LexisNexis® | *Regulatory Compliance*

API Integration Guide

Prepared by Mary Wong
Version V1.10
Date 21/05/2024

Table of Contents

Document Control

Document Author	**Mary Wong**
Document Date	**21/05/2024**
Current Version	**1.10**
Document Title	**API Integration Guide**

Document Revisions

Date	Version	Author	Comments
22/03/16	1.0	Mary Wong	Document Distribution
12/04/16	1.1	Mary Wong	Document redistribution
06/07/16	1.2	Mary Wong	Document redistribution
08/03/17	1.3	Mary Wong	Document redistribution
31/8/17	1.4	Mary Wong	New parameter – International Jurisdictions Document redistribution
18/9/17	1.5	Mary Wong	Corrected the from_date parameter format
10/02/20	1.6	Mary Wong	New field – jurisdictions on tools New field – historical_note on obligations
02/02/21	1.7	Mary Wong	Minor corrections and updates to reflect the recommendations from the process review
2/12/21	1.8	Mary Wong	New filters on the content endpoint
28/11/22	1.9	Mary Wong	New parameter for csv output file
21/05/24	1.10	Mary Wong	New fields on modules

Overview

Purpose

The purpose of this document is to provide the REST APIs implementation methods which provide programmatic access to read LexisNexis subscription data by API customers.

Background

A REST API will be provided and expose the endpoints for API customers with active subscriptions. They will retrieve this subscribed content in our format. The customer will then take this content and consume it, serving it using their system of choice. Token-based authentication will be used and a session token will be initialised after successfully authenticating the API client account. All sequential functions require the new established session token to be passed in the method to proceed.

Connection

Using an email and password pair, the user can authenticate and access the functions listed below.

The APIs will include the following functions:
1. User Authentication
2. User Subscriptions
3. Subscribed Contents
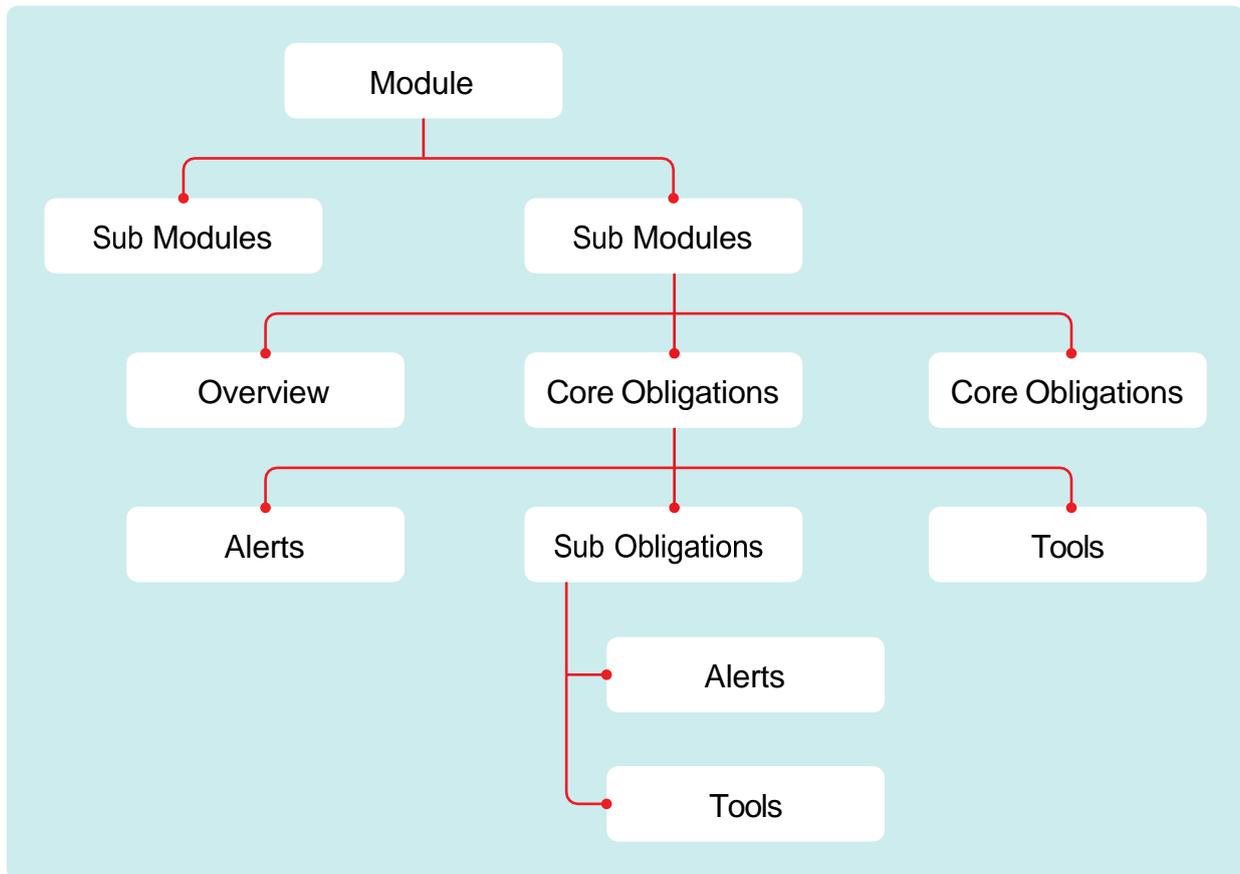4. Get Single Subscribed Content

Module Structure

Fig 1 Model Structure

Module Components

Each module is made of the following components:

Sub Modules
A module can have multiple submodules to group business activities, entity types, etc

Overview
Each module has only one overview record which basically gives an overview to the module outlining scope and coverage

Core Obligations
A core obligation represents a compliance area for the module and each module would have multiple core obligations.

Sub Obligations
A sub obligation represents specific actions an organisation must undertake in order to comply with the compliance sources, attestations are usually done against sub obligations. Each core obligation would have multiple sub obligations.

Tools
A tool is something that can assist the user with to comply an obligation; it is usually a checklist, template, flowchart or hyperlink to external government sites. A core obligation or sub obligation can have multiple tools and each tool can be associated with multiple obligations.

Alerts

An alert record is created every time there is a proposed or actual change in the compliance source relevant to the module. As the alerts are dependent on changes to the compliance source there is no set publishing schedule it is as changes are announced. There are 3 types of alerts:

- FYI – the user needs to be made aware of the change or upcoming change
- Action Required – the user needs to take action to ensure they remain compliant
- News – the user is provided a list of new or updated obligations and the related alerts that were published throughout the month. A News alert is also used to notify the user of a change to the penalty units (usually only annually) this would be linked to the Overview record.

New obligations and updates to existing obligations are published once a month – on the second Tuesday of each month (if that fall on a public holiday the next business day) note that an updated obligation record can include one that has been archived i.e. the obligation is no longer applicable. A core obligation or sub obligation can have multiple alerts and each alert can be associated with multiple obligations.

Fields within each module component

	Overview	Core Obligation	Sub Obligation	Tool	Alert
Id	X	X	X	X	X
Title	X	X	X	X	X
Archived	X	X	X	X	X
Practical_guidance	X	X	X		
Remedial_action	X	X	X		
Consequence	X	X	X		
Due_date	X	X	X		
Frequency	X	X	X		
Description_directional	X	X	X		
Description_questional	X	X	X		
Compliance_source	X	X	X		X
Definition	X	X	X		
Excerpt	X	X	X		
Sequence_id	X	X	X		
Parent_id	X	X	X	X	X
Jurisdictions	X	X	X	X	X
Historical_note	X	X	X		
Link				X	
Ext_link				X	
Category				X	
Type					X
Description					X
effectiveDate					X
Impact_on_obligation					X

Functions

User Authentication

Title	Authtoken User authentication and obtaining token. This function validates the email and password of an API user account and returns a token for the API client to establish connectivity. The system allows the usage of a token for accessing the rest of API functions in a certain period of time (24 hours by default).
URL	http://compliance.store.lexisnexis.com.au/rest/api/v1.1/authtoken
Method	GET

URL Params	Required:
	• email=[string]
	  example: email=test@lexisnexis.com.au
	• password=[string]
	  example: password=lntest1234
	
	Optional:
	• format=[json|xml]
	  example: format=xml
	  if format is not specified, JSON will be returned.

Success Response	Content in JSON: <code>{</code> <code>"token":"f563fb84f4b170413bae56b261a6fbd1",</code> <code>"customer_id":"9",</code> <code>"sq_api_user":true,</code> <code>"success":true</code> <code>}</code> Content in XML: <code><LexisNexisRI xmlns="http://www.lexisNexis.org" version="1.1"></code> <code><AuthtokenResponse></code> <code><token>f563fb84f4b170413bae56b261a6fbd1</token></code> <code><customer_id>9</customer_id></code> <code><sq_api_user>true</sq_api_user></code> <code><success>true</success></code> <code></AuthtokenResponse></code> <code></LexisNexisRI></code>

Error Response	Content in JSON:
	``
	{
	success: false,
	errorCode: xxxx,
	error: "Wrong email or password",
	sq_api_user: false
	}
	``
	
	Content in XML:
	``
	<LexisNexisRI xmlns="http://www.lexisNexis.org" version="1.1">
	<AuthtokenResponse>
	<success>false</success>
	<errorCode>xxxx</errorCode>
	<error>Wrong email or password</error>
	<sq_api_user>false</sq_api_user>
	</AuthtokenResponse>
	</LexisNexisRI>
	``

Sample Call	`curl http://{site_url}/rest/api/v1.1/authtoken?email=apiuser@test.` `com\&password=mypassword`

User Subscription

Title	Subscriptions This function returns the active subscriptions for the user account.
URL	http://compliance.store.lexisnexis.com.au/rest/api/v1.1/subscriptions
Method	GET

URL Params	Required:
	• token=[string]
	  example: token=b4684ce3-ca5b-477f-8f4d-e05884a83d3c
	• customer_id=[integer]
	  example: customer_id=12
	
	Optional:
	• format=[json|xml]
	  example: format=xml
	  if format is not specified, JSON will be returned.

Success Response	Content in JSON:

```
subscriptions: [
{
profile_id: "7",
customer_id: "29",
total_delegations: "1",
last_api_contact: "2016-04-13 01:05:20",
delegations_remaining: "0",
product_id: "1391",
status: "1",
ln_sku: "4565",
type_id: "bundle",
name: "Private Health Insurance - Test",
is_core_module: false,
is_delegated: false,
is_free: false,
bundle_ln_skus: [
"4570"
],
delegations: [ ]
},
success: true
}
```

Content in XML:

```
<LexisNexisRI xmlns="http://www.lexisNexis.org" version="1.1">
<AuthtokenResponse>
<subscriptions>
<profile_id>7</profile_id>
<customer_id>29</customer_id>
<total_delegations>1</total_delegations>
<last_api_contact>2016-04-13 01:05:20</last_api_contact>
<delegations_remaining>0</delegations_remaining>
<product_id>1391</product_id>
<status>1</status>
<ln_sku>4565</ln_sku>
<type_id>bundle</type_id>
<name>Private Health Insurance - Test</name>
<is_core_module>false</is_core_module>
<is_delegated>false</is_delegated>
<is_free>false</is_free>
<bundle_ln_skus>4570</bundle_ln_skus>
<delegations/>
</subscriptions>
<success>true</success>
</AuthtokenResponse>
</LexisNexisRI>
```

Error Response	Content in JSON:
	``
	{
	success: false,
	errorCode: 1001,
	error: "Empty customer id or token. customer id: , token: "
	}
	``
	
	Content in XML:
	``
	<LexisNexisRI xmlns="http://www.lexisNexis.org" version="1.1">
	<AuthtokenResponse>
	<success>false</success>
	<errorCode>1001</errorCode>
	<error>Empty customer_id or token. customer_id: , token:</error>
	</AuthtokenResponse>
	</LexisNexisRI>
	``

Sample Call	``` curl http://{site_url}/rest/api/v1.1/ subscriptions?format=xml&token= {token}&customer_id={customer_id} ```

Subscribed Contents

Title	Contents • This function returns the content of the subscription based on the user specified subscription id. • The content can contain one subscribed module or multiple subscribed modules. • The function allows API client to specify whether the response will return full content or updated content from the specific date.
URL	http://compliance.store.lexisnexis.com.au/rest/api/v1.1/contents
Method	GET
URL Params	Required: • token=[string] example: token=b4684ce3-ca5b-477f-8f4d-e05884a83d3c • •customer_id=[integer] example: customer_id=12 • •page=x example : page = 1

URL Params	Optional:
	• format=[json|xml]
	  example: format=xml
	  if format is not specified, JSON will be returned.
	• bom=true - only for csv output file in order for BOM character to be included
	• from_date=ddMMMyyyy
	  example: from_date=24FEB2015
	• end_date=ddMMMyyyy
	  example: end_date=28FEB2015
	• jurisdictions=[jurisdiction]
	  example: jurisdictions=NSW|VIC
	  where multiple jurisdictions is specified use "|" between each value
	
	Note: The below shows how many pages there are in total and you can add the page endpoint to specify the page to download.

```
{
  - results: {
        page: 1,
        items_per_page: 5,
        num_pages: 5,
        total_items: 26,
        isSuccess: true,
  - modules: [
        - {
```

Success Response	Content in JSON:
	`{`
	`results: {`
	`page: 1,`
	`items_per_page: 5,`
	`num_pages: 5,`
	`total_items: 28,`
	`isSuccess: true,`
	`modules: [`
	`{`
	`id: "7161",`
	`title: "Privacy & Data Protection",`
	`date_created: "20160303102242",`
	`date_changed: "20161221110905",`

Success Response

```
lineage: "7161",
archived: "FALSE",
keywords: "",
type: "module",
description: "<p>Regardless of which industry you are in, privacy
and data protection issues affect us all. The Privacy and Data
Protection module identifies your compliance obligations on how to
collect, manage and maintain personal information securely and
within the Australian legal framework.</p>",
is_core: "true",
apiOnly: "",
hot: "false",
banner: "https://compliance.store.lexisnexis.com.au/__data/assets/
image/0009/14958/1600x500px-privacy.jpg",
bannerAlt: "Privacy & Data Protection Banner",
topicListDescription: "",
coreModuleListDescription: "",
sequence_id: 6,
country: [
"Australia"
],
Industry: [
"All Industries"
],
topics: [
{
id: "7211",
title: "Privacy and Data Protection",
date_created: "20160303105617",
date_changed: "20161221110919",
lineage: "7211|7161",
archived: "FALSE",
keywords: "",
type: "topic",
description: "<p>Click here to view obligations for the Privacy
&amp; Data Protection module.</p>",
sequence_id: "1",
module_id: "7161",
hot: "false",
parent: {
id: "7161"
},
obligations: [
{
id: "8364",
title: "Privacy & Data Protection Overview",
date_created: "20160326144334",
obligations: [
{
id: "8364",
title: "Privacy & Data Protection Overview",
date_created: "20160326144334",
date_changed: "201701231112551",
lineage: "8364|7211|7161",
archived: "FALSE",
keywords: "",
type: "obligation",
practical_guidance: "<p>The Privacy &amp; Data Protection module
```

covers federal, state and territory privacy obligations in relation to:</p>
The management of personal information for private sector organisations and public sector agencies
The handling confidential information and communications
General and workplace surveillance
Workplace privacy (employee records, employee spent convictions and employees’ use of email and the internet)
<p>Note: the Privacy & Data Protection module does not cover industry-specific privacy obligations. This means that it does not cover privacy obligations for industries such as health, telecommunications or credit reporting.</p><p>Managing personal information under data privacy laws</p><p>Data privacy laws cover the management of personal information by private sector organisations and public sector agencies. Obligations under these laws are set out in federal, state and territory Acts, Regulations and instructions, including:</p>
Commonwealth: Privacy Act 1988 (Cth), Privacy (Tax File Number) Rule 2015 (Cth), Do Not Call Register Act 2006 (Cth), Spam Act 2003 (Cth) and Taxation Administration Act 1953 (Cth)
Australian Capital Territory: Information Privacy Act 2014 (ACT) and Territory Records Act 2002 (ACT)
New South Wales: Privacy and Personal Information Protection Act 1998 (NSW), State Records Act 1998 (NSW) and Privacy Code of Practice (General) 2003 (NSW)
Northern Territory: Information Act 2002 (NT)
Queensland: Information Privacy Act 2009 (Qld) and Public Records Act 2002 (Qld)
South Australia: Information Privacy Principles (IPPS) Instruction (SA), Freedom of Information Act 1991 (SA) and State Records Act 1997 (SA)
Tasmania: Personal Information Protection Act 2004 (Tas), Right to Information Act 2009 (Tas) and Archives Act 1983 (Tas)
Victoria: Privacy and Data Protection Act 2014 (Vic), Freedom of Information Act 1982 (Vic) and Public Records Act 1973 (Vic)
Western Australia: Freedom of Information Act 1992 (WA), Freedom of Information Regulations 1993 (WA) and State Records Act 2000 (WA), as well as non-mandatory guidelines. See Tools — Management of personal information
<p>Applicability of data privacy laws</p><p>Not all private sector organisations or public sector agencies will be required to comply with data privacy laws. As such, this module discusses:</p>
The types of private sector organisations and public sector agencies to which these laws apply
Which laws (federal or state/territory) 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
Which acts

and practices are exempt from data privacy laws
<p>If data privacy laws apply to the organisation or agency and to its acts and practices, the organisation or agency will generally be required to comply with the following obligations. Note: the extent to which these obligations apply to an organisation or agency vary between jurisdictions.</p><p> </p><p>Organisational governance</p><p>The organisation or agency and its chief executive officer have responsibilities to ensure that the organisation’s or agency’s policies, systems and procedures comply with relevant privacy laws. Recommended approaches to ensuring compliance with this obligation include undertaking privacy impact assessments; ensuring that privacy issues are included in processes and systems from the outset, according to privacy by design principles; and developing a data breach response plan.</p><p>Open and transparent management of personal information</p><p>The organisation or agency must be open and transparent about how it handles personal information. In many jurisdictions, this requires the organisation or agency to have a clearly expressed and up-to-date privacy policy that is publicly available. In addition, agencies are required to ensure that, upon request, an individual is provided with information about how privacy is handled. Agencies must also provide a person with access to information held about the person in accordance with applicable privacy and freedom of information laws.</p><p>The collection of personal and sensitive information</p><p>The organisation’s or agency’s collection of personal and sensitive information about an individual must be relevant to its functions and activities. The organisation or agency must use lawful and fair methods for collection, collect the information directly from the individual and ensure the individual is aware of the collection, unless the relevant data privacy laws allow an exception to these requirements. In addition, the organisation or agency must also comply with rules regarding the collection of tax file number information.</p><p>Anonymity and pseudonymity</p><p>An organisation or agency that is required to comply with federal, Australian Capital Territory, Northern Territory, Tasmanian or Victoria data privacy laws must allow individuals to remain anonymous during transactions unless it is unlawful or impracticable to do so.</p><p>In addition, an organisation or agency that is required to comply with federal or Australian Capital Territory data privacy laws must allow an individual to use a pseudonym unless it is impracticable to do so.</p><p>Using and disclosing personal information</p><p> </p><p>An organisation or agency must comply with the relevant privacy laws regarding the use or disclosure of:</p>
Personal and sensitive information — all jurisdictions except

Western Australia
Government-related identifiers — Commonwealth, Australian Capital Territory, Northern Territory, Tasmania and Victoria
Tax file numbers — all jurisdictions
Personal information for direct marketing purposes — Commonwealth, Australian Capital Territory and Queensland jurisdictions
<p>Cross-border transfers of personal information</p><p> </p><p>An Australian organisation or agency must comply with the relevant data privacy laws that restrict the disclosure or transfer of personal information about individuals to a recipient who is:</p>
overseas — Commonwealth, Australian Capital Territory and Queensland, or
outside the organisation’s or agency’s own state or territory — New South Wales, Northern Territory, Tasmania and Victoria
<p>In addition, if an Australian organisation or agency is the recipient of personal information, including sensitive information, about individuals located overseas, the organisation or agency must be aware of international and foreign data privacy laws that may apply to the personal information it receives.</p><p>Ensuring the quality of personal information</p><p>Under data privacy laws of all jurisdictions, except Western Australia, the organisation or agency must take reasonable steps to ensure that personal information is:</p>
Accurate — all jurisdictions
Up-to-date — all jurisdictions
Complete — all jurisdictions, and
Relevant — all jurisdictions except the Northern Territory and Victoria
<p>In Western Australia, the Ombudsman has issued guidelines that recommend public sector agencies ensure that personal information is accurate, current, complete and not misleading.</p><p>Ensuring the security of personal information </p><p> </p><p>An organisation or agency must ensure the security of personal information — including sensitive information and tax file number information — by protecting the information, managing security incidents, and securely disposing of the information when it is no longer needed.</p><p>In Western Australia, these obligations are not mandatory but are detailed in guidelines issued by the Ombudsman.</p><p>Enabling access and correction of personal information</p><p>The organisation or agency must enable individuals to access and correct their personal information. If requested by individuals or the relevant commissioner, the organisation or agency must review access or correction decisions, in compliance with the relevant federal, state or territory privacy or information laws.</p><p>Managing complaints and investigations </p><p>The organisation or agency must have procedures and processes in place for managing privacy complaints made by individuals to the organisation or agency, or to the relevant

privacy commissioner or ombudsman. The organisation or agency must comply with investigations by the relevant privacy commissioner or ombudsman into the organisation’s or agency’s handling of personal information, and with any enforceable orders, directions or undertakings arising from a complaint or investigation.</p><p>Managing confidential information and communications</p><p> </p><p>Confidentiality is a general obligation but also arises under privacy laws, freedom of information laws, and telecommunications laws, including:</p>
Commonwealth: Privacy Act 1988 (Cth), Freedom of Information Act 1982 (Cth) and Telecommunications Act 1997 (Cth)
Australian Capital Territory: Freedom of Information Act 1989 (ACT) and Workplace Privacy Act 2011 (ACT)
New South Wales: Government Information (Public Access) Act 2009 (NSW)
Northern Territory: Information Act 2002 (NT)
Queensland: Information Privacy Act 2009 (Qld) and Right to Information Act 2009 (Qld)
South Australia: Freedom of Information Act 1991 (SA)
Tasmania: Right to Information Act 2009 (Tas)
Victoria: Freedom of Information Act 1982 (Vic) and Public Records Act 1973 (Vic)
Western Australia: Freedom of Information Act 1992 (WA)
<p>Under confidentiality laws, an organisation or agency and its staff entrusted with confidential information in the course of their duties must keep that information confidential, and only disclose confidential information when the law requires them to do so.</p><p>In addition, an organisation, its employees and contractors working in telecommunications or providing emergency call services must keep certain types of communications and information confidential, and may only disclose confidential information or documents under allowed circumstances.</p><p>This section sets out:</p>
The obligations that apply to organisations and agencies in each jurisdiction
The ways in which these obligations apply to those organisations and agencies
The types of information add cell to which these obligations apply
</ ul><p>Managing general and workplace surveillance</p><p>Organisations and agencies are required to comply with surveillance and workplace surveillance laws. These are set out in federal, state and territory Acts and Regulations, including:</p>
Commonwealth: Surveillance Devices Act 2004 (Cth), Telecommunications Act 1997 (Cth), Telecommunications (Interception and Access) Act 1979 (Cth)
Australian Capital Territory: Listening Devices Act 1992 (ACT), Workplace Privacy Act 2011 (ACT)
New South Wales: Surveillance Devices Act

2007 (NSW), Workplace Surveillance Act 2005
(NSW)
Northern Territory: Surveillance
Devices Act (NT)
Queensland: Invasion
of Privacy Act 1971 (Qld)
South Australia: </
strong>Listening and Surveillance Devices Act 1972 (SA)</
li>
Tasmania: Listening Devices Act 1991
(Tas)
Victoria: Surveillance Devices
Act 1999 (Vic) as amended by Surveillance Devices (Workplace
Privacy) Act 2006 (Vic)</ li>
Western Australia: </
strong>Surveillance Devices Act 1998 (WA)
<p>Under
surveillance laws, an organisation or agency must ensure that
its surveillance operations are conducted lawfully and only for
allowed purposes. These laws restrict the use of surveillance
devices including:</p>
Listening devices
(restricted in all states and territories)
Optical
surveillance devices (restricted in New South Wales,
the Northern Territory, Victoria and Western Australia)</
li>
Tracking devices (restricted in New South
Wales, the Northern Territory, Victoria and Western Australia)</
li>
Data surveillance devices (restricted
by federal laws and also by the laws of the Australian Capital
Territory, New South Wales, Northern Territory and Victoria)
</
ul><p>The Australian Capital Territory, New South Wales and Victoria
impose further restrictions on the use of surveillance devices in
the workplace.</p><p>This section sets out organisations’
and agencies’ obligations under surveillance and workplace
surveillance laws for each jurisdiction.</p><p>Managing
workplace privacy</p><p>A person’s privacy in
the workplace is not absolute. Rather, it is limited by laws:</
p>
Allowing personal add cell information to be collected,
disclosed and used for specific purposes
Governing
access to communications
<p>This section covers
organisations’ and agencies’ obligations in relation
to the employee records, spent convictions and access to email
and the internet. . These obligations are set out in
federal, state and territory Acts and Regulations, including:</
p>
Commonwealth: Crimes Act 1914
(Cth), Criminal Code Act 1995 (Cth), Privacy Act 1988 (Cth),
Telecommunications (Interception and Access) Act 1979 (Cth)</
li>
Australian Capital Territory: Criminal Code
Criminal Records Act 1991 (NSW), Criminal Records Regulation
2014 (NSW), Workplace Surveillance Act 2005 (NSW), Workplace
Surveillance Regulation 2012 (NSW)
Northern
Territory: Criminal Records (Spent Convictions) Act 1992
(NT), Criminal Records (Spent Convictions) Regulations 1993 (NT)</
li>
Queensland: Criminal Law (Rehabilitation of
Offenders) Act 1986 (Qld)
South Australia:

Spent Convictions Act 2009 (SA), Spent Convictions Regulations 2011 (SA)
Tasmania: Annulled Convictions Act 2003 (Tas)
Western Australia: Spent Convictions Act 1988 (WA), Spent Convictions Regulations 1992 (WA)
<p> </p><p>Employee records exemption</p><p>Private sector employers are allowed to collect, use and disclose personal and health information about an individual if they have (or have had) a direct employment relationship with the person and the information is used lawfully under the Commonwealth privacy law.</p><p>Spent convictions</p><p>In each state and territory (except Victoria), a person who has a spent conviction has the right not to disclose their criminal record (providing they have no other convictions that are not spent), as though the record never existed, unless an exception applies. This means that organisations and agencies cannot disclose a spent conviction, or take account of the fact that the person was ever charged with, or convicted of, the offence.</p><p>The use of email and internet by employees</p><p> </p><p>An organisation or agency must ensure that their employees’ access to email and the internet is not unlawfully restricted or blocked under:</p>
Federal laws governing the interception of communications over computer networks
Workplace privacy laws in the Australian Capital Territory and New South Wales
", remedial_action: "<p>Personal information under data privacy laws</p><p>The organisation or agency should check whether it is required to comply with the federal, state or territory data privacy laws, and review, or update, its policies, procedures and systems to ensure compliance with those laws. </p><p>The organisation or agency should also establish a compliance program to manage the risk of non-compliance with privacy laws, and ensure staff are thoroughly trained and aware of their obligations.</p><p>Confidential information and communications</p><p>If the organisation or agency does not have systems or procedures in place to prevent or respond to breaches of confidentiality, it should implement those systems as soon as practicable. It should also review existing systems and procedures to ensure the organisation or agency meets compliance requirements.</p><p>If a breach of confidentiality may have occurred, the organisation or agency should take immediate steps to investigate the incident and determine whether there has been an actual breach. If so, it should consider what obligations exist to report the breach to relevant authorities. The organisation or agency should also contact any person affected by the breach.</p><p>General and workplace surveillance</p><p>The organisation or agency should review its systems, policies and procedures to ensure they are compliant with surveillance laws.</p><p>Workplace privacy</p><p>The organisation

	or agency should review: - Its current practices for collecting, using and disclosing personal and health information of individuals - The circumstances in which criminal history may be a relevant consideration for positions within the organisation or the industry The organisation or agency should review and, if required, update its procedures to ensure that: - Employee records are kept separate from non-employee records - Employee records are only used and disclosed for purposes that are directly related to the employment relationship - Information about spent convictions is handled appropriately - Unauthorised disclosure or access to information is documented and investigated The organisation or agency should review its policy and procedures for access to email and the internet, and check that it complies with applicable laws. ", consequence: " Personal information under data privacy laws In all jurisdictions except Western Australia, a person 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 person is not satisfied with the response provided by the organisation or agency, depending on the jurisdiction, thon 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. If a person’s complaint is upheld after internal review or external investigation, the organisation or agency may be required to take remedial action and make a formal apology to the complainant. Some states also allow for a successful complainant to be paid compensation, up to: $100,000 in the Australian Capital Territory, Queensland and Victoria $40,000 in New South Wales $60,000 in the Northern Territory The Commonwealth, the Australian Capital Territory, the Northern Territory, New South Wales and Victoria also impose heavier penalties for serious contraventions of the privacy laws: - Commonwealth: a civil penalty of $360,000 for a person or an unincorporated business or organisation, and $1.8 million for a corporation - Australian Capital Territory: a maximum fine of $7500 for an individual and $37,500 for a corporation, or imprisonment for 6 months, or both - New South Wales: a maximum fine of $11,000 or up to 2 years’ imprisonment, or both - Northern Territory: maximum fines of $15,400, $30,800 and $61,600 or, respectively, imprisonment for 6 months, 12 months or 2 years, depending on the offence - Victoria: a fine of $93,276 for an individual and $466,380 for a body corporate For more details, see Tools — Summary of consequences. A person, organisation or agency may be subject

to the additional consequences in relation to the access and correction of personal information, including:</p>
Legal actions, criminal charges and civil liability for providing access
Offences relating to access or correction — Queensland, Tasmania, Western Australia
Review of access or correction decisions — Northern Territory (correction only), Queensland, South Australia, Tasmania (access only), Victoria and Western Australia
Consequences in relation to reviews and complaints — New South Wales, Queensland, Tasmania, Victoria and Western Australia
<p>See Tools — Consequences regarding the access or correction of personal information.</p><p>Confidential information and communications</p><p> </p><p>Individuals and certain organisations — including corporations, companies and government bodies — may have the right to sue for compensation for any loss suffered as a result of a breach of their confidentiality. In particular circumstances, statute law may also set forth penalties for the same breach. However, where information is required by law to be disclosed for a specific purpose, the statutes which impose that requirement generally also include protections against liability for breach of confidence, as long as the disclosure complies with the law.</p><p>Under the Telecommunications Act 1997 (Cth), disclosure or use of confidential information or documents by a person working in telecommunications or emergency call services is a criminal offence punishable by up to 2 years’ imprisonment, unless the disclosure or use is allowed under that Act. Failure to make a detailed record of a disclosure within 5 days, and keep it for at least 3 years, incurs a maximum fine of $54,000 (Telecommunications Act 1997 (Cth) ss 306(7) and 306A(7)). Making an inaccurate record carries a penalty of imprisonment for up to 6 months (Telecommunications Act 1997 (Cth) s 307).</p><p>A breach of confidentiality that involves telecommunications or computers — including using either to commit or facilitate a serious offence — may also be a criminal offence punishable by up to 10 years’ imprisonment under the Criminal Code Act 1995 (Cth). See Tools — Telecommunications offences and Tools — Computer offences.</p><p>General and workplace surveillance</p><p> </p><p>Throughout Australia, anyone who intercepts telecommunications unlawfully, or who deals with intercepted information whether obtained lawfully or unlawfully, commits an offence punishable by imprisonment for up to 2 years (Telecommunications (Interception and Access) Act 1979 (Cth) s 105(2)).</p><p>Breach of state and territory surveillance laws is punishable by substantial fines or imprisonment or both. If the offender is a corporation, one or more executives of the corporation will be liable for the penalties if it can

Success Reponse	be shown they knew about or authorised the breach.</p><p>As these are criminal offences, anyone found guilty will have a criminal record.</p><p>In addition, any unlawful interception or surveillance that involves telecommunications or computers — including using either to commit or facilitate a serious offence — may also be a criminal offence punishable by up to 10 years’ imprisonment under the Criminal Code Act 1995 (Cth), or for as long as the period of the penalty for the serious offence. See Tools —Telecommunications offences and Tools — Computer offences.</p><p>Workplace privacy</p><p> </p><p>Employee records exemption</p><p> </p><p>Collection, use or disclosure of a person’s information in an employee record, other than for purposes directly related to a current or former employment relationship, under the employee records exemption for private sector organisations, is an interference with the privacy of the individual and the organisation or agency will be subject to the consequences set out under data privacy laws.</p><p>Spent convictions</p><p>In all states and territories except Victoria, monetary fines of up to $12,190 for an individual and $37,500 for a corporation apply to offences against the spent convictions laws. For some offences, the penalty may be imprisonment for up to 6 months. For details, see Tools — Spent convictions offences.</p><p>A person who believes their right not to disclose a spent, quashed or pardoned Commonwealth offence has been breached, or who is discriminated against on the grounds of a spent conviction (Western Australia), may lodge a complaint with the relevant commissioner (Crimes Act 1914 (Cth) ss 85ZZA–85ZZF, Spent Convictions Act 1988 (WA) s 24(1)).</p><p>The use of email and internet by employees</p><p>Throughout Australia, a person who intercepts telecommunications unlawfully commits an offence punishable by imprisonment for up to 2 years (Telecommunications (Interception and Access) Act 1979 (Cth) s 105(2)).</p><p>Employers in the Australian Capital Territory and New South Wales who unlawfully block electronic communications or access to websites may also be subject to fines (Workplace Privacy Act 2011 (ACT) s 20(1), Workplace Surveillance Act 2005 (NSW) s 17(1)).</p><p> Federal offences involving telecommunications and computers</p><p>In addition, any unlawful disclosure, interception or surveillance that involves telecommunications or computers — including using either to commit or facilitate a serious offence — may also be a criminal offence punishable by up to 10 years’ imprisonment under the Criminal Code Act 1995 (Cth), or for as long as the period of the penalty for the serious offence. See Tools — Telecommunications offences and Tools — Computer offences.</p>",

Success Response

```
due_date: "",
frequency: "",
description_directional: "<p>The private sector organisation or
public sector agency must comply with its obligations in relation
to personal information, confidential information, surveillance, and
workplace privacy.</p>",
description_questional: "<p>Does the private sector organisation
or public sector agency comply with its obligations in relation to
personal information, confidential information, surveillance, and
workplace privacy?</p>",
compliance_source: "<p><a href="https://www.legislation.gov.
au/Series/C2004A02796">Archives Act 1983 (Cth)</a></p><p><a
href="https://www.legislation.gov.au/Series/C1914A00012">Crimes
Act 1914 (Cth)</a></p><p><a href="https://www.legislation.
gov.au/Series/C2004A04868">Criminal Code Act 1995 (Cth)</
a></p><p><a href="https://www.legislation.gov.au/Series/
C2006A00088">Do Not Call Register Act 2006 (Cth)</a></p><p><a
href="https://www.legislation.gov.au/Series/C2004A02562">Freedom
of Information Act 1982 (Cth)</a></p><p><a href="https://www.
legislation.gov.au/Series/C2004A03712">Privacy Act 1988 (Cth)</
a></p><p><a href="https://www.legislation.gov.au/Series/
F2013L02126">Privac Privacy Regulation 2013 (Cth)</a></p><p><a
href="https://www.legislation.gov.au/Series/F2015L00249">Privacy
(Tax File Number) Rule 2015 (Cth)</a></p><p><a href="https://
www.legislation.gov.au/Series/C2004A01214">Spam Act 2003 (Cth)</
a></p><p><a href="https://www.legislation.gov.au/Series/
C2004A01387">Surveillance Devices Act 2004 (Cth)</a></p><p><a
href="https://www.legislation.gov.au/Series/C1953A00001">Taxation
Administration Act 1953 (Cth)</a></p><p><a href="https://www.
legislation.gov.au/Series/C2004A05145">Telecommunications Act
1997 (Cth)</a></p><p><a href="https://www.legislation.gov.au/
Series/C2004A02124">Telecommunications (Interception and Access)
Act 1979 (Cth)</a></p><p><a href="https://www.legislation.gov.au/
Series/F2007L00815">Telemarketing and Research Industry Standard
(Cth)</a></p><p><a href="http://www.legislation.act.gov.au/a/2002-
51">Criminal Code 2002 (ACT)</a></p><p><a href="http://www.
legislation.act.gov.au/a/alt_a1989-46co">Freedom of Information Act
1989 (ACT)</a></p><p><a href="http://www.legislation.act.gov.
.au/a/2014-24/default.asp">Information Privacy Act 2014 (ACT)</
a></p><p><a href="http://www.legislation.act.gov.au/sl/2014-25/
default.asp">Information Privacy Regulation 2014 (ACT)</a></p><p><a
href="http://www.legislation.act.gov.au/a/1992-57/default.
asp">Listening Devices Act 1992 1992 (ACT)</a></p><p><a
href="http://www.legislation.act.gov.au/a/2000-48/default.
asp">Spent Convictions Act 2000 (ACT)</a></p><p><a href="http://
www.legislation.act.gov.au/a/2002-18/default.asp">Territory Records
Act 2002 (ACT)</a></p><p><a href="http://www.legislation.
```

	act.gov.au/a/2011-4/default.asp">Workplace Privacy Act 2011 (ACT)</p><p><u> </u></p><p>Criminal Records Act 1991 (NSW)</ a></p><p>Criminal Records Regulation 2014 (NSW)</ a></p><p>Government Information (Public Access) Act 2009 (NSW)</p><p>Privacy and Personal Information Protection Act 1998 (NSW)</p><p>Privacy and Personal Information Protection Regulation 2014 (NSW)</p><p>Privacy Code of Practice (General) 2003 (NSW)</p><p>State Records Act 1998 (NSW)</p><p>Surveillance Devices Act 2007 (NSW)</ a></p><p>Workplace Surveillance Act 2005 (NSW)</p><p>Workplace Surveillance Regulation 2012 (NSW)</p><p>Criminal Records (Spent Convictions) Act 1992 (NT)</p><p>Criminal Records (Spent Convictions) Regulations 1993 (NT)</p><p>Information Act 2002 (NT)</ p><p>Surveillance Devices Act (NT)</ p><p>Surveillance Devices Regulations (NT)</p><p>Criminal Law (Rehabilitation of Offenders) Act 1986 (Qld)</ a></p><p>Information Privacy Act 2009 (Qld)</ p><p>Invasion of Privacy Act 1971 (Qld)</ p><p>Public Records Act 2002 (Qld)</ a></p><p>Right to Information Act 2009 (Qld)</ a></p><p><u> </u></p><p>Freedom of Information Act 1991 (SA)</p><p><a href="https://www. legislation.sa.gov.au/LZ/C/R/FREEDOM%20OF%20INFORMATION%20

(FEES%20AND%20CHARGES)%20REGULATIONS%202003.aspx">Freedom of Information (Fees and Charges) Regulations 2003 (SA)</p><p>Information Privacy Principles (IPPS) Instruction (SA)</p><p>Listening and Surveillance Devices Act 1972 (SA)</ a></p><p>Listening and Surveillance Devices Regulations 2003 (SA)</ a></p><p>Public Sector Act 2009 (SA)</ a></p><p>Spent Convictions Act 2009 (SA)</p><p>Spent Convictions Regulations 2011 (SA)</p><p>State Records Act 1997 (SA)</p><p>Archives Act 1983 (Tas)</p><p>Listening Devices Act 1991 (Tas)</p><p>Listening Devices Regulations 2014 (Tas)</p><p>Ombudsman Act 1978 (Tas)</p><p>Personal Information Protection Act 2004 (Tas)</p><p><a href="http:// www.thelaw.tas.gov.au/tocview/index.w3p;cond=;doc_ id=70%2B%2B2009%2BAT%40EN%2B20160714110000;histon=;pdfauthverid

=;prompt=;rec=;rtfauthverid=;term=;webauthverid=">Right to Information Act 2009 (Tas)</p><p><u> </u></p><p><a href="http://www.legislation.vic.gov.au/domino/web_notes/ldms/ publawtoday.nsf/95c43dd4eac71a68ca256dde00056e7b/

	29b81013dab5eb48ca257d72001bc6db!OpenDocument">Freedom of Information Act 1982 (Vic)</p><p>Privacy and Data Protection Act 2014 (Vic)</ p><p>PROS 10/13 Disposal Standard (Vic)</p><p> Public Administration Act 2004 (Vic)</p><p>Public Records Act 1973 (Vic)</p><p> Surveillance Devices Act 1999 (Vic) as amended by Surveillance Devices (Workplace Privacy) Act 2006 (Vic)</p><p>Surveillance Devices Regulations 2016 (Vic)</p><p>Victorian Protective Data Security Standards 2016 (Vic)</p><p>Freedom of Information Act 1992 (WA)</p><p> Freedom of Information Regulations 1993 (WA)</p><p> Public Sector Management Act 1994 (WA)</p><p>Spent Convictions Act 1988 (WA)</p><p>Spent Convictions Regulations 1992 (WA)</p><p>Spent Convictions Regulations 1992 (WA)</p><p>State Records Act 2000 (WA)</p><p><a href="https://www. slp.wa.gov.au/legislation/statutes.nsf/main_

Success Response

```
mrtitle_946_homepage.html">Surveillance Devices Act 1998 (WA)</a></
p><p><a href="https://www.slp.wa.gov.au/legislation/statutes.nsf/
main_mrtitle_2092_homepage.html">Surveillance Devices Regulations
1999 (WA)</a></p>",
definition: "<p></p>",
exerpt: "<p></p>",
submission_date: "20/10/2016",
author: "Kate Macumber/Linda Nix",
material_type: "material",
sequence_id: "0.0001",
module_id: "7161",
topic_id: "7211",
parent: {
id: "7211"
},
jurisdictions: [
"NSW",
"VIC",
"NT",
"QLD",
"WA",
"SA",
"TAS",
"ACT",
"COMMONWEALTH"
],
```

Content in XML:
```
<LexisNexisRI xmlns="http://www.lexisNexis.org" version="1.1"
encoding="UTF-8">
<response>
<results>
<page>1</page>
<items_per_page>5</items_per_page>
<num_pages>5</num_pages>
<total_items>28</total_items>
<isSuccess>true</isSuccess>
<modules>
<item>
<id>7161</id>
<title>Privacy & Data Protection</title>
<date_created>20160303102242</date_created>
<date_changed>20161221110905</date_changed>
<lineage>7161</lineage>
<archived>FALSE</archived>
<keywords/>
<type>module</type>
```

| **Success Response** | ```xml
<description>
<p>Regardless of which industry you are in, privacy and data
protection issues affect us all. The Privacy and Data Protection
module identifies your compliance obligations on how to collect,
manage and maintain personal information securely and within the
Australian legal framework.</p>
</description>
<is_core>true</is_core>
<apiOnly/>
<hot>false</hot>
<banner>
https://compliance.store.lexisnexis.com.au/__data/assets/
image/0009/14958/1600x500px-privacy.jpg
</banner>
<bannerAlt>Privacy & Data Protection Banner</bannerAlt>
<topicListDescription/>
<coreModuleListDescription/>
<sequence_id>6</sequence_id>
<topics>
<item>
<id>7211</id>
<title>Privacy and Data Protection</title>
<date_created>20160303105617</date_created>
<date_changed>20161221110919</date_changed>
<lineage>7211|7161</lineage>
<archived>FALSE</archived>
<keywords/>
<type>topic</type>
<description>
<p>Click here to view obligations for the Privacy &amp; Data
Protection module.</p>
</description>
<sequence_id>1</sequence_id>
<module_id>7161</module_id>
<hot>false</hot>
<parent>
<id>7161</id>
</parent>
<obligations>
<item>
<id>8364</id>
<title>Privacy & Data Protection Overview</title>
<date_created>20160326144334</date_created>
<date_changed>20170123111251</date_changed>
<lineage>8364|7211|7161</lineage>
<archived>FALSE</archived>
<keywords/>
``` |

Success Response	`<type>obligation</type>`
	`<practical_guidance>`
	` The Privacy & Data Protection module covers federal, state and territory privacy obligations in relation to: - The management of personal information for private sector organisations and public sector agencies - The handling confidential information and communications - General and workplace surveillance - Workplace privacy (employee records, employee spent convictions and employees’ use of email and the internet) Note: the Privacy & Data Protection module does not cover industry-specific privacy obligations. This means that it does not cover privacy obligations for industries such as health, telecommunications or credit reporting. Managing personal information under data privacy laws Data privacy laws cover the management of personal information by private sector organisations and public sector agencies. Obligations under these laws are set out in federal, state and territory Acts, Regulations and instructions, including: Commonwealth: Privacy Act 1988 (Cth), Privacy (Tax File Number) Rule 2015 (Cth), Do Not Call Register Act 2006 (Cth), Spam Act 2003 (Cth) and Taxation Administration Act 1953 (Cth) Australian Capital Territory: Information Privacy Act 2014 (ACT) and Territory Records Act 2002 (ACT) New South Wales: Privacy and Personal Information Protection Act 1998 (NSW), State Records Act 1998 (NSW) and Privacy Code of Practice (General) 2003 (NSW) Northern Territory: Information Act 2002 (NT) Queensland: Information Privacy Act 2009 (Qld) and Public Records Act 2002 (Qld) South Australia: Information Privacy Principles (IPPS) Instruction (SA), Freedom of Information Act 1991 (SA) and State Records Act 1997 (SA) Tasmania: Personal Information Protection Act 2004 (Tas), Right to Information Act 2009 (Tas) and Archives Act 1983 1983 (Tas) Victoria: Privacy and Data Protection Act 2014 (Vic), Freedom of Information Act 1982 (Vic) and Public Records Act 1973 (Vic) Western Australia: Freedom of Information Act 1992 (WA), Freedom of Information Regulations 1993 (WA) and State Records Act 2000 (WA), as well as non-mandatory guidelines. See Tools — Management of personal information Applicability of data privacy laws Not all private sector organisations or public sector agencies will be required to comply with data privacy laws. As such, this module discusses: - The types of private sector organisations and public sector agencies to which these laws apply - Which laws (federal or state/`

Success Response	`territory) 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 - Which acts and practices are exempt from data privacy laws <p>If data privacy laws apply to the organisation or agency and to its acts and practices, the organisation or agency will generally be required to comply with the following obligations. Note: the extent to which these obligations apply to an organisation or agency vary between jurisdictions.</p><p> </p><p>Organisational governance</p><p>The organisation or agency and its chief executive officer have responsibilities to ensure that the organisation’s or agency’s policies, systems and procedures comply with relevant privacy laws. Recommended approaches to ensuring compliance with this obligation include undertaking privacy impact assessments; ensuring that privacy issues are included in processes and systems from the outset, according to privacy by design principles; and developing a da`

Subscribed Content

Title	Content • This function returns the content of one module within the user's subscription. • The function allows API client to specify a module within their subscription
URL	**http://compliance.store.lexisnexis.com.au/rest/api/v1.1/content**

URL Params	Required:
	• token=[string]
	  example: token=b4684ce3-ca5b-477f-8f4d-e05884a83d3c
	• customer_id=[integer]
	  example: customer_id=12
	• ln_sku=[integer]
	  example: ln_sku=7156
	
	Optional:
	• format=[json|xml]
	  example: format=xml
	  if format is not specified, JSON will be returned.
	• bom=true - only for csv output file in order for BOM character to be included
	  from_date=ddMMMyyyy
	  example : from_date=24FEB2015

URL Params	- end_date=ddMMMyyyy
	  example: end_date=28FEB2015
	- jurisdictions=[jurisdiction]
	  example: jurisdictions=NSW|VIC
	  where multiple jurisdictions is specified use "|" between each value
	- id=xxxxx
	  example id=8190
	  the id being the asset id of the obligation, subobligation, alert or tool and multiple ids
	  can be specified using "|" between each value
	- record_type=[active|archived]
	  returning all assets within the module with the specified status
	- type=[obligation|subobligation|notice|tool]
	  returning all assets within the module with the specified asset type

Success Response	Content in JSON:

```
{
results: {
current_ln_sku: "7156",
requestURL: "http://search.apac.lexisnexis.com.au/s/search.
html?collection=lxnx-au-subscription-meta&amp;profile=_
default&amp;form=api&amp;query=lnsku:7156",
isSuccess: true,
modules: [
{
id: "7156",
title: "Corporations",
date_created: "20160303102240",
date_changed: "20160701093847",
lineage: "7156",
archived: "FALSE",
keywords: "",
type: "module",
description: "<p>This module provides you with your compliance
obligations, from setting up and operating your organisation
through to winding it down. We have reviewed all key legislation
administered by ASIC and other key government bodies.</p>",
is_core: "true",
banner:
"https://compliance.store.lexisnexis.com.au/__data/assets/
image/0006/14955/1500x900px_corporations.jpg",
bannerAlt: "Corporations Banner",
topicListDescription: "",
coreModuleListDescription: "Click on any of the below to view the
topic tree for the area",
sequence_id: "3",
country: [
"Australia"
],
industry: [
"All Industries"
],
```

<table>
<tr><td>Success Response</td><td>

```
topics: [
{
id: "7205",

title: "Proprietary Limited Companies",
date_created: "20160303105444",
date_changed: "20160706114624",
lineage: "7205|7156",
archived: "FALSE",
keywords: "",
type: "topic",
description: "<p>Click here to view obligations for the Proprietary
Limited Companies module.</p>",
sequence_id: "Proprietary Limited Companies",
module_id: "7156",
parent: {
id: "7156"
},
obligations: [
{
id: "8896",
title: "Ongoing Operations and Notification of Changes",
date_created: "20160406122710",
date_changed: "20160701121716",
lineage: "8896|7205|7156",
archived: "FALSE",
keywords: "",
type: "obligation",
practical_guidance: "<p>Once a company is registered with
ASIC it must comply with its ongoing operational and
notification obligations under the Corporations Act 2001
(Cth) by:</p><ul><li>Establishing and maintaining its
members&rsquo; register, and registers of option holders and/or
debenture  holders (if applicable) at its registered
office, principal place of business, the place in Australia
where the work involved in maintaining the register is done
or other place in Australia advised to ASIC</li><li>Establishing a
registered office where its business is conducted, registers
may be maintained, and to  which communications can be
sent</li><li>Establishing a principal place of business if
```

Content in XML:

```
<LexisNexisRI xmlns="http://www.lexisNexis.org" version="1.1">
<response>
<results>
<page>1</page>
<items_per_page>5</items_per_page>
<num_pages>1</num_pages>
<total_items>1</total_items>
<isSuccess>true</isSuccess>
<modules>
<item>
```

</td></tr>
</table>

Success Response	```xml
	<id>7156</id>
	<title>Corporations</title>
	<date_created>20160303102240</date_created>
	<date_changed>20240306143345</date_changed>
	<lineage>7156</lineage>
	<archived>FALSE</archived>
	<keywords/>
	<type>module</type>
	<description> This module provides you with your compliance obligations, from setting up and operating your organisation through to winding it down. We have reviewed all key legislation administered by ASIC and other key government bodies. </description>
	<is_core>false</is_core>
	<apiOnly/>
	<hot>false</hot>
	<banner>/__data/assets/image/0006/14955/1600x500px-corporations.jpg</banner>
	<bannerAlt>Corporations Banner</bannerAlt>
	<topicListDescription/>
	<coreModuleListDescription/>
	<sequence_id>0</sequence_id>
	<country>
	<item>Australia</item>
	</country>
	<industry>
	<item>All Industries</item>
	</industry>
	<topics>
	<item>
	<id>14910</id>
	<title>ASX Listing Rules</title>
	<date_created>20160608103504</date_created>
	<date_changed>20240514113715</date_changed>
	<lineage>14910|7156</lineage>
	<archived>FALSE</archived>
	<keywords/>
	<type>topic</type>
	<description> </description>
	<sequence_id>0</sequence_id>
	<module_id>7156</module_id>
	<hot>false</hot>
	``

Csv zip file

Instructions as per above the only difference is format=csv

Appendix

OBLIGATION		
Field name	**Data Type**	**Description**
id	integer	Asset ID
title	varchar	Obligation title
date_created	date	Asset creation date
date_changed	date	Asset update date
lineage	varchar	The asset IDs of its parent record all the way up to the top level, the module
archived	varchar	TRUE or FALSE
keywords	varchar	currently not used
type	varchar	obligation or subobligation
practical_guidance	varchar	content that contains html tags for the various format including table
remedial_action	varchar	content that contains html tags for the various format
consequence	varchar	content that contains html tags for the various format
due_date	varchar	content that contains html tags for the various format
frequency	varchar	content that contains html tags for the various format
description_directional	varchar	content that contains html tags for the various format
description_questional	varchar	content that contains html tags for the various format
compliance_source	varchar	content that contains hyperlinks and html tags for the various format
definition	varchar	content that contains html tags for the various format
exerpt	varchar	content that contains html tags for the various format
submission_date	date	not relevant for API
author	varchar	not relevant for API
material_type	varchar	not relevant for API
sequence_id	varchar	Number with 4 decimal places; used to sequence the obligation
module_id	varchar	Asset ID of module
topic_id	varchar	Asset ID of submodule
obligation_id	varchar	Asset ID of obligation
jurisdictions	varchar	applicable jurisdiction(s) for the obligation - multiselect
parent_id	varchar	Asset ID of its direct parent
historical_note	varchar	content that contains html tags for the various format

Appendix

TOOLS		
Field name	**Data Type**	**Description**
id	integer	Asset ID
title	varchar	Tool title
date_created	date	Asset creation date
date_changed	date	Asset update date
lineage	varchar	The asset IDs of its parent record all the way up to the top level, the module
archived	varchar	TRUE or FALSE
keywords	varchar	currently not used
type	varchar	tool
link	varchar	URL for tools that are not hyperlinks e.g. .doc, .xlsm, .pdf
ext_link	varchar	URL for tools that not hyperlinks
category	varchar	ext, doc, xls, pdf
module_id	varchar	Asset ID of module
topic_id	varchar	Asset ID of submodule
obligation_id	varchar	Asset ID of obligation
sub_obligation_id	varchar	Asset ID of subobligation
tool_function	varchar	Checklist/Audit, Form/Template, Hyperlink, Reference Material
jurisdictions	varchar	Not used
parent_id	varchar	Asset ID of its direct parent

ALERTS		
Field name	**Data Type**	**Description**
id	integer	Asset ID
title	varchar	Alert title
date_created	date	Asset creation date
date_changed	date	Asset update date
lineage	varchar	The asset IDs of its parent record all the way up to the top level, the module
archived	varchar	TRUE or FALSE
keywords	varchar	currently not used
type	varchar	FYI, Action Required
description	varchar	content that contains html tags for the various format including table
effectiveDate	varchar	content that contains html tags for the various format
compliance_source	varchar	content that contains hyperlinks and html tags for the various format
submission_date	varchar	not relevant for API
author	varchar	not relevant for API
impact_on_obligation	varchar	content that contains html tags for the various format including table
module_id	varchar	Asset ID of module
topic_id	varchar	Asset ID of submodule
obligation_id	varchar	Asset ID of obligation
sub_obligation_id	varchar	Asset ID of subobligation
jurisdictions	date	applicable jurisdiction(s) for the obligation - multiselect
parent_id	varchar	Asset ID of its direct parent

Appendix

MODULES		
Field name	**Data Type**	**Description**
id	integer	Asset ID
title	varchar	Module title
date_created	date	Asset creation date
date_changed	date	Asset update date
lineage	varchar	The asset IDs of its parent record all the way up to the top level, the module. As this is already the top level it is the same as the Asset ID
archived	varchar	TRUE or FALSE
keywords	varchar	currently not used
type	varchar	module
description	varchar	not relevant for API
is_core	varchar	TRUE or FALSE
banner	varchar	not relevant for API
bannerAlt	varchar	currently not used
topicListDescription	varchar	currently not used
coreModuleList Description	varchar	currently not used
sequence_id	varchar	currently not used
jurisdictions	varchar	currently not used
Country	varchar	Applicable country for the module
Industry	varchar	Applicable industry for the module

TOPICS		
Field name	**Data Type**	**Description**
id	integer	Asset ID
title	varchar	Module title
date_created	date	Asset creation date
date_changed	date	Asset update date
lineage	varchar	The asset IDs of its parent record all the way up to the top level, the module.
archived	varchar	TRUE or FALSE
keywords	varchar	currently not used
type	varchar	topic
description	varchar	content that contains html tags describing the module
sequence_id	integer	Used to order the sub modules
module_id	integer	The asset ID of the module that it belongs to
jurisdictions	varchar	currently not used
parent_id	integer	The asset ID of the module that it belongs to

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.

- Find relevant obligations faster with jargon-free registers that are aligned to your business processes.
- Stay up to date with near-real time alerts delivered straight to your inbox when you may be impacted by regulatory change.
- Explore your compliance obligations under a particular regulator, or a particular compliance source, with SourceData.
- Engage with the wider compliance community and LexisNexis experts through the Community Portal, our self-support platform.
- Access comprehensive, current LexisNexis content that meets your unique needs, with key core modules relevant to all businesses, and a rapid accelerating roadmap of industry-specific modules that guide your path to compliance.

Authored by leading legal and industry experts, and supported by flexible technology that works the way you do, LexisNexis Regulatory Compliance gives you peace of mind while saving time, and money.

LexisNexis® | *Regulatory Compliance*

lexisnexis.co.nz/compliance

AS052024MS