Chambers AND PARTNERS

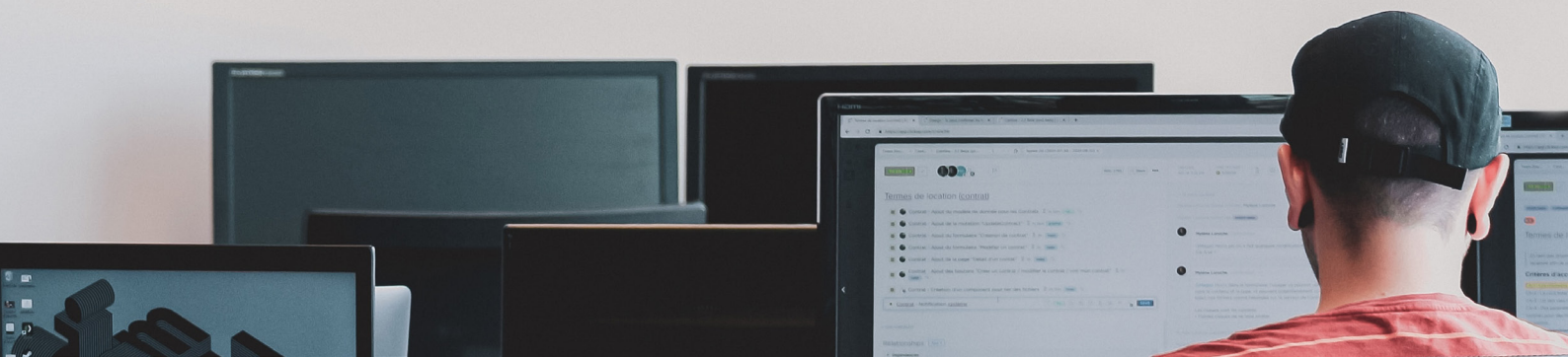
CHAMBERS GLOBAL PRACTICE GUIDES

Technology & Outsourcing 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

New Zealand: Law & Practice

Liz Blythe, Troy Pilkington, Emma Peterson and Craig Shrive
Russell McVeagh



NEW ZEALAND

Law and Practice

Contributed by:
Liz Blythe, Troy Pilkington, Emma Peterson and Craig Shrive
Russell McVeagh

Contents

1. Market Conditions p.4
1.1 IT Outsourcing p.4
1.2 Business Process Outsourcing (BPO) p.4
1.3 New Technology p.4
1.4 Outsourced Services p.5

2. Regulatory Environment p.5
2.1 Restrictions on Technology Transactions or Outsourcing p.5
2.2 Industry-Specific Restrictions p.6
2.3 Restrictions on Data Processing or Data Security p.8

3. Model Outsourcing Contracts p.9
3.1 Standard Contract Model p.9
3.2 Alternative Contract Models p.10
3.3 Digital Transformation p.10

4. Contract Terms p.10
4.1 Customer Protections p.10
4.2 Termination p.12
4.3 Liability p.13
4.4 Implied Terms p.13
4.5 Data Protection and Cybersecurity p.14
4.6 Performance Measurement and Management p.15
4.7 Digital Transformation p.15

5. Employment Matters p.16
5.1 Employee Transfers p.16
5.2 Role of Trade Unions or Workers' Councils p.17
5.3 Offshore, Nearshore and Onshore p.17
5.4 Remote Working p.17

Russell McVeagh is a premier law firm in New Zealand, with offices in Auckland, Wellington and Queenstown. Russell McVeagh's Outsourcing team boasts award-winning lawyers who offer exceptional thought leadership, depth of experience and the ability to translate complex legal issues into client success stories. The firm's Technology and Outsourcing practice collaborates with other specialist teams around the firm as necessary to provide clear, pragmatic and innovative advice. The team counts some of the world's largest technology companies among its clients and also acts for all of the major New Zealand banks, as well as many of New Zealand's largest companies (including the majority of New Zealand's largest listed companies). Russell McVeagh regularly advises clients on large-scale outsourcing and technology transactions across the public and private sectors – for example, acting for one of New Zealand's largest companies on the outsourcing of its global IaaS (third-party cloud environments) and application support, maintenance and development needs across more than 30 jurisdictions.

Authors

Liz Blythe is an outsourcing and technology specialist partner at Russell McVeagh, advising exclusively on strategic procurement, technology and digital matters. Liz has depth of experience in the outsourcing sector, both in New Zealand and in the UK, where she worked in Milbank's highly regarded Outsourcing and Technology team for a number of years. In addition to outsourcing, her practice includes advising on technology matters more broadly – for example, providing e-commerce arrangements, data protection and IP advice. Liz has been recognised and awarded for her expertise by various bodies and publications.

Troy Pilkington leads the Competition/Antitrust practice within Russell McVeagh's Government, Competition and Regulation department. He is one of New Zealand's most highly regarded competition/antitrust, consumer and regulatory lawyers, and has acted in New Zealand's most high-profile market studies, cartel and consumer law investigations/prosecutions, M&A transactions and joint ventures. He regularly advises a number of New Zealand's major electricity and telecommunications businesses and leading banks, media companies, insurance providers and private equity firms.

Emma Peterson is a partner in Russell McVeagh's Litigation team, where she specialises in employment law and health and safety. Emma advises on all aspects of employment relationships – for example, ensuring these relationships are appropriately documented (through employment agreements, policies and incentive schemes), advising on compliance issues, and dealing with employment disputes as they arise (including in litigation, if necessary). Emma has advised some of New Zealand's largest employers on the employment law implications of large-scale outsourcing projects.

Craig Shrive is a partner in Russell McVeagh's Government, Competition and Regulation team. He specialises in market regulation, including in the water, telecommunications, aviation and energy sectors. He has a detailed understanding of government and parliamentary processes, having previously worked in Parliament, and has helped a broad range of clients on matters involving policy, law reform, design and implementation of new regulatory regimes, and regulatory compliance.

Russell McVeagh

Vero Centre
48 Shortland Street
PO Box 8
Auckland 1140
New Zealand

Tel: +64 9367 8326
Fax: +64 9367 8163
Email: contactus@russellmcveagh.com
Web: www.russellmcveagh.com

1. Market Conditions

1.1 IT Outsourcing

New Zealand organisations continue to outsource in-house IT capability to local and global IT service providers and to consolidate previously multi-sourced environments with strategic partners. Key drivers tend to be:

- reducing cost and complexity;
- taking advantage of specialist capabilities and modernising ageing estates;
- increasing efficiency; and
- improving the security, performance and user experience associated with IT systems.

There has been a continued shift towards cloud computing, with organisations now moving away from owning or contracting for physical IT assets in favour of leveraging third-party cloud environments (IaaS) and utilising software (SaaS) and platform (PaaS) solutions. Among other things, this allows organisations to enjoy the cost efficiencies and other benefits associated with a fully scalable model. Further areas of development include:

- solutions that increasingly offer value-added services powered by AI and machine learning;
- core systems and functions (eg, payroll/HR, enterprise resource planning (ERP), finance, and – increasingly – security) commonly being outsourced to third parties on an end-to-end "as-a-service" basis; and
- internet of things (IoT) capability.

Increasingly, organisations that have IT at the core of their service offering are also demonstrating a desire to outsource both back-end and customer-facing IT functions to third-party IT outsource service providers.

1.2 Business Process Outsourcing (BPO)

Business process outsourcing has grown in line with IT outsourcing developments. However, solutions being procured are increasingly digitalised and a general convergence of BPO and IT outsourcing has been seen in many areas, including HR, ERP and finance functions.

1.3 New Technology

Emerging technologies (eg, AI, blockchain, IoT and next-generation robotics) are not new to the New Zealand market. It is also well understood that such technologies provide opportunities to solve business issues, improve efficiency and increase profitability.

The adoption of these technologies had previously not been as widespread in New Zealand as was perhaps initially expected, but particularly in the GenAI space, we have seen significant adoption activity in the last 12 months. As is the case in many jurisdictions, emerging technologies have suffered the effects of regulatory lag, which has caused uncertainty in terms of how regulators and legislators will react to novel or perceived high-risk applications. As such, it seems that many organisations have been wary of investing significant resources in new technologies early on – given that potentially costly re-engineering may be required as a result of subsequent changes in the law.

However, it is becoming increasingly common in IT and BPO outsourcing transactions for customers to require the supplier to utilise appropriate AI and/or other new technologies as continuous improvement initiatives as the technologies become available in the market. This trend is expected to continue in the AI space, particularly in light of New Zealand's recently introduced National AI Strategy which promotes organisational adoption of AI. Additionally, the government has indicated it will use an "agile" regulatory method, leveraging current frameworks and introducing new legislation to address emerging AI risks as required. The government has also issued guidance for biometrics regarding the adoption of AI, providing further certainty.

Key new regulatory developments in the new technology space include:

- the Digital Identity Trust Framework Act 2023, which is aimed at developing digital identity services that are trusted and people-centric;
- the Customer and Product Data Act 2025, which has established a consumer data right framework for New Zealand;
- the release by New Zealand's Office of the Privacy Commissioner (OPC) of guidance in September 2023 in relation to the use of AI and the Information Privacy Principles under the Privacy Act 2020; and
- the OPC's release in August 2025 of a Biometric Processing Privacy Code;
- as noted above, the government's National AI Strategy released in July 2025; and
- as part of the National AI Strategy noted above, the release of several guidance documents to support public and private sector agencies in using AI, including:
  (a) Responsible AI Guidance for the Public Service;
  (b) Public Sector AI Framework; and
  (c) Responsible AI Guidance for Businesses.

1.4 Outsourced Services

The most commonly outsourced services in New Zealand are (i) information technology services (such as IT infrastructure, network management, hosting services, cybersecurity services, software development, support and maintenance services) – see **1.1 IT Outsourcing** for more details; and (ii) business process outsourcing in areas such as call centres, HR, payroll and finance, as discussed further in **1.2 Business Process Outsourcing (BPO)**.

2. Regulatory Environment

2.1 Restrictions on Technology Transactions or Outsourcing

Outsourcing and technology transactions are not separately regulated in New Zealand. Rather, whether a particular outsourcing arrangement or technology transaction will be the subject of a specific regulatory regime largely depends on the customer's industry and the specific nature of the arrangement, including details of the customer, industry and type of outsourcing or technology transaction.

While not relating to outsourcing or technology transactions specifically, New Zealand's competition law (contained in the Commerce Act 1986) contains a prohibition against entering into or giving effect to a contract, arrangement or understanding that contains a "cartel provision" – that is, a provision between actual or potential competitors that has the purpose, effect or likely effect of:

- fixing, maintaining, or controlling the price of goods/services that the parties supply or acquire in competition with each other (known as "price fixing");
- allocating the people or geographic areas that the parties would otherwise supply to, or buy from, in competition with each other (known as "market allocation"); and/or
- restricting the supply or acquisition of goods or services that the parties supply or acquire in competition with each other (known as "output restriction").

These prohibitions could apply to an outsourcing agreement or other technology agreements where the provider of the relevant services is also a competitor of the customer of those services. A breach of the Commerce Act can occur even without a written agreement – an informal understanding or expectation between competitors that they will act (or refrain from

acting) in a certain way is enough. Therefore, discussions with outsourcing and technology partners that are also competitors must not "spill over" into informal arrangements about how each party competes for customers/suppliers. Parties should also avoid sharing commercially sensitive information (such as pricing information) with each other in the areas in which they compete.

The Commerce Act contains certain exemptions from the cartel prohibition, including the "vertical supply contract" exception, which can apply to cartel provisions contained in supply contracts (such as IT outsourcing contracts). To rely on this exception, the cartel provision must be contained in a contract and "relate to" the goods or services being supplied, and not have the "dominant purpose of lessening competition" between the parties. However, even where an exception applies, parties must still consider Section 27 of the Commerce Act, which prohibits entering into or giving effect to any contract, arrangement or understanding that has the purpose, effect, or likely effect of substantially lessening competition in a market. This prohibition applies irrespective of whether the vertical supply contract exception applies.

This is an area to watch in New Zealand, as IT service providers are increasingly outsourcing their IT operations to service providers who may also be competitors in some markets.

2.2 Industry-Specific Restrictions

Although there is no legislation that applies to outsourcing and technology transactions generally in New Zealand, specific guidance is provided for these arrangements by particular regulators and in particular industries. These include financial services, the public sector, certain infrastructure providers, and regulated businesses more generally.

Financial Services

The financial services sector in New Zealand is regulated by the Financial Markets Authority (FMA) and subject to the Financial Markets Conduct Act 2013 (FMCA) and other legislative requirements. The FMCA prescribes liability for compliance with statutory duties where brokers and financial advisers outsource their services. If a broker contracts out broking services to another business (eg, to a custodian), the broker remains responsible for broking services to the client. The person providing the outsourced broking services is required to register on the Financial Service Providers Register as providing broking services. Financial advisers must also take all reasonable steps to ensure that the person or entity to whom they have outsourced services complies with their duties under the FMCA. The FMA's 2024 guidance note advises that a reasonable level of due diligence be carried out when outsourcing client money or property services to third parties.

Banks

Large New Zealand banks are generally subject to a standard condition of registration that requires banks to continue to meet specific outcomes, despite outsourcing.

The Reserve Bank of New Zealand (RBNZ) – the prudential regulator of New Zealand banks – maintains an outsourcing policy (the current policy (BS11) was issued in September 2022). The RBNZ has the power to take enforcement action against any New Zealand bank to ensure compliance with the outsourcing policy as a condition of registration. Among the relevant requirements under the RBNZ outsourcing policy are that, depending on the circumstances of the outsourcing, New Zealand banks seeking to implement any outsourcing arrangement must:

- have the relevant risk mitigation requirements (as specified for particular circumstances in the outsourcing policy) in place at all times;
- have robust back-up capability in place if the arrangement is with another related or independent third party;
- ensure that the outsourcing arrangement contains the contractual terms prescribed in the outsourcing policy;
- obtain non-objection from the RBNZ before entering into the arrangement in some cases;
- maintain, annually review, and provide a compendium of outsourcing arrangements to the RBNZ on request; and
- have a separation plan (which is tested annually) providing the steps a bank would take to ensure the services covered by the outsourcing arrange-

ment would continue to be provided in the event of failure of the arrangement.

The RBNZ maintains an extensive "exempt list" of outsourcing arrangements that are exempt from the outsourcing policy.

Public Sector

All public service departments, including the New Zealand Defence Force, New Zealand Police, New Zealand Security Intelligence Service and Parliamentary Counsel Office (collectively, "the Agencies") are directed by the New Zealand government to implement the Protective Security Requirements (PSRs). The PSRs are a set of mandatory requirements – a number of which are focused on information security, which is the government's primary concern when outsourcing the Agencies' responsibilities.

The PSRs include guidelines and policies for managing protected information when outsourcing and offshoring – in particular, the following.

- Agencies considering using cloud services must contact the government chief digital officer for advice and guidance and follow that advice and guidance.
- Agencies planning to use cloud services must perform a formal risk assessment, which includes identifying the controls needed to manage the information security and privacy risks associated with their use of the service.
- Agencies must verify that they have put effective controls in place to manage security and privacy risks before certifying and accrediting the service for use.

More broadly, the Government Procurement Rules are mandatory for all government departments, the New Zealand Police and Defence Force, and most Crown entities when the procurement is worth more than NZD100,000 (or NZD9 million for new construction works). These rules focus on promoting public value and include explicit requirements for agencies to consider in their procurement arrangements – for example, increasing the domestic workforce and supporting the transition to a net-zero emissions economy.

Other Regulated Sectors

Many businesses in New Zealand that conduct operations in regulated industries are subject to licensing, approval and certification requirements, and other ongoing price, governance and quality obligations set out in statutes, rules and regulations. While outsourcing in these industries is not specifically regulated or prohibited, there are other considerations that those looking to outsource should take into account – for example, the following sectors are subject to industry-specific regulation in New Zealand.

- Aviation is governed by the Civil Aviation Act 2023 and the Airport Authorities Act 1966 (to be progressively replaced by the Civil Aviation Act 2023 by 2028), and the Civil Aviation Rules. The Civil Aviation Authority and the Commerce Commission monitor compliance with regulations.
- Electricity is governed by the Electricity Industry Act 2010 and Electricity Industry Participation Code. It is regulated by the Electricity Authority and the Commerce Commission.
- Food is governed by a number of acts and codes, in addition to being regulated by the Australia New Zealand Food Standards Authority and the Ministry of Health.
- Medicines and medical devices are governed by the Medicines Act 1981 and are monitored by the Ministry of Health.
- Road transport is governed by the Land Transport Act 1998, the Land Transport Management Act 2003, and associated rules and regulations. The New Zealand Transport Authority, local authorities and the Ministry of Transport regulate this industry.
- Telecommunications, gas and dairy are regulated under industry-specific legislation and are subject to the oversight of the Commerce Commission.
- Drinking water and water infrastructure is regulated under a range of legislation, including the recently enacted Local Government (Water Services) Act 2025, which set up a new enduring water services delivery framework. Under this framework, Taumata Arowai regulates drinking water suppliers, and the Commerce Commission is responsible for economic regulation.

Consumer Data Right

The Customer and Product Data Act 2025, which establishes New Zealand's consumer data right (CDR) framework, became law in March 2025. Once implemented, the CDR will provide individuals and businesses with a statutory right to require data holders to share information held about them with trusted third parties and the right to require them to carry out certain actions on the relevant individual's or business's behalf.

The government has announced that banking will be the first sector in scope for the CDR and has consulted industry on designating electricity next. Regarding the banking sector, the Ministry of Business, Innovation and Employment has announced that the banking regulations to be issued under the Act are anticipated to come into effect from December 2025.

2.3 Restrictions on Data Processing or Data Security

Organisations must comply with the Privacy Act 2020 and the Privacy Regulations 2020 (the "Privacy Act"). New Zealand organisations must ensure that they comply with the information privacy principles in the Privacy Act 2020, which govern the rights of individuals in relation to their personal information.

The Privacy Act includes a number of regulatory requirements relevant to outsourcing services and technology transactions. These include:

- restrictions on cross-border transfers of personal information, whereby agencies may only transfer personal information overseas if certain exceptions under the Privacy Act apply – noting that the export of personal information to a third party (eg, a cloud service provider) that merely holds that data as an agent on behalf of the first party (eg, for safe custody) is expressly excluded from the restrictions on cross-border transfers if the third party only stores or processes the personal information on the relevant agency's behalf (and not for the third party's own purposes);
- a mandatory breach notification regime for certain notifiable privacy breaches, which requires an organisation to:
  (a) notify the New Zealand Privacy Commissioner (and, in most cases, the individuals concerned) as soon as practicable after becoming aware of the breach; or
  (b) make a public notification regarding the breach;
- public notifications to be published on an internet website maintained by the organisation and in at least one other medium, with a range of requirements for the content of the notice (including a description of the breach and notification of the right to complain about the breach);
- specific reference to foreign agencies, expressly bringing them within the scope of the Privacy Act to the extent that they undertake regulated activities in the course of carrying out business in New Zealand; and
- clarification that the Privacy Act will apply to all actions by a New Zealand agency, whether inside or outside New Zealand.

In 2023, a bill was introduced in Parliament to amend the Privacy Act, whereby the notification requirements under the Privacy Act will be broadened so that they apply to the collection of personal information about an individual by agencies indirectly through a third party, rather than directly from the individual concerned. The bill's third reading in April 2025 was interrupted and it still awaits royal assent. Following enactment, agencies that obtain personal information indirectly from other agencies after 1 May 2026 will be subject to additional compliance requirements under the Privacy Act.

Additionally, New Zealand organisations that process the personal data of people residing in the UK or the EU are required to comply with the UK or EU General Data Protection Regulation (GDPR) (as applicable) in some circumstances – for example, where those businesses offer goods and/or services to such people residing in the EU or the UK.

In August 2025, the OPC released a new Biometric Processing Privacy Code (Code). The Code applies to all agencies regulated by the Privacy Act 2020 that collect or use biometric information (such as fingerprints or facial images) to verify, identify or categorise individuals using automated systems. Certain excep-

tions apply for health, intelligence, and security agencies.

Penalties for Breach of Such Laws

The maximum fine under the Privacy Act is NZD10,000 for failure to comply with an access order, compliance notice or transfer prohibition notice. The same maximum applies for failure to notify a privacy breach where required under the Privacy Act.

In addition, there is a process by which privacy complaints can be escalated to the Human Rights Review Tribunal, which may grant a number of remedies – for example, a declaration that the business has interfered with the privacy of the individual and the award of damages. The Human Rights Review Tribunal can award damages up to a maximum of NZD350,000 (with the maximum award for a privacy matter to date being just over NZD168,000).

3. Model Outsourcing Contracts

3.1 Standard Contract Model

Outsourcing contract models in New Zealand vary, depending on the specific circumstances of the particular outsourcing arrangement – for example, the types of services being procured and the size of the customer's business.

Direct Contracting

Although there is no one standard approach to outsourcing contracts in New Zealand, direct contracting tends to be the prevailing model. It is also increasingly common for customers to aggregate service providers by contracting with a core outsourcing provider directly for a number of different services, often involving third-party managed services or subcontracting arrangements. This allows these customers to take advantage of relative administrative simplicity, cost-efficiency, and a single point of end-to-end service provider responsibility – all while still making use of specialist third-party capability. These outsourcing arrangements are typically governed by a master services agreement, with each service falling under a separate service schedule or statement of work.

The master services agreement contains the general legal terms relating to the arrangement as a whole and will typically include:

- provisions relating to the initial term of the engagement;
- a process for agreeing to additional services;
- liability caps and exclusions;
- warranties;
- indemnities;
- a dispute resolution process and termination rights; and

the overarching principles and standards to which the services will be provided to the customer.

The specific details of the arrangement are detailed in the service schedules, which will set out the service levels and service credit regime, pricing, customer dependencies, assumptions, customer requirements and other specific service terms.

Existing Templates and Drafting Outsourcing Contracts

It is common for service providers to push to use their existing contractual template as the basis for the outsourcing contract. Depending on the type of IT services being procured, the size (and relative bargaining power) of the customer and the value of the transaction, it can be more challenging to negotiate amendments to such template agreements – or to use the customer's terms as a basis for negotiation – in the New Zealand market than it is in other larger markets where this practice is more widespread.

The drafting of outsourcing contracts in New Zealand has shifted in line with global developments in outsourcing. Parties are increasingly contracting on terms that focus on agility and partnership, rather than more traditional adversarial-style obligations. Furthermore, there is a trend towards customers becoming much more sophisticated purchasers of these types of services, with several larger organisations now at the second- or third-generation outsourcing stage. Contracts are increasingly focused on service outcomes, rather than prescribing the method of service provision in detail.

3.2 Alternative Contract Models

Indirect Outsourcing

When it comes to the procurement of services to perform discrete business functions or processes (eg, ERP, finance, accounting, HR processing or complex lease management), indirect outsourcing is fairly common. This is typically because the underlying provider of the service or technology is not based in New Zealand, so the New Zealand customer entity instead contracts with a local supplier entity, who then subcontracts out to the foreign third-party service provider. In these cases, it is typical for the local entity to provide second-level support services and on-site implementation, transition and configuration services to augment the overseas service provider's remote service offering.

Liability arrangements in these circumstances can become complex and – apart from where very large customers are involved – the underlying services are often contracted on the underlying foreign service provider's standard terms without significant negotiation.

Multi-Sourcing

Multi-sourcing involves the outsourcing of different services and/or different components of services to multiple service providers. Some organisations may have developed a multi-source outsourcing model, contracting for different IT services on an ad hoc basis over time, without any particular planning. The key benefit of multi-sourcing is that it allows organisations to contract with the best service provider for each particular service or component of a service.

However, multi-sourcing can result in complex chains of responsibility and accountability. As a result, it can be difficult to administer from the customer's perspective. As such, conscious multi-sourcing can often be a preferred approach, whereby the customer's ecosystem of suppliers is subject to common terms that mandate common governance rules, inter-supplier collaboration and a well-designed and managed service integration and management layer.

Other Models of Outsourcing

Alternative models of outsourcing arrangements are less common in the New Zealand market but may be selected in response to the unique commercial circumstances of the parties. These include joint ventures, captive centres and build-to-operate transfers.

Joint Ventures

Parties may wish to set up a joint venture or partnership, where both entities have voting rights in connection with the provision of the services. This affords the customer a greater degree of control over the operations of the service provider than simply agreeing to a contract on an arm's length basis. However, this model is typically perceived to be an expensive option and can result in the customer taking on additional obligations that may not be within its expertise.

3.3 Digital Transformation

The contract models for cloud computing, SaaS and IaaS services are similar to that of an outsourcing arrangement. They are typically governed by a master or framework agreement, with each service falling under a separate service schedule or statement of work. As such, the comments in **3.1 Standard Contract Model** also apply to contract models for such services. AI clauses are becoming more common in contracts related to AI-enabled services. In New Zealand, there is currently minimal guidance regarding standard model AI clauses, and it is not expected that further government-issued guidance (or suggested clauses) will be provided in the near future. The Australian AI Model Clauses, developed by the Australian Digital Transformation Agency, serve as a useful reference for guidance.

4. Contract Terms

4.1 Customer Protections

Customer protections in outsourcing contracts differ depending on the nature of the services being provided. However, a few commonly used customer protections are discussed here.

Warranties

The customer will typically require warranties from the service provider in order to protect the customer in key risk areas. Such warranties usually relate to the quality of service, the expertise and personnel of the service provider, obtaining (and maintaining) required consents and licences, and IP. A breach of the war-

ranties by the service provider would typically entitle the customer to bring a damages claim against the service provider for breach of the agreement.

Service Levels and Service Credits

Service levels and service credits are a further protection typically included in IT outsourcing contracts. Service levels are agreed performance metrics in respect of the services and/or components of the service. These vary depending on the type of service being provided but commonly include availability, response and resolution times and reporting obligations. Service levels can be used as a measure of the service provider's performance under the contract and the customer will usually seek to supplement these with a service credit regime in the event of service-level failures.

A service credit is an agreed reduction in price so as to reflect that the service provider's performance has not met the agreed standards. However, service credits that amount to a "penalty" are unenforceable in New Zealand, as discussed further in **4.3 Liability**. A customer will typically also include reporting and audit rights in relation to the service levels, thereby ensuring that it is able to monitor and verify the service provider's performance against the same (which it may otherwise be unable to do).

A customer may also seek to include milestones in particular statements of work, with the service provider receiving a specific payment if it meets the relevant date for achievement of that milestone. Conversely, failure to meet the relevant date may result in a discount on the price for the relevant service and/or deliverable. This incentivises the service provider to complete work in a timely and efficient manner, in addition to providing the customer with protection against unreasonable delays and additional costs (particularly in the initial transition phase).

Termination and Termination Assistance

The customer will want to ensure that it has sound termination rights in the contract, as further discussed in **4.2 Termination**. The customer may also seek to include a termination assistance regime, which requires the service provider to help the customer transition the services to a replacement service provider or in-house in the event that the agreement comes to an end. The outsourcing contract will typically require the parties to agree on an exit plan at the outset of the agreement, with obligations to continually refresh the same throughout the term of the agreement.

Relationship Management and Governance

Practising good contractual management is another way that a customer may obtain some protection and mitigate its risks in an outsourcing contract. To achieve this, the customer may seek to include specific governance requirements such as regular meetings, the appointment of a dedicated service-provider relationship manager, rights in respect of the replacement and removal of key personnel, and strong reporting and audit rights. These rights are particularly important in the context of outcomes-based outsourcing arrangements.

The contractual rights should be supported by a capable in-house team and relationship manager who are able to monitor the service provider's performance against contracted standards and enforce contractual protections afforded to the customer where required.

Indemnities

The customer may seek indemnity protection from the service provider in respect of certain key losses, including third-party breach of IP rights and breach of data protection laws. The liability regime in respect of a breach of these indemnities is discussed in **4.3 Liability**.

Business Continuity and Disaster Recovery

The customer will also typically seek to receive assurances from the service provider in respect of its business continuity and disaster recovery plans and may include obligations to review, test, update and report to the customer regularly or on request. This is also a mandatory regulatory requirement imposed on New Zealand banks, as discussed in **2.2 Industry-Specific Restrictions**.

Step-In Rights

Step-in rights were once commonly requested by customers in outsourcing arrangements for critical services, whereby the customer would have the right to

step into the shoes of the service provider in the event that the service provider materially failed to perform. However, "soft" step-in rights (eg, the right to make recommendations to the service provider and work with the service provider to improve service delivery in the event of significant failures) are agreed as a solution far more frequently.

4.2 Termination

Customary termination rights in outsourcing contracts vary depending on the nature of the services being provided. Where the services involve a significant portion of the customer's business (eg, an infrastructure outsourcing contract), the service provider will generally have very limited rights to terminate the contract – often only in the event that the customer has failed to pay an overdue invoice after receiving notice and a chance to settle that overdue invoice. However, a contract for discrete services or services that are readily replaceable by the customer may provide the service provider with additional termination rights, such as the right to terminate for material breach by the customer.

Right to Terminate

Customers typically seek to include a right to terminate for the service provider's material breach if this remains unremedied for a certain period of time (or cannot be remedied) and in circumstances where the service provider suffers an insolvency event or a persistent "force majeure" event. Following the advent of COVID-19, customer organisations have been increasingly careful to ensure that known pandemics, epidemics and associated government rules and restrictions do not constitute events of force majeure that would provide the service provider with relief from its responsibilities. In addition, the agreement may include a right for the customer to terminate in the event of specific contractual failures that do not meet the standard of a "material" breach – for example, serious or repeated service-level failures or failure of the service provider to meet specific milestones in respect of the services or deliverables.

The customer may also wish to include a right to terminate the agreement for convenience. However, this may be subject to a minimum term and it is common for the service provider to require the payment of termination compensation in these circumstances (particularly if the service provider plans to invest significant resources at the beginning of the arrangement on the basis that those costs will be recouped over the full term of the contract).

Additional termination restrictions may also apply in respect of the outsourcing of services by New Zealand banks. These restrictions largely operate to limit a service provider's ability to terminate contracts in the event that the bank goes into statutory management.

If no specific termination rights have been agreed in the contract, each party generally has a right to terminate the agreement for a "material breach" of the other party under common law. However, it is commonplace for contracts to include a detailed contractual termination regime.

Disengagement Assistance

Customers will usually seek disengagement assistance from suppliers post-termination, especially if the outsourcing or technology transaction relates to core business-critical technology and services. This is to ensure that the customer can successfully and smoothly transition the services to a replacement service provider. The particulars of the disengagement assistance are usually recorded in a disengagement plan approved by the customer, whereas the mechanism for producing the disengagement plan and the period for which the assistance must last are usually recorded in the agreement. Disengagement assistance is typically at the customer's cost, unless the contract provides that the supplier must bear the costs for such services in certain circumstances – for example, where the customer has terminated the contract because of the supplier's material breach.

Data Transfer/Disposal

Where the supplier holds customer data, customers typically seek the right to have their data either destroyed or returned to the customer on expiry or termination of the agreement. If the supplier is destroying the data, customers usually require certification from the supplier that they have done so.

Under the Privacy Act, an agency may not hold personal information for longer than is required for the purpose it may lawfully be used for. Customers

typically seek to restrict the supplier's rights to retain personal information on expiry or termination of the agreement in order to ensure compliance with the Privacy Act.

4.3 Liability

Liability at Law

The liability provisions are typically heavily negotiated in outsourcing contracts. It is common for the liability of both parties to be subject to a liability cap, with the quantum of that liability cap varying depending on the circumstances. In New Zealand, the courts will generally enforce such clauses where they are negotiated at arm's length between commercial parties. There is scope, under the Fair Trading Act 1986 (FTA), to challenge their enforceability if one of the parties is a "consumer" or for standard-form business-to-business contracts with a value of less than NZD250,000.

Liability in Contract and Loss of Profit, Goodwill and Business

Service providers will usually seek to exclude all "indirect" or "consequential" losses. Whether a loss is "direct", "indirect" or "consequential" depends on the context of the contract in which the words were used and is therefore a question of fact depending on the circumstances of the situation.

The New Zealand courts adopt an objective approach to this question. The aim is to ascertain the meaning that the clause would convey "to a reasonable person having all the background knowledge which would reasonably have been available to the parties in the situation in which they were at the time of the contract". In circumstances where the meaning of "consequential and indirect loss" is ambiguous, and the court is unable to discern what the clause from the contract is intended to mean as a whole and the factual matrix, the courts have been prepared to adopt the contra proferentem rule. This "tie-breaker" rule construes the meaning of these words against the party who drafted the clause in which these words were included.

To create more certainty as to what is recoverable in the event of a loss, the parties will often specify certain key losses as deemed direct (and recoverable) losses. Common examples of specified "deemed direct" losses include (but are not limited to):

- the reasonable cost of procuring alternative systems;
- the reasonable cost of implementing workarounds; and
- the costs incurred in taking steps to remedy the other party's breach.

Categories of Losses Excluded From a Liability Cap

The parties may also seek to include certain key uncapped heads of loss in the contract, such as breach of confidentiality, breach of the provisions relating to IP rights, wilful default, and fraud. Additionally, in the event that service providers have access to the personal information of the customer, customers typically seek uncapped liability for the service provider's breach of its data protection obligations, or look to agree a separate (higher) "super-cap" for such breaches.

Service Credits

Customers often seek to include service credits in the event of service-level breaches or seek other amounts that are payable should the service provider breach relevant terms of the contract (eg, failure to meet specific milestones). Such clauses are known as "liquidated damages" and disproportionate liquidated damages clauses in contracts (ie, penalty clauses) are unenforceable in New Zealand.

The test for whether or not a damages clause is a penalty is the same as in the United Kingdom. A provision will be a penalty only if it is a secondary obligation that imposes a detriment out of all proportion to any legitimate interest of the customer in the enforcement of the primary obligation. This is important to keep in mind when drafting liquidated damages clauses. It may be helpful to provide a justification that outlines the interest being protected – and the interest in enforcement – when drafting the relevant clause.

The service provider will typically also have insurance obligations in order to support the liability regime.

4.4 Implied Terms

Businesses may be protected against unfair commercial practices in New Zealand through the FTA, which prohibits a service provider from misleading or

deceiving another person and making unsubstantiated representations in trade.

Fair and Reasonable Contract Terms

It is common for the parties to expressly exclude the terms of the FTA and other implied consumer protections – for example, those pursuant to the Consumer Guarantees Act 1993 – in outsourcing and technology contracts and to instead document the specific warranties and service commitments applicable to the arrangement in the contract terms. However, certain provisions cannot be contracted out of in B2B transactions, where to do so would not be "fair and reasonable" (noting that the test of fairness explicitly considers the relative bargaining power of the two parties).

The unfair contract terms regime in the FTA, which traditionally only applied to consumer contracts, has been extended to also apply to standard form, non-negotiated B2B contracts with an annual value of less than NZD250,000 under the Fair Trading Amendment Act 2021 (the "Amendment Act"). The Amendment Act has also been expanded to introduce a statutory prohibition on unconscionable conduct in trade. While "unconscionable conduct" is not defined, the government has provided that the intention is for the prohibition to address similar conduct as in Australia, where the courts have found that conduct is unconscionable if it is "against conscience by reference to norms of society". The Australian courts have stated that such norms can include acting honestly, fairly, and without deception or unfair pressure; the New Zealand courts are likely to take a similar approach when assessing such conduct.

Implying Terms Into a Contract

Given the typically high-value and heavily negotiated nature of outsourcing and technology contracts for core business-critical technology, the New Zealand courts will be reluctant to imply terms into the contract – on the basis that, if the parties wanted the term to be part of the bargain, they would have set that out in the contract expressly. Specifically, in contrast to the UK and Australian positions, New Zealand courts have tended to be reluctant to imply a universal doctrine of good faith into commercial contracts.

The agreement of warranties, standards and prescribed obligations is therefore an important stage in the negotiation of outsourcing and technology contracts. However, the courts may still imply terms into outsourcing and technology contracts in some cases – for example, where it is necessary to make the contract work. The courts adopt the following test to determine whether a term should be implied in the contract.

- The term must relate to a business custom that is so well known that the parties must have known of it and intended it to form part of the contract.
- The term must be certain and reasonable.
- There must be clear and convincing evidence of the custom (unless the doctrine of judicial notice applies).
- The term must not be contrary to an express term of the contract or inconsistent with the tenor of the contract as a whole.

4.5 Data Protection and Cybersecurity

Contractual Protections on Data and Security

There has been an increased focus on privacy, data protection and security in outsourcing and technology contracts. Where an outsourcing arrangement or particular piece of technology relates to or involves the processing of data (and, in particular, personal data), the underlying contract will likely include:

- provisions ensuring that consent has been given to the sharing of that data with the service provider;
- provisions requiring the service provider to monitor and report security, data and privacy breaches when data is shared and provide the customer with all information and assistance reasonably required in respect of the same;
- restrictions on the transfer of information outside New Zealand;
- restrictions or limitations on onward transfers of information from the service provider to sub-processors or other third parties;
- provisions ensuring that individuals are provided with the requisite rights in relation to their personal data; and
- provisions demonstrating that the service provider complies with the Privacy Act and, where applicable, the EU or UK GDPR by:

(a) appointing a privacy officer (or data protection officer);
(b) providing training to staff; and
(c) meeting other general requirements regarding the security of information.

The customer may also seek to require that the service provider comply with the customer's security policies and/or other specified standards. The customer would also typically include audit rights in respect of the security standards and obligations on the service provider to provide the customer with the results of its security testing. The privacy, data protection and associated security obligations may also be supported by an express acknowledgement that the service provider's liability for a breach of the same is uncapped or subject to a separate, higher cap (as further discussed in **4.3 Liability**).

Business Continuity

Customers typically require suppliers to provide assurances regarding business continuity – for example, by requiring the supplier to:

- create and maintain an effective business continuity and disaster recovery plan;
- have effective back-up and disaster recovery solutions in place to ensure that critical systems are not impacted by a cyber-attack (for example) or other outage; and
- undertake regular testing of their business continuity plans to ensure they are effective when implemented in a real-time setting.

Customers will often contract for resiliency in critical systems by, for example, requiring the supplier to maintain a warm standby system or otherwise procuring or maintaining fully resilient failover functionality.

4.6 Performance Measurement and Management

Service levels (and associated performance reporting) and related credits or other rebates for failures are commonly used as a mechanism for supplier performance measurement and management under technology transactions and outsourcing arrangements. Please refer to the comments in **4.1 Customer Protections** (Service Levels and Service Credits).

The following are among the other mechanisms that are commonly included in IT contracts to help the customer manage and measure the supplier's performance.

- Key performance indicators (KPIs) or milestones, together with associated reporting obligations on the supplier, are usually time-bound (eg, the supplier has to perform a requirement by a particular date or within a specified timeframe). There can be consequences linked to a supplier not meeting KPIs – for example, the customer can terminate the contract without liability if three or more KPIs are not met within a three-month period.
- Performance notice mechanisms typically involve the customer issuing a performance notice to the supplier in the event of a service-level failure or other supplier breach and an obligation on the supplier to rectify the relevant issue. The customer will usually have the right to terminate the agreement if the supplier receives a specified number of performance notices in a period (eg, three are received in a six-month period).
- Specific reporting and governance requirements are commonly included to ensure the supplier shares relevant information with the customer and meets regularly with the customer to discuss any performance issues. This could include a review of any service levels, KPIs or milestones that are included in the agreement.
- Customer audit rights are also commonly included so the customer can gather information regarding the supplier's performance of the services or visit supplier premises to observe performance of the services.

4.7 Digital Transformation

The contract terms discussed in **4. Contract Terms** would also apply to technology or outsourcing contracts for cloud-based solutions. However, it is not always the case that the supplier of the cloud-based solution will provide all of the relevant services. It is common for third-party service providers to provide implementation and/or support services in relation to a cloud solution provided by the supplier. In these circumstances, it is likely that customers will place certain obligations on the supplier of the cloud solution with regard to:

- co-operating with the third-party implementation and/or support partner;
- limiting the customer's liability for any delays caused by the implementation partner during transition; and
- the right to terminate the contract with the supplier of the cloud solution should implementation under the customer's contract with the implementation partner fail.

A customer is likely to seek similar corresponding provisions in its contract with a third-party implementation and/or support partner.

Although rarely in the case of commercial off-the-shelf SaaS solutions, suppliers of more business-critical and/or customised software may sometimes agree to place the source code of their proprietary software in escrow for the customer's benefit. The parties may engage a third-party escrow agent who will keep the source code in escrow and oversee its release. The "release" events for the source code are usually negotiated by the parties and may include:

- termination for cause by the customer; or
- the supplier suffering an insolvency event.

5. Employment Matters

5.1 Employee Transfers

There are no rules that apply specifically to employee transfers for outsourcing (as opposed to transfers for other commercial reasons) in New Zealand. Employees are divided into two groups for the purposes of a transfer that arises in the context of a "restructuring" (which includes the outsourcing of work or the sale or transfer of all or part of a business).

Cleaning, Food Catering and Security Employees

Employees who perform cleaning, food catering or security work have the right to choose to transfer to the new service provider of the work on the same terms and conditions of employment, with service with the past provider recognised by the new provider. Leave entitlements transfer with the relevant employee. However, there are no additional restrictions on subsequent redundancies by the new service provider.

All Other Employees

There is no statutory right for any other employees to transfer to the new service provider. As such, the new service provider may – but is not required to – offer such employees employment on whatever terms and conditions it chooses (provided that minimum New Zealand employment law entitlements are met).

Market Standard

The potential for employee transfers is generally considered part of the broader commercial terms to be negotiated between the parties in New Zealand. This is the case regardless of whether the employees have the right to transfer – in which case, the additional potential liability may affect the contract price – or whether employment would need to be offered to (and accepted by) the employees that were to transfer.

There is often a tension between the motivations of the customer and the new service provider when considering the terms and conditions of employment to be offered by the new service provider. Although these are ultimately a matter for the new service provider, this is something in which the customer usually has an interest and about which the customer may wish to make recommendations. The new service provider will typically want to ensure that the terms offered to such transferring employees are consistent with the market and with the terms of other similar employees.

The customer will often want to ensure that the terms are the same as – or close to – the current terms and conditions of employment, as this is the best practical way to minimise employment issues. In addition, if the customer's employees transfer with the outsourcing and there is a contractual entitlement to redundancy compensation, the customer will usually want to ensure that (if possible) the offer of employment by the new service provider is such that this compensation is not triggered. There is no statutory entitlement to redundancy compensation or severance in New Zealand.

5.2 Role of Trade Unions or Workers' Councils

If an employer contemplates outsourcing that could lead to redundancies, it must consult with affected employees prior to making a decision. This is the case even if the new service provider would offer employment to all affected employees on the same terms and conditions of employment. Should the obligation to consult be triggered, the employees may decide whether they involve their union. However, if employees belong to a union, the union would typically be involved in consultation as the representative of affected employees. There is no independent obligation to consult with a union although there may be a contractual obligation to do so under a collective agreement.

Unlike other larger jurisdictions, New Zealand does not have workers' councils.

5.3 Offshore, Nearshore and Onshore

There has been no change in the frequency of – or customer preference for – onshore, offshore or nearshore resources in outsourcing transactions in New Zealand. There is typically always a desire by local organisations to ensure a minimum onshore presence of supplier personnel in New Zealand, even when contracting with large overseas outsourcing service providers. The requirement varies from client to client; however, for larger-scale outsourcings, a requirement of at least 20% onshore personnel can be expected.

5.4 Remote Working

Several legal issues arise when considering the possibility of remote working by employees.

First, it is important to consider whether an employee is asking to work from home or whether the request is being made by the employer. An employer may only require an employee to work from home if the employee agrees. Consent could be obtained in the "place of work" clause in an employee's employment agreement. Although an employee can ask to work from home (and an employer has an obligation to consider this request), an employee will require permission from their employer to work from home. An employee can make this request in the context of a request for flexible work; however, an employer is only required to genuinely consider such a request and cannot be compelled to agree.

Second, if an employee is to work from home, the following legal considerations apply:

- Health and safety obligations: The employer will need to be satisfied that the employee has a safe place to work, and this may require a workstation review or the provision of equipment.
- Employment obligations: An employer must put systems in place that monitor hours of work in order to ensure minimum rates of pay are met.
- Confidentiality obligations: Depending on the nature of the work, the employer may wish to ensure that the employee is able to comply with confidentiality obligations in a home environment.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com