# ADVANCES IN SOUTH ASIAN DATA PRIVACY LAWS: SRI LANKA, PAKISTAN AND NEPAL

**GRAHAM GREENLEAF**

(2019) (162) International Report December, 22-25
[2020] *UNSWLRS* 52

UNSW Law
UNSW Sydney NSW 2052 Australia

# Advances in South Asian data privacy laws: Sri Lanka, Pakistan and Nepal

Graham Greenleaf, Professor of Law & Information Systems, UNSW Australia*

Published in (2019) *Privacy Laws & Business International Report*, 22-25

Five years ago, the only significant data privacy laws in South Asia (or SAARC, the South Asia Area of Regional Cooperation) were India's new and extremely limited private sector law, and Nepal's public sector law. The region's data privacy protections were far more limited than in North-east Asia or the ASEAN countries.[1] India continues to prevaricate, but is expected to introduce a modernising Bill in the 2019 winter Congress sessions. Meanwhile, in addition to the Sri Lankan Bill which is the focus of this article, Bhutan and Nepal have enacted privacy laws, and Pakistan has a private sector Bill. Bangladesh, Afghanistan and the Maldives continue to be the states in the SAARC region where there are no significant developments.

## Sri Lanka's GDPR-inspired Bill

What is said to be the final draft of Sri Lanka's *Personal Data Protection Bill*[2] was released on 24 September 2019 by the Ministry of Digital Infrastructure and Information Technology (MDIIT). The previous 'Data Protection Framework',[3] released in June 2019, has been modified after government consultations with stakeholders.[4] Once enacted, its various provisions must be brought into force within 3 years, or 18 months for the formation of the DPA (s. 1).

### Scope and exceptions

The Bill is comprehensive in that it covers both the public and private sectors (s. 3, s. 4). It appears to have extra-territorial effect in similar terms to the GDPR art. 3 (offers to or monitoring of persons in Sri Lanka: s. 3(1)(iv) and (v)), but is actually much more limited because it only applies where the processing of the data 'takes place wholly or partly within Sri Lanka' (s. 3(1)(a)).

Although the Bill reserves significant powers to make delegated legislation to the Data Protection Authority (DPA) (ss. 19(1)(B), 22(2), 28(q), 29(h), 31(1)(b) etc), the Minister of MDIIT (s. 25(2)), or the Secretary of MDIIT (ss. 31(6), 43(1), 43(2) etc), there are no outright exceptions to its provisions for either public or private sector entities. In addition, any 'exceptions, restrictions or derogations' to its provisions are not allowed unless provided by

* Thanks to Angela Potter for information concerning Nepal, and to various anonymous commenters concerning Sri Lanka. Responsibility for all content remains with the author.

[1] G. Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 435-6.

[2] Draft Personal Data Protection Blll (Sri Lanka) <http://www.mdiit.gov.lk/images/news/Data_Protection_bill/Data_Protection_Bill_3-10-2019_-_Amended_Draft_FINAL_-_LD_Release.pdf>

[3] Summary of Data Protection Framework (July 2019) <https://www.medianama.com/2019/07/223-summary-sri-lanka-personal-data-protection-bill/>

[4] For a summary of changes, see Aryan Babele 'Sri Lanka introduces final draft of Personal Data Protection Bill' Medianama 10 October 2019 <https://www.medianama.com/2019/10/223-sri-lanka-final-draft-of-data-protection-legislation/>

law and 'respects the essence of the fundamental rights and freedoms and constitutes a necessary and proportionate measure in a democratic society' for protection of various public interests (listed (a)-(f)) (s. 35). However, s. 35 does not specify the sources of legitimate 'exceptions, restrictions or derogations', creating the risk that it might authorise unspecified exceptions other than those legitimated by existing statutory provisions (in this Bill or other laws), so this needs to be clarified. The broad regulation-making powers in s. 43 are particularly dangerous unless it is clarified that such regulations may not derogate from the right and protection of data subjects in the Bill. This is particularly so when the 'fundamental rights and freedoms' referred to in s. 35 do not include privacy rights in Sri Lanka.

The Bill is also comprehensive in that it defines 'personal data' by a conventional definition in terms of identifiability, but over-inclusive in that 'data subject' includes persons 'alive or deceased' (definitions, s. 46) with no time limit based date of death. 'Special categories of personal data' are defined by an extensive list including genetic and biometric data (definitions, s. 46).

The only exceptions to the data covered are for the usual 'personal, domestic, or household' use exception, and for anonymous data ('irreversibly anonymized in such a manner that causes the individual to be unidentifiable') (s. 3(2)). The use of 'irreversibly' makes this a more strict standard of anonymisation than the GDPR, which allows 'all the means reasonably likely to be used' to re-identify data, taking into account current technology, to determine whether data has been anonymized (GDPR, recital 26), rather than imposing an absolute requirement which may be impossible to meet.

### Principles with strong GDPR influence

The Bill does require lawful grounds for processing to take place at all (s. 5). Schedules I, II and III set out many similar grounds to those in the GDPR (including for special/'sensitive' data). The ground of consent (Schedule 1(a)) makes it appear that blanket consent to processing (i.e. not only for a specified purpose) is allowed, but s. 6 requires processors to ensure that processing is only for 'specified' and 'explicit' purposes, and that further processing is not incompatible with such purposes. The Minister, with the concurrence of the DPA, may expand any of these Schedules, by disallowable regulations (s. 43).

### Obligations of controllers and processors

Among many aspects of the Bill reflecting the influence of the GDPR are the requirements on controllers of proportionality in processing (s. 7(c)); minimality of processing, but only in the very weak form of 'not excessive' (s. 7(d)); and limited retention (but the word 'only' is missing) (s. 9). There is no absolute obligation to provide an appropriate level of security, but only an obligation to follow *prescribed* security measures (s. 10), defined by the Minister or the DPA. Data breaches must be reported, and the DPA is to specify when such reports must be made to it, and to the data subject (s. 22).

The previous draft included mandatory registration of controllers, but in the latest draft this has been replaced with a version of demonstrable accountability (s. 12), described as a 'Data Protection Management Program', and including numerous elements. Controllers must appoint Data Protection Officers (DPOs) (s. 20(1)), where they are in the public sector, or in such private sector categories as the DPA decides requires a DPO, or processing involving monitoring, large scale special categories of data, or high risk processing is involved (s. 31). Private sector entities aggrieved by a DPA requirement to appoint a DPO may appeal to the Secretary of the Minister's department (s. 31(6)).

They must carry out a data protection impact assessment (DPIA) prior to carrying out any processing 'likely to result in a high risk to the rights and freedoms of a data subject as

guaranteed under any written law' (s. 23(1)). Sri Lanka's *Constitution* provides in Chapter III various 'Fundamental Rights' which could be relevant, but this would be infrequent, as they do not include a right of privacy, or a general protection of liberty (as in s. 21 of India's Constitution). The rights most likely to be relevant are the protections against numerous forms of discriminations (*Constitution*, art. 12(2) and (3)). Such DPIAs are required (and possibly *only* required) where processing involves large scale or systematic evaluation of personal data such as by profiling, monitoring of public spaces or telecommunications networks, special categories of personal data, or other circumstances prescribed by the DPA (s. 23(3)). The DPIA results must be given to the DPA irrespective of the outcome, for the purpose of the DPA assessing compliance with the law (s. 23(5)). If the DPIA indicates that processing will involve high risks despite any mitigation, the controller must consult with the DPA before proceeding (s. 24).

Unsolicited messages using personal data in any medium are prohibited, with prior consent, and a right to opt out, being required (s. 26).

Processors are required to only carry out processing on the instructions of a controller, and in accordance with the same obligations as controllers (or they will be deemed to be controllers), and must erase or return data after processing (s. 21).

### Rights of data subjects

The rights of data subjects (Part II) expressed in terms familiar from the GDPR include, in addition to the rights of access and correction, the right to withdraw consent to continued processing (s. 13); 'right to erasure' including the 'right to be forgotten' where data is 'no longer necessary' (s. 16). Where controllers refuse data subject requests they must (in this draft) inform them of their right of appeal. Appeals are initially to the DPA, and either the data subject or the controller may then appeal to the Court of Appeal (s. 18). There is no right of data portability.

The rights of the data subject to request a review of automated decision-making (s. 19) only apply if it 'affects rights and freedoms … guaranteed under any written law' (a condition not found in GDPR art. 22). Unless such rights can be inferred from this Bill, this condition means that these rights will very rarely apply to the private sector, in areas such as employment, insurance etc, unless some other statutory rights are likely to be infringed, or the abovementioned constitutional protections against discrimination are infringed. This uncertain scope makes it difficult to evaluate the rest of the section. The application of the section to 'special categories' (sensitive data) is also unclear.

### Data localisation and export restrictions

Public authorities may only process personal data within Sri Lanka, unless the DPA and any relevant supervisory body classifies the data as permitted to be processed overseas (s. 25(1)). There is no such data localisation requirement applying to the private sector.

Private sector bodies may transfer personal data to a third country (or territory/sector within it) prescribed by the Minister (s. 25(2)). Otherwise, they are only permitted to process personal data outside Sri Lanka if they ensure compliance with specified sections of the Act (s. 25(3)), through a legally binding and enforceable instrument with the recipient, or one determined by the DPA (s. 25(4)). Such instruments will only allow enforcement by the exporting data controller, not the data subject, because the common law doctrine of privity of contract applies in Sri Lanka (even though its contract law is largely based on Roman-Dutch law). It is not clear that the section covers both transfers to another controller overseas, as well as to a controller processing data outside Sri Lanka.

## A DPA without apparent independence

The Minister is empowered to 'designate a Public Corporation, Statutory Body or any other public institution controlled by the government or established by or under any written law, as the "Data Protection Authority of Sri Lanka" ' (the DPA) (s. 27(1)). While this section would not preclude the Minister from designating a statutory body with guaranteed independence as the DPA, or prevent such an independent body being established by separate legislation, it also clearly enables the Minister to so designate a body with no such independence as the DPA.

This apparently intended lack of independence is underlined by s. 41, which provides that the Minister may convey relevant directions by the Cabinet to the DPA 'in connection with the exercise, performance or discharge of its powers, duties and functions'. Furthermore, there are no provisions in the Bill indicating that the DPA is to exercise its powers independent of the views of the Minister or the government. In similar vein, responsibility for the Act and its implementation is given to both the DPA (s. 27(3)) and the relevant Ministry (s. 2). This contradiction needs to be resolved.

Appeals against decisions of the DPA generally go to the Court of Appeal (s. 18(4)). However, appeals against DPA decisions on whether a DPO must be appointed go to Secretary to the Minister (s. 31(6)), which could also be considered to reduce DPA independence.

## Broad enforcement powers, but financial risks limited

The DPA has broad powers of investigation (s. 28(b)-(d)), and powers to 'receive complaints, hold enquiries and to make determinations or orders (s. 28(f)). It can direct controllers or processors to comply with their obligations (s. 28(c)), including by issuing both negative and positive 'directives' (injunctions) (s. 30(1)), enforceable by court orders if necessary (s. 30(4)).

The DPA may suspend a controller 'from the carrying on of a business or profession or the cancellation of a licence or authority' for such purposes, to the extent the law allows (s. 32(5)). It remains to be seen whether this sanction will be used. The DPA is not explicitly empowered to take the more direct approach of ordering suspension of particular forms of processing, but that could be implied by its injunctive powers.

The DPA also has powers 'to establish standards in relation to data protection' (s. 28(q)) (except in relation to what constitutes 'adequacy' for data exports: s 25(1)). It can enter into agreements with foreign states (s. 28(l)), and 'recognize certification and certifying bodies' (s. 28(k)).

The Bill empowers the DPA to levy maximum fines for breach of 10 million rupees (US$55,000), to be doubled on subsequent breaches (s. 32). Factors to be taken into account are set out (s. 33), somewhat similar to GDPR art. 83(2). This is a considerable reduction from the previous draft, which included fines up to 2% of global turnover of companies in breach, or 25 million rupees (US$122,500), whichever is the larger. The two other GDPR-influenced laws in Asia vary on this point, with Korea having fines with maxima based on global turnover (like the GDPR, and with one example reaching US$5,400,000), but Thailand having a maximum fine equivalent to only US$160,000. Singapore already has maximum fines of S$1 million (US$730,000), and has levied one fine approaching that. Fines in the new Sri Lankan Bill therefore have relatively little bite.

The Bill does not include other common means of enforcement: there are no provisions for compensation to aggrieved data subjects (comparing adversely with GDPR art. 82, or the laws of Korea, Singapore or Hong Kong); nor are suitably qualified NGOs given the ability to take

representative actions on behalf of data subjects (comparing adversely with GDPR art. 80, and laws in Korea, Thailand and elsewhere), except to exercise user rights if authorised in writing (s. 17(6)(c)).

### Comparative analysis

To put the Sri Lankan Bill in perspective, it is useful to compare it with other data privacy laws in Asia, and to consider what prospects, if enacted, it might have to assist Sri Lanka to obtain a finding of 'adequacy', or for it to accede to data protection Convention 108+.

If enacted, this would be the second 'post-GDPR' law in Asia, following Thailand, but it is (as yet) not as strong an implementation as that law. With Korea's law, it would be one of the three strongest data privacy laws in Asia, at least until India or Indonesia enact their proposed Bills.

#### Adequate in GDPR terms?

Whether Sri Lanka would wish to seek a finding of adequacy under the GDPR is not known. If it did so, the independence of the DPA would be the most obvious impediment. The ability of the Minister to allow data exports to selected countries would need to be restricted. Following Japan's adequacy assessment, it is not clear what other aspects of the GDPR are necessary in a third country's law.

#### Potential for Convention 108 accession

It is not known whether Sri Lanka wishes to accede to Convention 108+. If it does, the Convention requires acceding countries to meet all its substantive provisions (art. 4), which is not the case with 'adequacy' under the GDPR. Rights included in Convention 108+ which are not fully addressed in the Bill include the right to know the reasons underlying processing applied to the data subject (art. 9(1)(c)), including because of deficiencies in s. 19; and the right to object (art. 9(1)(d)), because s. 13(2) is too limited.

An unusual function of the DPA is to 'ensure domestic compliance of data protection obligations under international conventions' (s. 19(h)). The recitals to the Bill include references to its purposes being to 'improve interoperability among personal data protection frameworks' and 'respecting … applicable international legal instruments'. These provisions might enable the DPA to impose additional obligations needed for 108+ accession.

Otherwise, the principal problems that Sri Lanka is likely to face in an accession application are the lack of independence of the DPA, and the extent of the discretionary powers of both the DPA and the Minister. Provided there is effective enforcement, the limited extent to DPA enforcement powers is unlikely to pose a problem.

## Other South Asian developments

Bhutan enacted the *Information, Communications and Media Act of Bhutan 2018*[5] in 2017, in force from mid-2018. Although the data protection principles in the Act are stated briefly, they do more than give Bhutan a minimal data privacy law, because they include seven of the ten 'second generation' principles found in the 1995 EU Data Protection Directive, and are thus a moderately strong law for the Asian region.

[5] *Information, Communications and Media Act of Bhutan, 2018* <https://www.dit.gov.bt/information-communications-and-media-act-bhutan-2018>.

## Nepal's idiosyncratic privacy law

Nepal enacted *The Privacy Act 2018*,[6] but it is not a data privacy law because it does not include most of the set of basic principles shared by all such laws since 1980. In addition, most of the twelve chapters only have a significant effect on information held by public bodies,[7] the definition of 'personal information' only covers specific (although extensive) categories of information about a person, and not whatever information can identify a person, and there is no DPA created or designated, just enforcement through the District Court.

However, there are many provisions in the Act to which private sector bodies operating in Nepal should pay careful attention in order to avoid prosecutions or compensation claims. For example, personal data collected by bodies corporate may only be used 'for the purpose for which such data have been collected', or with consent, and some personal data cannot be disclosed without consent. This wide-ranging Act cannot be ignored, but Nepal still does not have a data privacy law covering its private sector.

## Pakistan: e-Commerce Policy, and data protection Bill(s)

Pakistan's Ministry of Commerce published a revised version of the country's e-commerce policy[8] on 13 November 2019. The Policy focuses on nine areas, including data protection, and ranging from fintech, to telecoms to consumer protection. It includes plans to establish a national e-commerce council to provide strategic direction. It states that 'the Data Protection Bill 2018 is … at an advanced stage of consultations', but does not clarify whether this is a revised version of the *Personal Data Protection Bill, 2018* (discussed below), or possibly will be more aligned with the GDPR. 'Regions such as EU do not allow their enterprises to transact with companies of such countries which do not offer same level of data protection which is available under the EU Regulations', the Policy notes. 'Such disclosure will also include disclosure about the country/legal jurisdiction where such data will be stored and the purpose for which it may be used'.

The Policy says that it 'is essential to have effective data protection laws and enable the local digital industry to make proper use of the data generated in Pakistan', and that 'Pakistan Data Protection Act & Cloud/Data Policy (under consideration) [are] to provide for data sovereignty, data localization and address issues relating to e-Commerce. There is no doubt some forms of data localization are on Pakistan's agenda, as they are in India and Sri Lanka.

The Policy also includes separate plans for 'a code of conduct applicable to all e-commerce businesses, which would require all e-commerce platforms to make full disclosures regarding data protection provisions on their websites and apps'.[9]

## Personal Data Protection Bill 2018

This Bill[10] only covers the private sector ('information in respect of commercial transactions'). It is legislation which, at best might meet most of the requirements of a 'second generation'

---

[6] *The Privacy Act 2018* (Nepal) <http://www.lawcommission.gov.np/en/archives/category/documents/prevailing-law/statutes-acts/the-privacy-act-2075-2018>.

[7] Nepal has had a basic data privacy law for the public sector since the Right to Information Act 2007: Greenleaf *Asian Data Privacy Laws* (OUP, 2014), pp. 440-445.

[8] *e-Commerce Policy of Pakistan*, October 2019 <http://www.commerce.gov.pk/wp-content/uploads/2019/11/e-Commerce_Policy_of_Pakistan_Web.pdf>

[9] 'Pakistan: MOC publishes e-commerce policy' *Data Guidance* 26 November 2019.

[10] *The Data Protection Bill 2018* (Pakistan) <https://moitt.gov.pk/userfiles1/file/PERSONAL-DATA-PROTECTIONBILLOctober18Draft.pdf>

law (based on the 1995 EU Data Protection Directive), but relatively little from the additional '3rd generation' requirements of the GDPR and Convention 108+. Of these, it includes a requirement of lawful ground for processing; some requirements of minimal processing ('necessary', 'not excessive'); rights to withdraw consent to process personal data; rights to prevent processing likely to cause damage or distress; and a right to erasure. Sensitive data is covered, but not including biometric or genetic data. The Bill would establish a National Commission for Personal Data Protection (NCPDP) with independence ('shall enjoy operational and administrative autonomy'). Since this is a Bill which is not certain to indicate Pakistan's legislative direction, further analysis is not justified here.

## Conclusions: SAARC is slowly catching up

The most important developments in South Asia are still incomplete (India, Sri Lanka, Pakistan), and where legislation has been completed it is of minor importance (Nepal, Bhutan). There are no regional (SAARC) initiatives. Nevertheless, the situation is a considerable improvement on five years ago, and negotiations between the countries with Bills, and Brussels and/or Strasbourg could possibly see South Asia emerge with a number of laws closer to current international standards.