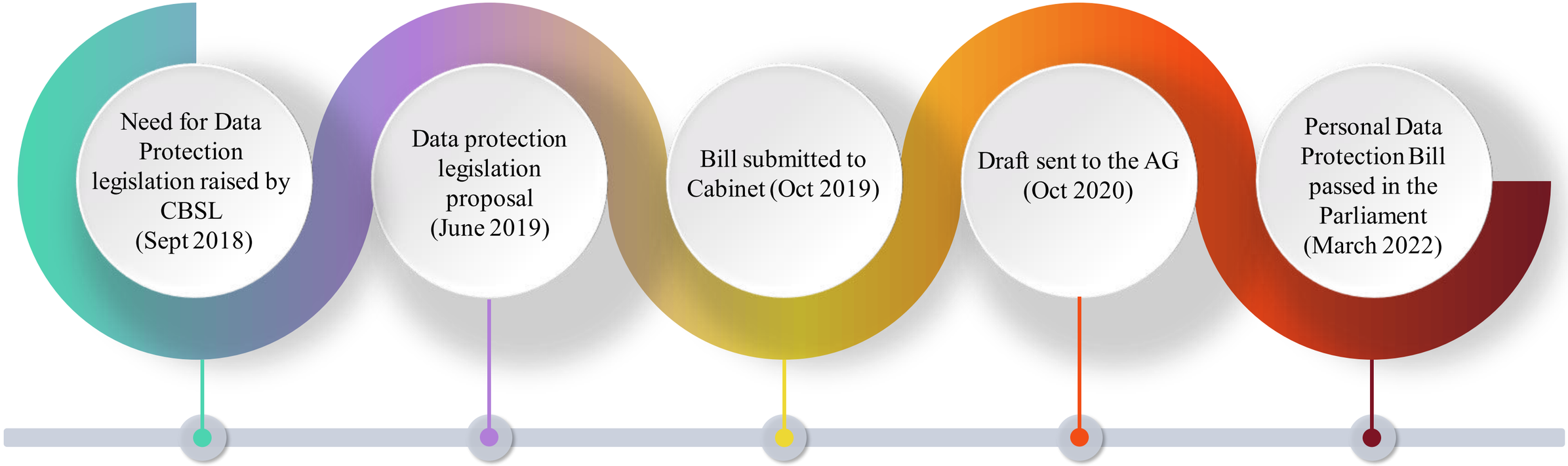
Section one of this report provides details of LIRNEasia comments and related schedules in the Act.

Section two of this report provides details of media coverage and reach of LIRNEasia comments.

1

Impact of written comments

PERSONAL DATA PROTECTION ACT – CONSULTATION PROCESS



Ministry of Telecommunications and Digital Infrastructure drafted a Bill with ICTA, CB and other stakeholders

The Draft Bill was subjected to 7 rounds of public stakeholder consultation and the committee received over 30 written submissions

The Bill was further viewed by the Attorney General and Bar Association of Sri Lanka

Further stakeholder consultation by Ceylon Chamber of Commerce, Ministry of Justice, CB and TRCSL.

The Parliament of Sri Lanka announced, that it had passed the Bill to provide the Regulation of Processing of Personal Data with amendments on 9 March 2022

LIRNEasia
Pro-poor. Pro-market.

ASSESSMENT ON THE IMPACT OF COMMENTS - 1

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
1. (2) The provisions of this section, shall come into operation on the date on which the certificate of the Speaker is endorsed in respect of this Act in terms of Article 79 of the Constitution. (3) All other provisions of this Act except the provisions of Part IV and Part V, shall come into operation on such date as the Minister may, appoint by Order published in the *Gazette*, which shall be a date not earlier than eighteen months and not later than thirty six months from the date of the certificate of the Speaker referred to in subsection (2). (4) The date of operation of the provisions of Part IV of this Act, shall be a date not earlier than twenty-four months and not later than forty-eight months from the date of certificate referred to in subsection (2). (5) The date of operation of the provisions of Part V of this Act shall be a date appointed by the Minister by Order published in the *Gazette* which shall be a date not later than the date appointed by the Minister under subsection (3).	A phased approach to implementation is necessary so as to give organizations (controllers and processors) time to implement the needed protection mechanisms. As such we recommend that alternative (3) be adopted which provides for a phased approach. Since, data protection obligations (Part II) would be in force, protection is afforded to data subjects. Additionally, it is strongly recommended that after the last part of (i) which reads as follows: "certificate is endorsed in respect of this Act in terms of Article 79 of the Constitution" the following be added *"or within a span of one (1) year".* This addition would guarantee that there is no unreasonable delay in the Act coming into force.	**Accepted**
2. (1) This Act shall apply to the processing of personal data— (a) where the processing of personal data takes place wholly or partly within Sri Lanka; or (b) where the processing of personal data is carried out by a controller or processor who– (iii) offers goods or services to data subjects in Sri Lanka including the offering of goods or services with specific targeting of data subjects in Sri Lanka; or (iv) specifically monitors the behaviour of data subjects in Sri Lanka including profiling with the intention of making decisions in relation to the behavior of such data subjects in so far as such behaviour takes place in Sri Lanka.	S. 1(b)(v) is very broad. It would for example apply to Google Maps, requiring Google to register in Sri Lanka. If Google refuses, will our citizens and visitors be deprived of the use of Google maps? The use of assistive technologies such as Google Transcribe or others such as Transliterate could be affected. This could possibly be resolved by changing the OR in s. 1(a) to "AND"	**Not accepted**
3. (1) The provisions of this Act shall have effect notwithstanding anything to the contrary in any other written law, relating to the protection of personal data of data subjects: Provided however, where a public authority is governed by any other written law, it shall be lawful for such authority to carry out processing of personal data in accordance with the provisions of such written law, in so far as the protection of personal data of data subjects is consistent with this Act.	Section 4(1): "It shall be lawful for a public authority to carry out the processing of personal data in accordance with its governing legal framework in so far as such frame work is not inconsistent with the provisions of this Act." Why limit to public authorities? Unclear. But section 3 brings in entities that are not public authorities.	**Not accepted**

Note: Section numbers given in the 'Schedule in the Act' column are according to the section numbers in the Act.
Section numbers given in the 'Related comment in written submission and Op-Ed's' coloumn are according to the draft documents that commented on.

LIRNEasia
Pro-poor. Pro-market.

ASSESSMENT ON THE IMPACT OF COMMENTS - 2

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
3. (2) In the event of any inconsistency between the provisions of this Act and the provisions of such written law, the provisions of this Act shall prevail.	Section 4(2): "In the event of any inconsistency between the provisions of this Act and the provisions of any other written law, the provisions of this Act shall prevail." It would be problematic if preservation requirements in National Archives Act and RTI Act are overridden by this section. But see, exceptions to s. 7 and s. 9 etc. which may look after the Archives Act.	**Not accepted**
5. The processing of personal data shall be lawful if a controller is in compliance with— (*a*) any condition specified in Schedule I hereto; (*b*) any condition specified in Schedule II hereto in the case of processing special categories of personal data; (*c*) all the conditions specified in Schedule III hereto in the case of processing personal data based on the consent of the data subject under item (*a*) of Schedule I or under item (*a*) of Schedule II hereto; or	Schedules are completely anchored on consent. But consent is incompatible with 21st century practices: "Many of the most-protected 'personal' data are not personal at all, but are created to facilitate the operation of larger (e.g. administrative, economic, transport) systems or inadvertently generated by using such systems. The protection given to such data typically rests on notions of informed consent even in circumstances where such consent may be difficult to define, harder to give and nearly impossible to certify in meaningful ways. The over-broad application of consent will be harmful to innovation and competition:	**Not accepted**
6. (2) Subject to the provisions of section 10 of this Act, further processing of such personal data by a controller for archiving purposes in the public interest, scientific research, historical research or statistical purposes shall not be considered to be incompatible with the initial purposes referred to in paragraphs (a), (b) and (c) of subsection (1).	S. 3. Purpose limitation, unless carefully handled can stifle most big data and AI applications. As currently stated, Section 3 only allows further processing "strictly for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes." This provision leads to ambiguity i.e. whether "archiving purposes" is only applicable to public interest or archiving is applicable to scientific, historical and statistical research too. Furthermore, this would be unduly restricting additional processing, only to instances of archiving, which would limit the productive uses of data. Instead we recommend the provision be amended to read as follows: *"However, further processing of personal data strictly for purposes in the public interest, or scientific, or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes."* The term 'archiving' is a form of further processing and has been removed in the suggested text since it.	**Accepted**

ASSESSMENT ON THE IMPACT OF COMMENTS - 3

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
9. Every controller shall ensure that personal data that is being processed shall be kept in a form which permits identification of data subjects only for such period as may be necessary or required for the purposes for which such personal data is processed: Provided however, subject to the provisions of section 10 of this Act, a controller may store personal data for longer periods in so far as the personal data shall be processed further for archiving purposes in the public interest, scientific research, historical research or statistical purposes.	Please refer to comments under Section 3 ("Purpose Limitation") to rectify the wording in relation to archiving as per our suggestions. The last part of the section states "implementation of the appropriate technical and organisational measures provided under this Act". It is noted while certain technical and organization measures have been included under the Act, they are generically worded. It is recommended that the provision be amended as follows "implementation of the appropriate technical and organisational measures as provided under this Act *and by rules issued hereunder.*"	**Accepted**
10. Every controller shall ensure integrity and confidentiality of personal data that is being processed, by using appropriate technical and organizational measures including encryption, pseudonymisation, anonymisation or access controls or such other measures as may be prescribed so as to prevent the – (*a*) unauthorized or unlawful processing of personal data; or (*b*) loss, destruction or damage of personal data.	Section 2(b): "any data, which has been irreversibly anonymized in such a manner that causes the individual to be unidentifiable." S. 10 mentions pseudonymization in addition to anonymization, indicating the former is not included within the s. 2(b) exception. Even the GDPR permits pseudonymization. The requirement of irreversible anonymization is far too strict and will cripple research. It is necessary to understand that there are no absolutes. What would be good is if acceptable/safe pseudonymization and anonymization is left to be determined by a working group of data scientists, rather than lawyers or judges because technologies of de-identification and re-identification will be constantly changing (almost an "arms race"). The draft proposes limitations to processing pseudonymized data under this act, and in its current form impedes the productive use of such data. Even the GDPR provides latitude for controllers when using pseudonymized data in further processing beyond the original intention of data collection. As noted earlier (Comment 3), the proposed act subjects pseudonymized data to all the obligations proposed under this Act. Even GDPR allows controllers who pseudonymize personal data more latitude in processing the data for a different purpose than the one for which they were collected. Article 6(4)(e) of GDPR allows controllers latitude in further processing without consent when their exists, amongst others, "appropriate safeguards, which may include encryption or pseudonymization." Similarly we strongly recommend that the proposed act loosen the restrictions in the use of pseudonymized data especially in instances of further processing.	**Accepted**

ASSESSMENT ON THE IMPACT OF COMMENTS - 4

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
12. (1) It shall be the duty of every controller to implement internal controls and procedures, (hereinafter referred to as the "Data Protection Management Programme") that—	S. 18. It is necessary to consider the burdens of compliance and formulate a lighter set of obligations for firms below a specified threshold.	**Not accepted**
14. (1) Every data subject shall have the right to withdraw his consent at any time upon a written request made by such data subject if such processing is based on the grounds specified in item (*a*) of Schedule I or item (*a*) of Schedule II of this Act:	There should be an exception for transaction-generated data, which is a by-product of a transaction. Consent cannot be practically withdrawn in these instances, except by discontinuing service (which does not require law). Rest of safeguards may apply, but consent is impractical, especially with regard to TGD. It may be useful to consider making this section apply only to data that is not TGD. This would require including TGD in s. 46.	**Not accepted**
16. Every data subject shall have the right to make a written request to the controller to have his personal data erased, under the following circumstances where–	S. 9. Internally contradictory: withdrawal must be in writing; must be as easy as giving consent. Most electronic systems depend on ease of giving consent.	**Partially accepted**
17. (1) Where a controller receives a written request from a data subject under sections 13, 14, 15 or 16, such controller shall inform the data subject in writing, within twenty-one working days from the date of such request, whether– (a) such request has been granted; (b) such request has been refused under subsection (2) and the reasons thereof unless such disclosure is prohibited by any written law; or (c) the controller has refrained from further processing such personal data under sections 14(2) or 15 and reasons thereof,	Section 11 (3) is vague and unclear. It currently states: "this section does not impose any *obligation* on the controller to process additional personal data that is not required for the purpose of processing..." It is unclear whether this implies that although there is no obligation, it would be permissible for a controller to process additional data for the purposes of fulfilling a request? This needs to be amended for better clarity. Section 12 (1) (a) states that erasure of data can be demanded when processing is not lawful including when consent has been withdrawn under (a) of Schedule 1 or (a) of Schedule 2. For avoidance of doubt it is recommended that other circumstances when erasure can be demanded are included here, since the terminology is inclusive and not exhaustive.	**Accepted**
18. (1) Subject to section 19, every data subject shall have the right to request a controller to review a decision of such controller based solely on automated processing, which has created or which is likely to create an irreversible and continuous impact on the rights and freedoms of the data subject under any written law.	In automated processing it is crucial for the data subject(s) to be provided with all information on the mechanism of automated processing i.e. how it was used or what is the software aiding with, etc. It is also of equal importance that when a request regarding automated processing is made to the Controller, a reasoned order be given. We recommend these concerns be addressed in this Act or under separate rules as has been stipulated under section 14 (2).	**Accepted**

ASSESSMENT ON THE IMPACT OF COMMENTS - 5

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
20. (1) Every controller and processor shall designate or appoint a Data Protection Officer, to ensure compliance with the provisions of this Act, in the following circumstances:– (a) where the processing is carried out by a ministry, government department or public corporation, except for judiciary acting in their judicial capacity; or (b) where the core activities of processing carried out by the controller or processor consist of the following:– (i) operations which, by virtue of their nature, their scope or their purposes, require regular and systematic monitoring of data subjects on a scale and magnitude as may be prescribed; or (ii) processing of special categories of personal data on a scale and magnitude as may be prescribed; or (iii) processing which results in a risk of harm affecting the rights of the data subjects protected under this Act based on the nature of processing and its impact on data subjects.	S. 18. It is necessary to consider the burdens of compliance and formulate a lighter set of obligations for firms below a specified threshold. Section 22 (1) (b) & (c) specify "large scale" business activities as a pre-condition for appointment of a data protection officer (DPO). We note that the GDPR also defines the requirement of appointing a DPO similarly. However, instead of leaving "large scale" undefined, we recommend adopting a definition. Early drafts of the GDPR included a definition of "large scale" ((but which were subsequently dropped) as "companies with more than 250 employees or the processing of more than 5,000 personal data records." It is very important that threshold similar to what GDPR originally considered, be adopted in Sri Lanka to reduce the onerous burdens especially in small companies/ organizations. Alternatively, this may also be defined in subsequent rules/ regulations.	**Partially accepted**
	Section 22 (2) requires the DPO to be an employee of the controller or processor. This could be an unnecessary burden on certain companies, especially those who do not require the services of the DPO frequently. Since the section, as it presently stands, does not give any indication of what constitutes "large scale", this requirement can be even more burdensome. Hence, we recommend this be amended.	**Accepted**

LIRNEasia
Pro-poor. Pro-market.

ASSESSMENT ON THE IMPACT OF COMMENTS - 6

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
20. (2) A Data Protection Officer shall possess relevant academic and professional qualifications as may be prescribed which may include academic background, knowledge and technical skills in matters relating to data protection having competency and capacity to implement strategies and mechanisms to respond to inquiries and incidents related to processing of personal data.	Section 22 (5) specifies the educational qualifications and expertise required of the DPO. This is too prescriptive as it deals with the appointment of an officer within a private entity and not a Government Agency. This leaves room for the Authority to question the credentials of an appointed DPO at a private organization and request his/her removal on the basis of irrelevant qualifications if this kind of overly authoritarian requirement is included in this Act. We recommend removing this specification.	**Accepted**
20. (5) The responsibility of the Data Protection Officer shall be to– (*a*) advise the controller or processor and their employees on data processing requirements provided under this Act or any other written law; (*b*) ensure on behalf of the controller or processor that the provisions of this Act are complied with; (*c*) facilitate capacity building of staff involved in data processing operations; (*d*) provide advice on personal data protection impact assessments; and (*e*) co-operate and comply with all directives and instructions issued by the Authority on matters relating to data protection.	Section 23 (2) enshrines several technical measures to protect personal data. The various methods are preceded by "such as" indicating it is not an exhaustive list. For avoidance of doubt we suggest incorporating "*including, but not limited to*."	**Partially accepted**
24. (2) The personal data protection impact assessment shall contain such information and particulars including any measures and safeguards taken by the controller to mitigate any risk of harm caused to the data subject by the processing referred to in subsection (1). (4) The controller shall conduct a fresh personal data protection impact assessment in accordance with this section whenever there is any change in the methodology, technology or process adopted in the processing for which a personal data protection impact assessment has already been carried out.	Section 26 (1) requires a controller to carry out an impact assessment when there is a potential "high risk to the rights of the data subject." It is recommended that some guidance be provided on what constitutes "high risk." Section 26 (5) requires a fresh data protection impact assessment, whenever there is a "significant change in methodology or technology". It is recommended that some guidance be added on what would constitute "significant change".	**Not accepted**

LIRNEasia
Pro-poor. Pro-market.

ASSESSMENT ON THE IMPACT OF COMMENTS - 7

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
[Registration requirement has been removed from the Act]	S. 19. There are likely to be thousands of data controllers. Annual registration adds workload to both the regulator and the controllers. May be useful to leave room for multi-year registrations to reduce costs on both sides. The first operative part "subject to exemptions provided under this Act" is of grave importance, to ensure that small organizations (deemed small on the basis of number of employees and/or the amount of personal data they process) are not burdened with unnecessary administrative burdens, especially since the current process (Section 17 and 19) are quite cumbersome. As such the ministry might consider different categories of requirements in relation to registration and in some case exclude smaller organizations all together from registration even if they would still be subject to this act. Op-ed's- Increasingly, individuals maintain databases in computerised form. A family's invitee list for a wedding is an example. Section 2(3) of the bill excludes "personal data processed purely for private, domestic or household purposes by an individual". If the invitee list is maintained by an event organiser, it is subject to the provisions of the Bill. Citizens need not concern themselves about the obligations imposed on data controllers by the proposed law. The scope of those who are required to register is so vast and the transactions costs are so high that many small businesses and organisations do not register. Even in Europe, data protection authorities do not have the personnel to actively compel registration and compliance.	**Accepted**
26. (3) A controller or processor other than a public authority may process personal data– (*a*) in a third country prescribed pursuant to an adequacy decision;	Op-Ed's - Somewhat peculiarly, adequacy provisions have also been extended to private entities that are not public authorities. The difference appears to be that public authorities may process only specified subsets of data even in countries that pass the adequacy test, while the entirety of the data held by private entities may be so processed. It is unlikely that the powerful cloud-based processing capacities of companies such as Google will be fragmented and located in national territories to satisfy data localisation rules. Restrictions that applied to private entities that are not public authorities have been considerably relaxed by the floor amendments. Appreciating the difficulties of making adequacy a condition for use of cloud services and data centres located outside Sri Lanka, the newly introduced language provides a series of exceptions, including consent to processing abroad and performance of a contract.	**Accepted**

ASSESSMENT ON THE IMPACT OF COMMENTS - 8

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
26. (1) Where a public authority process personal data as a controller or processor, such personal data shall be processed only in Sri Lanka and shall not be processed in a third country, unless the Authority in consultation with, that controller or processor as the case may be and the relevant regulatory or statutory body, classifies the categories of personal data which may be permitted to be processed in a third country, prescribed by the Minister pursuant to an adequacy decision made under subsection (2).	S. 29. This will deprive Sri Lanka entities from use of low-cost and high-quality cloud services and create price-gouging opportunities for local data centers. There should be a strong justification for such a blanket prohibition. Why not leave room for CLOUD Act provisions, which would at least allow for reasonable legal access? S. 33 seems to miss the whole point of cloud services. Prior approval makes no sense in a dynamic market. Ambiguities exist in section 25, where (1) applies only to public authorities, and the other subsections may apply more broadly. Why constrain options for data storage in a small economy? Cannot the legitimate law enforcement objectives be better achieved by CLOUD act like provisions, without driving up costs and compromising security of data storage by public authorities? Section 30 provides for the Minister in charge to prescribe foreign jurisdictions for which controllers located in those said locations do not require authorization from the Authority. In order to give certainty to businesses and foreign entities that currently provide important services to Sri Lankan citizens and business, it is strongly recommended a non-exhaustive list of foreign territories which have recognized data protection legislation be included as a guideline/regulation at the time of finalizing this act. Op-ed's - The Bill restricts the processing of data outside Sri Lankan territory. In the case of public authorities (ministries, departments, corporations, including companies where the State holds more than 50% of shares), the processing cannot be done outside, other than for specific categories of data in countries classified as "adequate" by the Minister. This means that entities such as SriLankan Airlines, Litro Gas Lanka and possibly even Sri Lanka Cricket are precluded from using cloud-based services such as those offered by AWS and Google. They will be limited to the cloud services with storage in the few tier 3 data centres located in Sri Lanka, where the price-quality package is inferior to those offered by global providers.	**Accepted**

ASSESSMENT ON THE IMPACT OF COMMENTS - 9

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
29. (3) The Board shall consist of not less than five members and not more than seven members appointed by the President from among persons who have reached eminence and proven	S. 35(1)(a). Have boards with large numbers of ex-officio members (generally senior and short of time) worked? Isn't six too many? Having the Chief Accounting Officer of the Authority on the Board may create confusion.	**Not accepted**
	S. 35(1)(b). Application process suggests some degree of independence is envisaged. Is this level of complexity necessary for DPA? When six members are ex-officio, what is the point?	**Accepted**
32. The Authority may exercise the following powers, for the purpose of performing duties and discharging functions under this Act:– (e) to conduct inquiries, receive complaints, require any person to appear before it, make directives and impose fines in accordance with the provisions of this Act; (f) to examine a person under oath or affirmation and require such person where necessary to produce any information relating to the processing of functions of a controller or processor in the manner prescribed, for the purpose of discharging the functions of this Act; (g) to enter into the premises of any controller or processor and inspect or seize records and carry out investigations where the Authority has reasonable grounds to believe that processing poses an imminent risk to the rights of the data subjects;	S. 38. DPA appears to have quasi-judicial powers and can impose massive fines. Should adherence to natural justice not be specifically mentioned? Is there a case for appointment by the Constitutional Council? S. 40(1). Wrong incentives are created by allowing a quasi-judicial entity to use fines as revenue. Fines should go to Consolidated Fund.	**Not accepted**
32. (n) with the concurrence of the Minister assigned the subject of Finance, to pay such remuneration and other benefits and to establish provident funds or pension schemes as may be determined by the Authority for the benefit of its staff and officers, consultants or advisors with whom a contract of employment or service is entered into by the Authority as the case may be; (o) to invest its funds in such manner as the Authority may deem necessary; (p) to open, operate and close bank accounts; (q) to establish standards in relation to data protection and data storage, data processing, obtaining consent and such other matters as may be necessary for the proper implementation of the provisions of this Act; (r) to receive grants, gifts or donations whether from local or foreign sources: Provided however, the Authority shall obtain prior written approval of the Department of External Resources of the Ministry of the Minister to whom the subject of Finance is assigned, in respect of all foreign grants, gifts or donations;	S. 40(1). Fail to see logic of creating a separate Fund for an entity that is funded by annual appropriations.	**Patially accepted**

ASSESSMENT ON THE IMPACT OF COMMENTS - 10

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
38. (1) Where a controller or processor fails to comply with a directive issued under the provisions of section 35, the Authority shall after taking into consideration the impact on data subjects, the nature and extent of relevant non- compliances and the matters referred to in section 39 of this Act, by notice require such controller or processor to pay a penalty, which shall not exceed a sum of rupees ten million for each non-compliance.	Section 52 (3)- wide powers have been given to "supervisory, regulatory or self-regulatory authority of an *Institution*". There is no definition for "institution" under the Act. It is necessary that the same be defined for clarity. Section 52 (4) imposes personal liability on the Director, General Manager, Secretary of a body corporate. When companies have a separate legal entity, personal liability on its Director(s), or other officials is arbitrary, capricious and unjustifiable, especially since the penalty is calculated on the basis of the global turnover of the company (or LKR 25 Million, whichever is higher). We recommend 52 (4) (a) be deleted.	**Partially accepted**
38. (7) A controller or processor who is aggrieved by the imposition of an administrative penalty under this section, may appeal against such decision to the Court of Appeal within twenty-one working days, from the date of the notice of the imposition of such administrative penalty was communicated to such person.	Section 38 (3) states that all Orders issued by the DPA are binding. Whist we note the importance of a binding order, there is no provision for an appeal against this order. In the interest of justice and equity, we strongly recommend that an appeal provision against the order of the DPA be enshrined thereunder.	**Accepted**
[this section has been removed from the Act]	Section 49(1)(a) requires clarity. While the minister has been given powers make regulations in future, currently data portability is considered only in relation to automated decision making. Data portability should instead be considered more widely, not least for data subjects to request their data, including for the purposes of providing to another controller. This is an area that should be considered as a section within the main body of this Act rather than through subsequent legislation. It could be given as a right to data subjects under Section 10(2) of the proposed Act.	**Accepted**
"consent" means, any freely given, specific, informed and unambiguous indication by way of a written declaration or an affirmative action signifying a data subject's agreement to the processing of his personal data;	29. Consent has been defined stringently. "Deemed consent" has not been included within its ambit. It is suggested that deemed consent be included under the Act. Guidance for the inclusion of, and definition of deemed consent may be taken from Section 15 in Singapore's Personal Data Protection Act of 2012.	**Not accepted**
"data concerning health" means, personal data related to the physical or psychological health of a natural person, which includes any information that indicates his health situation or status;	Section 53. "Data concerning health" has been defined extraordinarily broadly. This would for example include data from fitbit. The inclusion of data on psychological health pretty much brings everything in.	**Not accepted**

ASSESSMENT ON THE IMPACT OF COMMENTS - 11

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
"data subject" means, an identified or identifiable natural person, alive or deceased, to whom the personal data relates;	30. There is ambiguity introduced because of the conflation in the definition to include both a natural person as commonly understood as well as to the information pertaining to said natural person. Given that 'personal data' has been defined separately, it is recommended that that the parts of the current definition of 'data subject' which relates to information about the data subject, be moved under the definition of 'personal data' as per Comment 31. As such we recommend 'data subject' be redefined simply as "*means an identified or identifiable natural person*."	**Accepted**
"Minister" means, the Minister assigned the subject of data protection under Article 44 or 45 of the Constitution;	Section 53. Best not to define the Minister in terms used from current portfolio assignments. In any case, why have the Minister in charge of digital be permanently in charge of data protection? Why not justice?	**Accepted**
"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.	31. The definition is exceedingly wide and has potential to include *all information*, even if such information may not be personally identifiable in nature. This provision is of paramount importance as the entire enactment hinges on the definition of personal data.	**Accepted**
"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 the controller; for the avoidance of doubt, a processor shall be a separate entity or person from the controller and not a person subject to any hierarchical control of the controller and excludes processing that is done internally such as one department processing for another, or an employee processing data on behalf of their employer;	33. The current definition is problematic since it excludes "a person subject to *any* hierarchical control of the Controller." This wording can give rise to varied interpretation by Controller and Processor, where each may try to shift liability under the Act on the other. Either hierarchical control should be further qualified or this should be removed.	**Not accepted**
"special categories of personal data" means, the personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, personal data relating to offences, criminal proceedings and convictions, or personal data relating to a child;	32. The definition includes its definition "personal data relating to offences, criminal proceedings and convictions." What constitutes "personal data relating to offences" requires further clarity since it is couched in wide terminology. Information on convictions (which are post trial) are a matter of public record and should be excluded from the purview of the section.	**Not accepted**

ASSESSMENT ON THE IMPACT OF COMMENTS - 12

Schedule in the Act	Related comment in written submissions and Op-Ed's	Level of impact
"written" includes a document written manually or electronically.	All references to "in writing" should be interpreted to mean including by electronic means." Otherwise, transaction costs will be excessive.	**Accepted**
[This schedule has been removed]	Condition (b) should not be the responsibility of the controller but rather the data subject since a controller should not be responsible for contracts that a data subject may undertake with outside parties.	**Accepted**

Of these written and Op-ed comments;

1. Nineteen comments have been accepted
2. Five comments have been partially accepted
3. Thirteen comments have not been accepted

LIRNEasia
Pro-poor. Pro-market.

2

Media coverage and reach

Op-Ed's on Print & Digital Media

- Op-Ed's authored by Rohan Samarajiva published on mainstream print and online media
- Over 3000 views to date

මහාචාර්ය රොහාන් සමරජීව

සාමාන්‍ය ජනතාවගේ ජීවිතවලට විශාල ලෙස බලපාන පෞද්ගලික දත්ත ආරක්ෂාව පිළිබඳ පනත කෙටුම්පත් කිරීමේ අවසාන අදියරේ පවතින බවත්, එය ඉදිරියේදී ඉදිරිපත් කරන බවත් මාධ්‍ය වාර්තා කර තිබුණි. මහාචාර්ය රොහාන් සමරජීව ශ්‍රී ලංකාවේ මෙන්ම ජාත්‍යන්තර මට්ටමෙන් පෞද්ගලික දත්ත ආරක්ෂාව පිළිබඳ විශෙ හැදෑරූ, ඒ ගැන

themorning.lk/is-the-data-protection-bill-right-for-sri-lanka/

Is the Data Protection Bill right for Sri Lanka?

DECEMBER 11, 2021 BY NEWS ADMIN 0 COMMENTS

By Prof. Rohan Samarajiva

Data protection is considered an esoteric subject, but it can have a powerful effect in the emerging digital economy. Depending on the success of digitisation efforts, pretty much every organisation may soon fall within the scope of data protection regulation.

The use of data, and insights extracted from data, predates computers. The difference is that a lot more can be done with data, and more easily, now that computers are involved. Hospitals and dispensaries have long maintained medical records of patients. But there is a big difference between records maintained in paper files and those in databases; copies can be made and transferred easily, analyses may be conducted rapidly to identify patterns and relationships, and medical records can be combined with data from other sources to gain even deeper insights. This

MENU

Daily FT Be Empowered

FT TV E-PAPER

Implications of data protection bill for individuals, businesses and innovation

Tuesday, 7 December 2021 00:02 - 649

MENU

THE WIRE English हिंदी मराठी اردو ABOUT US LOGIN

POLITICS ECONOMY EXTERNAL AFFAIRS SECURITY LAW SCIENCE SOCIETY CULTURE

ANALYSIS TECH

Lessons India Can Draw From Sri Lanka's Efforts With Data Protection Legislation

The best law is not one that is optimal in a technical sense, but one which is most appropriate for the local conditions.

Online Publication Details in Sinhala and English + Regional

	Title	Media	Language	Date published
1	Implications of data protection bill for individuals, businesses and innovation	Daily FT	English	7 Dec 2021
2	ලංකාවේ දත්ත ආරක්ෂා පනත කොහොමද?	Anidda	Sinhala	7 Dec 2021
3	An assessment of Sri Lanka's Personal Data Protection Bill	bdNews24.com	English	10 Dec 2021
4	Is the Data Protection Bill right for Sri Lanka?	The morning	English	11 Dec 2021
5	Personal Data Protection Bill: Another draconian law to suppress media freedom?	Daily Mirror	English	21 March 2022
6	Personal Data Protection Act passed: What will it mean?	Sri Lanka brief	English	22 March 2022
7	Personal Data Protection Act passed: What will it mean?	Daily FT	English	22 March 2022
8	සම්මත වූ පෞද්ගලික දත්ත ආරක්ෂණ පනතෙහි අර්ථය කුමක්ද?	Anidda	Sinhala	29 March 2022
9	Lessons India Can Draw From Sri Lanka's Efforts With Data Protection Legislation	The Wire	English	No date

ONLINE PUBLICATIONS' URL

Regional

- https://thewire.in/tech/lessons-india-can-draw-from-sri-lankas-efforts-with-data-protection-legislation
- https://bdnews24.com/opinion/comment/an-assessment-of-sri-lankas-personal-data-protection-bill

Local

- https://srilankabrief.org/personal-data-protection-act-passed-what-will-it-mean-prof-rohan-samarajiva/
- https://www.themorning.lk/is-the-data-protection-bill-right-for-sri-lanka/
- https://www.ft.lk/columns/Personal-Data-Protection-Act-passed-What-will-it-mean/4-732307
- https://www.dailymirror.lk/print/news-features/Personal-Data-Protection-Bill-Another-draconian-law-to-suppress-media-freedom/131-233442
- https://www.advocata.org/sinhala-archives/2020/02/19-xldf-oa-wdrlaid-mk-fldfyduo
- https://www.anidda.lk/2022/03/29/%e0%b7%83%e0%b6%b8%e0%b7%8a%e0%b6%b8%e0%b6%ad-%e0%b7%80%e0%b7%96-%e0%b6%b4%e0%b7%9e%e0%b6%af%e0%b7%8a%e0%b6%9c%e0%b6%bd%e0%b7%92%e0%b6%9a-%e0%b6%af%e0%b6%ad%e0%b7%8a%e0%b6%ad-%e0%b6%86%e0%b6%bb/
- https://www.anidda.lk/2020/12/07/%e0%b6%bd%e0%b6%82%e0%b6%9a%e0%b7%8f%e0%b7%80%e0%b7%9a-%e0%b6%af%e0%b6%ad%e0%b7%8a%e0%b6%ad-%e0%b6%86%e0%b6%bb%e0%b6%9a%e0%b7%8a%e0%b7%82%e0%b7%8f-%e0%b6%b4%e0%b6%b1%e0%b6%ad-%e0%b6%9a%e0%b7%9c/#
- https://www.ft.lk/columns/Implications-of-data-protection-bill-for-individuals-businesses-and-innovation/4-727069

On LIRNEasia website

- https://lirneasia.net/2022/03/personal-data-protection-act-passed-what-will-it-mean/
- https://lirneasia.net/wp-content/uploads/2019/07/LIRNEasia-comments-on-framework-for-a-proposed-data-protection-legislation-for-SriLanka-1July2019.pdf

LIRNEasia
Pro-poor. Pro-market.

Back to slide # 2

Annex

Written comments submitted on Data Protection Bill

LIRNEasia
Pro-poor. Pro-market.

Written comments on Data Protection Bill

Note: Double click on the document below to see full text (use 'normal view' not 'slide show')

Comments on Data Protection Bill
16th of June 2019

It is obvious that data protection legislation is extremely important in the 21st Century. Therefore, it is necessary to anchor the legislation on the overall strategic direction of the country and the role likely to be played by personal data in the desired trajectory. Disregarding these larger objectives in the formulation of legislation is not an option.

If we see the future of our country as resting on processing European data in the context of the current business process management/outsourcing (BPO/BPM) model, it would make sense to make synchronization with European data protection standards (GDPR) the highest priority.

If on the other hand, we see our future as being defined by activities centered on data analytics and artificial intelligence (AI), building on our strengths in software, we would ensure that the law allows for the use of appropriate, massive data sets with the necessary safeguards. This is what is necessary to achieve the government's Vision 2025 that seeks to make us a knowledge-based, highly competitive, social-market economy that capitalizes on our location in the Indian Ocean.[1] This is a forward-looking vision, unlike the backward-looking approach focused on BPO/BPM.

If we make an assessment that many widely available and useful apps such as Google Maps and Amazon or Netflix search recommendations are of value to our citizens, we would ensure that the legislation has the necessary exemptions and would not create conditions wherein a global online service company has to seriously consider withholding certain services from Sri Lanka.[2] It is unlikely that a company like Google will subject itself to the authority of the DPA just for the sake of offering such services in Sri Lanka. This is a realistic approach.

If the future we envision for Sri Lanka is that of an "experiment nation" as set out in the government's 2030 Vision, we will capitalize on the country's size, diversity and openness to new ideas to create a vibrant innovation eco-system where invention and scaling by local as well as foreign innovators will be encouraged. This will be achieved by fostering an environment wherein user acceptance of product and process innovations can be systematically assessed using modalities such as sample surveys, data analytics, qualitative research and A/B testing conveniently, quickly, and at low cost.[3] To realize this vision, it would have to be possible for companies, both domestic and foreign, to conduct market trials and associated research here. This would require, at minimum, a less restrictive approach to data localization which would be necessary to realize the full potential of cloud computing. The data

[1] *V2025: A country enriched.* http://www.pmoffice.gov.lk/download/press/D00000000061_EN.pdf
[2] Samarajiva, R. (2019). A national strategy for artificial intelligence? *Daily FT*. http://www.ft.lk/columns/A-national-strategy-for-artificial-intelligence-/4-676192. For a more in-depth discussion of the need for large data sets for AI, see Lee, Kai Fu (2018). *AI Superpowers: China, Silicon Valley, and the New World Order*. Boston: Houghton Mifflin Harcourt.
[3] See Presidential Expert Committee (2019). *Sustainable Sri Lanka: 2030 Vision and Strategic Path*, pp. 221-229. http://www.presidentsoffice.gov.lk/wp-content/uploads/2019/05/Final-v2.4-Typeset-MM-v12F-Cov3.pdf

The Secretary
Ministry of Digital Infrastructure and Information Technology
No 437, Galle Road
Colombo 03

1 July 2019

Dear Madam/Sir,

LIRNE*asia*'s Response to Ministry of Digital Infrastructure and Information Technology's Invitation for Comments on the Framework for a Proposed Data Protection Legislation

LIRNE*asia* welcomes the opportunity to submit our views and comments on the proposed Framework for a Proposed Data Protection Legislation.

LIRNE*asia* is a pro-poor, pro-market think tank whose mission is catalyzing policy change through research to improve people's lives in the emerging Asia Pacific. LIRNE*asia* has been active in Sri Lanka and the rest of the Asia-Pacific region since 2005, conducting both demand- and supply-side research as well as advocating for policy changes in the ICT sector on issues ranging from universal service policy to open data, gender, big data and more.

Our response is attached for your kind consideration. These have also been uploaded to our website and is available from https://lirneasia.net/2019/07/comments-on-the-framework-for-a-proposed-data-protection-legislation-for-sri-lanka/.

For questions regarding this submission, please contact Sriganesh Lokanathan, Team Lead, Big Data, LIRNE*asia* at sriganesh@lirneasia.net or +94-11-2671160.

Thank you.

Yours truly,

Helani Galpaya
Chief Executive Officer
helani@lirneasia.net

cc: (1) Mr. Jayantha Fernando, Director & Legal Advisor, ICTA
(2) Mr. Gamini Wanasekera, Advisor to the Hon. Minister, MDIIT

Comments on Data Protection Bill
5th of Oct. 2019

I greatly appreciate the significant improvements made to the draft of the framework document in response to comments and suggestions. This is a much improved text that is more suited to our conditions.

It is unfortunate that the entire design is anchored on the obsolete concept of consent (see paras 11 and 12). I understand that it will be difficult to back away from consent at this point, especially because of the need for GDPR consistency. However, it is worth placing on record the objections.

The removal of the registration requirement addresses many of the concerns I raised in my previous comments and I commend your courage in deviating from European orthodoxy on that. However, this appears to have also knocked out the funding section, so now I cannot figure out how the DPA will be funded. Consolidated Fund is fine (and is possibly the best option), but I think it's best to be explicit.

1.0 Section 2(b): "any data, which has been irreversibly anonymized in such a manner that causes the individual to be unidentifiable."
- 1.1 S. 10 mentions pseudonymization in addition to anonymization, indicating the former is not included within the s. 2(b) exception.
- 1.2 Even the GDPR permits pseudonymization.[1] The requirement of irreversible anonymization is far too strict and will cripple research. It is necessary to understand that there are no absolutes. What would be good is if acceptable/safe pseudonymization and anonymization is left to be determined by a working group of data scientists, rather than lawyers or judges because technologies of de-identification and re-identification will be constantly changing (almost an "arms race").[2]

2.0 Section 4(1): "It shall be lawful for a public authority to carry out the processing of personal data in accordance with its governing legal framework in so far as such frame work is not inconsistent with the provisions of this Act."
- 2.1 Why limit to public authorities? Unclear. But section 3 brings in entities that are not public authorities.

3.0 Section 4(2): "In the event of any inconsistency between the provisions of this Act and the provisions of any other written law, the provisions of this Act shall prevail."

[1] : https://gdpr.report/news/2017/09/28/data-masking-anonymization-pseudonymization/
[2] Samarajiva, R.; Lokanathan, L. (2016). Using Behavioral Big Data for Public Purposes: Exploring Frontier Issues of an Emerging Policy Arena, p. 26 onward. https://www.semanticscholar.org/paper/Using-Behavioral-Big-Data-for-Public-Purposes%3A-of-Samarajiva-Lokanathan/b63d438d9de7d0f495cdf2db41cc4c5484b6c857

LIRNEasia
Pro-poor. Pro-market.