BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

"Modern Business Data and Privacy Policies"

Presented by

Tom Meagher
Director

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

Tom Meagher | Director

Tom has over 30 years' legal and business experience including:

- ✓ **working for local and major national Law Firms;**
- ✓ **being the majority owner and executive director of his former mid-tier Law firm;**
- ✓ **being a National Operations Manager for a financial advisory IT platform provider**
- ✓ **being the WA Legal Technology Group Manager for a National Law Firm**
- ✓ **qualified as a Microsoft-certified Project Manager;**
- ✓ **owning and managing an IT Consultancy Business; and**
- ✓ **being a Director and In-House Counsel for a Public Company.**

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

Tom is also a regular publisher of articles and is one of Australia's leading presenters of legal seminars to and for various professional bodies, associations and government authorities on a wide range of business law and professional development-training topics including:

WA Department of Commerce	Institute of Public Accountants	CPA Australia
Chartered Accountants Australia & NZ (CAANZ)	Governance Institute of Australia	Mortgage & Finance Association of Australia (MFAA)
Law Society of WA	National Electrical & Communications Assoc (WA)	City Insolvency Discussion Group
Innovation Centre of WA	Australian Hotels Association (WA)	Forum for Directors of Indigenous Organisations (FDIO)
LegalWise CLE	Small Business Development Corporation	Australian Computer Society
The Tax Institute	Australian Institute of Conveyancers (WA)	Institute of Certified Bookkeepers
Western Suburbs Business Association	Business Foundations Inc	WA Business Assist
Real Estate Institute of Western Australia (REIWA)	Australian Transformation and Turnaround Association (AusTTA).	Australian Institute of Business Brokers (AIBB)

Disclaimer

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

The contents of this presentation are for general information only and intended only as a guide. It does not constitute legal advice and must not be relied upon as such.

Balfour Meagher expressly disclaims all liability for any loss or damage arising from reliance upon any information in this presentation.

If you have a matter that relates to this presentation topic or you require legal advice, careful review and analysis of your matter's particular facts, information and documents are required before proper legal advice can be given or applied to your matter.

What we'll cover ✓

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

1. What is the *Privacy Act* and who does it apply to ?
    - 1.1 What are the Australian Privacy Principles (APPs)?
    - 1.2 What is "Personal Information", "Personal Data" and "Sensitive Information "?
    - 1.3 De-identifying Personal Information
    - 1.4 Interplay with Privacy Policies and Informed Consent
2. What Business Records (including possible Personal Information) are businesses statutorily-required to keep?
3. What is a "Notifiable Data Breach"?
    - 3.1 How a Data Breach may occur
    - 3.2 OAIC's Notifiable Data Breaches (January to June 2022…)
    - 3.3 Statutory Penalties for breaching the Privacy Act
    - 3.4 Broader Privacy Act Reforms
    - 3.5 Data Breaches: Threats and Consequences
4. **What is "Cyber Risk Insurance"?**
    - 4.1 Sample of modern Cyber Risk Insurance 'Application Proposal'!
5. **Before preparing a new Privacy Policy – Your related internal IT, Data &Security reviews**
    - 5.1 Sample overview of what a contemporary Privacy Policy may address
    - 5.2 new, Australian Privacy Policy Checklist
6. Useful Cyber Security Resources and Links

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

1. What is the *Privacy Act* and who does it apply to ?

- The Privacy Act 1988 (Privacy Act) was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations with an annual turnover of more than $3 million, and some other organisations, handle personal information.

- The Privacy Act includes 13 Australian Privacy Principles (APPs), which apply to some private sector organisations, as well as most Australian Government agencies. These are collectively referred to as 'APP entities'. The Privacy Act also regulates the privacy component of the consumer credit reporting system, tax file numbers, and health and medical research.

OAIC

Australian Government
Office of the Australian Information Commissioner

Australian Privacy Principles

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

1.1 What are the Australian Privacy Principles (APPs)?

Principle	Title	Purpose
APP 1	**Open and transparent management of personal information**	Ensures that APP entities manage personal information in an open and transparent way. This includes having a clearly expressed and up to date APP privacy policy.
APP 2	**Anonymity and pseudonymity**	Requires APP entities to give individuals the option of not identifying themselves, or of using a pseudonym. Limited exceptions apply.
APP 3	**Collection of solicited personal information**	Outlines when an APP entity can collect personal information that is solicited. It applies higher standards to the collection of sensitive information.
APP 4	**Dealing with unsolicited personal information**	Outlines how APP entities must deal with unsolicited personal information.
APP 5	**Notification of the collection of personal information**	Outlines when and in what circumstances an APP entity that collects personal information must tell an individual about certain matters.
APP 6	**Use or disclosure of personal information**	Outlines the circumstances in which an APP entity may use or disclose personal information that it holds.
APP 7	**Direct marketing**	An organisation may only use or disclose personal information for direct marketing purposes if certain conditions are met.
APP 8	**Cross-border disclosure of personal information**	Outlines the steps an APP entity must take to protect personal information before it is disclosed overseas.
APP 9	**Adoption, use or disclosure of government related identifiers**	Outlines the limited circumstances when an organisation may adopt a government related identifier of an individual as its own identifier, or use or disclose a government related identifier of an individual.
APP 10	**Quality of personal information**	An APP entity must take reasonable steps to ensure the personal information it collects is accurate, up to date and complete. An entity must also take reasonable steps to ensure the personal information it uses or discloses is accurate, up to date, complete and relevant, having regard to the purpose of the use or disclosure.
APP 11	**Security of personal information**	An APP entity must take reasonable steps to protect personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. An entity has obligations to destroy or de-identify personal information in certain circumstances.
APP 12	**Access to personal information**	Outlines an APP entity's obligations when an individual requests to be given access to personal information held about them by the entity. This includes a requirement to provide access unless a specific exception applies.
APP 13	**Correction of personal information**	Outlines an APP entity's obligations in relation to correcting the personal information it holds about individuals.

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

1.2 What is “Personal Information”, ”Personal Data” and “Sensitive Information ”?

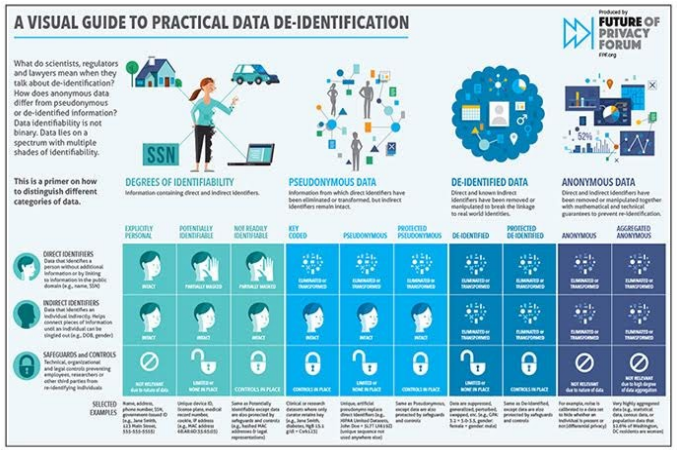
- “**Personal Information**” is *information or an opinion about an identified individual, or an individual who is reasonably identifiable: whether the information or opinion is true or not; and whether the information or opinion is recorded in a material form or not.**
- “**Personal Data**“ may be defined as things such as information about a person e.g. their name, address, email, mobile phone number, current location, medical information, date of birth, driver’s licence, passport, tax file number, etc.
- “**Sensitive information**” is *personal information which includes information or an opinion about an individual's: racial or ethnic origin, political opinions or associations, religious or philosophical beliefs.**
- ** Privacy Act 1988 (Cth)*

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

1.3 De-identifying Personal Information

De-identification and the Privacy Act

- De-identification is a privacy-enhancing tool. When done well, it can help your entity meet its obligations under the Privacy Act and build trust in your data governance practices.
- Information that has undergone an appropriate and robust de-identification process is not personal information and is therefore not subject to the Privacy Act.
- Whether information is personal or de-identified will depend on the context. Information will be de-identified where the risk of an individual being re-identified in the data is very low in the relevant release context (or data access environment).
- Put another way, information will be de-identified where there is no reasonable likelihood of re-identification occurring.
- De-identification involves two steps. The first is the removal of direct identifiers. The second is taking one or both of the following additional steps:
  - the removal or alteration of other information that could potentially be used to re-identify an individual; and/or
  - the use of controls and safeguards in the data access environment to prevent re-identification.
- The OAIC recommends that entities also refer to the De-Identification Decision-Making Framework, produced jointly by the OAIC and CSIRO-Data61, which provides a comprehensive framework for approaching de-identification in accordance with the Privacy Act.



1.4 Interplay with Privacy Policies and Informed Consent

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

- Under the Privacy Act, in many cases, the collection, use or disclosure of personal information is justified by the individual's consent.
- This is consistent with the "notice and choice" model for privacy regulation i.e we receive notice of the proposed treatment of our information and we have a choice about whether to accept.
- Though, **94%** of Australians do not read or privacy policies that apply to them – and that's rational behaviour - as it would take the average person 244 hours per year (six working weeks) to read or privacy policies that apply to them!*
- Therefore, in many cases, consumers are not truly providing their "informed consent" to current uses of their personal information.
  - In fact, the CPRC Report states around one in five Australians: "…*wrongly believed that if a company had a Privacy Policy, it meant they would not share information with other websites or companies*".

HOWEVER a very recent survey by research company Nature, conducted exclusively for The Australian Financial Review, found that 50% of respondents had refused to give their personal details to a company at least once since the Optus, Medibank and ATO cyber attacks. More than two in three people said they had become more worried about the security of their personal data held by companies.

- **More than three-quarters of people said they wouldn't share personal information with a service provider if they didn't have to, and 63% said they were rethinking which companies absolutely needed data on them.**
- **Less than a quarter of respondents were not worried about sharing their personal data with companies, Nature found.**

*Consumer Policy Research Centre (www.cprc.org.au - April 2018).

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

2. What Business Records (including possible Personal Information) are businesses statutorily-required to keep?

Category	Minimum Retention Period
Corporate Tax Records	
•Income •Expenses •Liabilities •Assets (receipts, sales, purchases, etc.)	5 years (min.) from the end of the accounting period. (Longer if tax returns are late…)
GST Records	
•Taxable supply •Importation •Creditable acquisition & importation	5 years following the assessment period
Company Documents	
•Statutory books •Board minutes •Resolutions	Keep indefinitely
•Accounting records with regards to transactions and all supporting documentation	7 years
•Other business registers	5 years (min.) from date of last entry
Personnel Files (HR documents)	
•Employee records*, payroll, wages, worker's comp, etc.	7 years from EOFY (*though there may be a ***limited*** exemption under the *Privacy Act*)

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

3. What is a "Notifiable Data Breach"?

- Under the *Notifiable Data Breaches (NDB) scheme* any organisation or agency the *Privacy Act 1988* must notify affected individuals and the OAIC when a data breach is likely to result in serious harm to an individual whose personal information is involved.
- A data breach occurs when personal information an organisation or agency holds is lost or subjected to unauthorised access or disclosure. For example, when:
  - a device with a customer's personal information is lost or stolen
  - a database with personal information is hacked
  - personal information is mistakenly given to the wrong person
- The notification to individuals must include recommendations about the steps they should take in response to the data breach. You should notify the OAIC using their online Notifiable Data Breach form. For more information, see Report a Data Breach

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

3.1 How a Data Breach may occur

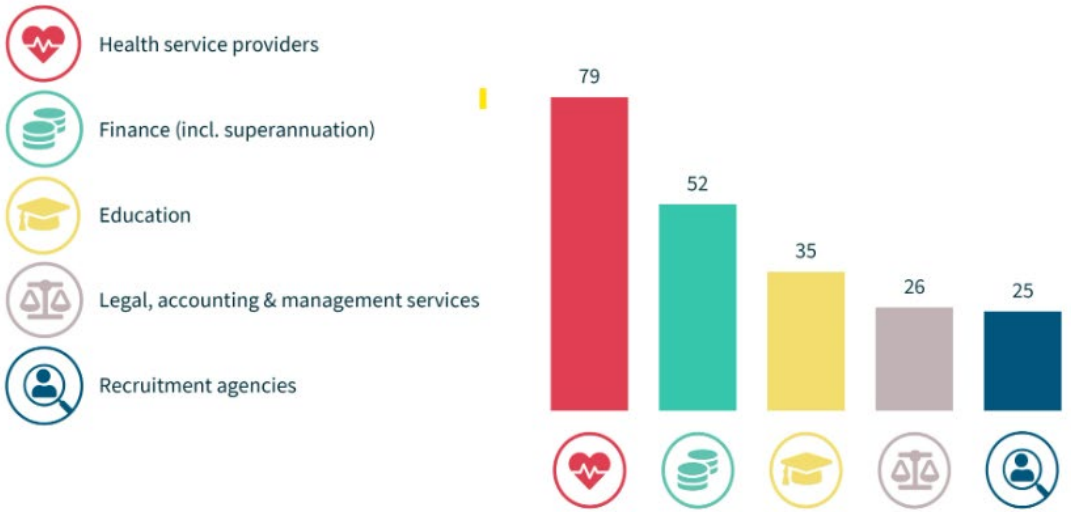
- Malicious or criminal attacks are a leading cause of data breaches notified to the OAIC.
- Strong password protection strategies, including raising staff awareness about the importance of protecting credentials, can greatly reduce the risk of this type of data breach.
- Australia's leading agency on national cyber security, the Australian Cyber Security Centre (ACSC), says credentials (usernames and passwords) are typically stolen when:
  - **a user is tricked into entering their credentials into a page that mimics the legitimate site;**
  - **a brute-force (automated trial-and-error) attack on username and password combinations is performed against a service, if it doesn't prevent such activity;**
  - **a service is compromised, and credentials are stolen and used to access the system or tested against other sites such as social media and email; and/or**
  - **a user's system is compromised by malware designed to steal credentials.**

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

3.2 OAIC's Notifiable Data Breaches (January to June 2022…)

396
notifications
Down 14%

Top 5 sectors to notify data breaches



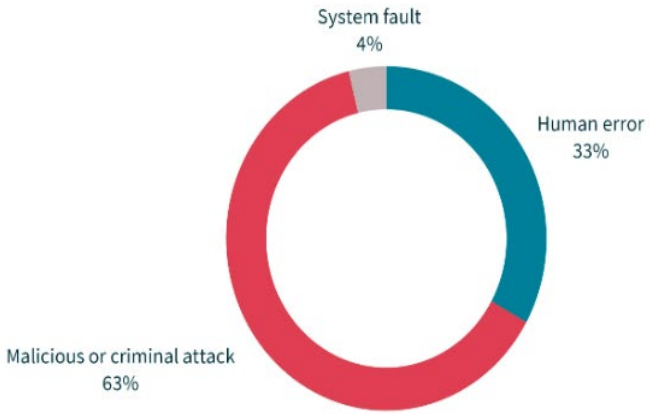
Australian Government
Office of the Australian Information Commissioner

3.2 OAIC's Notifiable Data Breaches (January to June 2022) cont'd

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

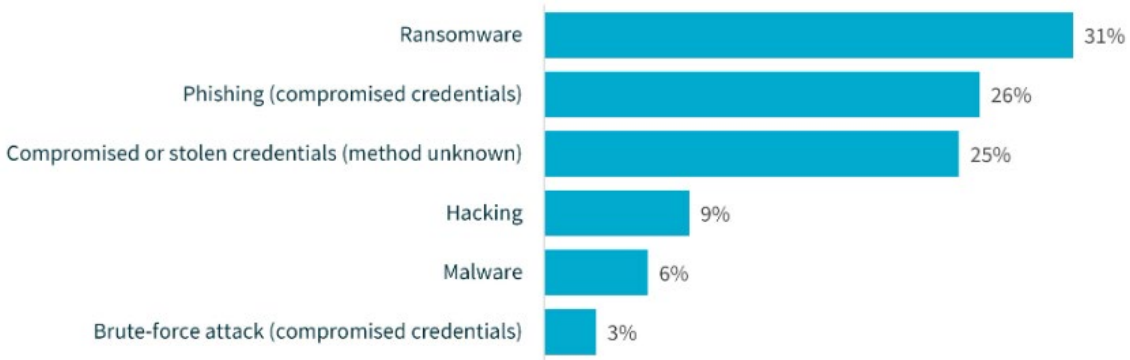
65%
of data breaches affected
100 people or fewer

Sources of data breaches



41% of all data breaches resulted from cyber security incidents (162 notifications)

Cyber incident breakdown



Top causes of human error breaches

Personal information emailed to the wrong recipient 38%

Unintended release or publication 24%

Personal information mailed to the wrong recipient 8%

3.3 Statutory Penalties for breaching the Privacy Act

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

- If an APP entity is found to have engaged in a serious, or repeated, interference with an individual's privacy, the APP entity may face penalties of up to:
  - $2.2 million for corporate bodies; and/or
  - $500,000 for non-corporate bodies (including government departments/agencies, sole-traders, partnerships, trusts, unincorporated associations)*.
- An APP entity will interfere with an individual's privacy if (among other things) it:
  - breaches an APP
  - breaches an APP code that is binding on the relevant entity (noting that the Australian Information Commission may impose an APP code on a particular organisation or industry)
  - breaches the credit reporting provisions of the Privacy Act
  - breaches the CR Code
  - breaches a provision of a Commonwealth contract for which it is to provide services and/or
  - handles a tax file number contrary to the Tax File Rule (which has been issued by the Australian Information Commissioner pursuant to the Privacy Act).

3.3 Statutory Penalties for breaching the Privacy Act cont'd

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

- After Optus and Medibank reported significant breaches of customer data, *including sensitive health information*, the Albanese government was now moving to increase penalties for serious or repeated breaches of customer data.

- The Federal Attorney General, Mark Dreyfus, who has had cybercrime added to his portfolio, will introduce the legislation (see over for detailed summary) which would increase penalties for serious or repeated data breaches from $2.2m to *whatever is higher*:

  i. **$50m;**
  ii. **three times the value of any benefit obtained through the misuse of information; or**
  iii. **30% of a company's adjusted turnover i.n the relevant period**

medibank PRIVATE

Yes OPTUS

3.5 Data Breaches: Threats and Consequences

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

Data Breach Targets

- Business data only becomes a target when it is of value to a third party. Different kinds of data are more or less valuable to third parties and represent different levels of risk to a business.
- The different types of data include the following:
  - **Personally Identifiable Information**. This includes data such as social security numbers, contact information, birth dates, education and other personal information.
  - **Financial Information**. This includes charge card numbers and expiry dates, bank accounts, investment details and similar data.
  - **Health Information**. This includes details on health conditions, prescription drugs, treatments and medical records.
  - **Intellectual Property**. This includes product drawings and manuals, specifications, scientific formulas, marketing texts and symbols, proprietary software and other material that the business has developed.
  - **Competition Information**. This includes data on competitors, market studies, pricing information and business plans.
  - **Legal Information**. This includes documentation on court cases the company may be pursuing, legal opinions on business practices, merger and acquisition details and regulatory rulings.
  - **IT Security Data**. This includes lists of user names and passwords, encryption keys, security strategies and network structure.

👉 *Some recent, Small Business Cyber Security statistics* 😲

3.5 Data Breaches: Threats and Consequences cont'd

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

Data Breach Consequences (in addition to fines & penalties…)

1. Revenue Loss

- Significant revenue loss as a result of a security breach is common. Studies show that 29% of businesses that face a data breach end-up losing revenue. Of those that lost revenue, 38% experienced a loss of 20% or more.
- A non-functional website, for example, may cause potential customers to explore other options.
- But any IT system downtime can lead to work disruptions.

2. Damage to Brand Reputation

- A security breach can impact much more than just your short-term revenue. The long-term reputation of your brand is at stake as well.
- For one, you don't necessarily want your emails leaked. In most cases, you need these emails to remain private.
- However, customers value their privacy, too — and breaches often involve customer payment information. Potential leads will be hesitant to trust a business with a history of shoddy data security.

3. Loss of Intellectual Property

- Loss of revenue and damaged reputation can be catastrophic. However, in some cases, hackers will also target designs, strategies, and blueprints.
- Businesses within the manufacturing and construction industries are more prone to this threat. Smaller businesses tend to believe they won't get hit. But 46 % of hacks target small businesses. This is because they're easier to attack.
- Losing intellectual property can impact the competitiveness of your business. Some rivals would not hesitate to take advantage of stolen information.

4. Hidden Costs

- Surface-level costs are just the beginning. There are many hidden costs related to breaches as well.
- For instance, legal fees may come into play. Also, you may need to spend more on PR and investigations, not to mention insurance premium hikes.
- Regulatory fines are another reality that many businesses overlook.

5. Online Vandalism

- Some hackers fancy themselves as pranksters. In these cases, a security breach might only lead to few word changes on your website.
- While this seems relatively harmless, it can actually cause a lot of damage. Subtle changes are harder to notice.
- For example, a hacker might change a few letters or numbers on your contact page. They may also add vulgar content to some of your webpages.

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

4. What is "Cyber Risk Insurance"?

- While all products are different, the range of assistance provided under a cyber policy includes coverage for:
  - ✓ forensic investigation;
  - ✓ data restoration;
  - ✓ customer notification and rectification e.g. call centres; and
  - ✓ indemnification of penalties imposed by government regulators.
- Where the data breach is due to the malicious acts of a foreign government actor or criminal gang coverage may include costs related to:
  - the services of a negotiator;
  - legal advice to determine if any ransom payment is legal or reportable; and
  - indemnification of the ransom the business decides to pay.

➢ **See also report by Insurance Council of Australia** *"Cyber Insurance: Protecting Our Way Of Life In A Digital World"*

Insurance Council of Australia

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

4.1 Sample of modern Cyber Risk Insurance 'Application Proposal'!

- **Very important to know/understand** all the various limitations, exclusions & undertakings an Insurer may require the Insured to attend to as part of their cyber risk insurance policy;
  - including not limited to the insured's extensive arrangements relating to data/records *purging* (cf. statutory responsibility to keep various business records) etc!

cfc

Cyber

Private enterprise

Application form
Australia

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

5. Before preparing a new Privacy Policy – *Your* related internal IT, Data &Security reviews

- So, whilst updating preparing Privacy Policy to also comply with the APPs (please note it's not just a legal advisor-drafting exercise yet also very much an internal procedures and compliance-aspect for each individual business and its owners).
  - Here's a link to a related article I've published in relation to the *Privacy Act* and the Europe Union's (EU) far more onerous *General Data Protection Regulations* (GDPRs).
  - ❖ (and, if you want a preview of how far and progressive privacy laws can be, then California's Consumer Privacy Act (CCPA) is one of the world leaders in such!)
  - plus also a general article in relation to Businesses' IT Security.

- Consider the various 'accountability and governance' plus the 'consent' requirements' in relation to GDPR data processing. As this too will be the most time and cost-effective way, and will also assist in being able to then suitably update/ prepare your new privacy policy to comply with the GDPRs.

- You ought to also undertake a 'privacy impact assessment', a 'data protection impact assessment" and evaluate your all current technology platforms:
  - ➢ (e.g. are your data systems obtaining 'personal information' and holding such in the (nebeulous) 'cloud' and, if they are in the cloud, do you know if your provider's cloud servers are only situated in Australia - such as Microsoft's Azure or Amazon Web Services?);
  - ➢ your key people who will be effectively your 'controllers'; and
  - ➢ if you outsource any of your data which contains 'personal data/identifiers, your third-party 'processors' e.g. contractors or third-party service providers.

- Lastly, again, please be sure to liaise with your licensed insurance broker to ensure you have appropriate cyber and other related digital risks' insurance policies in place (plus anything else they may recommend/advise for your particular).

5.1 Sample overview of what a contemporary Privacy Policy may address.

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

Your new Privacy Policy will amongst other matters incorporate the following elements:

1) introduction / explanatory statement to explain how 'Your Business' approaches privacy and the management of personal information, who to contact at 'Your Business' if there are any privacy issues, terms of reference, and some background about 'Your Business' and its business;

2) explanatory statement about the APP, their 2014 introduction, that they replaced the previous National Privacy Principles (2001), how the reader can find out more information about Australian Privacy Principles, and commentary about how your policy works;

3) the types of personal information 'Your Business' collects, and why this is collected, how the personal information is collected and used by 'Your Business' , details of any direct marketing communications from 'Your Business' to its clients and customers, how clients and customers are able to opt out of receiving communications from 'Your Business' , the method by which a client/customer/visitor can opt out, how information may be changed, what information 'Your Business' will not collect (such as sensitive information about racial or ethnic origin, political opinions of membership, religious or philosophical beliefs, memberships of trade associations or unions, sexual preferences or criminal records; however will necessarily collect information regarding health and medical details), and offering to anonymise client and customer information provide the option for a client and customer to not identify itself;

4) when and how personal information is collected, details of sources of information such as by post, telephone, email, or other electronic methods, by research or marketing campaigns, subscribing to email lists, or other third-party methods such as purchasing commercial lists from publicly available sources like online telephone directories;

5) information about third party software that 'Your Business' uses to collect and store information such as email marketing services and automated marketing platforms, details and links to those third parties' privacy policies, whether personal data will be used for analytics purposes, how analytics are performed such as clicking on email links or downloading email images, geolocation information, what personal information client/customer/visitor may be giving to such third parties (e.g. name, address and telephone number), whether 'Your Business' uses third parties to collect, store and process possible sensitive as well as financial information (e.g. Medibank, NDIS, health insurance, credit card details, cardholder details, expiration date, CCV could, etc) to enable electronic payments, and that 'Your Business' itself will not have access to a client/customer's financial information but may receive information about whether a particular individual has made payment;

6) how personal information is kept secure and protected, and that only 'Your Business' 's authorised staff members are allowed to access personal information;

7) when 'Your Business' may disclose personal information i.e. never without prior consent except required by law, or when information is provided on a confidential basis to third parties who provide services to 'Your Business' such as database management or mailing services, the 'Your Business' ensures such third parties are also bound by the APPs;

8) when information can be transferred overseas such as to third party financial processing services, steps taken to ensure information transferred overseas or to the 'cloud' is held used or disclosed by recipients in a manner consistent with the Australian Privacy Principles, disclosure of web traffic information to Google Analytics, and disclosure that communications through a social network service such as Facebook, LinkedIn or Twitter may be collected and held by such social network services overseas;

5.2 new Privacy Policy preparation checklist:

- ☐ **introduction and statement to explain how Your Business approaches privacy and the management of personal information;**
- ☐ **explanatory statement about the APPs;**
- ☐ **the types of personal information Your Business collects, and why this is collected, how the personal information is collected and used by Your Business;**
- ☐ **information about third party software and systems which Your Business may use to collect and store information;**
- ☐ **how personal information is kept secure and protected;**
- ☐ **when Your Business may disclose personal information;**
- ☐ **when any such personal information can be transferred overseas such as to third party provider;**
- ☐ **notification to visitors and users of Your Business' website;**
- ☐ **informing about Your Business' use of social networking services;**
- ☐ **when and how Your Business can make changes to its Privacy Policy;**
- ☐ **how a person can access, correct or update their personal information; and**
- ☐ **who to contact if there is complaint, question or concern about what information Your Business holds or about the accuracy of that personal information.**

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

PRIVACY POLICY CHECKLIST

© 2018 Brent J. Dreyer - DataEM.com

Company: Date:

Privacy URL:

INCLUDED | NEEDS ATTENTION | NOT INCLUDED | NOT APPLICABLE

CHANGES TO PRIVACY AND USE

- Identify the date of **LAST UPDATE** to the privacy policy, SUMMARY of last changes, and/or access to prior versions.
- Should be comprehensive and **EASY** to access and understand, using **CLEAR** and **PLAIN LANGUAGE**.
- Identify the conditions and method of notification when future updates or changes occur.
- Notification of when new data sources (partners, publishers, advertisers, 3rd parties) are added or removed.
- Notification of new or modified purposes for data collection, with any source, new or existing.

WHAT INFORMATION IS COLLECTED

- Describe information that is **KNOWINGLY PROVIDED**. Contact info, age, gender, payment, interests, social handles.
- Describe types of **DEVICE INFORMATION**, collected or acquired with purpose of data use.
- Device information, such as; Cookies, IP Address, mobile IDs, settings, browser data, mobile apps, beacons, etc.
- Describe what **COOKIES** are, their usage, functions and purpose. Review what will not function if disabled.
- Describe any access and collection of **SOCIAL MEDIA** data added to an individual's profile.
- Describe any access and collection of **DEMOGRAPHIC** data added to an individual's profile.
- Describe any individually identifiable data collected and stored from **WEBSITE VISITS**.
- Describe any individually identifiable data collected and stored from **EMAILS SENT**.
- Describe any collection of data from **INTERACTIVE AREAS**, like customer service, blogs, message boards, social or chat areas.

HOW INFORMATION IS COLLECTED

- Describe when it is from **DIGITAL DEVICES** when connected to website, mobile apps, etc.
- Describe what is collected from **CUSTOMER SERVICE** conversations and communications.
- Describe what is collected from **WARRANTY CARDS**.
- Describe what is collected **IN-STORE** from beacons, coupons, store reward cards, loyalty programs.
- Describe **LOCATION INFORMATION** from GPS, IP, bluetooth, beacons, 3rd party applications.
- Describe **PUBLIC INFORMATION** that is appended to other data provided or collected.
- Describe **COOKIES** and their use in the collection and exchange of data.
- Describe **MARKETING PARTNERS** collecting and appending data across multiple sources.
- Describe **ANALYTICAL PARTNERS** with tracking on website and data appended from other sources.
- Describe **SOCIAL PARTNERS** with tracking buttons on website and in apps.
- Describe **WIDGETS** on website or mobile apps (ie. LiveChat, Amazon, eBay).
- Describe **ADVERTISING TECHNOLOGIES** collecting and exchanging information when digital media is displayed.
- Describe **SEARCH PARTNERS** based upon search activity.
- Describe **AFFILIATES** collecting data from associated website.
- Describe **VIDEO CONTENT** Providers collecting view data.
- Describe **OTHER WEBSITE** Tracking Tags.
- Describe **OTHER PARTNERS** such as transactional vendors, credit checks, point of sale.
- Describe IoT (**INTERNET OF THINGS**) devices and data sources.

INCLUDED | NEEDS ATTENTION | NOT INCLUDED | NOT APPLICABLE

HOW INFORMATION IS USED

- Used to associate activity across your other devices and/or on other internet services.
- Used to detect and defend against fraudulent, abusive, or unlawful activity.
- Used to diagnose technical problems.
- Used for login validation, account access, and validation in email headers.
- Used to maintain, improve, and develop relevant features of the website, including content.
- Used to identify individuals to initiate and enable personal preferences.
- Used to verify an individual's identity when individual rights are being requested.
- Used to respond to customer service requests and questions asked by individuals.
- Used to create reports & analytics to share with partners, publishers, advertisers, apps developers, 3rd parties.
- Used in machine learning to model interests and behavior, to personalize and enhance effectiveness of marketing.
- Used to match and serve targeted advertising and digital content on the website and across the Internet.
- Used to identify location, geolocation, for location-targeted advertising, search results, and other content.
- Describe as shared within the organization, other departments, and with other subsidiary organizations.
- Describe where shared with other data collection sources, in accordance with contractual obligations.
- Describe where shared data is shared publicly (Directories, Group/Blog Discussions, etc.).

TRANSPARENCY & DISCLOSURES

- Should be intelligible, **EASY** to access and understand, using **CLEAR** and **PLAIN LANGUAGE**, especially for children?
- Identify **WHO** is managing their data (controllers, processors) with full CONTACT information.
- Detail **WHAT**, each type of Personal Data being collected, processed or shared, for current or future uses.
- Disclose the Purpose (**WHY**) data being collected or processed, for current or future uses.
- Disclose the **LEGAL BASIS** for all data being collected, processed or shared, for current or future uses.
- Disclose **WHO**, data partners, publishers, advertisers, 3rd parties, etc., that data is being shared with.
- Disclose **WHY**, the purpose each partners, publishers, advertisers, 3rd parties, etc. are receiving data.
- Disclose that privacy policies and practices of data partners may not subject to this Privacy Policy.
- Disclose the grounds for **LEGITIMATE INTEREST**, if this is selected as a lawful method.
- Disclose the logic behind any machine learning or **AUTOMATED DECISIONS**, consequences, including profiling.
- Disclose possible consequences if personal data is refused when part of a statutory or contractual requirement.
- Identify **CONTACTS** of data partners, publishers, advertisers, 3rd parties, etc., where data is being shared.
- Identify **CONTACTS** (name and contact details) for data controller and/or appropriate representative.
- Identify **CONTACTS** (name and contact details) for Data Protection Officer (DPO), if a DPO is appointed.

Useful Cyber Security Resources and Links

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

- Attorney-General's Department

Australian Government
Attorney-General's Department

- Australian Cyber Security Centre

Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

- Business.gov.au

Australian Government
Business
business.gov.au

- Office of the Australian Information Commissioner

OAIC

Australian Government
Office of the Australian Information Commissioner

- Australian Institute of Company Directors

Australian Institute of Company Directors

Thank You!

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

Top-tier quality legal work and business advice delivered directly by highly experienced, personable senior lawyers, business advisors & professional trainers. Balfour Meagher's services include:

- ✓ Commercial Law
- ✓ Technology & Internet Law
- ✓ Estate & Business Succession Planning
- ✓ Business and Equity Sales/M&As
- ✓ Loans and Securities Arrangements
- ✓ Property & Leasing Law
- ✓ IP Commercialisation & Brand Protection
- ✓ Specialist Medical, Pharmacy & Allied Health Services
- ✓ Conveyancing & Settlements
- ✓ Professional Training, Presentations & Seminars

www.bmlegaladvisors.com.au

BALFOUR MEAGHER
Legal & Business Advisors
expertise. service. results.

Tom Meagher

Director

E: tom@bmlegaladvisors.com.au

W: www.bmlegaladvisors.com.au

P: +61 8 9322 3842

A: The Park Business Centre

45 Ventnor Ave, West Perth, WA 6005

Email Disclaimer | Subscribe