

Protecting data centre contracts: Navigating the perfect storm

The convergence of geopolitical tensions, tighter export controls and substantial commercial commitments presents a particular challenge for data centres. For operators in Singapore, Malaysia, Indonesia and Thailand, the consequences may be felt as acutely in contractual disputes as in regulatory investigations.

A data centre may have secured its power, installed its cooling systems and committed its capacity to customers, yet find itself unable to provide the service it has agreed to supply. Restrictions on the delivery of advanced chips, or on who may use them remotely, can undermine a project without any failure of the physical infrastructure. The resulting question is a familiar one: who bears the loss?

The US Commerce Department has added Singapore based Megaspeed International to its Entity List, citing the risk of chip diversion. Singapore's investigation into whether Megaspeed breached local law remains ongoing.



A perfect storm for the sector

The sector faces a perfect storm of geopolitical, regulatory and commercial pressures. Following the US midterms, we expect sustained congressional scrutiny of China-related technology policy and bipartisan demands for stronger oversight.

The US Bureau of Industry and Security's measures, announced on 16 November 2026 and effective from 19 November, extend scrutiny beyond chip shipments to the overseas arrangements through which computing power is made available. They introduce additional licensing requirements for specified advanced-computing items supplied to or within Singapore, Malaysia, Indonesia, Thailand and Brazil, alongside controls on relevant transactions supporting substantial remote access for certain China-linked and other restricted companies.[1]

The rules are not a blanket ban on all chips or Chinese customers. The equipment, ownership, ultimate users and proposed use all matter. There are qualifications, including a conditional exclusion for certain US-headquartered businesses and a specific 90-day licensing provision for qualifying existing arrangements. The scope of any restriction requires careful consideration before services are suspended.[1]

Further US measures cannot be discounted. On 20 November, President Trump threatened "tremendous penalties" for US technology companies building data centres abroad, without providing details. That statement is a warning of possible policy, not itself an enacted penalty regime.[2]

Singapore's standing as a trusted technology and financial hub depends on confidence amongst Western and Asian partners. The challenge is not simply to choose between US alignment and legitimate trade with China, but to sustain both within applicable rules. Malaysia's investment opportunity likewise depends on its facilities not becoming a route around restrictions. US-origin technology may carry export-control obligations even where the hardware remains in either country.

Contractual consequences

When regulatory risk becomes a contractual dispute

The consequences will depend on the business model and the bargain struck. A provider of space, power and cooling may have fulfilled its obligations even if its tenant cannot obtain chips; a provider which has promised usable computing capacity may not. Relief from an equipment supplier will not necessarily answer a customer's claim. Contracts must therefore address responsibility for export-control compliance, customer screening and licensing, and who bears the consequences of regulatory changes or suspended services.

Development	Possible contractual consequences	Relevant contractual provisions
Chip deliveries are delayed	The opening date is missed and the developer faces claims for delay.	Responsibility for obtaining equipment and licences; notice requirements; time extensions and final completion dates.
The facility is online but computing capacity is unavailable	The promised computing capacity cannot be provided despite uninterrupted power and cooling.	The promised service and how it is measured; fee reductions; opportunities to remedy a failure; limits on damages.
Access for a customer is suspended	The customer challenges the suspension or withholds payment.	Rights to suspend and terminate; notice; minimum payments; the precise regulatory restriction.
A major customer postpones or abandons expansion	Revenue falls whilst the operator remains committed to power, rent and debt repayments.	Capacity commitments, deposits, guarantees, termination rights and obligations to lenders.

A facility operating at 95 per cent utilisation may still face a serious commercial problem if its principal customers cannot lawfully be served. Licensing can affect revenue forecasts, financing terms, debt servicing and whether a project remains bankable. These issues are best considered before investment, financing and capacity agreements are signed. The most resilient projects will combine commercial scale with regulatory credibility and the confidence of international technology partners.

Does a change in the rules excuse performance?

An export restriction does not, of itself, relieve a party of its contractual obligations. Under English law, force majeure depends on the contract; in Singapore, too, the precise wording is paramount. A clause concerned with events which "prevent" performance may operate differently from one addressing events which "hinder" or "delay" it. Commercial inconvenience or increased expense will not generally be enough on its own.[3]

A change-in-law provision may allocate additional cost, allow more time or require discussions, rather than excuse performance altogether. Frustration is a separate and exceptional doctrine: it is not a means of escaping a bargain merely because it has become less profitable. The governing law and the parties' allocation of risk remain important.[3]

Much is likely to turn on why performance failed. Was a licence refused, or was an application never made? Was the supplier legally prevented from delivering, or simply unwilling to proceed? Had the project already fallen behind? Notice requirements, reasonable efforts to overcome the difficulty and the availability of lawful alternatives may determine whether a claim succeeds.

There are limits to what an alternative can require. In *RTI Ltd v MUR Shipping BV [2024] UKSC 18*, the UK Supreme Court held that, absent clear wording, a reasonable endeavours obligation did not require acceptance of performance different from that agreed.[4] For a data centre, a different chip or location may change the commercial bargain. Any agreed substitution should therefore be recorded with care.

International arbitration

One project, several contracts and competing claims

The contractual arrangements behind a data centre commonly involve equipment suppliers, contractors, operators, resellers and customers in different jurisdictions. An operator facing a customer's claim may need to pursue its supplier at the same time. The difficulty is not simply establishing that a regulatory change caused disruption, but identifying the party which agreed to bear that risk and the forum in which that agreement can be enforced.

International arbitration is well suited to disputes of this kind. It offers a neutral forum, the ability to appoint arbitrators with appropriate experience and an established international framework for enforcing awards. Confidentiality can also be important where customer identities, access arrangements and commercially sensitive technical information are in issue, although it remains subject to applicable rules and disclosure obligations.[5]

Urgent protection and continuing operations

Where a threatened shutdown or removal of equipment could cause lasting damage, emergency arbitration or court assistance may offer protection before the main dispute is decided. The available relief and its enforceability require consideration at an early stage. SIAC's rules, for example, provide for emergency relief before the tribunal is constituted.[5] The commercial objective may be to preserve lawful operations whilst responsibility for the disruption is resolved.

Related disputes and the risk of inconsistent outcomes

Incompatible arbitration clauses may leave the operator defending one claim whilst pursuing substantially the same factual issues elsewhere. Depending on the agreements and rules, it may be possible to combine proceedings, coordinate hearings or bring an additional party into an arbitration. Those mechanisms have conditions: a commercial connection alone does not ensure that all parties can be heard together.[5]

Agreement on a common procedure may still be possible after a dispute arises. Where separate proceedings are unavoidable, a consistent approach to the evidence, regulatory explanations and settlement discussions becomes particularly important.

Establishing the commercial loss

The evidence should distinguish capacity which could not lawfully be supplied from capacity for which demand simply fell away. Delivery records, project schedules, licence correspondence and service measurements may be as important as the contracts themselves. Any claim for replacement costs or lost profit will also need to account for savings, contractual limits and credits already given. A well-supported claim can provide a basis for a commercial resolution, rather than simply a final hearing.

Supply contract	Operator's exposure	Customer contract
The supplier seeks more time or a right to suspend delivery.	The operator's obligations to its customer may nevertheless continue.	The customer seeks fee reductions, damages or termination.

Relief under one contract does not necessarily protect the operator under the next.

A lawful first sale is only part of the picture. The original seller may have acted properly, yet difficulties may emerge as chips or capacity pass through distributors, resellers, cloud providers and other users. Remote access can separate the server's location from both the paying customer and the ultimate user. End-user certificates, sanctions checks and contractual assurances remain important, but should be supported by continuing checks on the ultimate destination, ownership, control and use of the technology.

Due diligence and commercial value

Five questions which businesses should be asking

1. Who ultimately owns and controls the customer?
2. Who will actually use the computing capacity, and from which jurisdictions?
3. Is the proposed use consistent with the customer's business and stated commercial purpose?
4. Could intermediaries, sub-leasing or remote-access arrangements change the risk?
5. What happens if ownership, end users, location or intended use changes after the transaction?

Keeping compliance under review

While companies cannot always guarantee every downstream customer's conduct or investigate without limit, the relevant enquiry should be proportionate to the technology, country, customer and transaction. An established operator with transparent ownership differs from a newly incorporated intermediary with opaque owners or unidentified users. Warning signs require further enquiries, escalation and documented decisions, not automatic rejection or reliance on assurances alone. Checks should continue after onboarding and when ownership, users or end use changes. If a data centre cannot provide enough information to verify compliance with the remote-access control, the exporter may consider pausing the transaction until it resolves the concern or obtains the required licence.

What the contract should address	Why it matters
Who may use the service, and where	Obtain warranties identifying approved end users and countries, and prohibit unauthorised resale, sub-leasing or transfer of computing capacity.
Ownership and changes in use	Disclose beneficial ownership and changes in control; report suspected diversion or material changes in use immediately.
Access to records and inspections	Provide for audits and inspections, with accurate records identifying customers, chip locations and the computing capacity used.
What happens if concerns arise	Allow suspension or termination where export-control concerns arise, and require cooperation with regulatory enquiries and investigations.

Manufacturers, distributors, operators and cloud providers have different visibility and control. Their obligations should reflect those differences and be capable of being checked in practice, with clear responsibility for monitoring and acting on concerns.

Alongside power utilisation, rack occupancy, revenue per megawatt and service availability, management should track the share of capacity allocated to verified end users, the proportion of customers receiving enhanced checks, approval times for higher-risk customers and unresolved compliance concerns. The share of GPU capacity subject to geographic or end-use restrictions and revenue exposed to licensing changes are equally relevant. These are indicators of commercial risk and asset value, rather than additional contractual obligations unless agreed.

HFW comment

HFW's international arbitration experience includes AI data centre disputes, semiconductor businesses and cross-border chip-supply investigations. Our disputes, sanctions and export-control teams advise on claims, urgent protection, negotiated outcomes and practical compliance frameworks.

For further information, please contact :



SHAUN LEONG
Partner, Singapore
T +65 6411 5326
M +65 9028 5812
E shaun.leong@hfw.com

Source notes

1 BIS, *Addressing Remote Access to Advanced Semiconductors*, 91 Fed. Reg. 74,970–74,999 (19 November 2026), FR Doc. 2026-23529, RIN 0694-AK50; especially 15 CFR §§ 742.6(a)(6)(iii)(A)(1), 743.10 and 744.24. BIS announcement, 16 November 2026; Federal Register instrument.

2 The Guardian, 20 November 2026.

3 Contractual relief. Holcim (Singapore) Pte Ltd v Precise Development Pte Ltd and another application [2011] SGCA 1, [49]–[71]; Alliance Concrete Singapore Pte Ltd v Sato Kogyo (S) Pte Ltd [2014] SGCA 35, [33]–[40], [47]–[56]. The rules depend on the governing law, contractual wording and facts. Neither is authority that every regulatory restriction excuses performance.

4 RTI Ltd v MUR Shipping BV [2024] UKSC 18, [36]–[48], [57]–[59]. Clear drafting can require acceptance of non-contractual performance. A reasonably obtainable licence for contractual performance may be relevant. The decision does not stand for a general right to reject all mitigation or alternatives.

5 SIAC Rules 2025, rr 12, 15–18, 45, 50, 59, and sch 1; New York Convention, arts II–V. Palm Grove Beach Hotels Pvt Ltd v Hilton Worldwide Manage Ltd and another [2025] SGCA 14, [65]–[66], concerns the treatment of a particular force majeure defence on a challenge to arbitral awards.

HFW has over 700 lawyers working in offices across the Americas, Europe, the Middle East and Asia Pacific. For further information about our capabilities, please visit hfw.com.

© 2026 Holman Fenwick Willan LLP. All rights reserved. Ref: D0001493

Whilst every care has been taken to ensure the accuracy of this information at the time of publication, the information is intended as guidance only. It should not be considered as legal advice. Specific advice should be sought in relation to any particular transaction or dispute. Holman Fenwick Willan LLP is the Data Controller for any data that it holds about you. To correct your personal details or change your mailing preferences please email hfwenquiries@hfw.com

Americas | Europe | Middle East | Asia Pacific