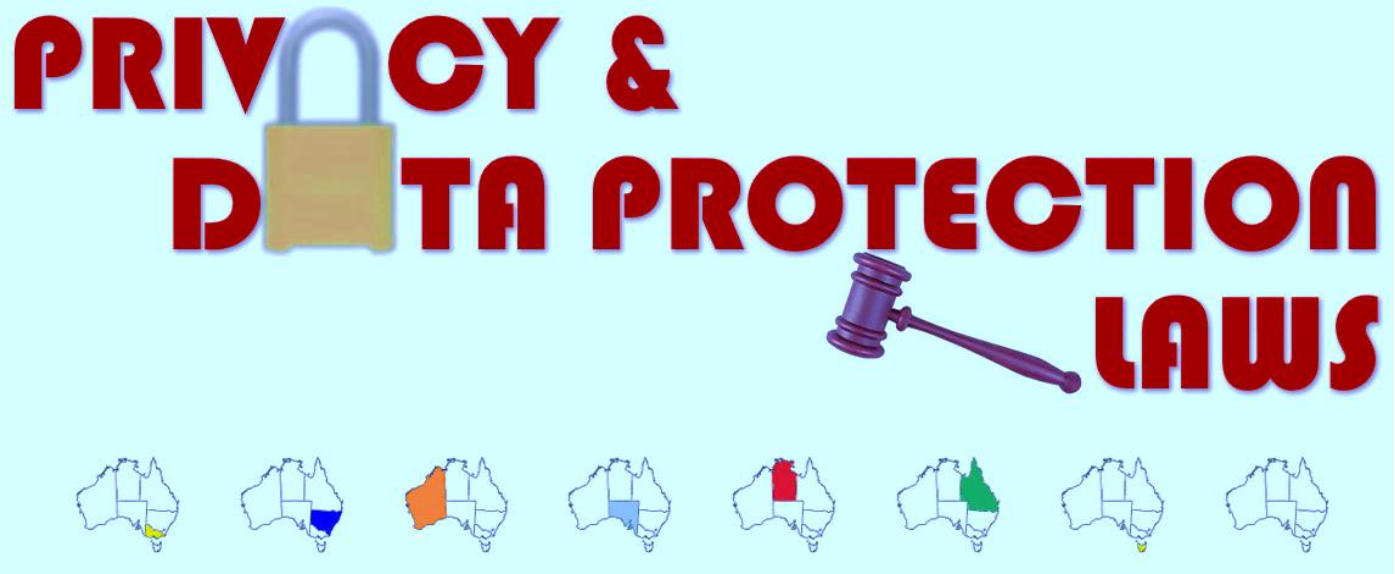


Management System Framework Helps Compliance with the Privacy and Data Protection Laws

1. AN OVERVIEW

Every organisation has an obligation to comply to applicable laws of the state and country or international laws. This article is specifically taken the Australian and its states Privacy and Data Protection Laws. Individuals and organisation have an obligation to assure compliance to applicable laws. Our international readers will have to consider their local, state and country specific applicable Privacy and Data Protection Laws.

The Privacy Laws of Australia and its states are applicable to individuals and organisation operating in all form of industries in Australia. The objective of this article is to familiarise organisations and individuals with

- an understanding to the privacy and data protection laws, and
- to assure compliance applicable in all form of industries.

The Privacy and Data Protection Laws compliance could be part of a certified or non-certified management system. A certified management system would have a formalised, robust and transparent systems and processes that would complement and support an effective outcome for the Privacy and Data Protection Laws.

A recent article 'Statutory and Regulatory Requirements - An Insight and Clarity...' published on 30 September 2019 has information that befits any management system. It illustrates how the legal requirements could be part of a management system. So, taking the Privacy and Data Protection Laws (legal requirements) factor into consideration, QPro Australia recommends organisation to use the guidance given in the 'Statutory and Regulatory Requirements - An Insight and Clarity...' be applied and benefit through the framework of assurance in achieving sustained compliance.

This article briefs a process for the Privacy and Data Protection Laws application in a management system framework. The article gives an overview, information, awareness and understanding to familiarise and summarises the process to ensure compliance by an organisation.

2. GENERAL AWARENESS

We know and have heard a lot about PRIVACY LAWS but how much knowledge and information do you or your organisation have about the Privacy and Data Protection Laws in Australia. The Australian Privacy Laws protect individual's personal information that organisation and other industries may collect and process through their organisation for various reasons. As an individual or an organisation, compliance to Privacy Laws is a must. So, QPro Australia have taken the effort to summarise, demonstrate the application and defined a process to assure compliance of Privacy and Data Protection Laws in a Management System framework.

3. HISTORICAL INFORMATION OF PRIVACY AND DATA PROTECTION LAWS IN AUSTRALIA

Noncompliance to the applicable laws have SEVERE penalties including jail terms. The following are the applicable penalties that were current at the time of publication of this article.

3.1 Implication for Privacy breach, violation, repeat offence

Government have increased penalties for failure to comply with Privacy Act. There are serious and severe implications for personal and data breaches. According to the Office of the Australian Information Commissioner (OAIC), an independent agency and national regulator for privacy and freedom of information within the Attorney General's portfolio.

Harm can include psychological, emotional, physical, reputational or other forms of harm and 'requires an objective assessment, determined from the viewpoint of a reasonable person in the entity's position.

4. PRIVACY AND DATA PROTECTION LAWS - OVERVIEW

4.1 What are Privacy Laws?

The Privacy Act 1988 (Commonwealth) regulates the handling of personal information about individuals. The Privacy Act includes the collection, use, storage and disclosure of personal information. The Commonwealth Privacy Act may be relevant to records held by a non-government organisation, where the organisation's records are not covered by the state or territory's information privacy laws.

The following are the Privacy Laws currently applicable in Australia

1. Commonwealth (Cth) law: Privacy Act 1988 (Cth)
2. Australian Capital Territory (ACT) law: Information Privacy Act 2014 (ACT), Health Records (Privacy and Access) Act 1997 (ACT)
3. New South Wales (NSW) law: Privacy and Personal Information Protection Act 1998 (NSW), Health Records and Information Privacy Act 2002 (NSW)
4. Northern Territory (NT) law: Information Act 2003 (NT)
5. Queensland (Qld) law: Information Privacy Act 2009 (Qld)
6. Tasmanian (Tas) law: Personal Information Protection Act 2004 (Tas)
7. Victorian (Vic) law: Privacy Data and Protection Act 2014 (Vic), Health Records Act 2001 (Vic)
8. South Australia (SA) law: Currently have no legislative scheme for privacy law. South Australia has an administrative direction on handling personal information that binds the public service: PC012 –Information Privacy Principles (IPPs) Instruction, Freedom of Information Act 1991
9. Western Australia (WA): Currently have no legislative scheme for privacy law. Freedom of Information Act 1992

For more information about the privacy of each states in Australia refer to the details on the Office of the Australian Information Commissioner (OAIC) website.

To understand the Privacy Laws, it is important as an organisation or as an individual to know, what is personal information? Office of the Australian Information Commissioner (OAIC) have briefed the details on their website - personal information.

The OAIC office helps individuals and organisation with various information and details required for an organisation including their roles and responsibilities, guidance and advice, tips for good privacy practice and more.

Apart from the basic Privacy Laws listed above there are similar other acts that are either state or territory specifics in Australia. Examples of such laws are;

- Health Records Act
- Telecommunication Act
- Workplace Surveillance Act
- Freedom of Information Act
- And many more

Refer the previous article 'Statutory and Regulatory Requirements' published on 30 September 2019.

For a study purpose, a research was done and did came across this online bulletin that provided a thoughtful commentary on Privacy Law in Australia and privacy reforms. Thought to share with the readers.

4.2 Why is Privacy laws important?

Privacy laws are important in our day to day businesses. It helps organisation to know their responsibilities as to how they process individual's personal information. The privacy laws assure that personal information in today's time are not misused or violated. Any violation and/or failure to comply a legal requirement e.g. federal and/or state laws can jeopardise business integrity, ethics and the consequences may result in a fine or penalty and possibly a custodial sentence for the person or persons responsible or organisation.

So, as an individual and organisation, we need to be aware, understand and comply to the privacy and data protection laws.

4.3 Do privacy laws apply to everyone?

Every organisation big or small, all have a responsibility to assure greater assurance in protecting the privacy of an individual e.g. collection, handling, storing, processing, using, recording, sharing, publishing, correction or disclosure of personal information etc. all aspects of our personal and business processes.

Organisation whose annual turnover exceeds A$3 million in any year since 2001 or if they have a lower annual turnover but are nonetheless a regulated organisation under the Privacy Act. If organisation is subject to the Privacy Act, they must take reasonable steps to protect personal information they hold from misuse, interference and loss, as well as unauthorised access, modification or disclosure (**Data Security Obligation**).

It doesn't mean that small operators and individuals can get away from compliance to the applicable Federal and state Privacy Laws.

To understand the privacy, it can be classified into some separate, but related models:

- Data Protection (Information Privacy) - which involves the establishment of rules governing the collection and handling of personal data such as credit information, medical and government records
- Communication Privacy - which covers the security and privacy of mail, e-mail, telephones and other forms of communication such as public announcements in media, newspaper, journals etc.
- Bodily Privacy - which concerns the protection of individual's physical being against invasive procedures such as genetic tests, drug testing and cavity searches; and

- Territorial Privacy - which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space. This includes searches, video surveillance and ID checks etc.

4.4 How aspects of privacy matters are typically handled in an organisation?

Many businesses these days operate and deliver their products and services locally, nationally or internationally. The organisation has various means to gather individuals or organisation personal information in person, electronically, company website (cookies), auto acceptance of terms and conditions and/or by third-party, supplier chain, contractors and so forth. In some cases, by theft knowingly or unknowingly e.g. online auto information gathering hack, misguiding information, violating the trust and privacy, collection of organisation information and marketing materials, organisation or individuals' intellectual properties by competitors etc.

So, all information that is processed in an organisation of their stakeholders (internal and external) needs to be protected and respected by the organisation. Just like any other legal requirements (statutory and legislative), organisation is obliged to comply the legal requirements including the Privacy Laws.

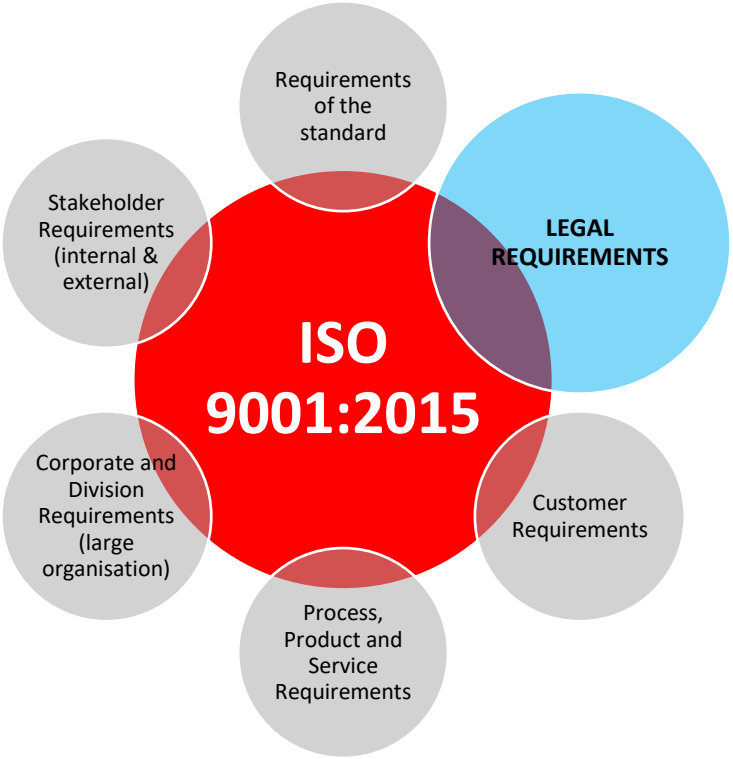
4.5 Integration of privacy law in a management system

Any certified or non-certified management system in an organisation must comply the mandatory legal requirements. Privacy and Data Protection Laws is one of the broader and generic law that is enforced by state and/or federal government. Hence, it becomes part of the business practices.

Organisation have an obligation to assure that they comply to the requirements of Privacy and Data Protection Laws, and their employees are aware, understand, respect and observe the requirements.

So, it makes sense to include and integrate the Privacy and Data Protection Laws (legal requirements) into the management system. A good practice for an organisation is to lead and demonstrate that they are committed, responsible, supportive and practice to ensure that legal requirements are effectively implemented across their business practices. The process involves formal training at all levels. Depending on the type of services the organisation provides, they may consider comprehensive training programs to assure compliance of the legal requirements e.g. Privacy and Data Protection Laws.

The figure below illustrates that the Privacy and Data Protection Laws (legal requirements) is part of the ISO 9001:2015 management system used for demonstration purpose. Legal requirements can be part of any other management systems too.



4.6 Typical examples of Privacy and Data Protection Laws in an organisation

The Privacy and Data Protection Laws covers broadly all aspects of an individual's privacy matters in Australia. For details, refer the links given in the section 4.1. The appropriate privacy and data protection laws applies to business processes and practices. Most business have processes that may have practices like information collection, recording, handling, storage (physically and/or electronically), processing of information, use and share of information, publishing, correcting or disclosing of personal information etc. Some of the typical examples includes e.g.

1. Collection and recording of private information through various medium for the scope of the topics by businesses or individuals or entity. Source examples such as
    - Forms (hardcopy or electronic) - various
    - Internet gathered information
    - Health and safety records | Medical reports
    - Personnel file
    - Employment records
    - Data and information recorded electronically
    - Voice recording devices
    - Mobile phones, computer, laptops and similar electronic equipment
    - Outsourced agents or organisation used by the organisation
    - Online and web-based recorder
    - Electronic notes
    - Telephone conversation and voice recording
    - Webcam recording | Video and audio conference recording
    - Statistical data and information | Survey results
    - Travel documents | Itinerary | Hotel stay | Business and personal credit cards
    - Voluntary jobs | Internship | Temporary & permanent staffs | Casuals | Contractors
    - Sporting events | entertainment & industrial events | commercial exhibitions…
    - Video, audio and photographic evidences | Filming
    - CCTV | Monitoring devices…
    - Assessment reports and notices
    - Invoices | Statements | Purchase orders | Contract orders | Agreements – various
    - Terms and conditions
    - Internal and external records management e.g. training records, source information
    - Business cards, contact details
    - Business travel and expenses
    - Sponsors details and contents
    - Tracking devices
    - Financial information
2. Handling of private information. Source examples such as
    - Processing of information through internal and/or external systems
    - Security and access levels
    - Confidentiality
    - Legible, transparent and accurate
    - Authority and responsibility defined
    - Sensitive and private information | Confidential & classified
    - Process and training materials
    - Research and development
    - Survey and data analysis
    - Identity fraud
3. Processing of private information. Source examples such as
    - How information is processed in a secure manner
    - Access levels (security and confidentiality)

- Think about who, what, why, where, when… before the information is processes
- Scope and applicability
- Users are trained, coached, aware of privacy laws, conduct information sessions etc.
- Passwords and login
- Management of information (internal and external)
- Information technology
- Equipment and user security
- Travel documents | Itinerary | Hotel stay | Business and personal credit cards
- Processing of information by personnel (internal and external)
- Confidential agreements by processors
- Office & location safety and security
- Access to cleaners, contractors (afterhours)
- Business ethics and practices
- Housekeeping rules working with sensitive and confidential information
- Identity theft due to weak processes and systems
- Lost or stolen data
- Handout of information to the wrong person (accidental or intentionally)
- Lack of mandatory guidelines and agreements (safety and security) for use of equipment e.g. laptops, vehicles, mobile phones, electronic gadgets, websites etc.

4. Storage of private information. Source examples such as
   - As hardcopy or electronically maintained (website, intranet, internet, extranet, record safe etc.)
   - Access to storage locations
   - Fire and water safe
   - Only authorised person access
   - Retrievable for audit, assessments, individuals right etc.
   - Database, public domain, cloud storage etc.
   - Standalone computers and laptops
   - Company mobile phones or similar electronic devices
   - Servers (onsite, offsite, remote…)
   - Intellectual property
   - Archives (physical and electronic)
   - Low level security encryptions & firewalls
   - Users are incompetent
   - Access to cleaners, contractors (afterhours)
   - Easy access to sources e.g. storage facilities, online login, cabinets, unlocked areas…
   - Use of public venues and locations to access information (potential business risks)
5. Using and sharing of private information. Source examples such as
   - Personal information is accessed or disclosed
   - Sharing electronically or as hardcopy with internal and external stakeholders
   - Agency or entity working for an organisation
   - Forwarding information between organisation
   - Transfer of information when an organisation is acquired
   - Records sharing in private and public domain
   - Minimum or no security and confidentiality protocols
   - Easily available
   - Local drives with access (organisation is unaware of it)
   - Poor management of information
   - Noticeboards, newsletters, marketing materials…
   - Employees sharing information through personal contacts and electronic means in social media world (intentionally or unknowingly)
   - Lack of formalised training and awareness to users/stakeholders

- Faxing and emailing of private information without encryptions
- Sending attachments that may contain sensitive and confidential information
- Use of public Wi-Fi systems to login (potential risk to business)
- Use of laptops and other electronic devices in public zones e.g. airports, hotels, restaurants, parks (desktop on the go have associated risks)
- Workshops, seminars and presentation done in public venues
- Sharing of login details including password with team or individuals (business risks)
- Unsecured portals and devices

6. Publishing of private information including personal data. Source examples such as
   - Organisation newsletter, website, intranet, internet, extranet, database
   - Public newspaper, journals, magazines, books
   - Social media e.g. Facebook, LinkedIn, Twitter, WhatsApp…
   - Conference, seminar, workshops, presentation, webinar etc.
   - Video and audio conference
   - Security breach and/or system hack (weak firewalls and encryptions)
   - Faxing and emailing of private information without encryptions
7. Correcting of private information. Source examples such as
   - Falsifying or fabricated information
   - Incorrect information
   - Defamation due to incorrect information that caused harm
   - Intentional or unintentional use of information
   - Data and information correction electronically
   - Systemic error during processing that may cause harm
   - Untrained personnel
   - Obsolete information
   - Security breach
   - IT system hack
   - No security or antivirus
   - Sharing of login details causing harm

Think of the applicability and scope for the information gathered by an organisation or individual or entity. It is no point in regretting later, if there is a serious breach of the conduct or violation to observe individuals' private information. The above practices are at bear minimum regular and routine observations. So, organisation, entity and individuals need to be aware, always understand and maintain safe practices in the management of personal and data information system. Ignorance is not an excuse in the event of a noncompliance or breach of Privacy and Data Protection Laws.

Depending on the type of business an organisation operates, it is crucial to have right measures in place and recommend operating an appropriate management system to safeguard the data, information and security of your customers, individuals, products and services.

To some businesses the Privacy and Data Protection Laws are critical due to the nature of products and services they offer to their clients e.g. medical, banking, information technology (IT), social security, sporting events, telecommunication, financial institutions, education departments, taxation departments, consultancy firms operating for security and high-tech industries, airport business, travel and hotel industry, entertainment industry, utility businesses etc.

4.7 Why would a management system help?

Management system framework brings in a discipline and formalises the processes of the organisation and ensures that applicable legal requirements are reviewed, assessed and complied through this formal process. Why take a chance of being ignorant or apply on a need basis? This would potentially be a risky way to operate a business.

Organisation operating a certified management system(s) have benefited directly or indirectly through certification process. There are several benefits for an organisation who have implemented, certified and maintained an effective management system. Read some of the articles published by QPro Australia.

Just like any legal requirements, a formalised management system framework would ensure that Privacy and Data Protection Laws are effectively developed and implemented. This process ensures that organisation would deliver with confidence the best possible products and services to their customers. It also assures and demonstrates best practices in a competitive and challenging environment. In return, organisation would sustain effective business practices, develop business growth, improve stakeholder's relationship, promote brand reputation, protect intellectual property and more.

A formalised management system also ensures that all business records are effectively maintained. This is vital information that organisation requires to retain records both hardcopy and/or softcopy (electronics).

4.8 Key aspects of a management system consideration

Any national or international management system standards have the basic consideration as illustrated in the figure at section 4.5

The management system standard requires the organisation to meet the following at minimum such as;

- Identify interested parties or stakeholders
- Top management and leadership commitment and support
- Purpose and scope of the management system
- Perform risk management (system, process, products, services, safety, environment, business processes, supplier and contractor risks etc.)
- To develop documented information required by the standard, organisation determined*, legal and regulatory requirements, customers etc. (*organisation specific including operational & service specific + supplier & contractor specific documents + corporate specific – if any)
- Training (coaching, mentoring and training) at all levels
- Supplier and contractor management system
- Implemented system works on a Plan-Do-Check-Act (PDCA) model
- Ensure systems and processes are audited regularly
- Corrective actions are taken when deviations and/or nonconformity is evident
- Ongoing management review
- Encourage continuous improvements
- And many more assurance

4.9 Which management system is relevant to your business?

There are several types of international and national management systems that could be implemented and certified to assure your customers with greater confidence in your system. The type of applicable management system could vary on various factors e.g. organisation needs, customer requirements, contract requirements, business commitments etc.

Immaterial of which management system, an organisation implements; the legal requirements would be part of the management system framework. Hence, a transparent system with clear pathway to all users of the management system.

The process would involve steps such as identifying the gaps, develop a plan, implement the process and certify to appropriate management systems to effectively manage their systems and processes. For additional guidance, organisation have the opportunity to consult their management system professionals or contact QPro Australia for assistance.

The author has series of articles published that may be of interest to organisation. Some of the articles may assist and guide the reader in the selection and the decision process of the management systems applicable to your organisation. Here is the link to the published articles on LinkedIn.

5. CONCLUSION

Be safe and take ownership of your business by doing the right thing. There is no easy way out.

The future is quite challenging in the digital world. To maintain business processes and practices effectively needs sustained commitment and support. Realise that all organisation has accountabilities to perform their best and this could be demonstrated through their leadership and commitment.

So, it's up to an organisation to decide, commit and lead the way for the best in the challenging and competitive world.

QPro Australia can assist organisation in the development and implementation of the legal requirements in the management systems and processes. The services can include training and coaching of personnel at all levels, audit and verify effectivity per management systems requirements.

6. SOURCE REFERENCES

- Office of the Australian Information Commissioner (OAIC)
- Communications and Media Law Association (CAMLA)
- For research purposes: Australasian Legal Information Institute
- Online resource links to respective federal and state legislation laws at section 4.1 of this article.

This information is intended to provide the reader and the organisation, a brief awareness and an overview of the Privacy and Data Protection Laws, it's mandatory obligation and compliance. The article is a guidance to assure that organisation with or without a management system certification must proactively support and comply as part of their business practices. The details and references in this article about the Privacy and Data Protection Laws (legal requirements and information) are current at the time of publication. The contents of this document should not constitute legal advice and legal advice should be sought as required.