Module	**PRIVACY AND DATA PROTECTION**
Jurisdictions	**CTH, NSW, VIC, SA, TAS, WA, NT, QLD, ACT**
Legal Expert	**DUDLEY KNELLER** Partner at Gadens https://www.gadens.com/people/dudley-kneller/ https://au.linkedin.com/in/dudleykneller

Module Application

Is the organisation responsible for managing personal or confidential information?

Does the organisation conduct general or workplace surveillance?

Does the organisation have appropriate policies in place for ensuring workplace privacy (i.e. employee records, employee spent convictions and employees' use of email or internet)?

Module Scope

The PRIVACY AND DATA PROTECTION module informs the private sector organisation and the public sector agency of their legislated legal privacy and data protection obligations. The module also demonstrates effective practical advice and assistance to the entity operating in Australia to implement procedures and processes that will ensure compliance and regulatory accountability throughout all levels of the organisation.

The PRIVACY AND DATA PROTECTION module advises private sector organisations and public sector agencies of the processes and procedures they need to implement to ensure compliance with all legal and regulatory privacy and data protection obligations. Core legal and regulatory obligations are based on considerations of the broad questions determining;

- decision making;
- accountability;
- stewardship;
- direction; and
- control.

To fulfil its purpose the module focuses on providing practical assistance to the organisation establishing and maintaining a robust foundational framework that determines;

- how the systems and processes will function;
- who is the responsible decision maker;
- what matters are relevant to the decision-making process; and
- whether the desired outcome has been achieved.

Private sector organisations and public sector agencies are all expected to be familiar with the broad landscape of legal obligations to which they are subject as well as more specific obligations relevant to the particular sector they are operating in. The PRIVACY AND DATA PROTECTION module should be subscribed by all private and public sector organisations, their employees and authorised individuals. The aim of the module is to equip the subscriber with knowledge of their obligations related to;

- personal information;
- confidential information;
- surveillance; and
- workplace privacy.

and the skills they require to establish relevant systems and processes to ensure compliance throughout the organisation.

The PRIVACY AND DATA PROTECTION module covers federal, state and territory privacy and data protection obligations related to;

- the management of personal information for private sector organisations and public sector agencies;
- the handling of confidential information and communications;
- general and workplace surveillance; and
- workplace privacy (employee records, employee spent convictions and employees' use of email and the internet).

Not all private sector organisations or public sector agencies will be required to comply with data privacy laws, so the module also covers;

- the types of private sector organisations and public sector agencies to which these laws apply;
- which laws apply to which organisations and agencies;
- what constitutes personal and sensitive information (if the organisation or agency is not handling personal or sensitive information then data privacy laws will not apply to them); and
- which acts and practices are exempt from data privacy laws.

The broad scope of the PRIVACY AND DATA PROTECTION module is to provide answers to these questions;

- what are our legal obligations?
- from where are our legal obligations derived?
- how can we ensure that we are complying with our legal obligations?
- what are the consequences if we are not complying with our legal obligations?

The PRIVACY AND DATA PROTECTION module covers all legislated legal obligations of private sector organisations and public sector agencies and demonstrates practical assistance and guidance to ensure that these obligations are complied with through the implementation and maintenance of best practice processes throughout the organisation. The module also covers the role of the regulator as well as exemptions to the obligations, if applicable, and how they may or may not apply in particular circumstances.

The module fulfils this objective by comprehensively covering three main areas;

1. The expansive legislative and regulatory landscape from which the primary legal obligations are derived;

Commonwealth legislation

- Archives Act 1983 (Cth);
- Crimes Act 1914 (Cth);
- Criminal Code Act 1995 (Cth);
- Do Not Call Register Act 2006 (Cth);
- Freedom of Information Act 1982 (Cth);
- Privacy Act 1988 and Privacy Regulation 2013 (Cth);
- Privacy (Tax File Number) Rule 2015 (Cth);
- Spam Act 2003 (Cth);
- Surveillance Devices Act 2004 (Cth);
- Taxation and Administration Act 1953 (Cth);
- Telecommunications Act 1997 (Cth);
- Telecommunications (Interception and Access) Act 1979 (Cth); and
- Telemarketing and Research Industry Standard 2007 (Cth).

State and Territory legislation

- Criminal Code 2002 (ACT);
- Spent Convictions Acts and Regulations (ACT 2000), (SA 2009, 2011), (WA 1988 & 1992), (NT 1992, 1993);
- Annulled Convictions Act 2003 (TAS);
- Criminal Law (Rehabilitation of Offenders) Act 1986 (QLD);
- Criminal Records Act 1991 and Regulations (2014) (NSW);
- Freedom of Information Acts and Regulations (ACT 1989 & 1991), (WA 1992 & 1993);
- Information Privacy Acts and Regulations (ACT 2014), (QLD 2009);
- Listening and Surveillance Devices Acts and Regulations (ACT 1992), (TAS 1991, 2014), (SA 1972, 2003); (NSW 2007), (NT 2007 & 2008), (VIC 1999 & 2016), (WA 1998 & 1999);
- Privacy and Personal Information Protection Act 1998 and Regulations (2014) (NSW);
- Privacy Code of Practice (General) 2003 (NSW);
- Government Information (Public Access) Act 2009 (NSW);
- State Records Acts (NSW 1998), (SA 1997), (WA 2000);
- Workplace Surveillance Act 2005 and Regulations 2017 (NSW);
- Information Act 2002 (NT);

- Invasion of Privacy Act 1971 (QLD);
- Information Privacy Principles (IPPS) Instruction 2016 (SA);
- Personal Information Protection Act 2004 (TAS);
- Privacy and Data Protection Act 2014 (VIC);
- Public Sector Management Act 1994 (WA);
- Public Administration Act 2004 (VIC);
- Victorian Protective Data Security Standards 2016 (VIC);
- Public Records Acts (QLD 2002), (VIC 1973);
- Right to Information Acts (QLD 2009), (TAS 2009);
- Freedom of Information Acts and Regulations (SA 1991, 2018) (VIC 1982);
- Archives Act 1983 (TAS);
- Ombudsman Act 1978 (TAS);
- Tertiary Records Act 2002 (ACT); and
- Workplace Privacy Act 2011 (ACT).

2. The specific areas where privacy and data protection legal and regulatory obligations apply to the particular entity.

The applicability of data privacy laws;

- Federal data privacy laws;
- State and territory data privacy laws;
- Personal and sensitive information; and
- Acts and practices covered by data privacy laws.

Organisational governance;

- Leadership, governance and culture; and
- Systems and processes.

Openness and transparency;

- Privacy policy; and
- Provision of information on request.

Collecting personal and sensitive information;

- Collection by private sector organisations and public sector agencies;
- Unsolicited information;
- Methods of collection; and
- Notification of collection.

Enabling anonymity and pseudonymity;

- Using and disclosing personal information and identifiers;

- Government related identifiers;
- Tax-file numbers; and
- Direct marketing.

Overseas and interstate cross-border transfers of personal information into and out of Australia;

- Ensuring the quality of personal information records before use or disclosure;
- Managing the protection and secure disposal of personal information;
- Enabling individuals to access and correct their personal information;

Managing complaints and investigations;

- Internal complaint system;
- External complaint system;
- Complying with investigations; and
- Enforceable orders and directions.

Keeping confidential information and communications confidential.

Surveillance;

- Listening devices;
- Optical devices;
- Tracking devices; and
- Data.

Workplace privacy;

- Employee records exemptions;
- Employee spent convictions; and
- Access to email and internet.

Complying with payment card industry data security standards;

- Firewalls;
- Use of vendor supplied defaults;
- Protecting stored cardholder data;
- Encrypting transmissions across public networks;
- Malware and anti-virus software;
- Developing and maintaining secure systems and applications;
- Restricting access to cardholder data;

- Identifying and authenticating access to system components;
- Restricting physical access to cardholder data;
- Tracking and monitoring access;
- Regularly testing systems and processes;
- Maintaining an information security policy; and
- Assessing and reporting on compliance.

3. Significant consequences can apply to private sector organisations and public sector agencies, their employees and authorised individuals found to have breached or not complied with their legal obligations. These consequences vary considerably depending on the nature and extent of the breach or failure. The PRIVACY AND DATA PROTECTION module covers specific consequences in detail. They can include monetary penalties, disciplinary measures and even terms of imprisonment for individuals found to have committed serious criminal offences.

In all jurisdictions except Western Australia, an individual who feels that an organisation or agency has not complied with data privacy laws, by misusing or disclosing their personal information, may make a complaint to the organisation or agency itself. If the individual is not satisfied with the response provided by the organisation or agency, depending on the jurisdiction, the person may take the complaint to a dispute resolution scheme or to a civil and administrative appeals tribunal and/or to the relevant federal, state or territory privacy commissioner or ombudsman.

The PRIVACY AND DATA PROTECTION module covers core federal, state and territory privacy and data protection obligations of private sector organisations and public sector agencies in relation to;

- the management of personal information;
- the handling of confidential information and communications;
- general and workplace surveillance; and
- workplace privacy.

The PRIVACY AND DATA PROTECTION module does not cover industry specific privacy and data protection obligations. Industries such as health, telecommunications and credit reporting have specific privacy and data protection obligations. These types of industry specific obligations are not covered by the module.

About LexisNexis Regulatory Compliance

LexisNexis Regulatory Compliance® helps you forge a clear path to compliance.

With LexisNexis® content know-how at the core, our compliance registers, alerts, and information-driven solutions make compliance uncomplicated for GRC professionals across the globe.