

lane neave.

Preparing for the Privacy Act 2020

Webinar for the Institute of Management Consultants NZ

Graeme Crombie – Partner, Corporate

14 October 2020



What I will cover

laneneave.

- **Timeframes**
- **Key changes to the IPPs**
- **Notifiable privacy breaches**
- **Australian learnings**
- **Other key changes:**
 - New powers for the Privacy Commissioner
 - New fines/offences
- **Actions for organisations**
- **Possible future changes**
- **Q&A**

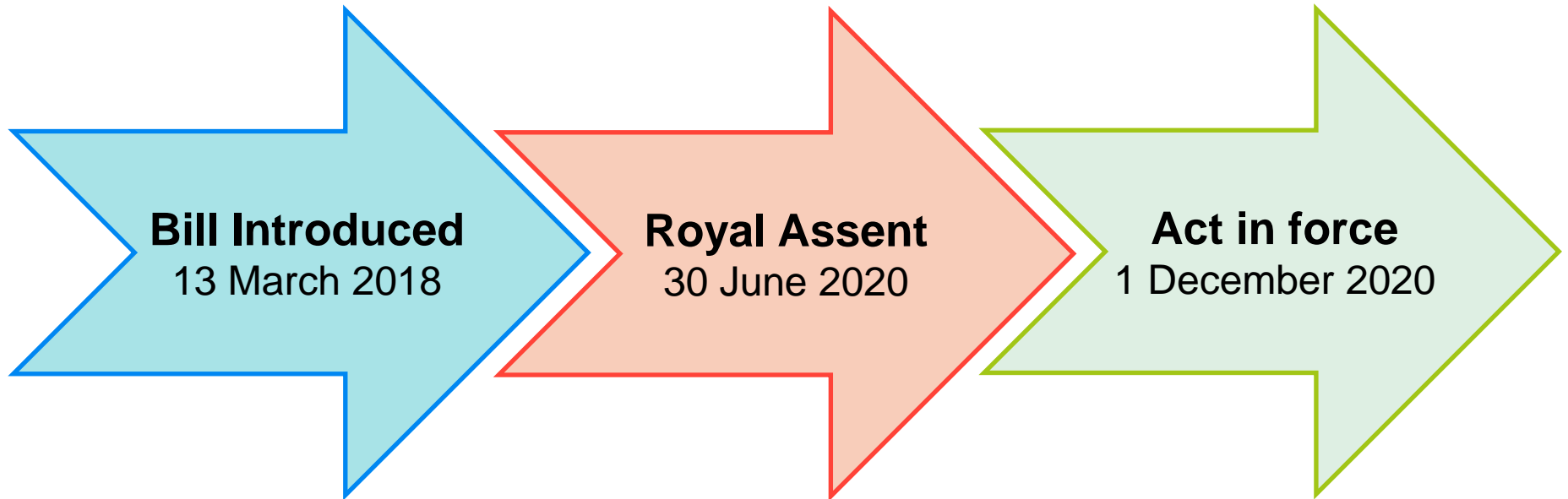


Timeframes



Timeframes

lane neave.



Information Privacy Principles



IPPs – The 13 Guiding Rules

lane neave.

Collecting Personal Information

1. Only collect information you need

2. Get it directly from the individual where possible

3. Be open about what you are going to do with it

4. Be fair about how you get it

Holding Personal Information

5. Keep it secure

6. Let people see their own information

7. Correct it if the person thinks it is wrong

Using and Disclosing Personal Information

8. Make sure it is accurate before you use it

9. Dispose of it when you no longer need it

10. Only use it for the reason it was collected

11. Only share it if you have good reason

12. Only send it overseas if it will be adequately protected

13. Only use unique identifiers when it is clearly allowed

New Principle 



IPPs – What is changing

laneneave.

- **Collection changes:**
 - IPP 1 – collecting identifying information restricted
 - IPP 2 – exception for serious threat to life or health added
 - IPP 4 – more care if collect from children and young persons
- **Use/Disclosure changes:**
 - IPP 8 – accuracy to be checked before disclosure
 - *IPP 12 – new rules if disclosing outside of New Zealand*
 - IPP 13 – minimise risk of misuse with unique identifiers

Action: Review privacy practices and update policies



IPPs – The New One

laneneave.

IPP12 – Disclosures outside NZ only permitted if:

- Individual authorises the disclosure
- Recipient subject to Privacy Act 2020 **or** privacy laws that provide comparable safeguards
- Recipient part of a prescribed binding scheme
- Recipient subject to privacy laws of a prescribed country
- Recipient otherwise subject to arrangements that ensure the information is subject to comparable safeguards

Action: Check contracts with third parties and update



Disclosure Outside New Zealand

lane neave.

scenario 1

- Retailer, ConsumeStuff, stores the data it collects in an AWS cloud, on servers in Australia. AWS does not access the data.
- ConsumeStuff uses a payment gateway provider based in the UK to process its credit card payments. The payment gateway also uses transaction data to improve its services.
- ConsumeStuff also works with a US vendor that provides complementary products to it and consumers who sign up to ConsumeStuff agree to receive marketing emails directly from that vendor.



Notifiable Privacy Breaches



Notifiable privacy breaches

lane neave.

Step 1 – Assess if there is a notifiable breach:

- *Trigger:* Breach of privacy + Serious Harm
- *But:* Exceptions + Defences

Step 2 – Notification:

- *Who:* Individual + Privacy Commissioner
- *When:* As soon as practicable, but delay right
- *What:* What happened + Actions taking

Note: Organisations responsible for breaches by service provider

Action: Put an assessment process in place



Notifiable Privacy Breaches

lane neave.

scenario 2

- Consumestuff also engages Emarketer, an email marketing platform provider, to communicate with customers.
- Chris, who works for Emarketer, detects Consumestuff's mailing list has been downloaded by an external party. The list includes name, email address, gender, mobile and home address. An IT sweep detects malware on Steve's computer, and that his login details were obtained when Steve clicked a link in an email from a malicious third party attacker.
- Consumestuff also discovers that some customers are receiving emails pretending to be from it and asking for credit card details.



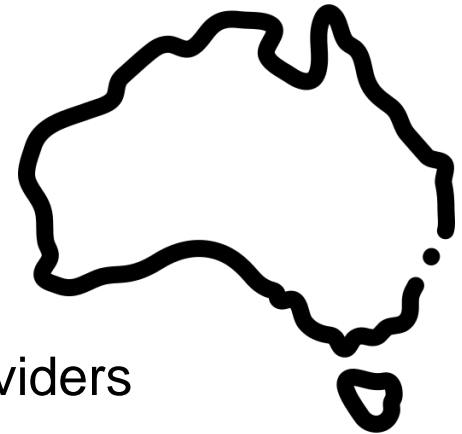
Australian Learnings



Australian learnings

lane neave.

- Breach reporting been in place since February 2018
- On average, over 80 notifiable breaches per month
- Most common are:
 - Human error
 - Compromised credentials
- **Key learnings:**
 - Have adequate contracts with service providers
 - Put individuals first in a breach situation



Action: Implement Learnings



Australian learnings

lane neave.

- **Best practice data breach practices:**
 - Staff knowledge and training
 - Preventative technologies and processes
 - Preparation
 - Assessment of harm
 - Post-breach communication



Action: Staff training and update security practices



Other Key Changes



Privacy Commissioner's New Powers

lane neave.

- **Compliance Notices:**

- Consultation process
- Steps required mandatory
- Enforceable, but can appeal
- Discretion to publish names



Privacy Commissioner
New Zealand
Te Mana Matapono Matatapu

- **Other Powers:**

- Directions on access
- More tools for investigations
- Able to share information with overseas agencies

Action: Regularly review Privacy Commissioner's website



New Offences

lane neave.

- **Offences (agency):**
 - Non-notification of a breach to Privacy Commissioner
 - Non-compliance with a compliance notice
- **Offences (individual):**
 - Misleading an agency
 - Knowingly destroying a requested document
- **Penalty:** Maximum of \$10k fine for breach of above offences



Actions for Organisations



Actions for organisations

laneneave.

**Update its privacy
breach response
plan**

**Check its security
practices and
training processes**



**Check its processes
to collect, store, use
and disclose
personal information**

**Update contracts
with suppliers and
other third parties to
whom it provides
personal information**



Possible Future Changes



Possible future changes

laneneave.

- **A Consumer Data Right?**
 - MBIE discussion paper released 5 August 2020
 - Four options considered
 - Would require portability of customer data
 - Submissions closed 5 October 2020
- **Other GDPR measures?**
 - Right to be forgotten
 - Increased security obligations
 - Mandatory privacy impact assessments
 - Mandatory data processing agreements
 - Transfers of data to other countries for processing



Questions





Graeme Crombie
Partner

D +64 3 372 6392

M +64 21 634 849

E graeme.crombie@laneneave.co.nz

The material contained in this webinar is necessarily in summary form. It is not intended to be a comprehensive statement on the law as it applies to the above topics. Accordingly, you must not rely solely on this information without first seeking detailed legal advice.