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

LIRNEasia's comments on framework for the proposed Personal Data Protection Bill

This submission is in response to Ministry of Digital Infrastructure and Information Technology's invitation to comment on the framework of the proposed Personal Data Protection Bill, uploaded on its website on 14th June 2019 (subsequently updated during the week of 17th June).

Our submission is divided into two parts. Part I provides comments on the overall thrust of the proposed bills and outlines some key areas of concern. Part II provides comments on sections of the proposed bill following the template structure provided by the Ministry.

Part I: Overall comments and concerns

1. It is commendable that the Ministry has chosen to address a key legislative deficit in the important area of data protection in Sri Lanka. A framework for data protection and its use is important not least because of the increasing momentum in the use of data for new services and products, not just in specific sectors, but also across sectors and across jurisdictions.
2. Given the rising importance of data to the economy, and the Government's Vision 2025 that seeks to make Sri Lanka a highly competitive, knowledge-based, social-market economy,[1] it is imperative that a comprehensive Data Protection Act (DPA) seeks to protect the rights of data subjects while also facilitating the greater use of data in a responsible manner. **The overall approach of this proposed act, however, seems to be heavily influenced by the European General Data Protection Regulation (GDPR) enforced in 2018, and in fact goes further in some instances in limiting the use of data**. While accounting for the importance of data protection, it is prudent to ask if GDPR represents the right aspirational goal for Sri Lanka's data protection framework.
    a. GDPR is the most stringent of extant data protection regimes around the world, and while compliance to it would in theory make it easier for Sri Lankan businesses to cater to the European market, it is highly questionable if these will in fact bring about the economy-wide benefits to Sri Lanka that Vision 2025 aims. A careful consideration of different international regimes, like what was done by LIRNE*asia* and ICTA in developing a discussion document on Healthcare Data Protection[2], would have been useful to better understand potential alternatives that could facilitate data protection whilst also enhancing its responsible use. **A potential middle ground is to consider Singapore's data protection model**.[3]
    b. Recent work (which was also considered during United State's Federal Trade Commission (FTC) hearings on Competition and Consumer Protection in November 2018), has shown that after the adoption of the GDPR, overall technology investment flowing to the European Union (EU) had decreased: 26.1% reduction in the number of

[1] *V2025: A country enriched*. http://www.pmoffice.gov.lk/download/press/D00000000061_EN.pdf
[2] https://lirneasia.net/2019/06/healthcare-data-protection-in-sri-lanka/
[3] https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview

monthly venture deals and a 33.8% decrease in the amount raised in an average deal.[4] Given the arduous compliance obligations set forth by GDPR and the proposed Sri Lanka bill, any potential benefits from increased ease of doing business with EU countries, would only flow to big Sri Lanka companies/conglomerates with large budgets; similarly so for the local Sri Lankan economy but that would also require high compliance costs. If we are to bring about the Government's desire for a highly competitive, knowledge-based, social-market economy then it is imperative that data protection legislation also enable data flows that can spur innovation, albeit with sufficient privacy protections. **Should the proposed legislation as currently drafted, be adopted, it is likely to stymie the local knowledge-based economy with reduced innovation, capitalization, and competitiveness in the short- to medium term. In particular we expect that the legislation in its current form would severely impact the cost of doing business for Small and Medium Enterprises (SMEs).**

3. **While we strongly think that the GDPR is the wrong aspiration model for Sri Lanka, given that the Ministry has chosen to go that route, our comments on the specific text of the draft Act attempts, to the extent possible, to provide suggestions within the existing framework so as to protect the rights of data subjects while also facilitating the greater use of data in a responsible manner.** Some of our main recommendations in this regard include,
    a. Tighten the definition of personal data (see Comment 31 in Part II) so as not to be exceedingly wide;
    b. Allow leeway when processing pseudonymized data (see Comment 3 in Part II);
    c. Reducing burdens in relation to Automated Individual Decision Making, whilst also enabling the right of 'data subjects' to ask for explanations (see Comment 12 and Comment 13 in Part II);
    d. The draft act in its current form leaves for a later date important guidelines and regulations, in some instances using language which suggests wide latitude and discretion. Specifically, in the following instances, this is strongly discouraged and should be addressed at the same time as this legislation, and NOT at an undetermined later date:
        i. Regulations in relation to automated Individual decision making (Section 14(2)). Please see our guidance in Comment 13 in Part II of this document in relation to Section 14.
        ii. An initial list of countries/territories under Section 30 so that controllers located in these countries can be exempt from authorizations from the Sri Lanka DPA. Please see our guidance in Comment 24 in Part II of this document in relation to Section 30.
        iii. Conditions for data portability. Please see our guidance in Comment 26 in Part II of this document in relation to Section 49.

[4] The Short-Run Effects of GDPR on Technology Venture Investment. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3278912

Part II: Comments on specific bill provisions

Provisions	Comment
Section 01: Application	1. 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. 2. Part (4) of Section 1 clearly stipulates that sections under this Act would be in addition to those under other written laws. However, it does not specifically address which law would prevail if there is a conflict between the other written laws and the Data Protection Act. Applying the general rule of statutory interpretation "generalia specialibus non derogant" i.e. general statutes should yield to a special one, it is recommended that the Act specifically states that if other laws require complying with certain conditions (for example record keeping requirements), they shall prevail over this Act or similar terminology to highlight that specific statutes would not be overridden. Furthermore, the Act should also address how conflict between two general statutes (for example the Right to Information and the Data Protection Act) be resolved (also see comment 36 under Schedule 1)
Section 02: Lawfulness in Processing	3. 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. Please see Comment 35 under Schedule 1 below for further discussion.
Section 03: Purpose Limitation	4. 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
Section 04: Data Minimisation	
Section 05: Accuracy	
Section 06: Storage Limitation	5. Please refer to comments under Section 3 ("Purpose Limitation") to rectify the wording in relation to archiving as per our suggestions. 6. 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*."
Section 07: Integrity and Confidentiality	
Section 08:	
Section 9: Right to Withdraw Consent	7. 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. Additionally, there is a typographical error whereby reference to section 10 (1) has been made instead of 11 (1).
Section 10: Right of Access by the Data Subject	8. In Section 10(2), the data subject should also be given access to their personal data in a structured, commonly used, and machine-readable format. Please also refer to Comment 26 below under Section 49 in relation to data portability.
Section 11: Data Subject's Rights to Rectification	
Section 12: Right to Erasure	9. 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.

	10. It is also suggested that the words *"or"* be added after each of the conditions. It is found after 12 (1) (c) but not after sub sections (a), (b) and (d) 11. There are several spelling and typographical errors that need to be corrected.
Section 13: Exercise of Rights under Sections 9, 10, 11 & 12	
Section 14: Automated Individual Decision Making	12. While commendable in paying attention to individual rights in relation to automated individual decision making, this proposed Act goes even further than the GDPR and allows it only in the instances where it is authorized by law. The GDPR however also provides for one additional permissible instance, which is when it "is necessary for entering into, or performance of, a contract between the data subject and a data controller" (see Article 22(2)(a) of the GDPR). A similar allowance is recommended for the proposed Act. 13. 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).
Section 15: Exercise of Rights through the DPA	
Section 16: Registration of Controllers and Processors	14. 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.
Section 17: Application for Registration	15. See comment 14 under Section 16 above.
Section 18: Exemption from Registration & Registration fee	
Section 19: Duration of the Registration Certificate	16. See comment 14 under Section 16 above.

	17. A 1-year validity is too short. Furthermore the renewal process should be clearly prescribed, rather than left open to be taken care of by future guidelines.
Section 20: Register of Controllers	
Section 21: Cancellation or Variation of Certificate	
Section 22: Designation of the Data Protection Officer	18. 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. 19. 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. If, however, the above-mentioned definition on "large scale" is incorporated (see Comment 18 above), this requirement of an employee being a DPO may be implemented without much inconvenience. 20. 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.
Section 23: Duties and Obligations of the Controller	21. 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*."
Section 24: Duties and Obligations of Processor	

Section 25: Data Breach Notifications	
Section 26: Data Protection Impact Assessments	22. 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." 23. 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".
Section 27: Prior Consultation	
Part V - Exceptions Section 28:	
Part VI - Cross Border Flow of Personal Data Section 29:	
Section 30:	24. 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.
Section 31:	
Section 32:	
Section 33:	
Part VII - Data Protection Authority Section 34: Establishment of the Data Protection Authority	
Section 35: Constitution of the Authority	
Section 36: Employees of the Authority	
Section 37: Powers of the Authority	
Section 38: Orders by the Authority	25. 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.
Section 39: Duties and Functions of the Authority	
Section 40: Funds of the Authority	
Section 41: Financial Year and Audit of Accounts	
Section 42: Part II of the Finance Act, 38 of 1971 to apply	
Section 43: Members etc, of the DPA deemed to be Public Servants	
Section 44: Application of the Bribery Act	
Section 45: Expenses incurred in any suit of prosecution	
Section 46: Procedural Requirements to be Published	
Section 47: Delegation of Powers of the Authority	
Part VIII - Direct Marketing Section 48: Use of Personal Data on Direct Marketing	
Part IX - General Section 49: Rules & Regulations	26. 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. Since this Act mimics the GDPR to a large extent, guidance may be taken from Article 20 of the GDPR which also mandates that it be provided in a structured, commonly used and machine-readable format. It would also be worth studying Singapore's recently released discussion paper on data portability available at https://www.pdpc.gov.sg/-/media/Files/PDPC/PDF-

	Files/Resource-for-Organisation/Data-Portability/PDPC-CCCS-Data-Portability-Discussion-Paper---250219.pdf
Section 50:	
Section 51:	
Section 52: Imposition of a Penalty by the Authority to Enforce Compliance	27. 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. 28. 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.
Section 53: Definitions	
"Anonymize"	
"Biometric data"	
"Child"	
"Consent"	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.
"Data concerning health"	
"Data Protection Officer"	
"Data subject"	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*."
"Encryption"	
"Financial data"	
"Genetic data"	
"Minister"	
"Personal data breach"	

"Personal data revealing racial of ethnic origin"	
"Personal data"	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. a. We draw your attention to the "Discussion paper on healthcare data protection policy for Sri Lanka" by LIRNEasia and ICTA available at https://lirneasia.net/2019/06/healthcare-data-protection-in-sri-lanka/. The section on Personal data in said discussion document (paragraphs 25 & 26) tabulates the various "personal data" definitions adopted across jurisdictions. For example, the Draft Data Protection Act (India) defines it as follows: "*Personal data means data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.*" b. Similarly, not all information about an individual is personal data (see paragraphs 27 to 29 in the discussion paper on healthcare data protection for Sri Lanka that has been linked above). Whether an individual is identifiable or not is a question of context and circumstance. For instance, a car registration number, by itself, does not reveal the identity of a person. However, it is possible that with other information, an individual can be identified from this information. c. It is strongly recommended that a more precise, unambiguous and strictly worded definition be incorporated. Specifically, we recommend limiting the definition to an identified or identifiable data subject here rather than in the definition of a 'data subject' (Comment 30). We recommend the following definition be used for personal data, incorporating wording currently used to define a data subject in this draft Act: *"means any data pertaining to a data subject who can be identified, directly or indirectly, in particular by reference to an identifier including but not limited to a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person;"*
"Profiling"	
"Pseudonymisation"	
"Public authority"	

"Recipient"	
"Special categories of data"	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.
"Controller"	
"Cross-Border flows of Personal Data"	
"Data Protection Authority (DPA)"	
"Processing"	
"Processor"	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.
"Sri Lanka"	
Schedule 1	34. 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. 35. 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. 36. Article 85 to 91 of the GDPR deal with provisions relating to specific processing situations, some of which this proposed Act should also be mindful of, and which we suggest should be addressed immediately. Specifically Article 85 of the GDPR, which deals with processing and freedom of expression and information is particular relevant in the Sri Lankan context. As such we highly recommend that exceptions be provided for processing that is carried out "for journalistic purposes or the purpose of academic artistic or literary expression." (see Article 85(2) of the GDPR).

Schedule 2	37. Provision (h) wording is vague. Please refer to comments under Section 3 (“Purpose Limitation”) to rectify the wording in relation to archiving as per our suggestions.
Schedule 3	
Schedule 4	
Schedule 5	