Cloud and ICT Outsourcings (UAE)

by *Ksenia Andreeva*, *Anastasia Dergacheva*, and *Alena Neskoromyuk*, *Morgan, Lewis & Bockius LLP*

Law stated as of 01 May 2026 • Middle East, United Arab Emirates

This Practice Note considers the specific issues that may arise when carrying out the disparate activities commonly involved in an information and communications technology (ICT) outsourcing in the United Arab Emirates (UAE), including the use of the cloud. This Note helps in-house lawyers and private practice attorneys to advise on outsourcing that involves the provision of services, or the transfer of data or assets, outside of the UAE. It also explores how to address common issues and provides measures to manage the associated risks.

The term outsourcing refers to any type of external service arrangement where either:

- The services being delivered from within an organisation (or by another group entity within an organisation) are to be delivered instead by an external third party.
- The externalised services that a third party is already providing are being considered for review and the related services contract for renewal.

The term outsourcing tends to be applied less frequently to transactions that are, in substance, outsourcing arrangements in all but name, for example:

- Certain cloud computing services.
- Digitisation projects and services.
- Technology platform managed services.

It is therefore important to analyse and understand the elements of such transactions to ensure that good outsourcing practices, risk management disciplines, deal optimisation, and suitable contract terms apply where appropriate and practical, regardless of whether the transaction is called an outsourcing.

Due to the reliance by businesses on computer systems, most outsourcing transactions involve an information technology (IT) element. That said, no two transactions involving an IT outsourcing are likely to be the same. IT and ICT (information and communications technology: a broader term encompassing communications services) cover a range of disparate commercial services. Frequently outsourced services include:

- Provision of data centre services.
- Helpdesk and call centres.
- Desktop, voice, and data networks.
- Other network and communications services.
- Applications support and maintenance.
- Applications development.

- IT procurement, and contract and vendor management.
- Project management.
- Disaster recovery and business continuity.

Despite this, ICT outsourcing projects often share common characteristics, including:

- The provision of an ICT service, which may include cloud computing.
- The transfer of assets, which may include complex IT systems, equipment, or other hardware.
- The transfer of employees, most commonly IT staff with relevant experience in understanding, operating, and maintaining the relevant IT systems.
- The transfer or processing of data connected with the IT systems, often including personal data.
- The provision of managed services, which involve the delivery and management of network-based services, applications, and equipment.

This Note considers the specific issues that may arise when carrying out some of the disparate activities involved in an ICT outsourcing in the United Arab Emirates (UAE), including the provision of cloud services, and how to address these issues.

As by their nature IT services often cross borders, this Note also considers the situation where the outsourcing involves the provision of services, or the transfer or processing of data or assets, outside of the UAE.

In this Note:

- The client or customer engaging an ICT outsourcing or cloud project is referred to as the customer.
- The cloud services provider or the IT service provider undertaking that project is referred to as the service provider.
- The cloud services or outsourced services are referred to as the services.
- The cloud service or outsourcing agreement is referred to as the services agreement.

Onshore and Offshore Jurisdictions

Within the UAE, various legal frameworks can apply to ICT outsourcing depending on the jurisdiction. The UAE legislative landscape consists of:

- Federal legislation.
- Legislation of the individual emirates (which, together with federal legislation, comprise "mainland" or onshore legislation).
- Regulations applicable in the multiple free zones (see *Practice Note, Onshore and Offshore Jurisdictions in the UAE: Overview: Free Zones*), including the two financial free zones:
    - the *Dubai International Financial Centre* (DIFC); and
    - the *Abu Dhabi Global Market* (ADGM).

The DIFC and ADGM each have their own set of comprehensive laws and regulations, financial regulators, and courts:

- The DIFC operates under common law, which is based on the English legal system to a high extent, and relies on precedents from courts in the UK.
- The ADGM also operates under common law but, unlike the DIFC, English law generally applies directly in the ADGM through the ADGM's *Application of English Law Regulations 2015*.

These jurisdictional variations create a complex landscape for ICT outsourcing, which must be assessed based on the unique requirements and context of each outsourcing arrangement.

For more information, see:

- *Practice Note, Onshore and Offshore Jurisdictions in the UAE: Overview*.
- *Practice Note, Legal and Regulatory Framework: Overview (ADGM)*.
- *Practice Note, Legal and Regulatory Framework: Overview (DIFC)*.
- *Quick Compare Chart, Free Zones in UAE - Overview of Legislative, Regulatory and Judicial Framework*.
- *Quick Compare Chart, Legal Regimes for Onshore, Offshore, and Free Zone Companies in the UAE*.

Data Issues

An ICT outsourcing or cloud project typically involves the transfer or processing of personal data (for example, employee or customer data) to be managed for internal purposes through the outsourced service or system. The outsourcing may itself generate new and unique data sets, which may have value to either the customer, its service provider, or both.

While data regulation was initially focused on privacy concerns, such as where data identified living human individuals, or sensitive or confidential information, the misuse of which could cause business damage or security concerns, regulation is now expanding to cover many different aspects of data usage, control, access, and removal.

Common data issues to address as part of ICT outsourcing or cloud arrangements include:

- Any restrictions on how data can be used, processed, and shared, including by whom, where, at what locations, and for what purposes.
- Any restrictions on how data may be transferred (particularly, whether it can be transferred across borders).
- Which party (if any) is entitled to asset ownership or control over that data (including any data that might be derived from it) and who takes regulatory responsibility for it.
- Any positive obligations to provide access to that data (for example, to facilitate switching services or prevent vendor lock-in).
- Any contractual restrictions or obligations that parties must put in place to comply with applicable legislation or regulatory requirements.

Data Transfer, Localisation, and Processing Restrictions

Many jurisdictions govern (and, often, restrict) the transfer or processing of data. This applies most commonly to:

- Data that presents privacy concerns, such as where it identifies a living human individual (commonly known as personal data).
- Sensitive data that may present national security issues.

In some cases, a jurisdiction may also impose data localisation requirements for certain types of valuable or sensitive data, such as health-related data.

Data Processing Restrictions: Onshore

In the ICT outsourcing context, it is common for businesses to delegate certain data processing activities to third-party service providers, known as outsourced processing. This involves tasks such as storing, managing, or analysing data on behalf of a business. Therefore, data protection requirements are highly relevant to ICT outsourcing arrangements, and businesses must ensure compliance with applicable regulations.

While data protection laws in the UAE are still evolving, there has been significant progress recently. The UAE's data protection laws are developing to align with international data protection standards, such as the EU's **General Data Protection Regulation ((EU) 2016/679)** (GDPR), making it possible to draw parallels regarding outsourced processing.

Notably, *Federal Decree Law No. 45 of 2021 Concerning the Protection of Personal Data* (Federal Data Protection Law) marked the emergence of the first comprehensive federal data protection law in the UAE.

Where entities provide outsourced processing services, the Federal Data Protection Law mandates that controllers engage processors who demonstrate the ability to implement effective technical and organisational measures to ensure compliance with legal requirements. Processors must handle personal data:

- Only as instructed by the controller.
- In line with the terms of a formal agreement, which must explicitly outline:
    - the purpose, scope, and subject matter of the processing;
    - the types of personal data; and
    - the categories of individuals whose data is involved.

Data Processing Restrictions: Free Zones

Separate from the Federal Data Protection Law, certain free zones (see *Onshore and Offshore Jurisdictions*) have their own data protection legislation:

- The *Data Protection Law DIFC Law No. 5 of 2020* as amended by *DIFC Amendment Law DIFC Law No. 1 of 2025* (DIFC Data Protection Law) and interpreted by the *DIFC Data Protection Regulations of 2023* (DIFC Data Protection Regulations).
- The DIFC's Commissioner of Data Protection also issued practical guidance on the DIFC Data Protection Law in its *Guide to Data Protection Law*.
- The *ADGM Data Protection Regulations 2021* (ADGM Data Protection Regulations), which are supplemented by the *Data Protection Regulations (Substantial Public Interest Conditions) Rules 2025*.

Where processing is outsourced under the DIFC Data Protection Law, organisations must implement sufficient technical and organisational measures to comply with applicable legal standards and safeguard the rights of data subjects. Controllers and processors must enter into a formal agreement that governs the processing, which addresses:

- The subject matter and the duration of the processing.
- The nature of the processing.
- The purpose of the processing.

- The type of personal data and data subject categories involved.
- The controller's rights and obligations regarding the processing.
- The processor's express commitment to process the personal data strictly as instructed by the controller.
- The extension of confidentiality and data processing obligations to any individuals who are authorised to process the personal data.

(Article 24(5), DIFC Data Protection Law.)

The ADGM Data Protection Regulation similarly requires a formal agreement between the controller and processor, which addresses:

- The processor's commitment to process the personal data only on documented instructions by the controller.
- Imposing binding confidentiality obligations on individuals involved in the processing of the personal data.
- The processor's obligation to assist the controller through appropriate technical and organisational measures that are fitting for the nature and type of the processing.
- The requirement to delete or return the personal data to the controller when the services are complete (on the controller's request).

(Section 26(3), ADGM Data Protection Regulations.)

Data Transfer Restrictions: Onshore

The UAE's data protection laws also provide requirements relating to cross-border personal data transfers. Personal data can be transferred to jurisdictions with a "proper protection level" (Article 22, Federal Data Protection Law).

Where the destination country does not have a proper protection level, transfers may be allowed under specific conditions:

- The UAE has a bilateral or multilateral agreement about data protection with the destination country.
- The data subject's express consent is validly obtained.
- The transfer is necessary to:
    - fulfil obligations and establish, exercise, or defend rights before judicial entities;
    - sign or implement a contract between the controller and the data subject (or the controller and third parties) to service the interest of the data subject;

- implement an action related to an international judicial cooperation; or
- protect the public interest.

(Article 23, Federal Data Protection Law.)

Non-compliance can result in administrative sanctions (Article 26, Federal Data Protection Law) and, in more severe cases, criminal liability (imprisonment and fines) under *Federal Decree-Law No. 34 of 2021 On Countering Rumors and Cybercrimes*.

Data Transfer Restrictions: Free Zones

Where the DIFC Data Protection Law or the ADGM Data Protection Regulation govern the transfer, cross-border data sharing is allowed to jurisdictions with an adequate level of data protection (like the onshore position).

However, the DIFC and ADGM websites provide definitive lists of jurisdictions designated as having an adequate level of protection (see *DIFC: Data Export & Sharing*; *ADGM: Adequate Jurisdictions*). Where the destination jurisdiction is not designated in this way, data transfers can be made if additional contractual and regulatory conditions are met and appropriate transfer mechanisms are implemented. Article 27 of the DIFC Data Protection Law (as amended by *DIFC Laws Amendment Law DIFC Law No. 2 of 2022*) and sections 42 and 43 of the ADGM Data Protection Regulation set out these requirements for the respective jurisdictions. These conditions can be satisfied, for example, by the parties:

- Entering into relevant approved model clauses, commonly known as standard contractual clauses (SCCs) (see *DIFC: Data Export & Sharing*; *ADGM: Office of Data Protection Guidance*).
- Having binding corporate rules (BCRs) in place. BCRs are legally binding and enforceable internal rules and policies that multinational companies can rely on for cross-border intragroup data transfers.
- Implementing other appropriate safeguards, as specified in the respective regulations.

Data Localisation Requirements: Onshore

The UAE requires data localisation in some instances. For example, *Federal Law No. 2 of 2019 Concerning the Use of the Information and Communications Technology in Health Fields* (ICT Health Law) imposes specific requirements and procedures for health information and data related to health services. This data cannot be stored, processed, generated, or transferred outside the UAE unless either:

- An exception specified in the *UAE Ministerial Resolution No. 51 of 2021 Regarding the Cases in Which Health Data and Information May Be Stored or Transferred Outside the Country* (Health Data Resolution) applies.
- Direct approval is obtained (Article 13, ICT Health Law).

While the Health Data Resolution outlines exceptions for health data transfers and does not explicitly require exemption approvals, such approvals are often necessary in practice. The criteria and process for obtaining exemptions vary across the seven Emirates, as each health regulatory authority independently implements the ICT Health Law based on its own regulations. A violation of the data localisation requirement can result in fines between AED500,000 and AED700,000 (Article 24, ICT Health Law). Any healthcare data must also be kept for at least 25 years from the date of the most recent procedure performed on the patient.

Another localisation requirement has been introduced regarding data collected and shared by **Internet of Things** (IoT) devices. Certain types of IoT data, which are classified as secret, sensitive, and confidential data, must primarily be stored in the UAE. However, it is possible to store such data outside the UAE if the destination country adheres to the same data protection principles and rules as those in the UAE.

Data localisation requirements may also apply in the context of financial services, such as under the *Consumer Protection Regulation (Circular No. 8 of 2020)*. Under the Consumer Protection Regulation, licensed financial institutions (LFIs), which the *Central Bank of the UAE* (CBUAE) regulates, must store data about transactions or consumers within the UAE as prescribed by the CBUEA.

Given the complex data protection framework in the UAE, companies engaging in outsourced processing (in the context of ICT outsourcing or otherwise) should carefully consider which laws and regulations apply to their activities. To comply with the relevant laws and regulations, businesses should:

- Ensure that their outsourcing agreements include:
    - appropriate data processing terms;
    - confidentiality obligations;
    - security measures; and
    - clear instructions for processors.
- Assess any restrictions on transferring data outside the UAE (or a specific free zone).

Data Ownership, Control, and Access

The legal ownership of data can be a tricky issue with parties usually citing traditional legal rights such as copyright, and rights in trade secrets or confidential information, to restrict access to and use of data. However, these legal structures may not provide a satisfactory basis for ownership of data.

Data ownership in the UAE poses similar questions. In the outsourcing context, data ownership mostly pertains to the legal rights (including contractual and IP rights), responsibilities, and control over data that service providers process or manage. There is no clear indication that data can be owned in the same way as a chattel or land on the basis of traditional property rights.

Ownership of data in ICT outsourcing agreements largely depends on the contractual terms between the service provider and the customer. The customer typically owns data processed as part of the ICT services or cloud project unless the contract specifies otherwise. Many UAE entities prefer to retain ownership over all data processed, especially given regulatory considerations in sectors like finance, healthcare, and government services.

The ownership of data generated by the ICT services or cloud projects, such as business insight data or analytics derived from the outsourced services, may be more complex. Service providers may seek rights to use or commercialise such data, but UAE contractual arrangements often prioritise customer control.

Accordingly, businesses outsourcing their ICT functions should ensure that their contracts with service providers include clear terms regarding data ownership, control, and access. In practice, this is usually achieved by including data within the definitions of IP rights or confidential information under a contract. Data can typically be protected by two IP regimes:

- Copyright, which protects data that is collected, selected, and arranged in such a way that the resulting work qualifies as an original work of authorship (*Federal Decree-Law No. 38 of 2021 On Copyrights and Neighbouring Rights* (Copyright Law)).

- Trade secrets, which protect commercially valuable and sensitive information that is known only to a limited group of individuals and safeguarded by confidentiality measures. There is no dedicated federal law defining and regulating the trade secrets regime. Instead, a patchwork of statutory provisions governs trade secrets.

Copyright protection does not extend to ideas, procedures, methods of operation, mathematical concepts, principles, or abstract facts (Article 3, Copyright Law). However, it does cover the innovative expression of any of these elements. Copyright protection also does not apply to official documents, news, or reports about current events. For more information on copyright, see *Practice Note, Copyright Litigation: Overview (UAE): Legal Framework for Copyright Litigation*.

There is no requirement to register copyright or trade secrets for these protections to apply. However, registering a copyright work may be advantageous in certain circumstances.

For trade secrets, additional steps are required to ensure protection, which may include:

- Categorising the information to be protected as trade secrets.

- Imposing access restrictions.

- Establishing contractual confidentiality obligations for employees.

- Implementing necessary organisational and technical measures to safeguard the trade secrets.

Standard ICT outsourcing agreements in the UAE frequently include clauses addressing data usage, ownership, and confidentiality considerations. Additionally, where service providers want to retain rights over derived or anonymised data, customers often negotiate explicit limitations.

Sector-specific regulations, such as the *Outsourcing Regulation for Banks (Circular No. 14 of 2021)* issued by the CBUAE, impose further obligations on financial institutions regarding data protection in outsourcing arrangements. For example:

- Banks must retain ownership of all data provided to an outsourcing service provider.
- Customers of those banks retain ownership of their data

(Article 4, Outsourcing Regulation for Banks.)

Other UAE-specific laws expressly aim to assign ownership of certain types of data. For instance, under *Dubai Law No. 26 of 2015 Regulating Data Dissemination and Exchange in the Emirate of Dubai*, the Government of Dubai owns "Dubai Data," meaning data that relates to the Emirate of Dubai and is made available to federal government entities, local government entities, and certain other entities as specified by that legislation.

Outsourcing IT Functions (Including to the Cloud) in Key Regulated Sectors

Many jurisdictions have recognised the increasing risk that ICT outsourcing and the use of the cloud can present for certain key sectors of their economy. ICT supports complex systems used for everyday societal activities, and keeps key sectors running, including finance.

Increased digitalisation and interconnectedness, and common reliance on a small pool of technology providers who are dominant in the market, also amplify ICT outsourcing risks. This makes society as a whole and, in particular, the world financial system, more vulnerable to cyber threats or ICT disruptions.

In addition, regulated organisations are increasingly outsourcing their operations to the cloud, which broadly encompasses a range of ICT services provided in various formats over the internet (for more information, see *Cloud Toolkit (International)*). This increased cloud usage gives rise to concerns on the part of regulators, including:

- Businesses finding it difficult to oversee service providers effectively, especially in the case of service providers that are dominant in the market.
- Service providers' market power adversely affecting businesses' ability to negotiate appropriate contractual safeguards and implement and test effective business continuity and disaster recovery plans.
- Risks to data security.
- Risks from sub-outsourcing in the context of service providers.

In recent years, ICT and the related outsourcing risks have attracted the attention of national and international policy makers, regulators, and standard-setting bodies, prompting attempts to enhance resilience, set standards, and coordinate regulatory or supervisory work.

Onshore Requirements

In the UAE, specific regulatory frameworks govern the outsourcing of services in banking services. The Outsourcing Regulation for Banks sets minimum standards for outsourcing arrangements that banks must follow to ensure robust risk management practices, especially where international service providers are involved (see *CBUAE: Outsourcing Standards for Banks*).

Accordingly, banks must implement policies, procedures, and controls that address the internal audit and operational risks associated with outsourcing. Outsourcing agreements must also ensure that:

- Banks retain full ownership of shared data.
- Sensitive customer data is not stored outside the UAE without:
    - the CBUAE's approval; and
    - customer consent.

The Outsourcing Regulation for Banks covers all forms of outsourcing, ranging from payroll outsourcing to IT and ICT outsourcing. The regulation's territorial scope covers entities in and outside the UAE.

Given the above, ICT outsourcing in the banking sector in the UAE remains a viable option, but it necessitates heightened scrutiny and the implementation of appropriate internal monitoring processes to ensure compliance with regulatory requirements.

To address these challenges, banks can adopt several mitigation strategies. These include:

- Conducting comprehensive risk assessments to identify potential compliance issues.
- Establishing clear contractual obligations with service providers regarding data protection and other regulatory adherence.
- Implementing continuous monitoring and auditing mechanisms to ensure ongoing compliance.
- Investing in staff training to enhance awareness of regulatory changes and fostering a culture of compliance within the organisation.

Free Zone Requirements

The DIFC and ADGM impose similar requirements for regulated entities in their respective rulebooks, ensuring compliance with local standards. In the DIFC, the *Dubai Financial Services Authority* (DFSA) *Rulebook* (DFSA Rulebook) requires DFSA-regulated entities to:

- Perform appropriate due diligence when selecting and monitoring (outsourcing) service providers.

- Implement and maintain appropriate outsourcing policies, contingency plans, and risk management programs.
- Enter into formal written outsourcing agreements with service providers.
- Establish business continuity and disaster recovery plans related to service providers.
- Introduce appropriate measures to ensure the security and confidentiality of information.
- Avoid the excessive concentration of outsourcing functions with a single service provider to mitigate risks.
- Agree on procedures with each service provider for terminating the outsourcing agreement.
- Grant the DFSA access to the service provider's books and records for inspection purposes.

The ADGM has its own rules on outsourcing contained in the *Financial Services Regulatory Authority's* (FSRA) *General Rulebook* (ADGM Rulebook). The outsourcing requirements in the ADGM Rulebook largely align with those in the DFSA Rulebook.

As with ICT outsourcing in the onshore part of the UAE (see *Onshore Requirements*), careful scrutiny and internal monitoring are advisable to meet these regulatory requirements, and appropriate measures should be put in place to that effect.

Security Issues

Security issues inherent in an ICT outsourcing commonly include:

- **Ensuring the security and operational resilience of the ICT services, and the network and information systems used to provide them**. Weak cyber or physical security controls and low operational resilience can expose the customer's operations to cyber threats or attacks, as well as other natural and human-caused risks, including natural disasters, terrorist offences, criminal infiltration, or sabotage. These risks can have critical consequences for the customer and may have wider implications for society (see *Security and Operational Resilience of ICT Services*).
- **Mitigating national security issues raised through new access to sensitive technologies.** For example, many ICT outsourcings involve the transfer of software and technology to external third parties and across borders, which can be problematic for several reasons (see *National Security Considerations*).

Security and Operational Resilience of ICT Services

Increasingly, governments across the world are looking to improve the security and resilience of ICT services by adopting regulation in this area. This recognises that many critical societal operators, such as banks and other financial institutions, increasingly rely on these services, and the interconnectedness of many ICT systems means that a vulnerability present in one system could impact multiple different entities in the supply chain and expose an entire network to increased risk.

In particular, many organisations now rely on managed service providers to provide essential digital services such as outsourcing an organisation's IT or managing key business processes. Managed service providers play a critical role in the modern global digital economy. However, when these service providers provide critical services at scale, any vulnerabilities could present a threat to the security and stability of key parts of the economy. This threat is increased because many managed service providers operate internationally and provide services across national borders. Many governments are, therefore, starting to identify managed service providers as a priority when addressing supply chain cyber security.

UAE Cybersecurity Council

In 2025, the UAE approved the *National Cybersecurity Strategy*. As part of this strategy, the *UAE's Cyber Security Council* (CSC) has updated and published a number of policies, which are aimed at corporate and governmental entities, dedicated to strengthening the country's cyber security framework. These include:

- *National Cloud Security Policy*.
- *National Cyber Security Accreditation Program*.
- *Cyber Incident Response Framework*.
- *Security Operations Centre (SOC) Baseline Capabilities*.
- *National IoT Security Policy*.
- *Cyber Security Information Sharing Framework*.
- *National Cloud Security Policy*.
- *Critical Information Infrastructure Protection (CIIP) Policy*.
- *Cyber Incident Response Plan*.

While the exact practical implications of these policies remain to be confirmed, it is generally accepted that companies are expected to comply with the guidance contained therein. Parties to a services agreement should:

- Carefully assess the policies' applicability to the outsourcing arrangement.
- Ensure that the underlying contractual structure reflects the CSC's requirements. This includes ensuring that any obligations are properly contractually passed down to the outsourced service provider for compliance purposes.
- Scrutinise guidance documents, which may contain additional obligations.
- Continuously monitor adherence to the requirements.

Further developments in the UAE's cybersecurity and operational resilience space are expected as the CSC continues to highlight the importance of building out the UAE's framework.

CBUAE Consumer Protection Regulation

More specific regulations already exist for financial services, where there is greater regulatory focus. The CBUAE issued the Consumer Protection Regulation, which sets out requirements for security and operational resilience applicable to all the LFIs that it regulates. These requirements apply to an LFI's activities, regardless of whether the LFI performs them internally or outsources their performance. The key requirements are:

- **Institutional oversight and governance.** LFIs must:
    - have robust oversight of all activities (including outsourced ones);
    - maintain up-to-date procedures;
    - conduct monitoring; and
    - ensure a culture of compliance.

    (Article 3, Consumer Protection Regulation.) When any function is outsourced, appropriate oversight systems and controls must extend to outsourced activities, ensuring service providers follow required policies and support regulatory compliance.

- **Complaint management.** LFIs are:
    - required to establish an independent complaint management function, with fair, accessible, and unbiased processes; and
    - responsible for complaints about all products or services, including those handled by agents or third parties.

    (Article 8, Consumer Protection Regulation.) If an LFI outsources complaint management or consumer support (for example, using call centres or complaint handling vendors), the LFI remains responsible for the integrity and compliance of the process.

- **Disclosure and transparency.** LFIs must provide accurate, timely, and transparent information at all stages. Disclosures must be clear, complete, and in accessible language (Article 2, Consumer Protection Regulation). If an LFI outsources disclosure-related communications or marketing activities, the service provider must deliver communications that meet all regulatory criteria.

- **Business and market conduct.** There is a requirement for LFIs to act fairly, honestly, and with professional diligence, including avoiding conflicts of interest and abusive sales practices (Article 5, Consumer Protection Regulation). Such rules of conduct extend to any outsourced activity, meaning that an LFI needs to ensure their agents and relevant third parties conduct themselves appropriately.

These rules resemble the standards that the GDPR and EU *Digital Operational Resilience Act ((EU) 2022/2554)* (DORA) impose. For more information on DORA, see *Practice Note, Hot topics: EU Regulation on digital operational resilience for the financial sector (DORA) and DORA Directive*.

From a data protection perspective, the Consumer Protection Regulation also lists well-established privacy and cybersecurity principles. These requirements include:

- Ensuring the protection and confidentiality of consumer data through the implementation of appropriate technical and organisational measures.
- LFIs must:
    - establish dedicated data management functions responsible for developing and maintaining policies, procedures, and controls to protect against unauthorised access and misuse; and
    - maintain up-to-date data policies, which comply with applicable laws and specify record-keeping and data retention periods.
- Conducting data processing on a lawful basis, ensuring consumers provide informed consent for data collection, use, and sharing, where this is legally required (see *Data Transfer, Localisation, and Processing Restrictions*).
- Secure data sharing practices must be enforced, both internally and with third parties, to prevent misuse of consumer information. For instance, appropriate transfer mechanisms need to be put into place (see *Data Transfer Restrictions: Onshore* and *Data Transfer Restrictions: Free Zones*).
- Implementing data management controls, including structured policies, procedures, and system controls to manage, protect, and monitor data effectively.
- Designing and implementing incident identification and response procedures, which should ensure that security incidents are detected, managed, and resolved as soon as they occur to minimise potential damage.
- Strengthening cybersecurity infrastructure and incorporating a comprehensive risk management approach to ensure security measures align with regulatory requirements.
- Regular training programs for employees to enhance awareness of security risks and ensure familiarity with best practices for data protection.
- Continuous monitoring of security systems, penetration testing, and reporting of identified vulnerabilities.

The above principles are particularly crucial in services agreements where significant data sharing occurs. LFIs must:

- Ensure that service providers adhere to the same data protection standards.

- Carry out regular audits and monitoring to maintain these standards.
- Conduct thorough due diligence on service providers.
- Include express compliance clauses in contracts.
- Promptly report any data breaches to the CBUAE and affected consumers.

By embedding these requirements into their outsourcing practices, LFIs effectively mitigate risks and uphold regulatory compliance.

National Security Considerations

Some software and technology, and their components, can be classified as dual use items, meaning that they have both civil and military uses. Giving an external service provider access to certain dual use technology could present unexpected national security concerns. This is particularly relevant if the service provider is based in a different jurisdiction from the customer.

In addition, governments across the world are becoming increasingly interested in scrutinising, and potentially intervening in, technology acquisitions and investments for the purposes of protecting national security interests. This reflects the fact that technology can often constitute a sensitive national security asset, and technological developments have further widened the potential scope of national security concerns to include such areas as data and IP. These regimes for intervention typically target acquisitions in technology. However, these concerns could arise where an ICT outsourcing provides outside access to a sensitive technology (by a cross-border IP licence or otherwise).

The UAE has also seen increased scrutiny of technology in terms of national security considerations (see, for example, the *UAE's Government Portal*, which sets out a variety of cyber safety and digital security measures). This heightened vigilance is directly relevant to cloud services and ICT outsourcing, as it necessitates a thorough examination of the legal and regulatory frameworks governing such transactions.

In the UAE the relevant export control regime is governed by *Federal Decree Law No. 43 of 2021 on the Goods Subject to Non-Proliferation* (Export Control Law). The Export Control Law sets forth a framework to regulate the trade of goods (including materials, systems, equipment, components, software, and technology) that are either:

- Included on the list of controlled commodities (the Control List).
- Designated by the *UN Security Council*.

The Control List, most recently updated in November 2025, includes 12 categories of commodities, including electronics (category three), computers (category four), and telecommunications and information security (category five).

The provisions of the Export Control Law are further detailed in the implementing regulations adopted by *Cabinet Decision No. 97 of 2024 Concerning the Implementing Regulation of the Export Control Law* (Export Control Implementing Regulations). The *Executive Office for Control and Non-Proliferation* (Executive Office), established under *Cabinet Decision No. 15 of 2022*, administers the Export Control Law and the Export Control Implementing Regulations.

The Export Control Law applies to the entire territory of the UAE, including free zones (see *Onshore and Offshore Jurisdictions*). For items on the Control List, the Export Control Law regulates activities concerning:

- Import.
- Export.
- Re-export.
- Provisional shipment.
- Transit shipment.
- Transport between ports.
- Brokerage.

The Export Control Law prohibits dealing with such items without a permit, as well as any delivery, transfer, publication, leaking, or sharing any document or device related to such items. It also prohibits any acts that will or may lead to any controlled commodity being used in activities related to weapons of mass destruction.

The Executive Office can also:

- Determine that a good not on the Control List is subject to the Export Control Law regime if:
  - it has sufficient evidence to suspect that the good may be used in an activity related to weapons of mass destruction; or
  - the end-user is listed on national or international lists of sanctions.
- In certain cases, seize commodities that are not on the Control List, such as where:
  - there are sufficient grounds to suspect that such commodity is to be used for a prohibited activity;
  - the end-user is listed in the national sanction lists;
  - any component of such commodity is prohibited or restricted; or
  - such commodity represents a raw material to create another commodity that is included in the Control List.
- Designate certain items on the Control List as prohibited goods and restricted goods and issue permits to deal with such goods, which are valid for at most 60 days (from the date of issuance).

The Export Control Law establishes robust penalties for a breach. Certain breaches are considered crimes against state security and trigger imprisonment and large fines. For corporate entities, the minimum fine is AED200,000, while the maximum fine is AED2 million (approximately USD550,000). The court can also dissolve the corporate body in breach.

In addition to criminal penalties, the Executive Office can apply administrative penalties, including:

- Permit cancellation.
- Fines.
- Seizure of the items or commodities in breach.
- Suspension or dissolution of a corporate entity.

It is also worth noting that, with Federal Decree No. 15 of 2022, the UAE ratified the *Common Customs Law of the Cooperation Council for the Arab States of the Gulf* (Common Customs Law), which unifies customs procedures in all member states of the **Cooperation Council for the Arab States of the Gulf** (Gulf Cooperation Council or GCC). Under the Common Customs Law, the *UAE Cabinet* has approved lists of prohibited and restricted goods in the GCC (*Cabinet Resolution No. 123 of 2024 on the Approval of the Lists of Prohibited and Restricted Goods in the States of the GCC*).

In the context of ICT outsourcing, engaging with prohibited or restricted goods may occur if the outsourced services involve handling or transferring technology that falls under these categories. Outsourcing could trigger these prohibitions or restrictions if it involves either:

- Cross-border data transfers.
- The use of technology that is classified as subject to the export controls.

Therefore, it is crucial for companies to conduct thorough legal and technical due diligence to ensure compliance with these regulations and avoid potential legal issues.

Overall, when drafting a services agreement, it is advisable to:

- Include specific provisions that address compliance with the UAE's Export Control Law and any other regulations that may apply. This should encompass obligations for both parties to adhere to relevant export control regulations, particularly concerning dual-use technology.
- Outline procedures for obtaining necessary permits and managing the transfer of controlled commodities, ensuring that all activities align with national security requirements.
- Include clauses that allow for regular audits and updates to compliance measures as regulations evolve.

Employee Transfer Issues

An ICT outsourcing or cloud project could involve the transfer (or notional transfer) of employees, particularly those:

- Familiar with the outsourced technology.
- Who work on the development or maintenance of the outsourced technology.

These employees may need to move with the business function that is being outsourced, whether as a matter of practicality or under a legal obligation.

In the UAE, there are no automatic transfer regulations for employees. Any existing employment contract and visa must be cancelled, and a new formal agreement must be entered for the new employment arrangement. This means any employee must expressly agree to a new employment contract for the "transfer" to be effective.

Under *Federal Decree-Law No. 33 of 2021 Regulating Labor Relations* (UAE Labor Law), employment may be terminated by either party at any time on notice for a legitimate reason. The UAE Labor Law does not specify what constitutes a valid reason, and therefore, in practice, the outsourcing arrangement would have to be evaluated on a case-by-case basis.

For more information, see Practice Notes:

- *Labour Laws: Overview (UAE): Termination*.
- *In-House Counsel's Overview of Labour Laws in EMEA: Business Transfers*.
- *Hiring in the UAE: Overview: Requirements on Termination*.

Tax Considerations

The global digital economy has grown rapidly in recent years, together with the number of businesses deriving profits from jurisdictions in which they have no physical presence.

The work to produce a long-term solution to the perceived failure of the international tax rules (particularly, the existing nexus and profit allocation rules, specifically the arm's length principle) is taking place at the **Organisation for Economic Co-operation and Development** (OECD), through the Task Force on the Digital Economy (TFDE) and the Inclusive Framework (see Practice Notes, OECD pillar one proposal for taxing right over largest and most profitable multinationals and OECD Inclusive Framework proposal for global minimum corporate tax rate).

The OECD has developed a two-pillar proposal to address tax challenges arising from the digitalisation of the economy (known as "pillar one" and "pillar two"). Pillar one proposes changes to traditional nexus rules for allocating taxing rights, enabling a portion of the residual profit generated by some of the largest groups (outside of financial services and extractives) to be taxed in their market jurisdictions (amount A), along with simplified rules for applying the arm's length principle to baseline marketing and distribution activities (amount B).

Pillar one would replace some existing norms for taxing multinationals and run counter to some policies that countries have put in place to tax digital companies in recent years. The most common form is a unilateral digital services tax (DST), which is a tax on selected gross revenue streams of large digital companies.

Because pillar one is focused on changing where profits are taxed, including for many large digital companies, governments are expected to repeal domestic DSTs in a transition process. However, because amount A has not been implemented, many unilateral DSTs remain. For more information, see *Pillar two toolkit* (UK).

For large outsourcing transactions, especially those with cross-border aspects, it is advisable to seek separate and specialist tax advice.

The UAE taxation system reflects the federative composition of the seven emirates, where the federal and local governments have powers to levy tax. On the federal level, the relevant taxes are the corporate tax and the value added tax (VAT).

Corporate tax is regulated by *Federal Decree Law No. 47 of 2022 Concerning Corporate and Business Tax* (as amended) and applies to an entity's net income or profit at a rate of 9% on the taxable amount exceeding AED375,000. Entities registered in free zones may benefit from a 0% corporate tax rate on income derived from qualifying activities. The corporate tax regime is new, therefore the UAE tax authorities are still developing taxation practices. As such, both providers and recipients of outsourced services are recommended to seek professional tax advice to assess their specific arrangements and determine any tax obligations under the UAE law.

Additionally, the UAE recently issued *Cabinet Decision No. 142 of 2024 on the Imposition of Top-up Tax on Multinational Enterprises*, which introduced top-up tax for subsidiaries and consolidated entities of large multinational groups (in line with Pillar Two of the OECD's Inclusive Framework).

On 1 January 2018, the UAE implemented a VAT of 5% on most goods and services, including on services provided via electronic communication (*Federal Decree Law No. 8 of 2017 Concerning Value-Added Tax*). Regarding services, the VAT treatment is uniform across the UAE mainland and multiple (but not all) free zones (see *Onshore and Offshore Jurisdictions*). If the service is provided from the territory of the UAE (including from a free zone) to an individual or legal person outside the GCC states that implement the *Common VAT Agreement of the GCC*, then the service is considered "exported" and may be zero-rated.

In relation to this, many outsourced services are subject to the UAE's VAT, including those provided via electronic communication. If the outsourced service provider is not based in the UAE but provides services to a UAE-based customer, the VAT treatment would depend on the specific circumstances, such as the location of the service provision and the nature of the services. Generally, services provided to a UAE-based customer would be subject to VAT, but specific rules may apply depending on whether the service is considered "exported" and eligible for zero-rating.

Contractual Issues

Typical contractual issues to deal with in an ICT outsourcing or cloud services project include whether the governing law and enforcement jurisdiction of the contract:

- Recognise, and will enforce:
    - any agreed service level and service credit regime (see *Service Levels and Service Credits*);

    - any agreed liability limits and exclusions (see *Liability Limits and Exclusions*);
    - specific performance of certain obligations (see *Specific Performance*); and
    - any preferred payment terms or models (see *Payment Terms*).

- Imply any minimum service standards or other protections into the contract, or any other implied terms, including an obligation for the parties to act in good faith (see *Implied Terms*).
- Allow rights of termination beyond those that the contract expressly provides (see *Termination Rights and Transition Assistance*). The following sections consider these issues and whether they require the parties to enter into a local services agreement to govern certain aspects of the outsourced services to be performed in the UAE when engaging in a global outsourcing (see *Common Contracting Structure when Engaging in a Global Outsourcing*).

In the UAE, commercial contracts are mainly governed by:

- Until 1 June 2026, *Federal Law No. 5 of 1985 On the Civil Transactions Law of the United Arab Emirates*.
- From 1 June 2026, *Federal Decree-Law No. 25 of 2025 Promulgating the Civil Transactions Law* (Civil Code), which sets out general contract law principles, including:
    - offer and acceptance;
    - valid consent;
    - capacity to enter into agreements; and
    - object and cause of contracts.

- *Federal Decree-Law No. 50 of 2022 On the Promulgation of the Commercial Transactions Law* (Commercial Transactions Law), which concerns commercial transactions, specifically addressing:
    - commercial agency;
    - sale of goods;
    - commercial obligations; and
    - other matters relevant to commercial transactions.

- *Federal Decree-Law No. 46 of 2021 On Electronic Transactions and Trust Services* (Electronic Transactions Law), which regulates the use of electronic contracts and signatures.

The DIFC and the ADGM (see *Onshore and Offshore Jurisdictions*) have their own laws dealing with commercial contracts. The key laws are:

- For the DIFC:
  - *Contract Law DIFC Law No. 6 of 2004*;
  - *Implied Terms in Contracts and Unfair Terms Law DIFC Law No. 6 of 2005*; and
  - *Electronic Transactions Law DIFC Law No. 2 of 2017*.
- For the ADGM, by virtue of the *Application of English Law Regulations 2015*, commercial contracts are predominantly governed by the laws of England (see *Contract law toolkit* (UK)).

Service Levels and Service Credits

Typically, a services agreement requires the service provider to perform the services in accordance with a set of service levels (sometimes referred to as key performance indicators (KPIs)). The parties should unambiguously incorporate the KPIs into their main agreement.

It is important that the service levels clearly address the crucial elements of the services and the standard to which the service provider must perform them. Then, the services agreement can make falling below the required level of performance by a specified percentage subject to a service credit regime.

The service level arrangements should, therefore, address the monitoring of the service levels and detail a set of service credits to address the possible failure on the part of the service provider to achieve the required service levels. This should enable the customer to seek redress for poor service without the need to pursue legal action or terminate the services agreement. Accordingly, for the customer, service credits provide a way of focusing the service provider's management on avoiding sub-standard service delivery.

However, where a service credit regime can be seen to constitute a contractual penalty, this may present enforcement issues, particularly in jurisdictions where penalty clauses are considered unenforceable on grounds of public policy or due to other local laws.

In the UAE, service levels and service credits are generally enforceable in the context of outsourcing arrangements with certain exceptions. Under the UAE's federal law, the parties must ensure that any provisions in respect of service levels and service credits are in line with the duty of good faith, as dictated by the Civil Code (see *Standard Document, Heads of Terms for Commercial Transactions (UAE): Drafting Note: Good Faith* and *Quick Compare Chart, Contracts - Good Faith and Fair Dealing*). In addition, any terms must be fair and must not contradict established custom or practice (see *Implied Terms*).

In the context of services agreements in the UAE, service levels may not be enforceable if they lack clarity or are deemed unfair. For instance, a provision requiring the delivery of "high-quality customer support" without further definition would be ambiguous. Such a clause lacks specific metrics, such as response times, resolution times, or customer satisfaction scores, leaving the term "high-quality" open to subjective interpretation. This ambiguity can lead to disputes over whether the service

provider has met the contractual obligations, ultimately rendering the service level unenforceable. To ensure enforceability, it is crucial to define clear, measurable standards that align with the parties' expectations and legal requirements.

Additionally, if the service level imposes disproportionately harsh penalties on the service provider for minor breaches, it may be considered unfair and thus unenforceable under UAE law.

Further, excessive or punitive service credits that do not align with the customer's actual losses can create complications. If service credits are disproportionately high compared to the actual impact of a service failure, they may be deemed unenforceable or unfair under the UAE's legal framework. For instance, if a service credit amounts to a penalty that far exceeds the customer's actual losses, the service provider could challenge it as a punitive measure rather than a genuine pre-estimate of loss. This misalignment can also undermine the principle of good faith and fair dealing, potentially leading to strained business relationships or even litigation.

In certain circumstances, such as under the Outsourcing Regulation for Banks, having service level agreements in place is an express requirement for regulated entities that seek to outsource certain functions. For more information on the Outsourcing Regulation for Banks, see:

- *Data Ownership, Control, and Access*.
- *Outsourcing IT Functions (Including to the Cloud) in Key Regulated Sectors*.

In practice, practitioners should adopt a broadly similar approach should in the DIFC and ADGM, though certain jurisdiction-specific differences may apply.

Liability Limits and Exclusions

In relation to the recovery of losses under the relevant services agreement, both parties should consider the types of losses that are recoverable and the cap on liability.

Where the ICT services are critical to the operation of the business of the customer, the losses that the customer could suffer if the service provider fails to provide the service could be significant. It is important, however, not to impose contractual liabilities that are disproportionate to the value of the services agreement. As a result, the parties often consider setting limits on the service provider's liability that relate to:

- Payments due under the services agreement, possibly on a multiple basis.
- The insurable level of loss on a project-specific basis.

Limitation of liability clauses are usually the subject of intense negotiations between the parties, who should ensure that the negotiated position does not go beyond those exclusions and limitations of liability that applicable law generally permits.

UAE law upholds the principle of freedom of contract, allowing parties to agree on contract terms provided their contracts do not interfere with public policy or breach mandatory provisions of law. In practice, the parties can agree to limit liability, which can take several forms, including:

- Capping total contractual liability based on specific circumstances or a maximum limit.
- Excluding consequential and indirect losses.
- Pre-defining the quantum of damages in certain cases (analogous to liquidated damages in common law jurisdictions).

Contractual provisions on limitation of liability are generally enforceable, subject to statutory restrictions, which typically prohibit a party from limiting its liability arising from:

- Tort.
- Illegality.
- Wilful misconduct.
- Death or injury.

(Articles 184, 257, and 334, Civil Code.)

While Article 334 of the Civil Code may not, at first glance, expressly address the limitation or exclusion of liability, the UAE courts have consistently relied on it as the legal foundation for this principle. For instance, in case DCC 134/2006, the Dubai Court of Cassation applied Article 383 of Federal Law No. 5 of 1985 On the Civil Transactions Law of the United Arab Emirates.

Additionally, limitations may be unenforceable if they:

- Breach the duty of good faith (see *Standard Document, Heads of Terms for Commercial Transactions (UAE): Drafting Note: Good Faith* and *Quick Compare Chart, Contracts - Good Faith and Fair Dealing*).
- Contain unfair terms.
- Contradict established custom or practice (see *Implied Terms*).

The parties may agree in advance on the amount of compensation. However, the court may reduce the agreed compensation if the debtor establishes that it is excessive, or the obligation has been partially performed, or the creditor contributed to the losses. Conversely, the creditor may claim an amount exceeding the agreed compensation if the debtor committed fraud or gross fault. Any agreement to the contrary is void under Article 340 of the Civil Code.

Implied Terms

The applicable laws of a jurisdiction can imply terms into services agreements, and parties should consider these when contracting for an ICT outsourcing or cloud project.

Under UAE law, one of the most significant statutory obligations implied in contracts is the duty of good faith. Article 221 of the Civil Code requires parties to perform contracts in accordance with:

- Good faith.
- The law.
- Customs.
- The nature of the transaction (for example, subject matter, sector, and transaction value).

The court may decide to imply a specific term into a services agreement, where it finds that either:

- It is reasonable to believe it would have been the intention of the parties to agree to such a term.
- The term is required to give business efficacy to the services agreement and the transaction in question.

The duty of good faith extends beyond mere compliance with the express terms of an agreement, requiring parties to uphold standards of fairness and cooperation in their commercial dealings. In practice, the duty of good faith:

- Prohibits contracting parties from taking unfair advantage of each other.
- Combats exploitative conduct.
- Imposes a duty of cooperation, ensuring the parties work together to:
    - fulfill the contract's purpose; and
    - avoid disputes (where feasible).

Beyond its direct application, the duty of good faith serves as a foundation for implying additional terms in contracts. When an agreement is silent on a particular matter, the courts can infer terms that are necessary to ensure it:

- Operates in a fair and reasonable manner.
- Aligns with the parties' intentions.
- Has business efficacy, meaning the agreement functions in line with commercial logic.

For more information, see *Quick Compare Chart, Contracts - Good Faith and Fair Dealing*.

For example, absent an express provision regarding a contract's duration, the court may determine that the contract should continue for a reasonable period, considering the nature of the transaction and the surrounding circumstances.

Specific Performance

An order for specific performance compels a party to perform their positive contractual obligations; that is, to do what they promised to do.

Specific performance (or the equivalent) is typically a discretionary remedy. The court can decide whether it is appropriate to order specific performance under the circumstances.

Specific performance can often be an important tool in the enforcement of ICT outsourcing or cloud arrangements, including:

- Compelling performance of a particular task that the service provider is contractually required to complete, particularly where that task is specialised, unique, or difficult for a replacement contractor to perform.
- Compelling audits, for example to enable a customer to review the service provider's performance and charges. A services agreement may require audits for regulatory reasons as well as to ensure the service provider's employees are complying with their obligations under the services agreement.
- Enforcing obligations of confidence in relation to business sensitive or confidential information that the service provider may have learnt or discovered, as part of the ICT outsourcing arrangement.

In the UAE, the court can order specific performance where monetary compensation is not sufficient. Specific performance requires the breaching party to carry out their original obligations under the contract. This remedy is particularly useful in breach of business contracts involving unique goods or real estate, where finding an alternative remedy may not be practical.

Article 234 of the Civil Code provides that, in bilateral contracts, if one party fails to fulfil its contractual obligations, the other party can (after giving notice to the defaulting party) seek either enforcement (including specific performance) or termination of the contract. This provision ensures that contractual obligations are upheld and provides legal recourse for the non-defaulting party.

However, Article 331 of the Civil Code limits specific performance right where it would be unduly onerous for the obligor. In such instances, on the obligor's request and provided this does not seriously prejudice the obligee, the judge can substitute a monetary award for specific performance.

Termination Rights and Transition Assistance

A services agreement should typically contain detailed provisions for termination and exit management. Parties should include rights of partial termination if the services are capable of separation.

When drafting and negotiating a services agreement, the parties should consider what rights of termination may apply under the law of the governing jurisdiction, even if the agreement does not express these.

Article 232 of the Civil Code governs the termination of contracts. Under Article 232, a contract can only be terminated by mutual consent, a court order, or a legal enactment. In practice, this means parties can negotiate termination grounds in their contracts, such as termination for material breach or convenience, without requiring judicial intervention.

In certain circumstances, a contract can also terminate by operation of law. For instance, if a party's performance becomes impossible due to a force majeure event (see *Ongoing Conflict in the Middle East: Practical Law Resources Toolkit: Force Majeure*), the party is relieved from its obligations, and the contract is deemed terminated (Article 236, Civil Code). However, Article 236(2) clarifies that if the force majeure event renders performance only partially impossible, the party invoking force majeure is discharged only from the impossible obligations under the contract, while other obligations remain in force.

Notably, the Civil Code does not explicitly define force majeure, leaving courts to determine its applicability on a case-by-case basis. Judicial precedent in the UAE has generally recognised force majeure in instances of unforeseeable and uncontrollable events, such as natural disasters. Conversely, the courts have not found economic fluctuations, including the 2008 financial crisis, to be force majeure events. The reasoning is that market instability is a foreseeable risk, which businesses should account for in their contractual planning.

There are no positive obligations on outsourcing service providers to enable customers to switch to other providers ("switching rights") on termination. However, providers should factor in their obligations to act in good faith under Article 221 of the Civil Code (see *Implied Terms*).

Payment Terms

A services agreement inevitably sets out payment terms that apply in consideration for the outsourced services. However, the enforceability of some payment structures may vary from jurisdiction to jurisdiction.

UAE law permits various payment structures, including advance and deferred payments. Price is considered a material term of a contract. The parties should aim to determine the price and the payment terms in sufficient detail to avoid disputes. If the parties fail to determine the price, the court may deem the contract was concluded at the prevailing market price.

For business-to-business agreements, Article 84 of the *Federal Decree Law No. 50 of 2022 Promulgating the Commercial Transactions Law* (Commercial Code) permits contracting parties to apply interest on late payments as compensation for payment delay. Such compensation is subject to:

- Articles 72 and 73 of the Commercial Code, including the prohibition on imposing an interest rate of over 9% per year.
- Article 87 of the Commercial Code, which prohibits compound interest.

A contract can require payment by instalments. For example, such instalments can be linked to achieving particular milestones, and the contract can require payment of each instalment as a condition for the contractor to proceed to the next milestone. If the customer fails to pay in such circumstances, the outsourcing service provider can, after serving a formal notice of debt on the customer, demand rescission of the contract or payment by way of specific performance. This is subject to the court's discretion to either award the customer additional time to pay or rescind the contract and award damages (Article 234, Civil Code). This structure helps mitigate the risks of non-payment.

A contracting party can abstain from performing its obligations if the other party does not honor its obligations (Article 222, Civil Code). Articles 350(3), 512, and 820 of the Civil Code allow a contractor to retain the object of the contract (such as the goods or the results of services) until they receive due consideration. To avoid disputes over a milestone-based payment structure, the parties should clearly define conditions when the payment obligations arise, including the milestone criteria and procedures for delivery and acceptance.

The contracting parties can also agree on a pre-determined amount of damages (analogous to liquidated damages), however, a competent court can (on a party's request) amend the contract in this respect and award damages in the amount of actual losses suffered (Article 340, Civil Code). Any agreement precluding the court's power in this regard is void (see *Liability Limits and Exclusions*).

The Civil Code permits set-off. It regulates:

- Compulsory set-off that applies by operation of law, where:
    - each party is a creditor and a debtor of the other party; and
    - both debts are similar in kind, description, maturity, force, and weakness.

    A compulsory set-off is also conditional on the fact that it would not prejudice the rights of third parties (Article 320, Civil Code; DCC 271/2025).
- Contractual set-off to which the parties can agree (Article 322, Civil Code).

In either case, an interested party (that is, a party who is entitled to the amounts owed) has to request set-off be carried out (Article 324, Civil Code).

Common Contracting Structure when Engaging in a Global Outsourcing

Many multi-jurisdictional outsourcing arrangements are structured using a global framework agreement (GFA) that the parties then implement locally through local agreements. For more information on how this structure commonly works, see *Practice Note, Multi-jurisdictional outsourcing: Structuring a multi-jurisdictional outsourcing*.

In most outsourcing arrangements in the UAE, it is possible to apply the governing law of the GFA to ensure the terms of the local agreements are consistent with the GFA, subject to mandatory provisions of UAE laws and public policy considerations. Where the contracting party is a governmental entity or a state-controlled company, UAE law typically governs the agreement, and the parties should consider the duty of good faith (see *Implied Terms*) and other statutory provisions that may affect the express provisions of the local agreement.

It is also common to attach jurisdiction-specific schedules to the local agreement to govern issues like data transfers (see *Data Transfer, Localisation, and Processing Restrictions*). Each schedule incorporates that jurisdiction's data protection laws. For example, a schedule for Saudi Arabia would require Saudi laws to apply to allow for the incorporation of certain standard contractual clauses for data processing.

Procurement Issues

In a typical ICT outsourcing, the customer should decide whether to:

- Follow a competitive tender process.
- Approach one or more individual service providers separately.

When public procurement is involved, special procurement rules often dictate the specific procedures and principles that a supplier must follow for the award of a public contract.

In the UAE, there are public procurement laws on the federal and Emirate level, including:

- *Federal Law No. 11 of 2023 Concerning Procurement in the Federal Government* (Public Procurement Law).
- *Cabinet Resolution No. 122 of 2024 on Executive Regulation of the Public Procurement Law*.
- Abu Dhabi Decision No. 36 of 2021 on the Procurement Standards in Abu Dhabi.
- *Dubai Law No. 12 of 2020 Concerning Contracts and Warehouses Management in the Government of Dubai*.

On the federal level, ministries and governmental agencies must comply with the Public Procurement Law and implementing regulations. The relevant bodies must generally hold public tenders via secure and transparent procurement systems, subject to certain limited exemptions outlined in Article 4 of the Public Procurement Law. For example, the Public Procurement Law exempts procurement by the *Ministry of Defence*, Armed Forces, or state security entities. Otherwise, as a general rule, outsourcing by federal authorities must follow the public procurement procedures established by the Public Procurement Law.

Under the Public Procurement Law, the relevant entities can hold a pre-qualification process among the participants. Pre-qualification is expected for all strategic, complex, and high-cost projects. Pre-qualification assessment criteria can include:

- "Emiratisation" requirements.
- Localisation of the products and services according to the local (national) content programme (see *Cabinet Resolution No. 72 of 2021 Regarding the National Content Programme*).
- Meeting the necessary level of technical, financial, and administrative capabilities.
- Demonstrating sufficient experience.
- Following sustainable procurement practices.

Antitrust or Competition Issues

A jurisdiction's antitrust or competition law may be relevant to an ICT outsourcing transaction in two distinct ways:

- If a services agreement falls within the scope of a jurisdiction's merger control legislation (if any exists), the parties may need to notify that transaction to the relevant regulator.
- If an outsourcing imposes anti-competitive restrictions, such as restrictions that seek to limit the customer's freedom to engage rival service providers, it may breach that jurisdiction's relevant antitrust or competition laws.

The competition regime in the UAE is regulated by:

- *Federal Decree Law No. 36 of 2023 Regarding Regulating Competition* (Competition Law), which repealed *Federal Law No. 4 of 2012 Regulating Competition*.
- *Cabinet Decision No. 3 of 2025 on the Ratios Related to the Implementation of the Competition Law* (effective 1 March 2025).
- *Cabinet Decision No. 37 of 2014 Concerning the Executive Regulations of Federal Law No. 4 of 2012 Regulating Competition* (Executive Regulations), which remains in force until the replacing executive regulations are issued under the Competition Law.

The Competition Law broadly prohibits activities that restrict competition, including:

- Any agreement where the "subject, purpose[,] or impact is to distort, lessen, prevent[,] or restrict competition" (Article 5, Competition Law).
- Any conduct that abuses a dominant position or economic dependence, including:
    - unjustifiably discriminating between customers in identical contracts with respect to prices, quality of goods, or terms of sale;
    - prohibiting customers from dealing with competing businesses; and
    - controlling or limiting technological development.

    (Articles 6 and 7, Competition Law.)

Economic concentration controls apply where a transfer of property, rights, equity, shares, or obligations results in one market player gaining control over another (Articles 1 and 12, Competition Law). Because of this broad definition, in principle, an ICT outsourcing could qualify as an economic concentration. Where an ICT outsourcing arrangement envisages exclusivity or non-compete undertakings or involves a market player with a dominant position, this may trigger provisions of the Competition Law.

The Competition Law does not provide any exemptions beyond the above broad prohibitions (such as for vertical agreements between vendors and customers) but envisions that a resolution of the *Minister of Economy* can exempt certain categories of contracts (Article 11, Competition Law). Absent such a resolution, the contracting parties can apply for an individual exemption from the Minister of Economy if they prove that the agreement both:

- Is reasonable and necessary for:
    - promoting economic development;
    - improving the performance and competitiveness of the relevant business;
    - developing production or distribution systems; or
    - bringing certain benefits to customers.
- Does not result in:
    - imposing unreasonable restrictions that are not proportionate to the above objectives; or
    - complete elimination of competition in the relevant market or a significant part of it.

(Article 9, Competition Law.)

There are currently no established enforcement practices for competition law because the UAE's regime is so recent.

Other Considerations

The ICT outsourcing landscape in the UAE is expected to keep evolving dynamically, driven by emerging market trends, innovative legal frameworks, and the increasing importance of data protection regulations.

As organisations expand their reliance on data centers and cloud services, managing contractual risks and risks related to data privacy and security is crucial. Businesses should:

- Proactively adopt effective risk mitigation strategies to navigate this shifting environment.
- Keep abreast of regulatory developments and industry best practices.

