

## Why Data Protection Matters: Know what you share!

January 28, 2021

Have you ever used WhatsApp or Viber? Have you paid with KBZPay or WaveMoney? Do wear a fitness wristband or call taxis using Grab? Have you ever “liked” a Facebook post? Or taken an online quiz on your ideal tourism destination, or that funny personality test that your friend in the USA sent you? If you answered yes to any of these questions you have been sharing your personal information, either online or offline, with private or public entities — including some that you may never have heard of.

Sharing data may bring benefits, and it has often also become necessary for us to do everyday tasks and engage with other people in today’s society, particularly during the COVID-19 pandemic. But it is not without risks. Your personal data reveals a lot about you, your thoughts, and your life, your ID card details, your friends, even where you had lunch today, whether you walked or took a taxi. These data can easily be exploited to harm you and that is why these data must be strictly protected.

Today, 28 January, many countries across the world are celebrating Data Privacy Day. Myanmar is not yet one of them. But today is still a good opportunity for people in Myanmar to stop and ask themselves: Is my personal data safe? What happens to my personal data? Where does it go?

### So what is personal data?

The International Association of Privacy Professionals (IAPP) provides a definition:

“Any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly — in particular by reference to an identification number or to one or more factors specific to their physical, physiological, mental, economic, cultural or social identity”

In the digital space, where vast amounts of personal data are shared and transferred around the globe instantaneously, it is increasingly difficult for people to maintain control of their personal information flow. This is where data protection comes in.

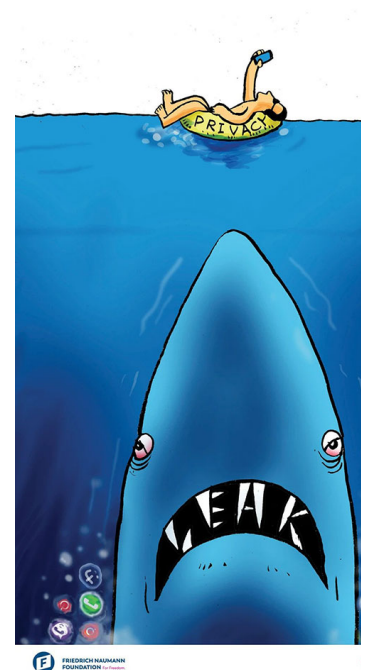
**Data protection refers to the various laws, practices, safeguards, and binding rules put in place to protect your personal information and ensure that you remain in control of it. In short, you should be able to decide whether or not you want to share some information, who has access to it, for how long, for what reason, and be able to modify some of this information, and more.** We should also highlight that data protection is different from data security since it extends beyond securing information to devising and implementing policies for its fair use.

Governments also have a security interest in ensuring the protection of personal data. In 2018, it was discovered that the personal details of 1.5 million users of SingHealth’s clinics had been hacked, over three years. Hundreds of thousands of credit card details from at least six Southeast Asian countries – including Malaysia and Singapore – have been leaked online, reported [by India-based cybersecurity start-up Technisanct](#). These types of attacks are happening more frequently across the globe, and countries must take action to better protect individuals’ information.

Many countries have adopted data protection laws to ensure that governments, companies, and anyone else who collects your personal data are legally obliged to collect it only for specific purposes and protect it properly. This includes most of Myanmar’s neighbours. For example,



The day has several names: Data Protection Day, Privacy Day or Data Privacy Day; it does as long as it protects your private data.



The Council of Europe published film to highlight the dangers pose who wish to illegally obtain private

Thailand adopted a Data Protection Law in 2019, loosely modeled on the EU's General Data Protection Regulation.

However, Myanmar does not yet have a Data Protection Law. This is a problem not only for those who are worried about whether their personal data is safe but also for those who want to trade across borders [through e-commerce platforms](#). As other countries establish laws that protect personal data, they will be less and less willing to allow trade with those that don't have such laws.

But can't we just trust the government, companies and others to self-regulate and be responsible with our data? Certainly, we can encourage them to act in accordance with the concept of '[Privacy by Design](#)'. That means, for example, not asking for unnecessary personal data or using it for purposes other than the reason it was collected, notifying you if there is a risk, and letting you know how they make your data safe.

And it's true that simply adopting a data protection law won't stop systems being hacked. But laws allow the government to fine organisations whose cybersecurity is lax or restrict the abuse of data. SingHealth had to pay a fine of SGD 1 million. The prospect of significant financial penalties drives companies and other organisations to invest in better cybersecurity and data protection. It's good for business too: at the very least, customer confidence collapses when personal data is leaked, even if there is no financial loss. A data protection law can improve [public trust in the digital space](#), particularly if it is human-centric international digital rights organisation.

Privacy keeps you, your information, and your reputation safe. Once your reputation is compromised, it will be hard to restore. So be careful when you share your personal data with unknown apps and platforms without a privacy policy consent.

[Myanmar Centre for Responsible Business](#) has been advocating since 2016 for a Myanmar [Data Protection Law](#) that protects the right to privacy in line with international standards. We encourage the new government and parliament to take this step. We believe it will build trust in government, trust in business and keep you safe. Together, we can build strong and concrete safeguards for the right to protection of personal data.

[Facebook](#)[LinkedIn](#)[Twitter](#)

## Read also

- [Update on Draft Cybersecurity Law and its Impacts on Digital Rights and the Digital Economy](#)
- [Myanmar's Legal Framework For Cybersecurity Needs To Be Built To International Standards](#)
- [MCRB Provided Comments on Draft E-commerce Strategy for Myanmar and Draft eCommerce Guidelines 2020](#)
- [Recorded discussion panel: "In Privacy and Data Protection We Trust!"](#)
- [Lift the Restrictions on Internet Access](#)
- [MCRB provides initial comments to government on the draft cybersecurity framework, and discusses cybersecurity with MPs](#)

[Previous article](#)[Next article](#)

Statement by Concerned Businesses Operating in  
Myanmar

Bringing Assistive Technologies for B2C Services to  
Myanmar

Funding from governments of UK, Norway, Switzerland, Netherlands, Ireland and Denmark.



Schweizerische Eidgenossenschaft  
Confédération suisse  
Confederazione Svizzera  
Confederaziun svizra



Government of  
the Netherlands



DENMARK