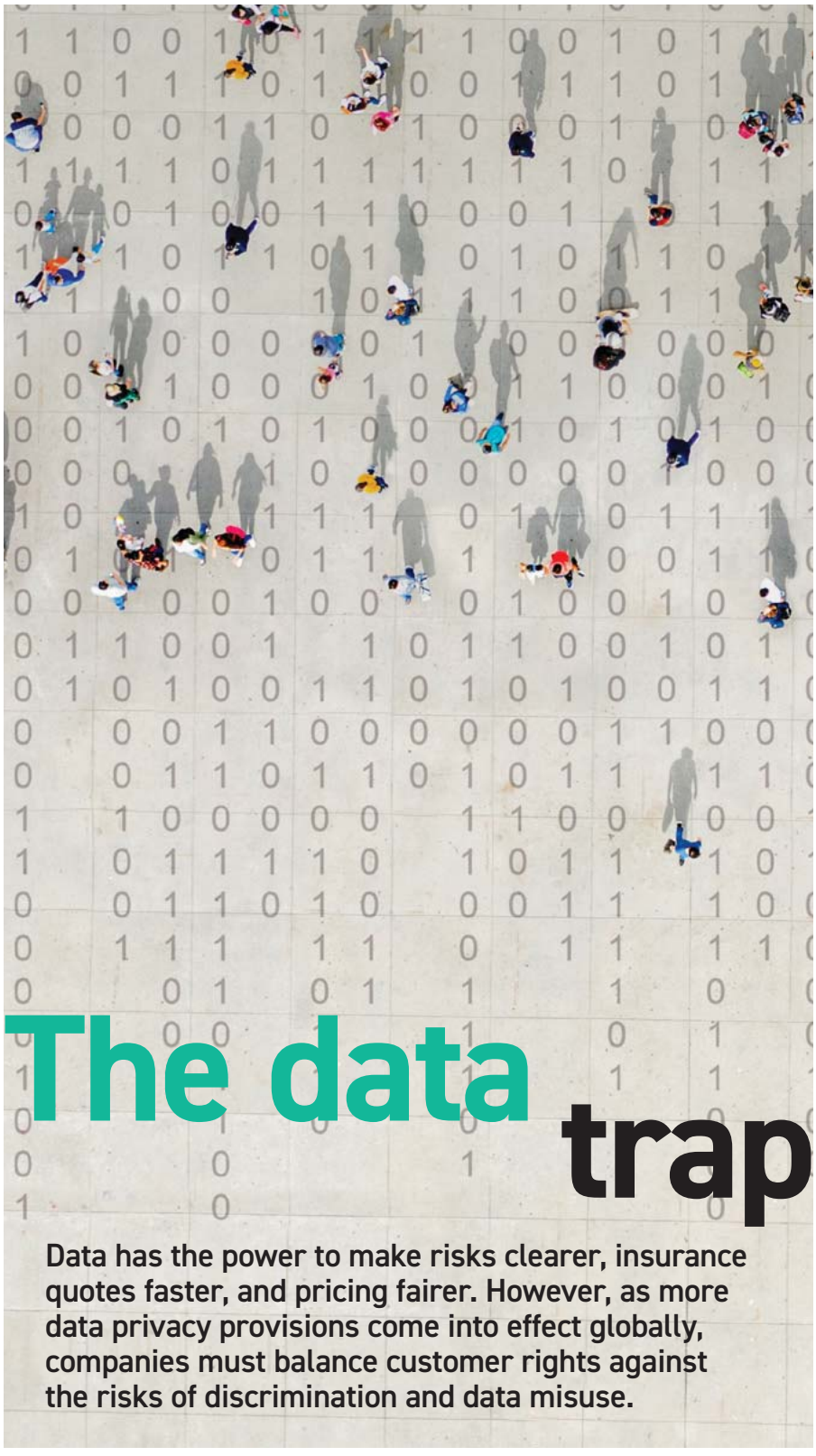
by Ben Falkenmire



The data trap

Data has the power to make risks clearer, insurance quotes faster, and pricing fairer. However, as more data privacy provisions come into effect globally, companies must balance customer rights against the risks of discrimination and data misuse.

Australia's move to reform its Privacy Act more in line with the European Union's General Data Protection Regulation (GDPR) is expected to see insurers do more heavy lifting around de-identified data and data that is deemed sensitive.

The 116 flagged changes could see de-identified data captured under the Act and additional safeguards around the data of vulnerable persons put in place.

Clyde & Co's privacy and data protection expert Alec Christie says the proposed reforms come down to the view that there is almost no such thing as de-identified data. "If there's any way that personal and anonymous data can be linked, then it's not de-identified data, it's always personal information," he says.

In response to the new laws, Christie says insurers will need to put a "wall" in place between personal data and anonymous data used for actuarial activities, to meet de-identified data and anti-discrimination provisions. Such a wall might take the form of an information barrier, or some physical or digital separation between the de-identified data and identified personal data, and anything that could re-identify the de-identified data.

Says Christie: "For example, if an insurer has de-identified data to run analytics but anyone who has access to that de-identified data has access to any other data — a look-up table, key or other mechanism which, when combined, re-identifies it — then the so-called de-identified data is considered never to have been de-identified and it remains personal information. It could be that the easiest way to ensure that data remains de-identified is to have it held in a separate or third-party space where there is little risk of re-identification but, of course, giving the data to a third party has its own different set of risks."

One thing insurers can do is extract aggregate data from a third party or a pool in the region. "That is considered separate processing, and it's almost impossible then for any particular country to re-identify its information," Christie says.

IN SHORT

- **Insurers need to assess their risk in light of data privacy reform in Australia and other countries across the Asia Pacific.**
- **In particular, the way the data of vulnerable customers is treated may require closer attention.**
- **Insurers operating across international borders need to be aware of the nuances of privacy laws in different countries and adopt one standard that meets the strictest provisions.**

> "If there's any way that personal and anonymous data can be linked, then it's not de-identified data, it's always personal information."
>
> **Alec Christie** / Clyde & Co

Another option is to upload the data into separate, secure cloud analytics storage and robustly de-identify the data as it leaves the insurer's day-to-day system or de-identify it as soon as it lands in the cloud. However, Christie stresses that both these options require the creation and implementation of a data de-identification framework to ensure that the data is truly not re-identifiable.

"In order to prove that their company has de-identified its data, insurers will need a de-identification policy. The ones we've done range between 25 and 65 pages. It's almost like a data retention plan or data breach response plan, looking at how you both de-identify data and maintain an anonymous aggregate database."

In addition, Christie says insurers will have to test the framework every 12–24 months and adjust the steps taken to de-identify the information to ensure it remains de-identified against new added data points and technological advances, such as AI analytics.

Assessing the risk

For large insurers like Zurich, separating data is not a straightforward process.

"The solution is not as simple as having separate processes for actuarial teams and functions," says Zurich's chief data officer in Australia and New Zealand John Kim.

"We take an organisation-wide approach to the management of structured and unstructured data to ensure we meet our privacy and data retention obligations. This includes the use of a data and records retention policy, framework, and approach for managing sensitive customer data, and de-identifying information where appropriate and required."

The idea of a wall may be more palatable for life and health insurers. Partners Life managing director Naomi Ballantyne says her organisation is already fit for purpose, thanks

Photography: iStockphoto

RECENT PRIVACY LAW CHANGES IN ASIA PACIFIC

Australia

Major reform is taking place in 2023, including proposals to add a right to erasure, explanation and objection, a direct privacy right, broad interpretation of consent and personal information, a new fair-and-reasonable test, privacy impact assessments and others. Increased penalty provisions were added in 2022.

Thailand

In mid-2022 Thailand's Personal Data Protection Act entered into force, specifying security standards for controllers, record keeping for processors, the handling of data breaches and criteria for fines, as well as providing guidance around obtaining valid consent.

New Zealand

The government is considering making changes to current privacy laws that would broaden the requirements for an individual to be notified when an agency collects their personal information indirectly through a third party.

Japan

Privacy laws were changed in 2022 to cover local and offshore businesses, increase penalties and add new rules around breach notification, cross-border transfers, the use of cookies (which can be deemed personal information) and prior notice and opt-in consent provisions in some circumstances.

Vietnam

A Decree on Personal Data Protection came into effect in July 2023 that mirrors the European Union's General Data Protection Regulation around data controlling and processing, consent, sensitive data and privacy impact assessments.

Sri Lanka

Sweeping privacy reforms were implemented in early 2022, addressing data processes and controllers, consent, transfers to countries offering adequate protection, the need for a data management program and data officer, breach notifications and privacy impact assessments.

Indonesia

Effective from October 2022, the new personal data law covers data processing, impact assessments, breach notification, the appointment of a data officer, cross-border transfer rules, data portability and non-compliance penalties.

China

The 2021 Personal Information Protection Law and its follow-up provisions impose demanding requirements for cross-border transfers (standard contract clauses can be an out), security assessments, certification and breach notification.

India

A Digital Personal Data Protection Bill was introduced for consultation in late 2022, covering grounds for processing data, consent and basic individual rights, with the law to apply to local and offshore entities.

Singapore

In October 2022, tougher financial penalties came into effect for contravening Singapore's Personal Data Protection Act. These include the higher of S$1 million or 10 per cent of an organisation's annual turnover.

to a hotly contested market in New Zealand.

"We operate in a small market and reputation is everything," says Ballantyne. "We mostly deal with independent financial advisers who provide customers with choice, so if you don't get it right, they take the customers with them. It forces the industry to do the right thing for customers, as opposed to being regulated to do it."

Less individual pricing for vulnerable customers

New vulnerable-customer protections proposed as part of a review of Australia's Privacy Act are expected to further impact insurers' ability to price for individual risk, particularly when it comes to pricing for mental-health factors.

The draft bill, which was still being reviewed by the government at the time of writing, proposes protections such as a fair-and-reasonable test for the handling of personal information; privacy impact assessments; rights to seek an explanation and object; and additional safeguards around customer consent.

"Individuals will need to have capacity in order to provide valid consent, and the reforms also propose that consent needs to be unambiguous," says Annelies Moens, managing director of privacy risk management consultancy Privcore.

In practice, this means that prefilled checkboxes and assumptions of consent if a person continues to fill in a form or read a webpage are out. Customers may need to actively tick a checkbox or click an 'I consent' button presented with the company's privacy statement. They may also be required to choose from a range of privacy settings — including opting out of all cookie-style web tracking and data collection.

> "We mostly deal with independent financial advisers who provide customers with choice, so if you don't get it right, they take the customers with them."
>
> **Naomi Ballantyne** / Partners Life

HOW DO OUR PRIVACY LAWS MEASURE UP?

Below are some of the differences — and proposed changes — in privacy laws between the European Union's GDPR and regulation in Australia and New Zealand.

Company obligations	GDPR	Australia	New Zealand
Individual consent to data can be implied	No	Limited	Yes
Privacy impact assessments required	Yes, in some circumstances	Yes, for government (change expected to include private companies)	No, but recommended
Separate data controller and data processor definitions	Yes	No (change proposed)	No
Keep records of processing activities	Yes	No (some change proposed in relation to source of data)	No
Penalties	Up to 2% of annual global turnover or €10 million, or up to 4% of annual global turnover or €20 million	Greater of A$50 million, 3x value of the benefit obtained, or 30% of company's turnover	Up to NZ$10,000
Individual rights	**GDPR**	**Australia**	**New Zealand**
Right to explanation	Yes	No (change proposed)	No
Right to erasure	Yes	No (change proposed in limited circumstances)	No
Right to object	Yes	No (change proposed)	No
Right to data portability	Yes	No (though partially enacted through the Consumer Data Right)	No

Sources: privcore.com, dataguidance.com, termsfeed.com

Photography: iStockphoto

WANT MORE?
CLAIM YOUR CIP POINTS

WATCH //
Impacts of the Privacy Act review
By Alison Baker and Jonathan Cohen
0.75 CIP pts
→ Take me there

LEARN //
Short course: Privacy Act
2 CIP pts
→ Take me there

The proposed changes also include a provision to prevent customers being discriminated against or penalised if they choose not to let an organisation collect data about them or track them, or if they request their data be corrected or deleted. That said, insurers can also explain that their ability to provide a quote or insurance cover may be limited without access to relevant data — which could include health records, details of assets and personal information.

Ballantyne is concerned that if further reforms reduce insurers' ability to price for individual risk, there will be an increase in premiums.

"The consequence of removing the ability to assess individual risk is that everybody pays for it. If that then reduces affordability for other chunks of the population, what is the benefit?" she asks.

> "I generally advise companies that if they want to be operating globally ... [they need] to pick one standard, which inevitably needs to meet the strictest provisions of privacy laws globally."
>
> **Annelies Moens** / Privcore

Aim for the highest standards

Regulators across the Asia Pacific are playing catch-up on data privacy laws. Australia's proposals set the bar high, matching the European Union's General Data Protection Regulation (GDPR) on the personal information definition and on three additional consent provisions (see breakout, left).

Much of the world looks to the GDPR as best practice in data privacy management, with some of the strictest data privacy laws in the world and some of the toughest monetary penalties for companies that breach them. Insurers operating across borders could be tempted to relax their data strategy in countries where laws are less strict. According to Moens, that would be a mistake.

"Customers don't want to be treated differently just because they happen to be in country A as opposed to Country B," she says. "I generally advise companies that if they want to be operating globally, the simplest and most effective approach is to pick one standard, which inevitably needs to meet the strictest provisions of privacy laws globally."

According to Kim, that's Zurich's modus operandi. He says that where regional or global requirements differ, the insurer takes a pragmatic view to do what is right by the customer, which can mean adhering to stricter regional and global standards.

This means that even if some countries decide to move to more business-friendly privacy provisions, insurers will likely err on the side of caution. Says Christie: "Since the GDPR was enacted, Britain has moved away from some of the provisions around consent that impacted insurers," he says. "Meanwhile, we [in Australia] seem to be going back to the original GDPR and putting in very strict rules.

"I think any insurance company that holds a lot of personal and sensitive information will be impacted."

BEN FALKENMIRE
Freelance journalist

"Governments are weighing in in favour of the consumer. However, there's market share on offer here for insurers who can get their systems primed and pitch transparency and trust to the consumer, while keeping their overheads in reasonable check."