European Data-Centre Carve-Outs: Separating Power Contracts, Networks and Operating Data

A Standalone-Perimeter Framework for Infrastructure, Customer Obligations and Separation Execution

Authored by Chennakeshav Adya

Independent Researcher

September 2026

Abstract

European data-centre carve-outs divide facilities that were often built inside telecommunications, cloud, managed-service or corporate groups. A sale can transfer land, buildings and cooling equipment while leaving power procurement, carrier relationships, software, security operations, customer obligations, people and operating data embedded in the seller. The resulting perimeter may look complete in a legal schedule and remain unable to operate, invoice or satisfy customers independently.

This paper develops a European Data-Centre Carve-Out Framework for corporate sellers, infrastructure investors, private-equity sponsors, lenders and management teams. It traces the standalone perimeter across legal entities, power and grid rights, interconnection, customer contracts, servers and service layers, software, operating data, cybersecurity, employees, permits, land, working capital and shared functions. It converts each dependency into a transfer, replacement or time-bound transitional service with an accountable exit test.

The worked case is wholly hypothetical. A buyer evaluates seven facilities in five European countries. Management describes 190 MW of facility capacity, while diligence identifies 132 MW of commissioned critical capacity, 96 MW of customer-usable capacity, 72 MW contracted and 58 MW billable. The case models a EUR 1.85 billion enterprise value, EUR 420 million of separation and growth capital, and EUR 800 million of acquisition debt. These figures are illustrative and do not describe an identified company or transaction.

The conclusion is that carve-out value depends on the chain from enforceable power and network rights to accepted service, invoicing and collected cash. A buyer should pay operating value for assets that can stand alone at closing, conversion value for dependencies with funded and measurable exit plans, and contingent value for rights that remain subject to consent, construction or customer acceptance. The separation programme should protect service continuity while producing a business that can refinance, integrate and exit without hidden reliance on the former parent.

JEL Classification: G31, G34, L86, L94, Q41

Keywords: European data centres, carve-out, data-centre M&A, power purchase agreements, grid connection, carrier networks, operating data, transitional services, NIS2, Data Act

1. Define the carve-out investment decision

The investment committee must decide whether the proposed perimeter can operate as an independent data-centre platform and whether the purchase price recognises the cost, time and risk of achieving that state. The decision should begin with cash-generating services and work backwards through customer contracts, network delivery, facility operations, power, land, people, systems and licences. A legal asset list is necessary. It is not an operating model.

European transactions illustrate the variety of perimeters. Telefónica sold eleven data centres while retaining servers and customer management under a long-term housing arrangement. Proximus transferred its Belgian data-centre business to a newly formed company while retaining its role as a cloud and ICT integrator. Apollo announced the acquisition of seven European enterprise-colocation assets from STACK for a new standalone company. Each design requires different rights, services and controls at closing. [1][2][3]

The board should approve one evidence hierarchy. Assets and cash that are controlled, commissioned, contracted, accepted and collected support operating value. Rights requiring consent, migration or construction support probability-weighted conversion value. Strategic possibilities support option value only. The acquisition agreement, financing model and separation plan should use the same classifications.

Table 1. Standalone perimeter and valuation treatment

Layer	Required evidence	Principal failure	Valuation treatment
operating facility	title or lease, permits, commissioned systems and service records	physical asset cannot deliver contracted service independently	operating value
power and grid	transferable supply, connection, metering and credit support	capacity is shared, conditional or parent-backed	consent or milestone value
network	carrier contracts, meet-me-room rights, cross-connect inventory and routing	connectivity depends on seller network or personnel	replacement cost and delay
customers	transferable contracts, acceptance, invoices and collections	consent, service split or pricing prevents continuity	customer-specific adjustment
software and data	licences, access, ownership, history and migration rights	buyer lacks operating visibility or lawful data use	separation reserve
people	identified roles, transfer process, retention and replacement	knowledge and authority remain with seller	cost-to-standalone
shared functions	mapped service, SLA, charge and executable exit	transitional service becomes permanent dependency	funded TSA and exit gate

Proposed diligence framework; transaction documents and local law determine actual rights.

2. Fix the legal perimeter and transaction form

The seller and buyer should establish whether the transaction transfers shares, assets, a business undertaking or a combination. A share sale may preserve contracts and licences inside an entity while leaving shared services and guarantees outside it. An asset sale can select a cleaner perimeter while requiring individual transfers, novations, registrations, tax analysis and employee processes. Country differences can make one global form impractical.

The entity map should identify ownership, branches, permanent establishments, joint ventures, minority interests, licences, land, customer contracts, power arrangements, network agreements, employees, intellectual property, data controllers, bank accounts, guarantees and debt. Each item should have a transfer mechanism, consent authority, timing, cost and fallback. Rights held by a group procurement vehicle or telecommunications affiliate should not be assumed to follow the facility.

The perimeter should also identify excluded services. A telecommunications seller may retain cloud, managed services, cybersecurity, customer relationship management or active network equipment. The buyer then needs a precise demarcation between facility service and retained service. Revenue, liability

and customer communication should follow that boundary. The transaction documents should prevent an excluded layer from silently depending on transferred people or systems.

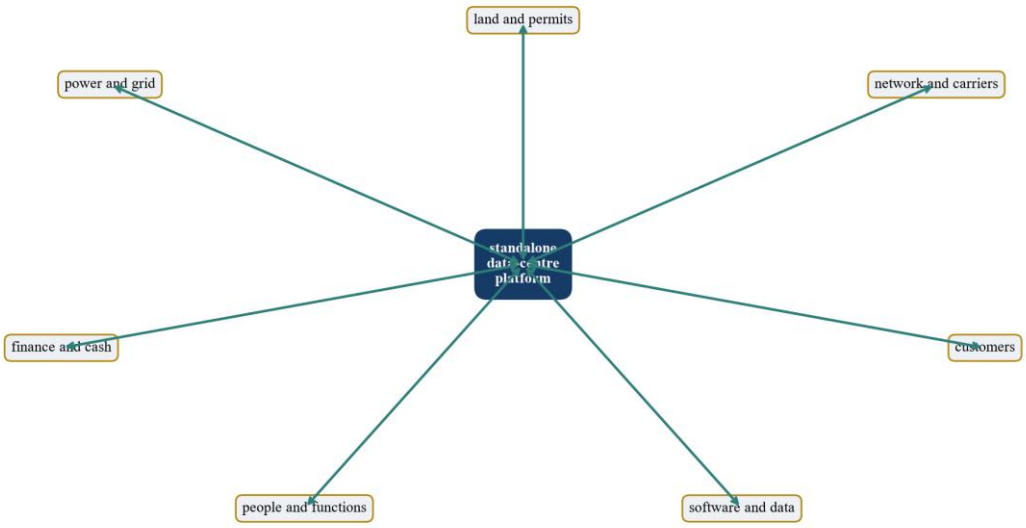
3. Reconstruct the asset and entity map

The physical register should connect every site to land, buildings, substations, generators, uninterruptible power supply, cooling, fire systems, halls, cages, meet-me rooms, offices, spares and construction projects. It should state ownership, lease, useful life, condition, capacity, redundancy, maintenance, warranty and encumbrance. Group-level fixed-asset ledgers frequently fail to preserve this operating detail.

The buyer should reconcile drawings, commissioning records, maintenance systems, insurance schedules, tax registers and site inspections. Equipment can be legally owned by the seller, leased from a financier, supplied under an energy-service contract or dedicated to a customer. Customer-owned servers and network equipment must be segregated. Shared substations, access roads, water systems and security infrastructure need continuing rights.

A separation control room should maintain one dependency register. Each dependency should identify the current provider, receiving entity, required consent, target design, day-one solution, end-state solution, budget, accountable owner and evidence of completion. A dependency closes only when the receiving business can operate and evidence the function without informal support.

Figure 1. Proposed carve-out dependency map



Analytical framework; the actual perimeter is determined by contracts, assets and local law.

4. Separate power supply and grid rights

Power value begins with legal entitlement and physical deliverability. The buyer should identify the connection agreement, supply contract, meter, contracted capacity, firmness, energisation, reinforcement obligations, security, credit support, tariff, indexation, imbalance exposure, curtailment and termination. A group contract covering several sites may require allocation, novation or replacement. A parent guarantee may cease at closing.

The model should distinguish reserved grid capacity, connected capacity, energised capacity, tested critical load, customer-usable IT load, contracted load and billable load. These figures answer different questions. A reservation can lapse if milestones are missed. Connected capacity can remain unavailable

until downstream works are commissioned. Critical systems and cooling consume capacity before customer IT load becomes billable.

Change-of-control, assignment and credit provisions should be scheduled early. Where consent cannot be obtained before closing, the parties need a lawful interim arrangement, clear economic ownership and a long-stop. The buyer should avoid a model in which the seller buys power indefinitely without corresponding control, security or regulatory permission.

Table 2. Power and grid separation matrix

Issue	Diligence evidence	Day-one solution	End-state test
grid connection	executed agreement, milestones and meter	consent or agency arrangement	buyer is recognised connection party
electricity supply	contract, tariff, volume and collateral	novation or short bridging supply	buyer contracts and settles directly
parent credit support	guarantee, letter of credit or deposit	replacement instrument	seller instrument released
shared infrastructure	ownership, capacity allocation and access	easement and operating protocol	enforceable access and measured allocation
renewable claim	PPA, certificate and matching method	allocated instruments	buyer owns auditable claim
expansion	queue position, works, land and permits	protected milestones	commissioned capacity passes acceptance

Illustrative control matrix; site-specific utility and market rules apply.

5. Test power-purchase agreements and energy attributes

A corporate power-purchase agreement can contain volume shape, balancing, floor, cap, settlement, credit, change-of-control and assignment terms that differ from the facility load. The buyer should determine whether the agreement is physically or financially settled, whether it is linked to a particular legal entity, and whether guarantees of origin or other attributes transfer with the economics.

ACER's monitoring shows that European PPA conditions and liquidity differ by country. A portfolio arrangement should therefore be disaggregated by site, market and contract. The carve-out model should compare the target's load profile with contracted generation, residual supply, imbalance, curtailment and certificate treatment. A favourable headline strike price can coexist with material shaping and collateral cost. [4]

Accounting and tax analysis should be aligned with commercial treatment. A derivative, executory contract or own-use conclusion can affect reported volatility and covenants. The buyer should test downside cases for market price, generation volume, load ramp, basis, imbalance and counterparty credit. Green claims used in customer contracts should be traced to auditable instruments and allocation rules.

6. Map network and interconnection dependencies

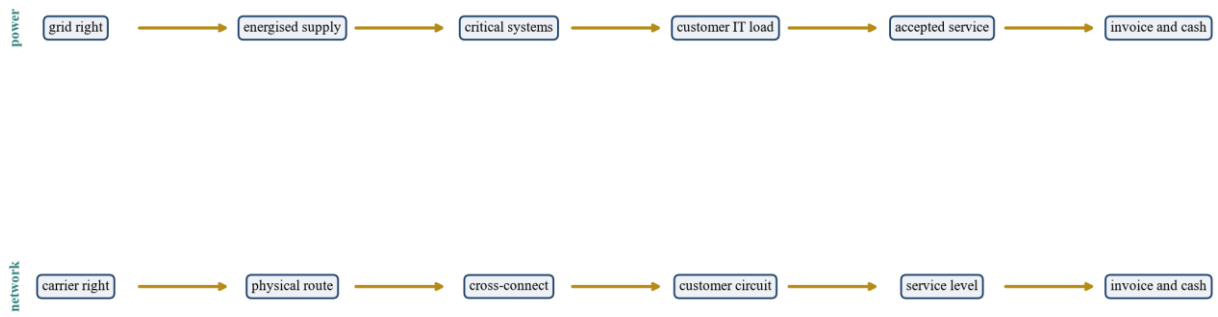
Data-centre connectivity is a service chain rather than a single cable. The buyer should map duct and fibre ownership, building entry, meet-me rooms, carrier points of presence, cross-connects, internet exchanges, wavelengths, dark fibre, active equipment, network operations, route diversity, maintenance, spares and fault response. Each component should identify the contracting entity and operational controller.

A telecommunications parent may provide network access under internal arrangements that do not survive separation. Customer contracts may combine colocation with connectivity, cloud or managed network services. The buyer should identify whether it will provide the combined service, resell the seller's

retained service or split the customer contract. Liability, service credits and incident command should match that design.

Route diversity should be verified physically. Two contracts can use the same duct, bridge, landing station or exchange. The separation programme should preserve access to meet-me rooms, customer cages and monitoring systems while respecting security. Any replacement network should be installed and tested before the corresponding transitional service exits.

Figure 2. Power-to-cash and network-to-service chains



Proposed operating trace; each arrow requires an enforceable right and tested process.

7. Reconstruct customer obligations

The customer register should map every legal customer to site, space, power, density, connectivity, service, contract, term, renewal, pricing, acceptance, service level, security requirement, invoice and collection. Group customers should be aggregated where procurement or renewal decisions are linked. Resellers and managed-service intermediaries should be traced to the economic end user where permitted.

The buyer should separate facility obligations from retained services. A contract may promise colocation, cloud, backup, network, security, remote hands and hardware management under one price. Revenue and cost must be allocated to the transferred perimeter, and the customer must know which entity is responsible after closing. A service split can require consent, amendment or replacement.

Change-of-control, assignment, data, audit, subcontracting, location and termination provisions should be reviewed customer by customer. Revenue should enter the base case only when the buyer has an enforceable and operational route to deliver it. A consent-dependent contract can be protected through a closing condition, holdback, earn-out or customer-specific price adjustment.

Table 3. Customer and retained-service allocation

Service component	Likely owner after carve-out	Key evidence	Separation control
powered space and cooling	data-centre company	site schedule, acceptance and SLA	facility contract or novation
cross-connect	data-centre company or carrier	order, route and demarcation	operating protocol

Service component	Likely owner after carve-out	Key evidence	Separation control
wide-area network	retained telecom or third party	carrier contract and circuit inventory	resale or direct contract
cloud platform	retained seller or cloud provider	subscription, data and support terms	customer amendment
managed security	retained seller or specialist	scope, monitoring and incident authority	responsibility matrix
customer hardware	customer or managed-service provider	asset register and access rights	custody and access schedule

Proposed classification; executed customer documentation governs obligations.

8. Design the anchor seller agreement

The former parent can remain a major customer, reseller or service provider. That relationship can support occupancy and continuity, while concentration and related-party pricing can weaken financeability. The agreement should state committed capacity, ramp, term, price, indexation, service levels, credit, deposits, termination, migration, audit, data, security and change rights.

Telefónica's transaction retained a long-term housing relationship, and KPN described the sold platform as a preferred supplier for future services. These structures demonstrate the commercial importance of a carefully defined continuing relationship. The buyer should assess whether volume is committed or merely preferred, whether pricing covers standalone cost, and whether the seller can redirect customers or workloads. [1][5]

The model should show anchor revenue, third-party revenue and customer concentration separately. Debt sizing should use enforceable contracted cash after downside assumptions. The agreement should avoid broad most-favoured pricing or unilateral service changes that prevent independent commercial development.

9. Split servers, cloud and facility layers

Facility ownership does not necessarily include servers, storage, accelerators, orchestration software or customer workloads. The asset register should identify ownership and responsibility for each layer. The buyer needs enough information to operate power, cooling, physical security and access without receiving unnecessary rights to customer systems or data.

Where the seller retains cloud and managed services, service demarcation should define incident detection, escalation, remote hands, maintenance windows, access, evidence and liability. A facility alarm can affect a cloud service, and a cloud workload change can alter power density. The operating model should allow coordination while preserving customer confidentiality and cyber boundaries.

Migration plans should identify capacity, sequencing, downtime, rollback, data handling and customer approval. A separation should not force unnecessary workload migration when a contractual split can preserve service. Any required migration should have funded resources, technical rehearsal and acceptance criteria.

10. Establish rights to software and operating technology

Data-centre operations rely on building management, electrical monitoring, data-centre infrastructure management, computerised maintenance, access control, CCTV, ticketing, customer portals, billing, finance, procurement, identity, cyber monitoring and reporting. The buyer should inventory applications, versions, licences, hosting, interfaces, data, administrators, vendors and support.

An enterprise licence may prohibit transfer or use by a divested entity. A bespoke application may belong to the seller or a contractor. Interfaces can depend on group identity, network or data warehouses. The separation design should decide which systems transfer, which are licensed, which are replaced and which are supported temporarily.

The end-state test is operational, not documentary. Users must authenticate; sensors and meters must feed the system; incidents and work orders must flow; invoices must reconcile; reports must be produced; backups must restore; and administrators must have controlled access. Parallel running and reconciliation should precede cutover for critical systems.

Table 4. Software and operating-data separation

Domain	Critical data	Separation risk	Exit evidence
facility control	alarms, telemetry, set points and history	loss of visibility or unsafe control	tested independent control and historian
maintenance	assets, work orders, spares and warranties	incomplete maintenance or warranty loss	reconciled register and live workflow
customer service	orders, tickets, SLA and contacts	service failure or disputed responsibility	accepted portal and ticket migration
billing	contracts, meters, tariffs, invoices and cash	revenue leakage	parallel invoice reconciliation
identity and access	users, roles, logs and credentials	excessive or orphan access	new directory and certified roles
reporting	energy, water, cyber and regulatory records	missing compliance history	complete archive and repeatable report

Proposed application control; cyber and privacy requirements apply to each migration.

11. Separate operating data lawfully

The business needs historical telemetry, maintenance records, customer service history, invoices, asset documents, incident records and compliance reports. The seller should classify each dataset by ownership, purpose, personal data, customer confidentiality, security, retention and transfer restriction. The buyer should receive the minimum complete dataset required to operate and evidence the business.

The European Data Protection Board has highlighted privacy implications in mergers and acquisitions. The parties should identify controllers, processors, legal bases, notices, data-processing arrangements, international transfers, security measures and data-subject rights. A data room should avoid excessive disclosure of customer or employee personal data. [6]

Operating history should preserve provenance and auditability. Extracts should reconcile to source totals, timestamps and control logs. Where data cannot transfer, the seller should provide an agreed derived dataset or controlled access consistent with law and contract. Retention and deletion duties should be allocated after closing.

12. Build the Data Act switching and portability plan

The EU Data Act applies obligations to providers of data-processing services, including contractual and technical support for switching. The regulation includes transition requirements and provides for the abolition of switching charges from 12 January 2027. Infrastructure-as-a-service providers face functional-equivalence requirements within the regulation's framework. [7]

The carve-out should determine which entity is the provider for each service and whether contracts, interfaces, export tools, assistance and records meet the applicable requirements. A seller that retains

cloud services and transfers facilities can leave different obligations with each party. Customer communications and service descriptions should reflect the actual allocation.

The buyer should test whether required data export, migration support and interoperability depend on seller systems or people. These dependencies should enter the TSA and end-state build. Contract templates, billing and customer support should be updated before the buyer originates new business.

13. Preserve cybersecurity and NIS2 controls

Commission Implementing Regulation (EU) 2024/2690 specifies cyber risk-management requirements for data-centre service providers and other covered digital entities. The separation programme should map governance, risk assessment, incident handling, continuity, supply-chain security, vulnerability management, access, cryptography, asset management, personnel security and authentication. [8]

Cyber controls frequently span the parent group. Security operations, identity, endpoint protection, vulnerability scanning, vendor assessment, threat intelligence and incident response can sit outside the carved business. A short TSA can preserve coverage, but the buyer needs authority, information and escalation from signing through exit.

The cyber separation plan should define trusted connections, data flows, privileged accounts, certificates, keys, monitoring, logging and breach responsibilities. Old access should be removed only after replacement access is proven. New environments should be tested without weakening live facilities. Material incidents and regulatory notifications require a single command structure.

14. Transfer people and operating knowledge

The people perimeter should identify employees and contractors who perform facility, engineering, network, security, customer, commercial, finance, procurement, legal, compliance and leadership roles. Time allocation and reporting lines should be tested where functions are shared. A title or cost centre alone may not identify the people required to operate.

Directive 2001/23/EC provides an EU framework for safeguarding employee rights in transfers of undertakings, with national implementation. Country counsel should determine which employees transfer, the required information and consultation, and the treatment of terms, benefits, collective arrangements and liabilities. [9]

The buyer should protect critical knowledge through retention, structured handover, documentation, shadowing and succession. Seller personnel who do not transfer may still be required during transition. The TSA should name roles, service levels and replacement milestones. Management incentives should reward safe separation, customer continuity and verified standalone capability.

15. Re-establish licences, permits and reporting

The licence register should cover corporate, planning, environmental, energy, generator, fuel, water, waste, fire, security, telecommunications, building, operating and construction requirements. Each entry should identify the holder, site, scope, expiry, transferability, change-of-control requirement and responsible authority. A permit held by the parent or landlord may need a new application.

EU energy-efficiency rules require reporting by data centres above 500 kW of installed information-technology power demand under the delegated reporting framework. Reported indicators include energy, water, renewable energy and waste-heat information. The Commission is developing a rating scheme and considering minimum performance standards. [10][11]

The buyer should secure historical and current data needed for reporting, customer claims and financing. Meter boundaries, calculation methods and assurance should remain consistent through separation.

Expansion projects should retain environmental, planning and connection milestones. A permit gap should have a closing condition or funded remediation plan.

Reporting ownership should be made explicit. The seller may currently aggregate site information, calculate indicators and submit a group return. The carved business needs its own reporting calendar, data lineage, methodology, review, sign-off and archive. Where the legal obligation stays with a landlord or another group entity, the operating agreement should still give the buyer timely access to the data and evidence needed for customers, lenders and internal governance.

Waste-heat and water obligations deserve separate attention. Technical studies, municipal agreements, network connections and customer commitments may be held outside the target entity. A public announcement or engineering concept should not be treated as an operating entitlement. The buyer should verify the rights, remaining capital, service responsibility, pricing and performance measure before including revenue, avoided cost or sustainability value.

Energy-performance data can influence more than compliance. Customers can use it in procurement; lenders can use it in sustainability-linked terms; insurers can use it in risk assessment; and authorities can use it in future performance standards. The transaction model should preserve the raw meter evidence and calculation logic so that reported improvements can be reproduced. A changed meter boundary after separation can create a false trend unless the historic series is restated on a consistent basis.

16. Protect land, access and shared infrastructure

The property review should cover title, leases, easements, rights of way, access, utilities, ducts, substations, water, drainage, parking, security perimeters, roof rights, expansion land and reinstatement. Shared campuses require binding rules for access, maintenance, cost allocation, emergencies and future works.

Lease terms should support customer and debt tenors. Change of control, assignment, use, alterations, subletting, security, insurance, rent review, break and termination provisions can constrain value. A sale-and-leaseback or property split can alter the operating company's control over critical infrastructure.

Environmental diligence should examine contamination, generators, fuel, refrigerants, noise, water, waste, heat and decommissioning. The buyer should identify historic liabilities and the cost of compliance. Expansion value should follow controlled land and approvals, not a conceptual site boundary.

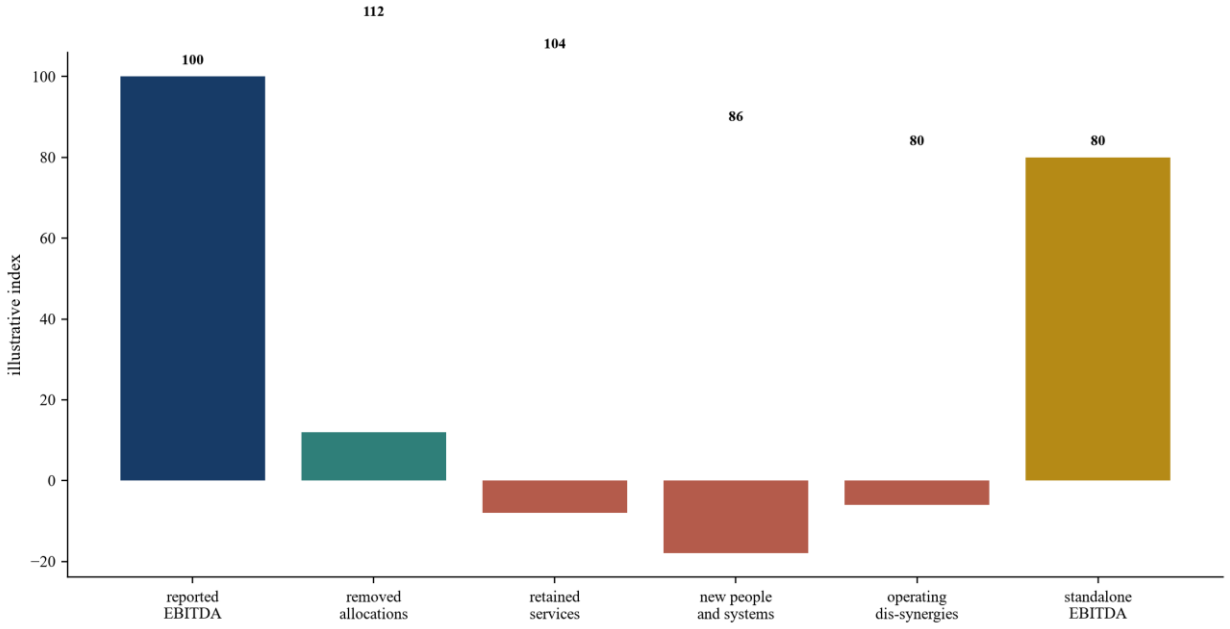
17. Calculate the cost to stand alone

The standalone cost model should begin with functions currently provided by the seller: leadership, finance, treasury, tax, insurance, procurement, legal, compliance, HR, payroll, IT, cyber, network, customer service, sales, engineering, project management and reporting. It should state headcount, systems, vendors, facilities, implementation cost and recurring cost.

Allocated parent overhead is not a reliable standalone estimate. Some allocations disappear; other capabilities must be rebuilt at greater cost. The model should reconcile the target's historical earnings to standalone earnings through removed charges, retained services, replacement cost, dis-synergies and planned efficiencies.

One-time cost should include advisers, systems, data migration, licences, recruitment, retention, branding, banking, insurance, procurement, network replacement, cyber tooling, duplicate running and contingency. A buyer should fund the whole programme at closing rather than depend on future operating cash that may be delayed by separation.

Figure 3. Cost-to-standalone bridge



Illustrative categories; amounts depend on the transaction perimeter.

18. Design transitional services for exit

A TSA should preserve a defined service while the buyer builds or migrates the replacement. It should state scope, users, locations, service level, operating hours, security, data, subcontractors, change control, price, liability, audit, continuity, exit assistance and termination. Broad labels such as IT support are insufficient.

Each service needs an exit plan agreed before signing. The plan should identify the target solution, procurement, build, migration, testing, acceptance, owner, budget and long-stop. Critical services need contingency and extension mechanics. Pricing should encourage disciplined exit without allowing the seller to force an unsafe cutover.

The buyer should govern all TSAs through one programme office and dependency register. Exit requires evidence that the target service operates under realistic load and reconciles to the old service. A contractual end date alone does not prove readiness.

Table 5. Transitional-service exit controls

TSA	Day-one service	Buyer build	Exit evidence
energy procurement	seller contracts and settles power	buyer supply, collateral and settlement	full billing-cycle reconciliation
network operations	seller monitors and dispatches	buyer NOC, tools and carrier contracts	live incident rehearsal
facility systems	seller hosts selected applications	buyer environment and migrated data	parallel alarms and work orders
billing	seller produces invoices	buyer contract, meter and finance integration	two reconciled cycles
cyber operations	seller monitoring and response	buyer SOC and incident authority	penetration, logging and exercise
corporate functions	seller finance, HR and procurement	buyer team and vendors	close, payroll and payment rehearsal

Proposed governance; each service requires transaction-specific scope.

19. Establish day-one operational control

Day one should preserve safety, service, customer communication, cash, cybersecurity and regulatory compliance. The buyer needs named authority for facilities, incidents, customer decisions, payments, access, communications and projects. Contact trees and escalation paths should be rehearsed before close.

The cutover plan should cover legal completion, bank mandates, payment routes, insurance, payroll, supplier notices, customer notices, system access, identity, physical badges, network connections, incident bridges, data extraction and evidence capture. A command centre should track exceptions and avoid simultaneous high-risk changes.

The buyer should freeze unnecessary changes around closing. Major system migration, network redesign and facility work should proceed after control is stable unless required for separation. Customer-facing teams need approved messages and responsibility maps. The first operating, billing and cash cycles should receive enhanced review.

20. Normalise working capital and cash

The carve-out should have opening cash, bank accounts, receivables, payables, deposits, accruals, deferred revenue, taxes, payroll and intercompany balances. Historical cash may have been swept through group treasury, while suppliers and customers transact with multiple group entities. The buyer needs a cut-off and settlement mechanism that matches service delivery.

Receivables should reconcile to customers, invoices, acceptance, disputes and cash. Supplier balances should identify shared contracts, volume rebates, deposits and termination cost. Customer deposits and prepaid amounts should follow the corresponding obligation. Power collateral, utility security and PPA credit support can create significant funding needs.

The purchase agreement should define normal working capital using the future standalone perimeter rather than an unadjusted historical average. The model should include duplicate-running cost, delayed collections, VAT and tax timing, capex creditors and TSA billing. Liquidity should cover downside separation and customer-ramp cases.

21. Build the hypothetical transaction case

The hypothetical target has seven facilities across five European countries. Management describes 190 MW of facility capacity. Diligence identifies 132 MW of commissioned critical capacity after removing unbuilt phases and shared infrastructure constraints. Cooling, redundancy and operating limits leave 96 MW of customer-usable IT load. Executed customer contracts cover 72 MW, and 58 MW has completed service acceptance and become billable.

The proposed enterprise value is EUR 1.85 billion. The buyer identifies EUR 170 million of separation cost and required remediation, plus EUR 250 million of near-term growth capital. Acquisition debt is EUR 800 million. The case assumes no value for 58 MW of conceptual or consent-dependent capacity until grid, construction and customer milestones are achieved.

The buyer's base case uses collected cash from 58 MW, probability-weighted conversion of contracted capacity and no pipeline revenue. The downside delays power consent, network replacement and customer acceptance while increasing TSA and collateral cost. The upside requires evidenced third-party leasing and completion within approved capital.

The separation programme contains 146 recorded dependencies. Twenty-three are classified as critical because failure could interrupt power, connectivity, facility control, security, billing or regulatory reporting. The model assumes that critical services remain supported under documented TSAs until replacement systems pass testing. It also assumes that the buyer recruits dedicated treasury, cyber,

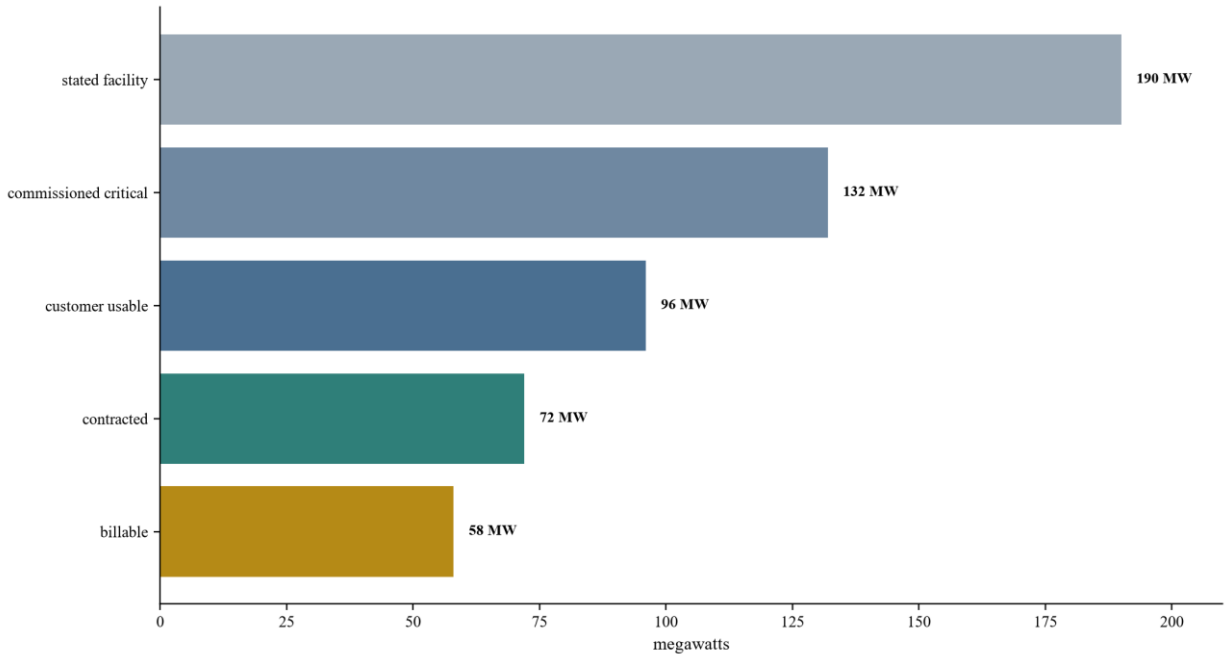
procurement and regulatory-reporting capability. These are management assumptions for the hypothetical case; they are not market benchmarks.

The power review identifies two sites supplied through parent arrangements, one shared substation and one PPA requiring consent. The network review identifies three seller-operated network-control dependencies and shared carrier procurement across five sites. Customer review finds that 18 per cent of recurring revenue combines facility and retained managed services. The buyer therefore allocates part of the purchase price to consent and separation milestones rather than treating all reported recurring revenue as independently transferable.

The downside case assumes a nine-month delay in one power consent, a six-month extension of network and billing TSAs, and delayed customer acceptance for 10 MW. It also adds replacement collateral and duplicate-running cost. The severe case combines those effects with the non-renewal of the largest anchor contract at its first break opportunity. The investment committee uses these cases to set opening liquidity, debt headroom and the maximum price payable at completion.

The upside case remains controlled. It includes conversion of contracted capacity after acceptance, third-party leasing supported by executed terms and procurement savings supported by supplier offers. It excludes conceptual expansion and uncommitted pipeline. This treatment allows the buyer to recognise genuine operating improvement without converting market enthusiasm into present value before evidence exists.

Figure 4. Hypothetical capacity conversion



Wholly hypothetical figures; they do not describe an identified company or transaction.

22. Bridge enterprise value to funded equity

The investment model should add purchase price, assumed debt, fees, taxes, refinancing, working capital, separation, remediation, committed capex, utility collateral, reserves and contingency. Sources should identify acquisition debt, equity, seller financing and any asset-level facilities. A purchase price expressed as enterprise value does not describe the equity cheque.

For the hypothetical case, the EUR 1.85 billion enterprise value combines with EUR 420 million of separation, remediation and growth capital. Financing fees, taxes and reserves create additional uses. EUR 800 million of acquisition debt leaves a large equity requirement and material execution exposure. The buyer should compare this funded basis with standalone cash flow and milestone value.

Deferred consideration can align price with power transfer, customer consent, commissioned capacity or collected revenue. The metric should be objective and protected from manipulation. Contingent value should not substitute for adequate working capital or the ability to complete the programme.

Table 6. Hypothetical sources, uses and value gates

Item	EUR million	Evidence gate
enterprise value	1,850	transferred perimeter and customer rights
separation and remediation	170	approved work packages and vendor plans
near-term growth capital	250	grid, permit, construction and customer milestones
acquisition debt	800	resilient accepted cash and security
base equity before fees and reserves	1,470	funded at close
contingent seller value	separate	consent, commissioning or collected-revenue test

Wholly hypothetical; rounded figures exclude transaction-specific tax and accounting effects.

23. Size debt from resilient cash

Lenders should underwrite revenue that the carved business can lawfully deliver, invoice and collect. The model should deduct standalone operating cost, maintenance capital, recurring compliance, lease payments, taxes and working capital. Customer concentration, renewal, power pass-through, service credits and capex should enter downside debt service.

Security should match the legal location of assets and cash. The financing review should identify permitted security, landlord and utility consents, customer restrictions, bank accounts, insurance, shares, intercompany balances and local financial-assistance rules. A holding-company facility may depend on distributions from country subsidiaries.

Covenants should use definitions that reconcile to the operating model. Capacity or contracted revenue should not enter borrowing value without conversion evidence. Liquidity and capex facilities should remain available through TSA exit and customer ramp. Refinancing assumptions should follow improved operating evidence rather than a higher market multiple.

24. Convert diligence findings into transaction terms

The purchase agreement should allocate identified dependencies through perimeter schedules, conditions, covenants, warranties, indemnities, price adjustments, holdbacks and transitional services. Generic warranty protection rarely replaces a missing power contract, licence, customer consent or operating system.

Conditions should focus on matters essential to lawful operation and value. These can include merger clearance, foreign-investment approval, utility consent, key customer consent, licences, property rights, financing and employee processes. Pre-closing covenants should preserve maintenance, staff, customers, contracts, permits, cyber controls and capital projects.

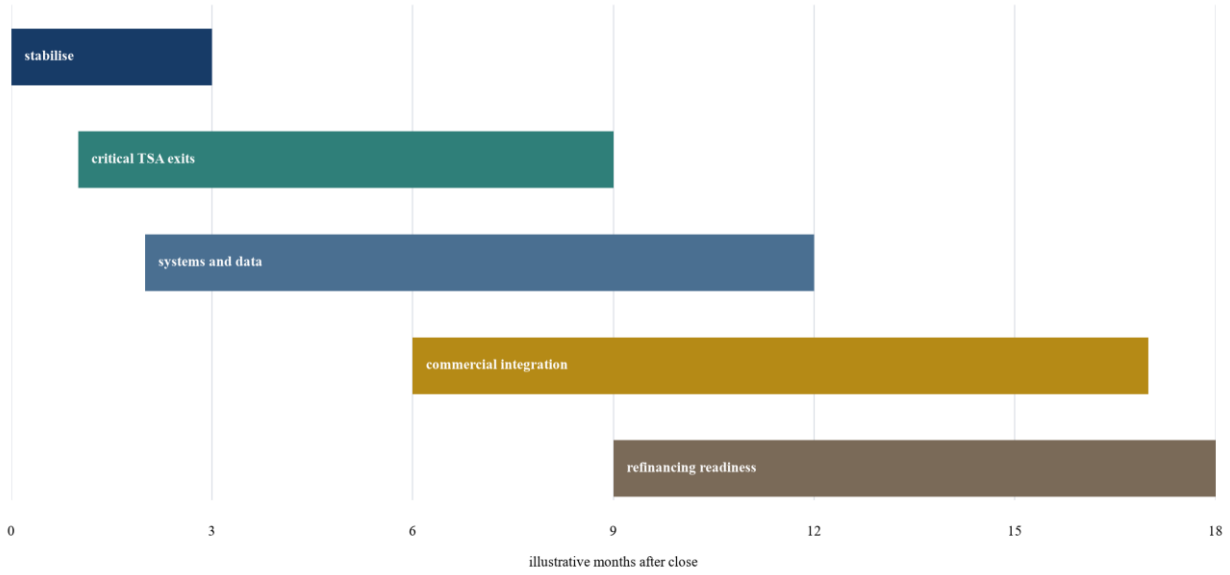
Completion accounts or locked-box provisions should address intercompany balances, leakage, working capital, deposits and shared contracts. Specific indemnities can address identified tax, environmental, employee, data, cyber or contract exposures subject to legal advice. The disclosure process should link each qualification to the dependency register.

25. Sequence separation and integration

The buyer should distinguish separation from integration. Separation creates independent control and exits seller dependencies. Integration combines the acquired platform with the buyer's group. Combining the programmes too early can obscure accountability and add change during a fragile period.

The first phase stabilises service, safety, cash, access and incident control. The second exits critical TSAs and establishes independent power, network, systems, cyber and corporate functions. The third standardises selected processes and captures commercial or procurement benefits. Country-specific customer and regulatory boundaries should remain protected.

Figure 5. Proposed separation and integration roadmap



Timing is illustrative; dependency criticality determines the actual sequence.

26. Establish board gates and management information

The board should receive one dashboard covering service, safety, customers, power, network, cyber, people, systems, finance, capex, consents and TSAs. Metrics should have definitions, sources, owners and thresholds. Red status should trigger an action and decision, not a narrative explanation.

Investment gates should include legal perimeter approval, day-one readiness, critical consent, financing, opening liquidity, each major TSA exit, system cutover, customer migration, growth-capex release and refinancing. Gate packs should contain evidence, residual risk, contingency and accountable approval.

Management information should reconcile facility telemetry, customer contracts, invoices, collections and financial reporting. Capacity definitions should remain consistent across sites. The buyer should retain the transaction dependency register as a permanent operating control until every item closes.

Table 7. Investment committee and board gates

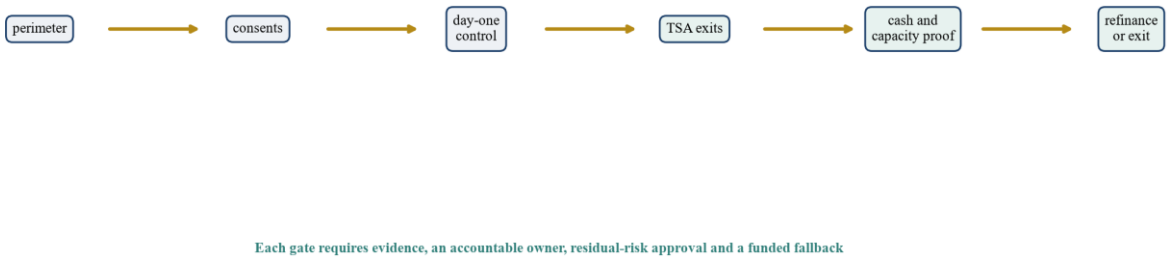
Gate	Required evidence	Decision
perimeter	complete asset, contract, people, system and data map	approve signing basis
day one	authority, liquidity, access, incident and customer plans	approve completion
critical TSA exit	replacement tested under realistic load	approve cutover

Gate	Required evidence	Decision
customer transfer	consent, service allocation and billing readiness	recognise base revenue
capacity conversion	grid, construction, commissioning and acceptance	release growth capital
leverage	resilient standalone cash and covenant headroom	draw or refinance debt
integration	stable independent control and protected obligations	combine selected functions

Proposed governance; the board should tailor thresholds to the transaction.

27. Prepare for refinancing and exit

Figure 6. Proposed evidence-gated carve-out decision sequence



Analytical framework; the board should tailor gates to the transaction.

A future lender or buyer will examine the same perimeter. The separation programme should therefore create a durable evidence base: current contracts, consents, licences, property rights, asset registers, operating history, cyber controls, employee records, financial reporting and capex documentation.

Refinancing readiness should track accepted customer service, collections, power rights, network diversity, maintenance, energy and water reporting, insurance, permits and covenant headroom. Growth capacity should enter the financing case only after objective milestones. The platform should maintain a current virtual data room rather than reconstruct one at exit.

Potential exits include infrastructure funds, strategic operators, pension investors, sovereign investors, listed vehicles and continuation funds. Value should follow independent cash generation, transferable rights, operating resilience and credible growth. A platform that still depends on the former parent can face a discount or restricted buyer universe.

28. Conclusion

European data-centre carve-outs succeed when the transferred business controls the complete path from physical infrastructure to customer cash. Power, grid rights, connectivity, software, operating data, people and customer obligations should be separated with the same discipline as land and equipment.

The buyer should pay operating value for a verified standalone platform, conversion value for funded dependencies with measurable exit tests, and contingent value for uncertain rights. Debt should follow accepted and collected cash after standalone cost and required capital. The seller should receive clear relief when services and guarantees exit safely.

The framework in this paper connects legal perimeter, engineering, customer service, technology, regulation, finance and execution. It provides boards and transaction teams with a practical route from a complex corporate dependency map to an independent, financeable and exit-ready data-centre company.

Frequently asked questions

Q: What is the principal risk in a European data-centre carve-out? A: The principal risk is an incomplete operating perimeter. Facilities can transfer while power, network, software, people, data or customer obligations remain dependent on the seller.

Q: How should grid capacity be valued? A: Operating value should follow transferable and deliverable capacity. Reserved, conditional or future capacity should receive milestone or contingent value after consent, construction and commissioning.

Q: Can a long-term TSA solve separation risk? A: A TSA can preserve continuity for a defined period. It requires a funded replacement plan, measurable service levels, security controls and an executable exit test.

Q: How should the former parent be treated when it remains a customer? A: The anchor agreement should define committed volume, price, term, service, credit, migration and termination. Concentration should remain visible in valuation and leverage.

Q: Which operating data must transfer? A: The buyer generally needs asset, telemetry, maintenance, service, billing, incident and compliance history required to operate and evidence the business, subject to contract, confidentiality, privacy and security rules.

Q: How does NIS2 affect the carve-out? A: Covered data-centre service providers need effective cyber risk-management controls. The separation plan should preserve governance, monitoring, incident response, access and supplier security through cutover.

Q: Should contracted but unaccepted capacity support acquisition debt? A: Base debt should use resilient cash from services that can be delivered, invoiced and collected. Future capacity should enter only through agreed evidence gates and conservative scenarios.

Q: When should integration begin? A: Governance, service, cash and critical controls should stabilise first. Functional integration should follow independent control and safe exit from critical seller dependencies.

References

[1] Telefónica, Telefónica agrees the sale of 11 data centers for EUR 550 million to Asterion Industrial Partners, 8 May 2019. https://www.telefonica.com/en/communication-room/press-room/telefonica-agrees-the-sale-of-11-data-centers-for-e550-million-to-asterion-industrial-partners/

[2] Proximus, Proximus sells its datacenter business for EUR 128 million, 25 October 2024. https://www.proximus.com/fr/news/2024/20241025-proximus-sells-its-datacenters.html

[3] Apollo Global Management, Apollo Funds to Acquire Pan-European Highly Interconnected Data Centre Platform, 29 April 2025. https://ir.apollo.com/news-events/press-releases/detail/551/apollo-funds-to-acquire-pan-european-highly-interconnected

[4] European Union Agency for the Cooperation of Energy Regulators, Power Purchase Agreements monitoring. https://www.acer.europa.eu/electricity/market-monitoring/ppas

[5] KPN, KPN to sell NLDC to DWS, 20 May 2019. https://ir.kpn.com/news-and-events/news/news-details/2019/KPN-to-sell-NLDC-to-DWS-05-20-2019/default.aspx

[6] European Data Protection Board, Statement on privacy implications of mergers. https://www.edpb.europa.eu/documents/statement/statement-on-privacy-implications-of-mergers_en

[7] European Union, Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32023R2854

[8] European Union, Commission Implementing Regulation (EU) 2024/2690 laying down NIS2 cyber risk-management requirements. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32024R2690

[9] European Union, Council Directive 2001/23/EC on safeguarding employees' rights in transfers of undertakings. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32001L0023

[10] European Commission, Energy performance of data centres. https://energy.ec.europa.eu/topics/energy-efficiency/energy-efficiency-targets-directive-and-rules/energy-efficiency-directive/energy-performance-data-centres_en

[11] European Commission, Commission adopts EU-wide scheme for rating sustainability of data centres, 15 March 2024. https://energy.ec.europa.eu/news/commission-adopts-eu-wide-scheme-rating-sustainability-data-centres-2024-03-15_en

[12] European Commission, Minimum performance standards for EU data centres. https://energy.ec.europa.eu/resources/preparatory-studies/minimum-performance-standards-eu-data-centres_en

[13] European Commission, EU merger procedures. https://competition-policy.ec.europa.eu/mergers/procedures_en

[14] European Commission, EU merger legislation. https://competition-policy.ec.europa.eu/mergers/legislation_en

[15] European Commission, Review of the EU merger guidelines. https://competition-policy.ec.europa.eu/mergers/review-merger-guidelines_en

[16] European Commission, Case M.11843, Prime Data Centers transaction decision, 2025. https://ec.europa.eu/competition/mergers/cases1/202512/M_11843_10567975_126_3.pdf

[17] Orange, Orange and Morrison announce contemplated French data-centre joint venture, 27 July 2026. https://newsroom.orange.com/orange-et-morrison-annoncent-un-projet-de-creation-de-coentreprise-de-data-centers-pour-renforcer-la-souverainete-numerique-de-leurope-486247/?lang=eng

[18] Cellnex, Cellnex reaches an agreement for the disposal of Towerlink France to Vauban Infra Fibre, 2025. https://www.cellnex.com/fr-fr/news/cellnex-accord-towerlink-france-centres-donnees-vauban-infra/

[19] Proximus, Proximus completes sale of its data centres, 2025. https://www.proximus.com/nl/news/2025/202503-news-proximus-datacenter-sale-completed.html

[20] TINC, Acquisition of Proximus data centres by Datacenter United consortium, 25 October 2024. https://live.euronext.com/sites/default/files/company_press_releases/attachments/2024/10/25/cpr03_lesechos_16165_1292961_TINC_PB_DCU_ENG.pdf

[21] European Union, Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

[22] ACER, Electricity Market Integration 2025. https://www.acer.europa.eu/monitoring/MMR/electricity-market-integration-2025

[23] European Commission, New impetus for energy efficiency. https://energy.ec.europa.eu/topics/energy-efficiency/new-impetus-energy-efficiency_en

[24] IFRS Foundation, IFRS 15 Revenue from Contracts with Customers. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-15-revenue-from-contracts-with-customers/

[25] IFRS Foundation, IFRS 16 Leases. https://www.ifrs.org/issued-standards/list-of-standards/ifrs-16-leases/

[26] IFRS Foundation, IAS 36 Impairment of Assets. https://www.ifrs.org/issued-standards/list-of-standards/ias-36-impairment-of-assets/

About the Author

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and closure.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners, he is Managing Partner and leads the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.