Myanmar Centre for Responsible Business

POLICY BRIEF
A DATA PROTECTION LAW THAT PROTECTS PRIVACY: ISSUES FOR MYANMAR

This Policy Brief[1] provides an overview of terminology, concepts and good practices in addressing **data protection and privacy.** These terms are widely used but often poorly understood. The Brief aims to contribute to an informed discussion in Myanmar on these topics, to support the Myanmar Government, private sector and civil society in establishing a Data Protection Law that protects that protects data and human rights. This will in turn support Myanmar's ambitions to develop its digital ecosystem to help prepare it for the 4th Industrial Revolution (4IR), including its E-Governance Master Plan and Digital ID. These projects must be underpinned by robust data protection to function effectively.

WHAT IS DATA PROTECTION? AND HOW IS IT RELATED TO THE RIGHT TO PRIVACY?

Data protection and the human right to privacy[2] are fundamentally linked.[3] A comprehensive approach to data protection[4] is based on the twin goals of:

- Recognising data protection as a fundamental right, and protecting the range of rights that enable individuals to control their personal data and any processing of it
- Setting up systems of accountability, and imposing clear obligations on entities processing and controlling personal data

This comprehensive approach to data protection should form part of an even broader national **cyber security** strategy.[5]

WHY IS DATA PROTECTION NECESSARY?

The global **digital economy** is leading to **increased demands for personal data** from:

- **Governments**, to identify individuals and to provide them access to public services
- **Companies**, to provide targeted products and services to users

Both are increasingly using data-intensive systems to process data about people, generate additional data about people, and use data to make decisions about people.

More extensive and innovative uses of personal data bring greater economic and social benefits, but also increase risks to personal privacy. If the data is not made secure and kept private, including through regulation, people will not trust the systems that underpin the digital economy.[6] Without

[1] With thanks to Privacy International. This Briefing Paper draws on information featured in Privacy International, "The Keys to Data Protection: A Guide for Policy Engagement on Data Protection," (August 2018), and OECD, Privacy Framework (2013), the EU General Data Protection Regulation (2016/679) and the Council of Europe Council of Europe's Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (2018) in particular. See also APEC Privacy Framework (2015) that aims at promoting electronic commerce throughout the Asia Pacific region, and reaffirms the value of privacy to individuals and to the information society. The updated Framework (2015) "draws upon concepts introduced into the OECD Guidelines (2013) with due consideration for the different legal features and context of the APEC region."

[2] See Article 12 of the Universal Declaration of Human Rights (UDHR), Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 21 of the ASEAN Human Rights Declaration.

[3] Report of the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, UN Doc. A/HRC/17/27, para. 58 (May 16, 2011).

[4] Other sectoral legislation may also be needed to complement a general data protection law in specific circumstances (e.g. in the field of telecommunications, health, education).

[5] See MCRB's companion Policy Brief on Cyber Security and Cyber Crime.

[6] In a 2014 OECD survey on the digital economy, governments identified security as the second highest priority area and privacy as the third out of 31 possibilities, with only broadband coming higher.

protection, there can be new possibilities for crime, and for exacerbating existing inequality and discrimination. This can ultimately undermine the technological advances that can spur development.[7]

As of September 2018, over 100 countries have enacted comprehensive data protection legislation, and around 40 countries are in the process of enacting such laws.[8] However, Myanmar currently does not have any effective data protection requirements in place. This will undermine its ambition to keep up with the 4IR.

Personal data is the fuel of the global information economy that is using innovation to enhance prosperity and opportunity. But to keep the fuel flowing, governments now recognise that data must be protected. For example, the EU is in the process of determining which countries outside the EU have adequate data protection measures that will allow personal data to flow from the EU to that third country without any further safeguards.[9] If Myanmar does not have appropriate data protection laws in place and fully implemented, it risks being excluded from the global digital economy.[10]

On the other hand, data protection laws should not be either misused to hide wrongdoing and corruption or so overly broad that they can be used to prosecute or shut down legitimate criticism of public figures and their actions. They should be coordinated with other laws that underpin transations that will increasingly rely on data protection, such as the Consumer Protection Law.[11]

SIX SETS OF PROVISIONS NEEDED FOR A COMPREHENSIVE DATA PROTECTION LAW FOR MYANMAR

A comprehensive data protection law[12] for Myanmar should include the following typical provisions found in data protection laws:

1. A clear purpose and scope of application

This means the law should:

- Be based on a **legitimate purpose**, that includes a direct reference to international human rights and constitutional protections of the right to privacy and related rights.
- Include a **broad definition of personal data** to capture a wide range of types of information, including data that can indirectly identify a person. The definition should also cover the entire lifecycle of processing of data[13] on a computer, on a phone, on an Internet of Things (IoT) device, and also via paper records.
- Provide **higher protection for 'sensitive' data** that relate to potential areas of discrimination, such as race or ethnic origin, religious affiliations, trade union membership, etc.
- Make sure the law **applies to private and public entities.** Law enforcement, national security and intelligence agencies should not be exempt. Any exemptions from coverage should be as few as possible and be made known to the public.[14]
- Be **very clear about the limitations and conditions** that should be placed **on government surveillance** through internet and communications technology (ICT) to protect privacy and data protection.[15]

---

[7] OECD, Digital Economy Outlook (2017), p. 17

[8] Source: Banisar, David, National Comprehensive Data Protection/Privacy Laws and Bills 2018 (Sept, 2018).

[9] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/adequacy-protection-personal-data-non-eu-countries_en

[10] UNCTAD, Data protection regulations and international data flows: Implications for trade and development, (2016), p. 8.

[11] http://www.myanmartradeportal.gov.mm/uploads/legals/2018/5/Consumer%20Protection%20Law%202014%20(eng).pdf

[12] A recent UNCTAD study noted that Governments - specifically in those developing countries attempting to adopt data protection legislation … most opt for an approach consistent with the EU General Data Protection Regulation." UNCTAD, Data protection regulations and international data flows: Implications for trade and development, (2016), p. xii.

[13] European Commission, What is personal data?

[14] OECD, Privacy Framework (2013).

[15] See: Myanmar Centre for Responsible Business, "Sector Wide Impact Assessment of Myanmar's ICT Sector, Recommendations, Annex I: Lawful Interception and Government Access to User Data: The Characteristics of a

- Ensure data protections should **follow data of the individual** rather than relying on where the data controller or processor is based, in view of globalised infrastructure.

2. Set out specific legal requirements to address data protection principles

These important and well-recognised principles[16] include:

- **Fair, lawful and transparent**: There should be limits on the collection of personal data that should be obtained by lawful and fair means. Data collection should be done in a transparent manner - individuals should be clearly informed and aware of how their data is going to be processed and by whom. There should be no secret processors of data.
- **Purpose limitation**: Personal data should be processed for a specified, explicit and legitimate purpose. That purpose should be clearly specified at the time of collection. Data collected should be used only for that agreed purpose(s). It is not acceptable to collect data for one purpose and then to use it for something else without notice, consent or justification.
- **Data Minimisation**: Only the minimum data necessary should be collected.
- **Accuracy**: Personal data should be accurate and complete, and kept up to date to make sure the data does not become inaccurate.
- **Storage Limitations**: Personal data should be stored only for the period of time necessary for the purpose for which it was collected and stored and not longer.
- **Integrity and Confidentiality**: Personal data should be protected by reasonable security safeguards to protect from loss, unauthorised access, destruction, use, modification, or disclosure.
- **Accountability**: Any entity that processes personal data, in its capacity as data controllers or data processors, should be accountable for demonstrating compliance with the legal requirements. They must be able to explain, show, and prove that they respect people's privacy - both to regulators and individuals.

3. Set out specific legal requirements to protect the rights of data subjects

These are important and well-recognised rights of data subjects.[17] People have the following rights:

- **Right to Information**: to be provided with information about who is using their data and for what purpose.
- **Right to Access**: to obtain information about whether a data controller processes data about them, the purpose of processing, the legal basis for processing, where the data came from, who it has been/might be shared with, how long it will be stored for, whether their data is being used for profiling and automated decision-making, together with a copy of information held.
- **Rights to Rectify, Block and Erasure**: to ensure the data is accurate, complete and kept up-to-date – or entirely blocked or erased.
- **Right to Object:** to object to their data being processed at any point. Certain rights to object should be absolute, such as in relation to direct marketing. Other processing of data must be justified as necessary.
- **Right to Data Portability:** to request that their personal data is transmitted to another service with the specific consent of the individual.
- **Rights Related to Profiling and Automated Decision Making** to object to processing, including profiling and to not be subject to purely automated decision-making processing without any

Rights-Respecting Model" (2016), p. 35 and UNCTAD, Data protection regulations and international data flows: Implications for trade and development, (2016), pp. 15-16 and see the "emerging 'test' for achieving a balance between data protection and surveillance.", p. 59.

[16] See UNCTAD, Data protection regulations and international data flows: Implications for trade and development, (2016) - pp. 56-57, which recognises that there "is a recognized set of core data protection principles" the countries should draw on in developing data protection laws.

[17] See OECD Recommendation: Digital Security Risk Management for Economic and Social Prosperity (2015).

human intervention, if such a decision significantly affects them.

- **Right to an Effective Remedy, including compensation and liability:** to an effective remedy against a data controller and/or data processor, including compensation for damage suffered.

4. Set out specific and limited grounds for processing of personal data

The grounds for processing personal data should be limited and clearly spelled out in the law. They may include:

- **Consent** of the person – this should require an explicit and active process for the individual, and should be freely given, specific, informed and unambiguous. For example, 'consent' should not be obtained by requiring a pre-ticked box to be unticked; it should be an active choice. Consent should also be as easy to withdraw.
- Explanation that the personal data is **necessary** for:
    - **the performance of a contract** with the person or to take steps to enter into a contract
    - compliance with a **legal obligation**
    - the performance of a **task carried out in the public interest** or in the exercise of official authority vested in the controller – such as for public health reasons
    - the **legitimate interests** pursued by the data controller
    - for the **vital interest** of the data subject

5. Set out specific legal requirements on the obligations of data controllers and processors

The law should **clearly identify the parties responsible for complying** with the law and **their obligations and duties** to ensure compliance and protection of the rights of individuals. These should include the duty and responsibility to **safeguard the security of data. If there are breaches** these should be investigated and reported to the authorities and to the persons whose data may have been stolen**.**

6. Establish an independent supervisory authority for data protection

At least 90% of countries with data protection laws have opted for an independent supervisory authority on data protection.[18] They typically have a **mandate to investigate**, to receive and respond to complaints, to provide advice, information and to promote public awareness. They should have **the power to impose sanctions**, including administrative fines, criminal sanctions and impose direct liability on directors of companies.

[18] Privacy International, "The Keys to Data Protection: A Guide for Policy Engagement on Data Protection," (August 2018), p. 85. See also UNCTAD study, p. xii.