UNSW Law & Justice Research Series

Sri Lanka's Personal Data Protection Act Is Finalised With a Stronger DPA

Graham Greenleaf

[2022] *UNSWLRS* 53
(2022) 177 *Privacy Laws & Business International Report* 25-27.

UNSW Law & Justice
UNSW Sydney NSW 2052 Australia

E: LAW-Research@unsw.edu.au
W: http://www.law.unsw.edu.au/research/faculty-publications
AustLII: http://www.austlii.edu.au/au/journals/UNSWLRS/
SSRN: http://www.ssrn.com/link/UNSW-LEG.html

Sri Lanka's Personal Data Protection Act is finalised with a stronger DPA

Graham Greenleaf, Professor of Law & Information Systems, UNSW Sydney

(2022) 177 *Privacy Laws & Business International Report* 25-27

Sri Lanka's Personal Data Protection Act, No. 9 of 2022, was adopted ('certified') on 19 March 2022, with final amendments passed without a vote.[1] The Act's provisions will come into force between 18 and 36 months from that certification date, on a date to be gazetted by the Minister. The Minister must also gazette a date no later than this, from which the provisions concerning the data protection authority will be operational (s. 1).

Successive versions of a draft have been available for comment from the government since early 2019, and the changes between versions have been substantial. Sri Lanka thus becomes the first South Asian country to enact a comprehensive data privacy law, ahead of Bills still under consideration in India[2] and Pakistan.[3] This article concentrates on those aspects of the previous Bills that have been criticised,[4] asking whether the Act has addressed the issues raised.

An independent Data Protection Authority?

A major criticism was that, while the Bills did provide for the functions of a Data Protection Authority of Sri Lanka (DPASL), they did not include provisions creating such a body, but instead provided that the government would designate some existing public body to carry out that role.

The Act has finally abandoned that approach and establishes the DPASL (the 'Authority') (s. 28). A Board of Directors will exercise all powers and functions of Authority (s. 29). The President of Sri Lanka is to appoint between 5 to 7 members to the Authority 'who have reached eminence and proven professional expertise' in a number of specified fields. 'At least two members shall have prior experience in the public sector entities'. The persons appointed to the Board shall also have experience and knowledge in regulatory matters, privacy and data protection, information security, data science, data analytics, economics, finance,

---

[1] Personal Data Protection Act, No. 9 of 2022 <https://www.parliament.lk/uploads/acts/gbills/english/6242.pdf>

[2] G. Greenleaf 'Parliamentary Report Keeps India's DP Bill Partly within GDPR Orbit' (2022) 175 *Privacy Laws & Business International Report* 1, 6-9.

[3] G. Greenleaf 'Pakistan and Sri Lanka's Data Privacy Bills Move Forward' (2021) 173 *Privacy Laws & Business International Report* 24-27.

[4] ibid

information technology or related fields' (s. 29(4)). So 'eminence' must be combined with 'experience and knowledge' in relevant fields. The President is also to appoint one member as Chairperson (s. 30).

There is no provision in the Act allowing the government to give directions to the Authority, but on the other hand there is no explicit guarantee that its members must act independently. Other indicia of independence are rather scant in the Act. The extent of the Board's independence will therefore have to be judged by its actions once its members are appointed.

A Director-General will be appointed by the Board as CEO of the Authority (s. 36) but will not be a member of the Board. Eminence and professional expertise in providing leadership are required, and grounds for removal are specified.

The 'objects' of the Authority are broadly specified (s. 31), but more significant is the detailed specification of the powers (s. 32), duties and functions (s. 33) of the Authority, in over 30 sub-clauses. It has ample authority to issue directions relating to compliance with the Act, and to make rules concerning matters such as sharing of personal data between public authorities (s. 33(n)), and 'make rules in relation to the use of special categories of personal data, the use of personal data for the dissemination of solicited messages, in compliance with section 27, the use of personal data for profiling of individuals, the use of personal data for automated decision making (s. 33(p)). The result is that there are many substantive obligations or rights arising under other provisions of the Act, where it will be necessary to also check whether the Authority has made any rules on the topic.

The Board's rule-making powers are constrained by the requirements that any such rules must be the subject of public consultations for at least two weeks, must be approved by the Minister, and must be 'brought before Parliament for approval' within three months of being gazetted (s. 52(3) - (6)).

The Minister also has extensive regulation-making power (s. 53), 'with the concurrence of the Authority'. Regulations may cover such matters as the inclusion of countries on data export 'white lists', and the categories of licences which may be required. Requirements of gazettal and Parliamentary approval are the same as for rules made by the Authority.

Some stronger enforcement

There has been some strengthening of the enforcement aspects of the Act, previously criticised as weak and ambiguous. Data subjects can appeal to the Authority if a controller is alleged not to have complied with any of their rights under sections 14-18, with the controller then required to 'take steps to give effect to the decision of the Authority' (s. 19(4)), but with no penalties or compensation provided. There is a further right of appeal by either party against the Authority's decision to the Court of Appeal (s. 19).

In relation to other breaches of the Act, it seems that data subjects cannot be a party to an action to force compliance by controllers or processors, but they can make a complaint, on which the Authority may choose to conduct an enquiry (s. 35(1)). As a result of such enquiry the Authority may issue a directive to the controller or processor requiring cessation of acts in breach of the Act, or performance of necessary rectifying acts (s. 35(2)). In addition, the Authority may require to make a payment of compensation 'as determined by the Authority

to an aggrieved person who has suffered harm, loss or damage as a result of any contravention' (s. 35(2)(c)). There is no explicit right of appeal to the courts, either by controllers or data subjects. This power to award compensation, with no monetary limit stated, is an unusual and potentially substantial sanction. It was not found in previous versions of the Bill. There is no obvious reason why these procedures cannot be used by data subjects to attempt to obtain compensation for breaches of their rights under sections 14-18.

The failure of a controller or processor to comply with a directive under section 35 is a necessary pre-condition for the Authority to require payment of a penalty, to a maximum of 10 million rupees (less than US$30,000, due to the current decline in the exchange rate of the rupee) (s. 38(1)). The Authority must consider 'the impact on data subjects, the nature and extent of relevant non-compliances and the matters referred to in section 39' (s. 38(1)). The factors set out in section 39 are similar to some of the factors set out in GDPR article 83(2). Where a penalty is imposed for a second occasion because a controller or processor has failed to comply with a directive, the penalty will be doubled (s. 38(3)). Individuals who are directors or managers of companies, or partners of firms, against which penalties are issued will be individually liable to pay those penalties unless 'he proves that he had no knowledge of the failure to comply with the [directive] or that he exercised all due care and diligence to ensure the compliance therewith' (s. 38(6)).

None of these enforcement measures are individually at the strong end of the scale, but they do make up a useful combination of compliance orders, open-ended compensation payments, and modest financial penalties which will at least encourage compliance by local businesses, if not by multinational companies.

Extra-territorial scope

Multinational companies, and particularly 'platforms' such as Google and Facebook which can monitor the interaction of data subjects with many other companies, will be within scope of the law, because of extra-territorial provisions (s. 2(b)(iii) and (iv)) which are similar to GDPR article 3(2), but not identical. They apply to 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 behaviour of such data subjects in so far as such behaviour takes place in Sri Lanka."

Clause (iii) may be broader than the GDPR, because, on a literal reading, it is sufficient if the external entity 'offers goods or services to data subjects in Sri Lanka', whether or not there is 'specific targeting'. Clause (iv) appears to be of the same scope as the GDPR, because it is satisfied wherever the external party 'specifically monitors the behaviour of data subjects in Sri Lanka', with any intention of making decisions not being required. However, if a Sri Lankan court interprets 'includes' as imposing a necessary condition, the outcome will be different.

Data exports and localisation

The final version of the Act has only minor changes concerning data exports and data localisation.[5]

Private sector bodies may process personal data outside Sri Lanka in three situations:

(i) The processing is in a third country prescribed in an 'adequacy decision' (s. 26(3)(a)) made by the Minister in consultation with the Authority who are to 'take into consideration the relevant written law and enforcement mechanisms' in the third country, specified parts and sections of the Act, and 'such other prescribed criteria' as may exist (s. 26(2)(a)). Adequacy decisions must be reviewed by the Minister at least every two years and remain in force until amended or revoked (in consultation with the Authority) (s. 26(2)(b)).

(ii) The processing is in a third country not prescribed in an adequacy decision, but the controller or processor ensures compliance with specified Parts and sections of the Act (s. 26(3)(b)), and adopts instruments specified by the Authority to ensure enforceable commitments by the recipient of the data, and appropriate safeguards and remedies (s. 26(4)). These may be equivalent to the EU's Standard Contractual Clauses.

(iii) In the absence of (i) or (ii), other bases for exports are allowed, similar to the 'derogations for specific situations' allowed in the GDPR, article 49, covering such matters as explicit consent with notice; contractual requirements; legal claims; public interest and emergencies (s. 26(5)). Exports are also allowed 'under any other conditions as may be prescribed under this Act', an open-ended exception not provided in the GDPR.

The position is very different where the controller or processor is a public authority, where the only exception allowing overseas processing is where the Authority, 'in consultation with … 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' (s. 26(1)). The default position is therefore that public authorities cannot process personal data overseas. How these provisions are interpreted will determine how strict the data localisation of public sector data will be in Sri Lanka.

Conclusions

Many other smaller changes could be noted in the finalised Act, but these are probably the major areas of the law of most interest to foreign businesses. Overall, the Act is a rather strong implementation of GDPR-influenced principles. It includes requirements on controllers to only process personal data for specified, explicit and legitimate purposes, and not to further process them in a manner incompatible with such purposes (s. 6(1)). Other equally generally stated obligations on processors follow, covering matters that the GDPR deals with in more specific terms. Controllers and processors are also required to implement internal controls and procedures, referred to as the 'Data Protection Management Programme' and performing a function similar to 'demonstrable accountability' in GDPR terms (s. 12). As

[5] For more details, see Greenleaf 'Pakistan and Sri Lanka's Data Privacy Bills Move Forward'.

in the GDPR, in some situations a Data Protection Officer must be appointed, and in others a data protection impact assessment is required (s. 24). There are some specific obligations on processors (s. 22).

The rights of data subjects include the right to withdraw consent to processing, and a very limited right 'to request a controller to review a decision of such controller based solely on automated processing'. An unusual right is that of 'an heir to exercise a deceased data subject's rights within a period of ten years from the date of demise of such data subject' (s. 17(5)(d)). Data subjects may appeal to the Court of Appeal if dissatisfied with how the Authority has enforced their rights.

This Act imposes many detailed obligations on controllers and processors, and will require care by controllers and processors, both local and foreign, to ensure compliance.