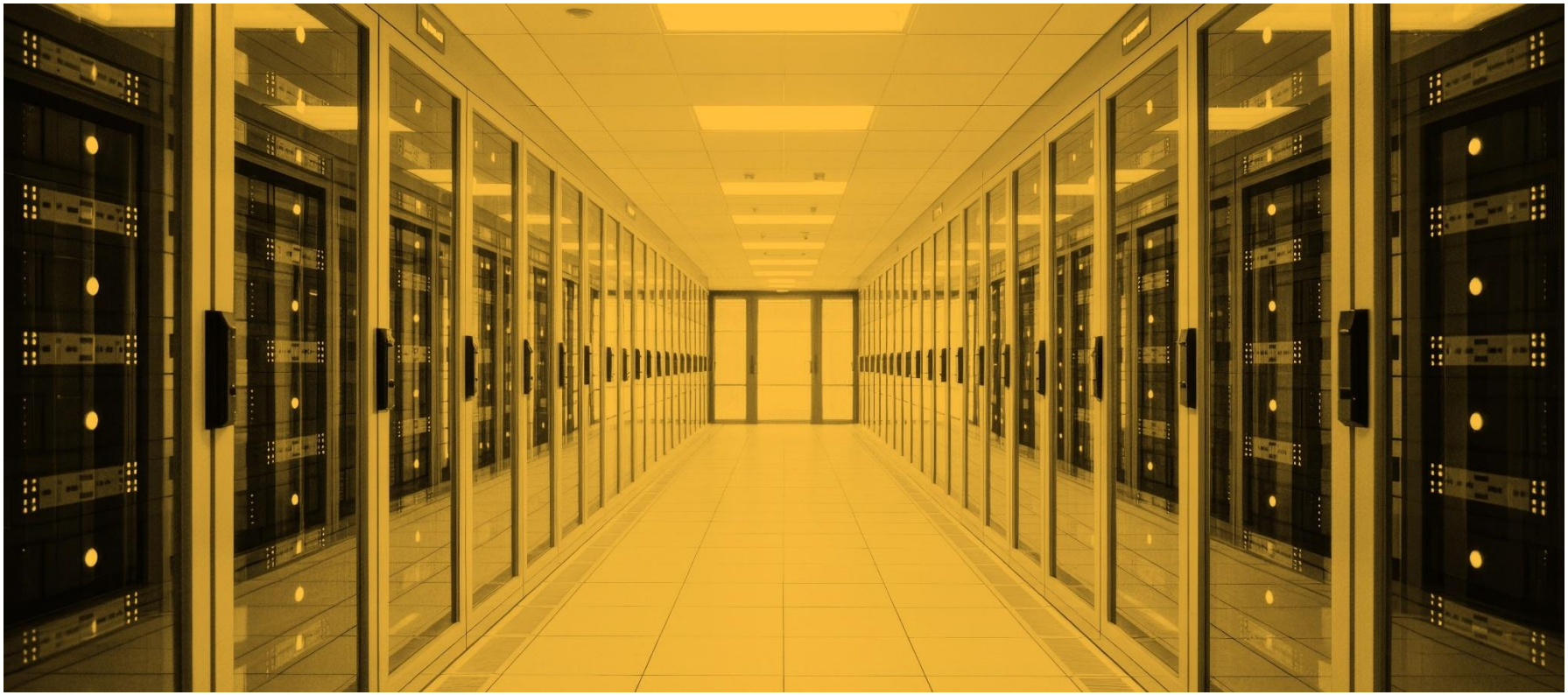


BONELLIEREDE
BREDIN PRAT
DE BRAUW
HENGELER MUELLER
SLAUGHTER AND MAY
URÍA MENÉNDEZ

JULY 2026

POWER AND PLACE:
A REGULATORY GUIDE TO DATA CENTRE DEVELOPMENTS IN EUROPE

CONTENTS

Executive Summary

Data centres have become foundational infrastructure for the global economy. The sector is attracting investment at a scale and pace without modern precedent. Accelerating digitalisation, the computational demands of AI, and the strategic priority that governments now attach to sovereign compute capacity have together transformed data centres into pillars of national industrial strategy. Yet the regulatory and infrastructure frameworks that govern their development have not kept pace with that demand.

A defining feature of the sector is a collision between the political and economic imperative to build at speed on the one hand, and the physical and regulatory constraints on the other. Congested electricity grids, lengthening grid connection queues, inflexible planning regimes, tightening environmental obligations, and an increasingly assertive foreign investment-screening apparatus are factors that ultimately determine whether, where, when, and on what terms a project can in fact proceed.

Prepared by the European Best Friends network, this publication maps those constraints and opportunities that accompany them across seven jurisdictions – France, Germany, Italy, the Netherlands, Portugal, Spain, and the United Kingdom – together with the EU-level framework on which six Member State regimes build. It applies a common comparative framework organised around five principal themes that recur across the jurisdictions surveyed: (i) securing grid access; (ii) procuring power; (iii) national strategy, investment, and planning incentives; (iv) environmental regulation and sustainability; and (v) real estate and site structuring.

Power, common regulatory foundations, and UK divergence

Power access has emerged as the single greatest constraint on data centre development in every jurisdiction surveyed. Connection queues are extensive, with grid connection timelines extending over several years. Structural reform is accompanying that scarcity of power access. The traditional “first-come, first-served” model of allocating connection capacity is giving way, jurisdiction by jurisdiction, to merit- and maturity-based systems that prioritise project readiness, financial commitment, and policy alignment at an earlier stage than the regimes they replace.

Diverging foreign direct investment regimes and sector-specific data localisation

The divergence in national approach is perhaps most acute in relation to foreign investment screening. Each jurisdiction has a bespoke regime: Germany's mandatory notification requirement, triggered at a 10% of voting rights level for non-EU acquirers of facilities meeting its 3.5 MW critical-facility threshold; the Netherlands' 50 MW threshold under its telecommunications regime; the UK's designation of "data infrastructure" as a mandatory notification sector under the National Security and Investment Act 2021 ("**NSI Act**"); and France's composite test of facility size, multi-site operation and client sensitivity.

Data localisation follows a related logic. No European jurisdiction imposes a general localisation mandate for private sector data. However, each European jurisdiction overlays that permissive baseline with sector-specific constraints – for health data, defence and classified information, financial services outsourcing, and government workloads – that operate as implicit localisation requirements whose practical effects depend on the operator's anticipated customer base.

Increasingly prescriptive sustainability and energy efficiency standards

Energy efficiency and sustainability regimes are matters on which national regimes are moving both fastest and farthest apart. Yet, the direction of travel is from disclosure towards prescription. For example, Germany already mandates a Power Usage Effectiveness ("**PUE**") ratio of 1.2 or below for data centres commissioned after 30 June 2026, together with an escalating energy-reuse factor. Spain's draft regime would tie compliance with efficiency and sustainability reporting directly to the grant and retention of grid access permits. France imposes detailed efficiency disclosure while declining, for now, to set a mandatory PUE floor.

Waste heat recovery is emerging as a parallel obligation across several jurisdictions, and the credibility standard for renewable energy claims is expanding, by market and procurement practice rather than by regulation, towards hourly temporal matching; the statutory certificate regimes on which such claims still rest – Guarantees of Origin ("**GOs**") and, in the United Kingdom, Renewable Energy Guarantees of Origin ("**REGOs**") – continue to operate on an annual accounting basis and impose no temporal-correlation requirement, so that hourly matching, like additionality, remains in most jurisdictions a contractual rather than a regulatory requirement. Greenwashing exposure remains latent – as no enforcement action has yet been taken against a data centre operator in any surveyed jurisdiction.

Beyond the contested credibility of environmental claims lies a more structural divergence. The United Kingdom imposes no mandatory, data centre-specific efficiency-reporting obligation equivalent to that under the recast EU Energy Efficiency Directive, and it has adopted a single- rather than a double-materiality basis for sustainability disclosure. This asymmetry confronts operators active in both markets with a choice between voluntary alignment with EU standards and the maintenance of separate compliance frameworks.

Planning: acceleration and constraint

A structural tension runs through every planning and environmental regime surveyed in this report. While jurisdictions are seeking procedurally to accelerate strategically important projects, they are simultaneously tightening the substantive obligations those projects must satisfy. National AI and digital infrastructure strategies have recast data centres as instruments of industrial and sovereign compute policy. Several jurisdictions have responded by introducing fast-track consenting routes for data centres: including the UK's Nationally Significant Infrastructure Project ("**NSIP**") regime from January 2026; France's extension of its project-of-major-national-interest ("**PINM**") regime; Spain's new category of Strategic Investment Projects; Portugal's project-of-national-interest regime; and Italy's unified, simplified authorisation, supplemented by a strategic national interest designation for projects of €1 billion or more.

The procedural acceleration coincides with tightening environmental obligations, and environmental impact assessment ("EIA") requirements triggered in every jurisdiction by the ancillary infrastructure on which data centres depend, typically standby generation. The screening triggers diverge sharply in their level of calibration and, in each case, they are set by reference to the capacity of that standby generation rather than to the data centre's own demand. Italy's threshold of 50 MW of standby capacity (with a full assessment above 150 MW), for example, sits well below the German (200 MW) and Dutch (300 MW) equivalents, exposing certain projects to more scrutiny than elsewhere. This risks regulatory arbitrage undermining the functioning of the internal market and its level playing field.

Lessons for sponsors and investors

Read together, the chapters trace a regulatory environment converging in overall trajectory, while diverging in national form. As power scarcity deepens, the contest for grid capacity will increasingly be resolved by administrative judgments of readiness and strategic value, rather than by the order of application. Regulation across all the surveyed jurisdictions is increasingly dependent on capacity thresholds. A consequence is that a single facility may be subject to different rules – particularly regarding efficiency reporting, critical infrastructure designation, foreign investment screening, and planning – at different capacity values (measured variously by installed IT load, total site load, and floorspace).

Beneath the national variation lies a shared regulatory foundation, and the six EU Member State regimes build upon a common foundation of EU law governing grid access, cybersecurity and physical resilience, energy efficiency, renewable certification, and corporate sustainability reporting. The national regimes diverge principally in the speed and ambition of national execution rather than in the underlying design. However, the UK's position increasingly diverges more significantly.

Efficiency disclosure may well follow a conveyor belt trajectory towards mandatory performance standards. Security designation and foreign investment scrutiny of data centres will widen. Actions at the EU level, meanwhile, are likely to press EU Member State regimes toward a more prescriptive and harmonised position. By way of example, the EU Tech age gives that trajectory concrete form, and adds a further axis to it: alongside efficiency and security, the sovereignty of compute itself – who owns it, where it sits, and which workloads it may carry – is becoming a regulated characteristic of the asset.

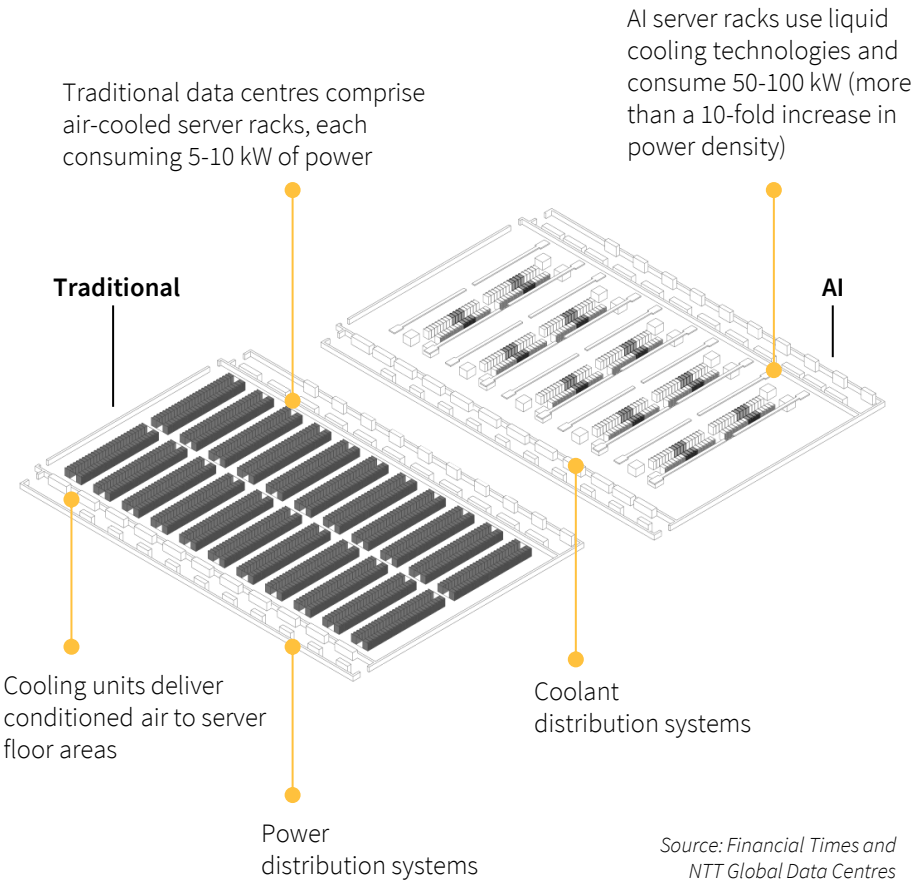
For sponsors, investors, and corporates, the practical consequence is that the constraints which determine a project's viability – grid, security, planning, and environment – should be addressed cohesively. Those who engage network operators at the earliest stage of site selection, who pre-empt changes to efficiency standards, who structure ownership, financing, and data flows with foreign investment and localisation exposure in view from the outset, will find the advantage runs with them.

What makes a data centre?

A data centre is, at its most elementary, a physical facility that houses the computing systems on which digital services depend – servers, data storage arrays and network equipment – together with the power, cooling, and supporting building systems that keep them operating securely and without interruption. Its distinguishing features from ordinary commercial buildings are the intensity and criticality of those supporting systems: the redundant power supply, the standby generation, the dedicated cooling, and the connectivity infrastructure that sustain continuous operation are integral to the asset, rather than ancillary to it.

A data centre is therefore best understood as an engineered environment whose entire purpose is the uninterrupted, secure processing and storage of data. This requirement for continuity shapes both a data centre's physical design and the regulatory regimes to which it is subject.

COMPARING AI AND TRADITIONAL DATA CENTRES



Source: Financial Times and NTT Global Data Centres

Defining infrastructure: power, storage, water and cooling

The defining characteristic of a data centre is its dependence on a continuous and resilient supply of electricity. Its electrical topology is built in three layers, each addressing a different mode of failure. The first is a grid connection, either to the public transmission or distribution network, or a private wire or onsite arrangement. The (optional) second layer is an uninterruptible power supply ("**UPS**"), which bridges the interval before standby generation comes online and, in normal operation, conditions the incoming power to protect sensitive equipment. The third is standby generation. These layers are often designed to ensure redundancy. *For details, see figure 1.*

Figure 1. Three layers of power resilience

Grid Connection

Connection to the public transmission or distribution network, or a private wire or onsite arrangement.

Uninterruptible Power Supply (UPS)

Where implemented, these can include battery-based or sometimes rotary flywheel systems that hold stored energy in reserve and supply the IT load instantaneously upon mains failure and, in normal operations, conditions incoming power against voltage fluctuations.

Standby Generation

Generators (e.g. gas- or diesel-fuelled, renewable and/or fuel cells) supported by on-site fuel reserves, sized to carry the facility's full load for the duration of a sustained outage.

Redundancy: These layers are often duplicated – configurations described as N+1 (one redundant unit beyond the minimum required) or 2N (full duplication) – so that the facility remains operational and can be maintained without any interruption to the load it serves.

The standby-generation fleet is the feature that most often brings a data centre within the scope of emissions control and environmental permitting, because it tends to comprise combustion activities. Furthermore, the scale and redundancy of the power supply determines the connection capacity a project must secure from the network operator, the constraint that dominates site-selection and grid analysis. Another distinct and growing function of energy storage systems is the deployment of larger battery units that interact with the grid.

Heating is a by-product of power usage. Almost all of the electricity drawn by IT equipment is ultimately converted into heat, which must be removed continuously if the equipment is to operate within its tolerances. As power densities have risen, air cooling has approached its physical limits, with liquid cooling increasingly displacing air cooling for the most demanding workloads and experimental use of immersion cooling also beginning. *For details, see figure 2.*

Many cooling systems consume water, whether through evaporative cooling towers or adiabatic systems that exploit evaporation to reject heat. A large facility may require both a substantial supply of, and a means to, discharge warmed or treated water. Both the abstraction and the discharge are subject to permitting rules. Water scarcity has become a major constraint on both cooling-technology choice and site selection alike: the specific licensing thresholds, and their bearing on where or how a facility can be built, are addressed in the section on site selection and in the jurisdiction chapters that follow.

Figure 2. Cooling systems.

ENERGY EFFICIENT

Free Cooling
Uses ambient outside air directly to cool the facility, substantially reducing energy consumption. May use air or direct liquid cooling. Particularly effective in cooler climates.

CONVENTIONAL

Air Cooling
Chillers, computer room air conditioning units, and air-handling systems circulating cooled air through contained hot and cold aisles. The established approach to heat rejection.

HIGH DENSITY

Direct Liquid Cooling
Circulates coolant through cold plates in direct contact with processors, addressing the physical limits of air cooling as rack densities increase.

ADVANCED

Immersion Cooling
Submerges entire equipment in a non-conductive dielectric fluid. The most advanced method, serving the most power-dense workloads.

Typologies

The sector conventionally uses several overlapping typologies. For present purposes, the five most relevant are enterprise, colocation, hyperscale, AI inference, and AI training. Those typologies are distinguished partly by who owns or operates the physical infrastructure, partly by who owns and manages the computing equipment housed within it, and partly by the scale, architecture, and principal workload for which the facility is designed. In some regulatory regimes, the allocation of operational responsibility—and, in some cases, the resulting classification—carries direct regulatory consequences.

An enterprise data centre is dedicated to a single enterprise or corporate group and is typically operated under its control, although particular facilities-management functions may be outsourced. A colocation facility, by contrast, provides managed space, power, cooling, physical security, network access, and, often, interconnection services to one or more third-party customers, which typically install and manage their own computing equipment.

A hyperscale data centre is a very large, highly scalable facility designed to support cloud platforms or other large-scale digital services. It may be owned and operated by the hyperscale company itself, or provided on a leased basis. An AI inference data centre is designed principally to run trained models in production, processing new inputs to generate predictions, responses, or other outputs; its architecture typically prioritises high throughput, network connectivity, and, where the application requires it, low latency and proximity to users. An AI training data centre is designed principally to develop or refine models using large datasets and computationally intensive, highly parallel processing; it therefore typically requires high-density accelerator clusters, high-bandwidth interconnects, and substantial power and cooling capacity.

These categories are not mutually exclusive. The classification therefore identifies the facility's predominant operational model, scale, or workload rather than imposing an exclusive technical boundary.

Capacity, efficiency and the regulatory significance of scale

Two technical measures recur throughout the regulatory analysis that follows. The first is PUE: the ratio of a facility's total energy consumption to the energy consumed by its IT equipment alone. A theoretically perfectly efficient facility, in which every unit of energy reached the IT load and none was lost to cooling, lighting, or power conversion, would achieve a PUE of 1.0. In practice, the global average has sat closer to 1.58, the gap representing the energy overhead of the supporting infrastructure. PUE has become the principal metric of data centre energy efficiency, and it is increasingly accompanied by related measures: water usage effectiveness ("**WUE**"), carbon usage effectiveness ("**CUE**"), and the energy reuse factor ("**ERF**") that quantifies the proportion of waste heat recovered for use elsewhere.

The second is rack density: the electrical load drawn by a single rack or cabinet of equipment, expressed in kilowatts. Conventional enterprise deployments have historically operated at densities of 5 to 10 kW per rack. The computational demands of AI have transformed this picture, with the densest training and inference workloads now commonly drawing 50 to 150 kW per rack, and the most advanced configurations exceeding even that range. Rising density is the principal driver of the shift to liquid cooling, and it also mediates the relationship between a facility's power capacity and its physical footprint: a given quantity of IT load may occupy a fraction of the floorspace at high density that it would at conventional density.

The last point carries direct regulatory salience, because European and national legislation increasingly define and regulate data centres by reference to capacity thresholds, rather than to typology, and those thresholds are measured against several different metrics. The recast EU Energy Efficiency Directive imposes reporting obligations on facilities with an IT power demand of 500 kW or more, and waste heat recovery obligations on those with a total rated energy input exceeding 1 MW. The EU NIS2 Directive and the EU Critical Entities Resilience Directive identify data centre providers as essential, important, or critical entities by reference to size. National tests add further thresholds of their own – Germany's designation of facilities of at least 3.5 MW (and 10 racks) as critical, the UK's forthcoming distinction between colocation facilities at or above 1 MW and enterprise facilities at or above 10 MW – each measured variously by installed IT load, total site load, or floorspace.

Main criteria for site selection

Site selection for a data centre is governed more by the availability of power, connectivity, and the regulatory headroom to build, rather than solely by conventional real-estate considerations. A viable site must satisfy a cluster of interdependent requirements: a grid connection of sufficient capacity and realistic delivery date; access to dense and diverse fibre routes; the water and climatic conditions to cool the facility efficiently; buildable land with a workable consenting route; and a tolerable profile of natural hazard and community-opposition risk. These constraints lie largely outside a developer's control, and frequently set the entire project's timetable. They are also cumulative rather than severable: a parcel with abundant power but no fibre, or buildable land with no realistic grid connection, will not support a facility, however attractive its other attributes.

As foreshadowed in the previous sections, access to power has become the single greatest constraint, displacing the traditional primacy of proximity to the populations a facility serves. That displacement has been reinforced by the rise of latency-tolerant AI workloads, which loosen the historic need to site capacity close to end users, and allow developers to follow available power to more remote locations. Grid congestion and lengthening interconnection queues now extend connection lead times by several years in the most established markets. Developers are, accordingly, prioritising regions with robust transmission and distribution infrastructure, and are increasingly transacting in "powered land" sold on the strength of confirmed capacity: a practice that makes early engagement with the network operator a crucial step in site identification.

Connectivity is equally decisive. Sites are valued for their proximity to dense and diverse fibre routes, internet exchange points, cloud on-ramps, and for the resilience of redundant paths. Latency sensitivity varies by workload. AI training is relatively latency-tolerant, and may be sited remotely, whereas colocation serving financial trading or content streaming requires network-rich locations adjacent to the users it serves.

Operators continue to cluster where power, connectivity, and a skilled construction and operations workforce converge, weighing the advantages of established hubs against congestion and regulatory pressures. They are also increasingly expanding into secondary markets where capacity remains available. Community sentiment has itself also become a seminal factor: local opposition has halted significant projects, making early engagement with the host community integral to responsible site selection.

A site's viability turns, ultimately, on the convergence of power, connectivity and a workable consenting route at a single location, and on the timetable within which each can be secured. Power capacity and grid-connection lead times are now primary constraints, followed closely by connectivity, water, and applicable planning routes. The absence of any one condition defeats a project that satisfies all the others. The practical discipline is to resolve these questions in parallel and at the earliest possible stage, before committing significant development capital, since each is capable on its own of affecting whether, and when, a project can proceed.

Land use and planning are also determinative. Buildable land is scarce in key connectivity hubs, and the applicable consenting route is often decisive, with jurisdictions diverging between general commercial planning and dedicated fast-track regimes for strategically significant projects. Whether a project requires an EIA is frequently determined on a case-by-case basis by reference to ancillary infrastructure, such as standby generation. The consequences of an inadequate assessment are significant. Developers assess natural-hazard exposure – flood plains, seismic activity and ground stability – to screen out sites whose physical characteristics would compromise resilience.

Cooling and water access shape both operational efficiency and regulatory exposure. Lower ambient temperatures reduce cooling loads and operating costs, whereas water availability is subject to ever-closer scrutiny in resource-constrained regions.

Comparative Overview Matrix

REGULATORY THEME								
Grid connection and queue reform	✓	✓	✓	✓	✓	✓	✓	✓
Demand flexibility and interruptibility	✓	✓	✓	✓	✓	✓	✓	✓
Planning and consenting (including fast-track routes, if applicable)	✓	✓	✓	✓	✓	✓	✓	✓
National targets or strategy	✓	✓	✓	✓	✓		✓	✓
Investment support (eg. tax, grants, etc)	✓	✓				✓	✓	✓
Critical infrastructure designation and cyber security	✓	✓		✓	✓	✓	✓	✓
Renewable energy procurement	✓	✓		✓	✓	✓	✓	✓
Environmental regulation (energy efficiency, EIA, water)	✓	✓	✓		✓	✓	✓	✓
Heat recovery and waste heat obligations	✓	✓		✓	✓	✓	✓	✓
Sustainability reporting requirements	✓	✓		✓	✓	✓	✓	✓
Data localisation and foreign investment screening requirements	✓	✓		✓	✓	✓	✓	✓

EU-wide regulatory overview

Many national regulations in EU jurisdictions applying to data centre operators are based on, or transpose, EU law. This chapter provides an overview of the principal EU-level legislation that forms the baseline for the national transpositions examined in the jurisdiction chapters that follow. Readers should treat this chapter as contextual reference material: where a national chapter references an EU directive or regulation, this chapter provides the underlying EU-level framework. The principal areas addressed are the internal electricity market framework, renewable energy and guarantees of origin, cybersecurity and physical resilience (NIS2 and the CER Directive), environmental and planning regulation (including the EIA Directive and the Industrial Emissions Directive), energy efficiency and eco-design requirements, corporate sustainability reporting (the CSRD), greenwashing and consumer protection, AI and supercomputing, and data protection and governance regimes.

ELECTRICITY MARKET FRAMEWORK

The Internal Electricity Market Directive (Directive (EU) 2019/944) establishes common rules within the EU for the generation, transmission, distribution, energy storage, and supply of electricity. Of greatest relevance for data centre operators, the Directive stipulates the basic rules governing third-party access to the transmission and distribution grid. Such access must be based on published tariffs that apply to all customers, and must be applied objectively and without discrimination between grid users. A grid operator may refuse access only in defined circumstances, in particular where it lacks the necessary capacity. Under the Electricity Market Regulation (Regulation (EU) 2019/943), the European Commission is empowered to adopt delegated network codes which establish harmonised rules for the European wholesale electricity markets and the operation of grids, including, by way of example, a network code on demand connection.

RENEWABLE ENERGY

The Renewable Energy Directive (Directive (EU) 2018/2001) establishes a common framework for the promotion of energy from renewable sources in the EU. It lays down rules on, among other things, financial support for electricity from renewable sources, consumption of such electricity, and accelerating permitting in "renewables acceleration areas". It also establishes a scheme for guarantees of origin ("**GOs**"), which data centre operators may use to evidence their use of renewable energy to regulatory authorities, customers, and lenders.

CYBERSECURITY AND RESILIENCE

The NIS2 Directive (Directive (EU) 2022/2555) establishes a comprehensive cybersecurity framework for operators of essential and important entities in the EU, and was required to be transposed into national law by 17 October 2024 (although a number of Member States were late in completing transposition). Under NIS2, data centre providers are expressly identified as essential or important entities, depending on size, and EU Member States must ensure that data centre operators are able to prevent, manage, and report security incidents. Most notably, Member States must ensure that data centre operators take appropriate and proportionate technical, operational, and organisational measures to manage the risks posed to the security of their network and information systems, and to minimise the impact of incidents on the recipients of their services and on interconnected systems. These measures must be based on an "all-hazards approach" designed to protect network and information systems and the physical environment of those systems from incidents.

As at mid-2026, the substantial majority of Member States have completed transposition. The focus has now shifted from implementation to enforcement: national authorities have begun the first wave of supervisory activity, encompassing entity registration, incident-reporting compliance, supplier-risk management, and the personal accountability of designated senior managers.

In addition, the Critical Entities Resilience Directive (Directive (EU) 2022/2557) ("**CER Directive**") sets out requirements for the physical resilience of critical infrastructure and was required to be transposed by 17 October 2024. Digital infrastructure – including data centre service providers and certain cloud computing service providers – is one of the eleven sectors expressly within the scope of the CER Directive. However, where an entity is identified as a critical entity under the CER Directive, it will automatically be treated as an essential entity under NIS2, with the result that both the physical resilience obligations under the CER Directive and the cybersecurity obligations under NIS2 apply cumulatively. Member States retain discretion to impose stricter requirements at national level.

A further resilience regime operates on the sector by indirect effect. The Digital Operational Resilience Act (Regulation (EU) 2022/2554) ("**DORA**") applies to financial entities and their ICT third-party service providers. In November 2025, the European Supervisory Authorities designated the first cohort of critical ICT third-party providers – a list of nineteen that includes the principal hyperscale cloud platforms – subjecting them to direct EU-level oversight, on-site inspection rights, and daily penalties of up to 1% of average worldwide daily turnover for remediation failures. Data centre operators serving financial sector customers should expect its requirements – exit and substitutability planning, ICT risk registers, and audit and access rights – to flow through contractually into colocation and hosting arrangements, and should anticipate that financial tenants will negotiate accordingly.

ENVIRONMENTAL AND PLANNING REGULATION

The EU has adopted several directives on environmental regulation which are relevant for the planning and permitting of data centres. The Environmental Impact Assessment Directive (Directive 2011/92/EU) ("**EIA Directive**") requires EU Member States to assess the likely significant effects on the environment of certain infrastructure projects before development consent is granted. This includes stakeholder and public participation requirements. These processes are a critical step in the development of a data centre, as they directly affect project timelines and permit decisions. Under the EIA Directive, data centres are not expressly listed in either Annex I (mandatory EIA) or Annex II (case-by-case screening). EU Member States therefore retain discretion as to whether, and on what thresholds, a data centre project (typically captured under Annex II categories such as "urban development projects" or "industrial estate development projects") is subject to a full EIA.

The Strategic Environmental Assessment Directive (Directive 2001/42/EC) ("**SEA Directive**") applies to certain plans and programmes prepared and adopted by public authorities at national, regional, or local level, including those that set the framework for projects likely to have significant environmental effects. Under the SEA Directive, the competent authority must conduct a strategic EIA of any such plan or programme. Data centres are regularly accounted for in land-use and zoning plans prepared by local or regional authorities. As a result, the SEA may also impact the consenting environment for the development of a data centre. Furthermore, the Habitats Directive (Directive 92/43/EEC) and the Birds Directive (Directive 2009/147/EC) establish protection regimes for specific habitats and species which regulatory authorities consider in zoning and land-use plans (including, where required, an "appropriate assessment").

The Industrial Emissions Directive (Directive 2010/75/EU) ("**IED**") commits EU Member States to control and reduce the impact of industrial emissions on the environment. It applies to combustion plants with a rated thermal input of 50 MW or above; for plants below that threshold, but with a rated thermal input of at least 1 MW, the Medium Combustion Plants Directive (Directive (EU) 2015/2193) ("**MCPD**") applies instead. Both instruments are potentially relevant for data centres. A single emergency power generator – which would typically combust diesel, gas, or other fossil fuels – will rarely reach the 50 MW threshold that triggers the IED. However, the IED's aggregation rules treat technically connected units operated by the same operator as a single installation for the purposes of calculating rated thermal output. This means that hyperscale facilities operating large generator fleets may nonetheless fall within its scope. For most data centre operators, the MCPD will be the operative instrument: it sets emission limit values for sulphur dioxide, nitrogen oxides, and particulate matter from fossil fuel combustion plants.

ENERGY EFFICIENCY AND ECODESIGN

The Energy Efficiency Directive (Directive (EU) 2023/1791) ("**EED**") recognises the economic importance of data centres while addressing their significant energy consumption. The EED and the supplementary Commission Delegated Regulation (EU) 2024/1364 impose reporting obligations on data centres with an IT power demand of at least 500 kW. The EED also obliges EU Member States to ensure that data centres with a total rated energy input exceeding 1 MW utilise waste heat recovery applications or supply waste heat to a district heating network, unless a cost-benefit analysis demonstrates that this is not technically or economically feasible. The Commission Implementing Regulation (EU) 2019/424 on Ecodesign Requirements for Servers and Data Storage Products sets energy and material efficiency requirements for certain servers and data storage products that are essential to data centre infrastructure.

The Commission's Strategic Roadmap for Digitalisation and AI in the Energy Sector (COM(2026) 501 final) is a non-binding communication organised around three pillars – the sustainable integration of data centres into the energy system, the deployment of digital and AI solutions across it, and the supporting data-governance framework – and foreshadows both a model agreement between operators, energy actors, and public authorities (to be published in the second half of 2026), and, if voluntary coordination proves insufficient, a possible legislative proposal to secure that integration.

Most significantly for operators, the Roadmap was accompanied by a Data Centre Energy Efficiency Package, the central element of which is a second Delegated Regulation establishing a common EU-wide sustainability rating scheme. The draft Regulation, published for consultation in March 2026 and scheduled for adoption in mid-2026, provides for electronic ratings to be issued automatically by the European database on data centres, rating facilities by reference to PUE and WUE classes calculated under a harmonised methodology, with the first ratings expected in 2027. The reporting cycle under Delegated Regulation (EU) 2024/1364 in respect of calendar year 2025 closed on 15 May 2026, and the data submitted in that cycle will form the baseline against which the rating scheme – and any future minimum performance standards – is calibrated. Operators should therefore treat the definitional and boundary choices made in their submissions as positioning decisions rather than merely being a compliance response: the rating may rapidly become a benchmark in procurement, financing, and leasing across the EU.

CORPORATE SUSTAINABILITY REPORTING

In addition to the reporting obligations under the EED, some data centre operators may be subject to reporting requirements set out in national regulations which implement the Corporate Sustainability Reporting Directive (Directive (EU) 2022/2464) ("**CSRD**"), as amended by the Omnibus Directive on Sustainability (Directive (EU) 2026/470). Under the CSRD, certain EU and non-EU companies must report on their environmental and climate impacts across their supply chain. Companies subject to the CSRD have to report according to the European Sustainability Reporting Standards ("**ESRS**") that are currently in the process of being revised in view of the Omnibus Directive on Sustainability.

With the amendments of the CSRD, as introduced by the Omnibus Directive on Sustainability, effective as of March 2026, the EU legislator drastically narrowed the CSRD's scope: only companies with over 1,000 employees and €450 million net turnover will be subject to mandatory CSRD reporting, effective from the financial year 2027. This removes approximately 90% of previously in-scope companies. Data centre operators will only be subject to the CSRD if they meet these high thresholds.

GREENWASHING AND CONSUMER PROTECTION

The Directive on Empowering Consumers for the Green Transition (Directive (EU) 2024/825) prohibits general environmental claims – such as "climate neutral", "eco-friendly", or "green" – where these are not scientifically substantiated. Data centre operators must take this requirement into account when advertising their data centre as climate neutral to prevent greenwashing litigation.

AI AND SUPERCOMPUTING

The AI Act (Regulation (EU) 2024/1689) has been in force since 1 August 2024 and classifies AI systems by risk level: unacceptable (use of which is prohibited), high (subject to extensive regulation), and limited (subject to additional transparency obligations). Many other AI systems pose only minimal risk and are subject to limited obligations (for example, AI literacy).

The Act is being implemented on a staged basis: the prohibitions and AI literacy obligations apply from 2 February 2025, the rules on general-purpose AI ("**GPAI**") from 2 August 2025, and the transparency and enforcement rules from 2 August 2026. Following political agreement on the Digital Omnibus on AI, the obligations on high-risk AI systems have been postponed to 2 December 2027 for stand-alone high-risk AI systems and 2 August 2028 for high-risk AI systems embedded in certain products. A grace period also applies to certain of the transparency rules.

Providers of general-purpose AI models trained using more than 10^{25} floating-point operations are presumed to have high-impact capabilities, which carry specific notification and risk-management duties. That threshold has rapidly become a commercial reference point in hyperscale compute procurement. Data centre operators hosting in-scope training or inference workloads may find that these obligations begin to flow through into hosting and colocation contracts as compute-related disclosure and data governance requirements, even where the operator itself owes no direct duty under the Regulation. For example, although the direct duty for data governance and quality is owed by the provider, the provider may require the operator's assistance in producing supporting evidence, such as compute records or evidence of infrastructure resilience.

Data centre operators may also fall directly within the scope of the Act, particularly because one of the high-risk categories concerns AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, which could include data centres.

In addition, the EuroHPC Joint Undertaking pools EU and national resources to build world-class computing infrastructure across Europe. Two amendments have materially expanded its mandate: the 2024 amendment established AI Factories (compute clusters of approximately 25,000 AI-optimised processors linked to supercomputing centres to support AI experimentation, training, and startup access), and the January 2026 amendment (Council Regulation (EU) 2026/150, in force 20 January 2026) extended it to AI Gigafactories (state-of-the-art facilities of approximately 100,000 processors each, built on energy-efficient data centre infrastructure and covering the full AI lifecycle from development to large-scale inference), supported by the InvestAI facility targeting €20 billion in mobilised investment across up to five Gigafactory sites in the EU.

A major pending development is the proposed Cloud and AI Development Act ("**CADA**"), adopted by the Commission on 3 June 2026 as the centrepiece of its European Technological age. That package pairs two legislative proposals – CADA and the proposed Chips Act 2.0 – with two policy instruments – the EU Open Source Strategy and the Strategic Roadmap for Digitalisation and AI in the Energy Sector – bringing cloud, compute, semiconductors, software, and energy-system integration into a single sovereignty programme. CADA aims to triple the EU's data centre capacity within five to seven years, principally through each Member State's designation of at least one data centre acceleration zone, in which qualifying projects benefit from streamlined, aggregated permitting, a 12-month consent deadline, and improved access to energy, land, water, and financing. The Commission may also designate individual projects as strategic, unlocking preferential access to EU funding, and CADA would establish an EU-wide framework for assessing the sovereignty of cloud and AI services procured by the public sector, with progressively stricter requirements for sensitive sectors.

The proposed framework is structured around four Union assurance levels, moving from EU-located infrastructure and data, through demonstrated independence from third-country control and software supply chain transparency, and EU ownership and control, to effective control over the entire software supply chain with no third-country interference. Its significance lies in its downstream reach: public sector bodies would assess which cloud and AI services suit particular use cases by reference to those levels, and essential entities under NIS2 may be drawn into the same logic – initially voluntarily and, through future secondary legislation, potentially as a binding requirement in designated sectors. For operators serving public sector or otherwise sensitive workloads, sovereignty would therefore become a procurement criterion in its own right, absorbing the cybersecurity-certification and data localisation requirements they already face and recasting them as gradations of a single sovereignty test.

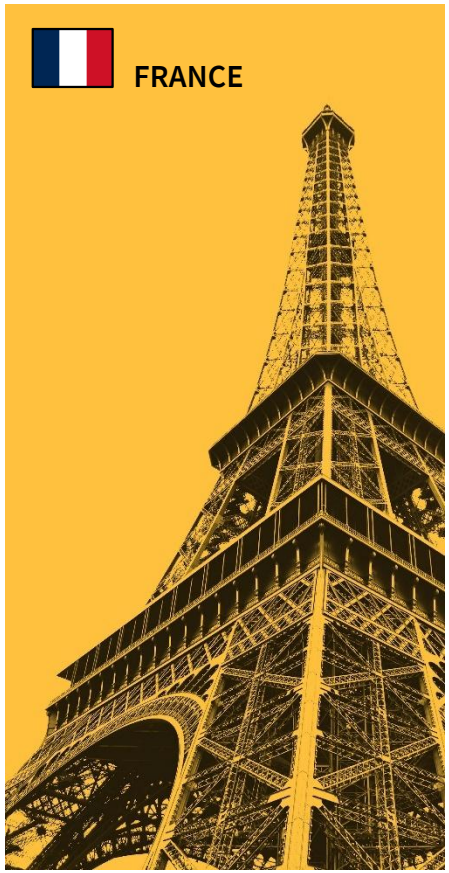
The proposal now enters the ordinary legislative procedure, likely to run for one to three years. The most contested element is expected to be the sovereignty framework, on which the Council and Parliament are likely to divide, while the permitting provisions – more directly relevant to data centre development – engage competences that Member States guard closely. The direction of travel is not in doubt, however: because CADA would take effect as a directly applicable regulation, its acceleration-zone and consent-deadline obligations would overlay and, in time, reshape the national consenting regimes described in the jurisdiction chapters that follow.

DATA PROTECTION AND GOVERNANCE

The General Data Protection Regulation (Regulation (EU) 2016/679) ("**GDPR**") is the principal data protection framework within the EU. It confers privacy rights on EU residents with regard to how their data is collected, used, stored, and processed. If data centre operators also operate the servers (ie. process personal data on behalf of customers), they can qualify as data processors or data controllers and be subject to obligations under the GDPR. The EU Data Act (Regulation (EU) 2023/2854) complements the GDPR by setting specific obligations on data processing services – such as cloud and edge services typically operated from data centres – particularly in relation to switching between providers and removing contractual, commercial, and technical barriers to interoperability. For non-personal data, the Free Flow of Non-Personal Data Regulation prohibits unjustified localisation requirements, while preserving public authorities' access to data stored or processed in either another Member State, or in the cloud. However, it does not displace sector-specific sovereignty, cybersecurity, or national security rules that may shape where sensitive workloads are hosted.

The European Health Data Space Regulation (Regulation (EU) 2025/327) seeks to ensure the effective use of health data within the European Union, while guaranteeing a heightened level of protection for such sensitive data. For operators of hosting data centres, national implementation of the Regulation may give rise to a de facto obligation to store electronic health data within the EU, the EEA, or a specified Member State.

Country Chapters



In terms of the number of data centres, France ranks sixth worldwide and third in Europe, behind the United Kingdom and Germany. Paris has become the third-largest European hub in terms of installed capacity (683 MW as of the end of 2024), behind Frankfurt (approximately 2,900 MW) and London (1,000 MW). At the Paris AI Action Summit in February 2025, more than €109 billion in private investment was announced for data centres and AI, and in 2025, according to the Trendeo Observatory, data centres alone accounted for approximately €67 billion of the €125 billion in industrial investments announced in France, making the country the world's leading recipient of foreign investment in data centre construction that year.

The French Government's ambition is to make France 'an AI powerhouse', as outlined in the third phase of the National Strategy for AI launched in February 2025 as part of France 2030. To date, 63 sites have been identified as suitable for data centre development, including five so-called 'fast-track' sites with a connection potential exceeding 700 MW within three to four years, and the total power capacity sought by project developers amounts to 28.6 GW, of which 5.8 GW has already been secured. France can rely on major strengths in this respect: 95% carbon-free electricity, record production from a powerful nuclear fleet, a reliable extra-high-voltage grid (99.9995% availability), and attractive prices for energy-intensive users. However, these aspirations are increasingly coming up against difficulties linked to development timelines and issues of local acceptance, with growing concern over environmental issues, particularly those relating to water usage. What follows is a thematic analysis of France's position according to the four principal dimensions of the comparative framework applied throughout this publication: securing grid access (referred to in this chapter as 'Securing Network Access'), power procurement ('Sourcing Power'), national strategy and planning ('Policy framework, incentives, and consenting'), and environmental obligations.

SECURING NETWOTK ACCESS

The unbundling framework and site selection implications

France operates a strict unbundling model. Transmission at high and extra-high voltage is the exclusive responsibility of the French electricity transmission system operator, RTE. Distribution is handled by Enedis and the local distribution companies, all operating under the supervision of the Energy Regulatory Commission ("CRE"), the independent national regulator. All network users benefit from non-discriminatory access rights. As a consequence of the unbundling framework, data centres may not own or operate public network infrastructure. The sole exception, a closed distribution network, is a marginal and rarely used structure in practice.

For sponsors and investors, the principal practical implication is the need to identify and secure a suitable site at a very early stage: specifically, one that is proximate to a RTE or Enedis substation of sufficient capacity for the project's power requirements. This is particularly important in areas that RTE and the State have already identified as suitable for high-power demand.

Navigating the connection queue

Connection to the network is governed by the French Energy Code, which establishes a right of connection for all users on transparent and non-discriminatory terms. The standard RTE connection procedure comprises the following stages: firstly, a feasibility study (completed within six weeks); secondly, a technical and financial proposal ("PTF") issued within three months of the feasibility study; thirdly, placement on the connection queue upon acceptance of the PTF, on a first-come, first-served basis; fourth, execution of a connection agreement; and fifth, completion of works and commissioning.

Overall delivery timelines vary considerably, depending on the scale of the connection works, the project's location, and the planning and environmental procedures applicable to the relevant substation and power line infrastructure.

Demand pressure on the queue is very high. Several dozen gigawatts of capacity are already reserved, with the backlog particularly concentrated in Île-de-France. Under the standard procedure, sponsors should plan for connection timelines of seven to ten years. RTE's fast-track procedure, introduced in 2025, can reduce this to 3 to 4 years for projects above 400 MW, subject to payment of a specific congestion contribution. This is a significant concession that sponsors of large-scale projects should assess carefully against the premium cost.

In principle, the connection application does not require a planning permit to have been obtained at the time of submission. However, the application must contain sufficiently precise and finalised project details to satisfy RTE's requirements, and any material changes to those details may lead to the applicant losing their position in the queue. The procedure effectively locks in relatively mature projects, so sponsors should not underestimate the degree of design and site certainty required before submitting.

Connection costs follow a split allocation regime. The costs of dedicated connection works are borne by the project. Upstream network reinforcement costs are shared through the network usage tariff ("**TURPE**"), and recovered from all French consumers. Under the standard regime, the costs resulting from a given connection are in principle borne in full by the first applicant requesting that capacity; cost-sharing between multiple projects is not a general entitlement, but is available under a specific scheme introduced in 2023 for major high-voltage works, which sponsors of large-scale or campus-style developments should investigate at an early stage.

Finally, since 2025, RTE has the authority to reduce a project's reserved connection capacity where actual power drawn falls materially below the subscribed level. This mechanism is designed to address speculative reservations and free up capacity across the queue. For new installations, this operates either as an immediate full-capacity connection subject to reassessment after five years, or a gradual ramp-up over a minimum of ten years with at least three adjustment points. For existing installations, reserved capacity is recalculated on the basis of the maximum power drawn over the preceding five years, uplifted by 25%. Compensation for capacity reduction is available only for agreements signed before 1 August 2025 and is capped at 60% of residual costs. Sponsors negotiating connection agreements after that date should assume no compensation entitlement and structure their power take-up commitments accordingly.

Demand response, tariff optimisation, and load flexibility

Data centres are not subject to any sector-specific flexibility requirements. However, they may participate in demand response, capacity, and interruptibility schemes, as well as in demand response tenders administered by RTE. Participation across the sector remains limited in practice, although growing grid pressure and RTE's evolving demand-side strategy make greater engagement increasingly likely over the medium term. For operators able to adjust their load profile, these mechanisms offer a potential route to both tariff savings and improved connection terms, a consideration that sponsors should factor into site selection and operational modelling from an early stage.

Connection contracts are also increasingly incorporating power modulation clauses in exchange for tariff concessions, offering a further lever for managing network costs at high-consumption sites. The network usage tariff, TURPE 7, applicable to the French electricity transmission and distribution networks for the 2025–2028 period, reinforces the price signal during peak periods and typically accounts for 30–40% of the electricity bill. Large, stable consumers may qualify for reductions of up to 80%, subject to conditions that include maintaining an appropriate consumption profile and, for the deepest discounts, holding an ISO 50001 energy management certification.

France has simultaneously completed the roll-out of smart meters, and is significantly increasing grid investment at scale, which will result in a gradual rise in transmission tariffs that should be reflected in financial models from the outset.

SOURCING POWER

Procurement routes: PPAs, CAPNs, and the post-ARENH landscape

Data centres may source electricity in several ways: firstly, spot market purchases; secondly, renewable PPAs (whether on-site or off-site); thirdly, nuclear production allocation contracts ("**CAPNs**"), and fourth, in limited cases, self-consumption arrangements or direct supply lines (the latter subject to prefectural authorisation, and still rarely used in practice). One structural feature of the French market warrants early attention: unlike several other European jurisdictions, the vast majority of PPAs executed in France are physical rather than virtual, with consequences for network charging, tax treatment, and hedging structure that sponsors must address at the outset of any procurement process.

The expiry of the regulated nuclear access scheme ("**ARENH**") at the end of 2025 and the progressive ramp-up of CAPNs are together expected to increase the relative appeal of long-term renewable PPAs as a price-hedging instrument for large consumers. Hybrid PPAs, combining renewable generation with co-located or co-contracted battery storage, are also gaining traction, particularly among data centre operators seeking a stable, continuous power supply.

The choice of procurement route carries material tax and charging consequences. Off-site physical PPAs attract the full suite of grid-related charges, including TURPE, excise duty on electricity, the territorial contribution on electricity consumption ("**CTA**"), and VAT. On-site PPAs and self-consumption arrangements significantly reduce this burden by avoiding or limiting exposure to TURPE and certain other charges, and should be carefully evaluated as part of any site-level cost modelling.

Excise duty on electricity is subject to a reduced-rate regime for highly electricity-intensive sites that meet applicable environmental performance criteria. Data centres exceeding the relevant consumption thresholds may qualify, with applicable rates ranging from €0.5 to €7.5 per MWh, scaled according to the site's electricity intensity and its degree of exposure to international competition. Operators should take early advice on whether their facilities qualify, as well as on the interaction between the reduced rate and the energy management certification requirements that condition access to the deepest TURPE discounts.

Guarantees of Origin: structure, additionality and temporal matching

France operates exclusively within the European GOs system, administered through the European Energy Exchange ("**EEX**") and the Association of Issuing Bodies ("**AIB**") hub. Unlike several other jurisdictions, France does not recognise RECs, REGOs, or I-RECs. GOs are fully interchangeable across the European system, though operators and their counterparties frequently favour French-issued GOs in practice, due to the commercial and reputational demand for geographic anchoring.

GOs are decoupled from the physical sale of electricity, and may be purchased separately on the secondary market. One important exception applies to generation assets that have received public support: in those cases, GOs vest in the State and are made available through public auction, rather than passing to the generator or being available for bilateral purchase.

There is no statutory additionality requirement within the GO framework. However, the voluntary VertVolt label, administered by the French public agency for ecological transition ("**ADEME**"), introduces more stringent criteria for operators intending to make credible renewable energy claims. These criteria include the joint procurement of electricity and GOs from the same source, a minimum proportion of generation from installations not receiving public support, as well as certain vintage and proximity requirements. Operators pursuing externally verified sustainability commitments, or subject to CSRD disclosure obligations, should assess whether their GO procurement strategy meets VertVolt criteria or an equivalent standard, given the growing scrutiny of unqualified "100% renewable" claims.

Temporal matching in France currently operates on a monthly basis. This is increasingly out of step with the direction of European policy and market practice, which is moving towards hourly matching as the credibility standard for renewable energy claims. Emerging EU guidance and the reporting frameworks of several sustainability rating agencies already reflects this shift. Operators and sponsors should therefore treat monthly-matched GOs as a transitional compliance tool rather than a durable reputational asset, and build into their procurement strategies the flexibility to migrate to hourly matching as market infrastructure and regulatory requirements evolve.

Nuclear baseload: CAPNs and SMRs

EDF offers CAPNs as long-term supply instruments, typically structured over 10 to 15 years, entitling the holder to a defined share of output from EDF's existing nuclear fleet at a price reflecting the fleet's operating and capital costs. These contracts succeed the ARENH, and are designed to offer long-term price certainty, currently €65 to €70 per MWh, decoupled from the volatility of short-term wholesale markets. They deliver inherently low-carbon baseload power supply without reliance on the GO framework for emissions accounting purposes. CAPNs may be combined with renewable PPAs to construct a diversified, low-carbon supply portfolio. A number of industrial consumers and at least one leading data centre operator, Data4, have already signed CAPNs, illustrating that the product is commercially available and bankable, rather than a merely prospective option.

SMRs represent a potential long-term option. Co-location of SMRs with large data centre campuses is under active study in France, with the main benefits being controllable, scalable output, and proximity to load. Both are highly valuable to hyperscale operators seeking to manage grid dependency. However, SMRs remain at the pre-commercial stage in France, and the realistic deployment timeframe, taking into account regulatory approvals, site selection, and construction, extends well beyond the current investment horizon for most data centre projects. .

POLICY FRAMEWORK, INCENTIVES, AND CONSENTING

France's AI strategy and the available fiscal levers

France's National AI Strategy ("**SNIA**") makes data centres a pillar of public policy. The strategy explicitly presents France's highly decarbonised energy mix, strong electricity export capacity, and grid reliability as competitive advantages in attracting computing infrastructure at scale. The scale of private investment already announced validates that proposition in practice: major commitments from hyperscalers and established operators confirm that France is regarded as a Tier 1 destination for large-scale campus development in Europe.

The government's principal instruments are facilitative, rather than financial. Policy priorities are concentrated on site identification, permitting support, and strategic coordination, notably through the DGE task force and the France 2030 programme, rather than on direct capital subsidies. Direct financial support is available in one principal area: heat recovery, through ADEME's Heat Fund, and the mandatory recovery obligations applicable since 2025.

The main tax incentives include reduced excise duty and the TURPE allowances (as described in section 6.1.3), both of which can materially reduce the operating cost base for qualifying sites.

The standard corporation tax regime is 25%, with no dedicated data centre economic zone or ring-fenced relief. The most significant tax variables at project level are local in nature: principally property tax and CFE, where the classification of a data centre as industrial rather than commercial premises has a significant impact on the applicable tax base.

OIV status, NIS2 compliance, and ANSSI engagement

Data centres that meet the relevant criteria may be designated as operators of vital importance ("**OIVs**") under French law, and will in any event qualify as essential entities within the NIS2 regulation, as transposed into French law, with enhanced cybersecurity and supervisory obligations imposed and enforced by ANSSI, the French national authority. ANSSI imposes robust technical and organisational measures. The current framework reflects an ongoing consolidation of obligations previously spread across the French OIV, NIS1, and NIS2 regimes. Operators must comply with a structured incident reporting regime comprising an initial alert, interim reports, and a final report, with timelines and content requirements specified by ANSSI. Sponsors and operators should take early advice on whether their facilities will attract OIV designation, which carries more demanding obligations than essential entity status alone, and should build ANSSI engagement into their project development and operational governance programmes from the outset.

Cloud service providers serving the French public sector or operating in sensitive sectors should also consider SecNumCloud certification, which has become the de facto standard for certain public procurement contracts. SecNumCloud imposes stringent requirements regarding data localisation within France, governance structures, and shareholder control, all of which may present structural challenges for non-EU headquartered cloud providers and should be assessed at the earliest possible stage of any market entry strategy.

Foreign investment controls and emerging EU coordination

Data centres may constitute sensitive infrastructure for the purposes of France's foreign investment screening regime. Whether prior authorisation is required for a given transaction currently depends on a combination of factors: firstly, the size of the data centre; secondly, whether the target operates across multiple sites; and thirdly, the sensitivity of the clients served (with exposure to OIV clients being a particularly significant trigger).

The French framework is converging with the proposed European FDI Regulation to increase scrutiny of acquisitions involving critical digital infrastructure and greenfield data centre projects. We anticipate this will involve tighter controls and broader notification obligations for investors.

Data sovereignty: localisation requirements and transfer restrictions

There is no general obligation to localise private data in France. Localisation or quasi-localisation requirements arise principally in: sector-specific regimes (notably for certain health data, defence-classified information, and some police and justice data); the SecNumCloud qualification framework described above and the associated "cloud de confiance" doctrine, which in practice lead French public bodies and certain sensitive operators to use EU and often France-hosted trusted cloud services; and GDPR's restrictions on transfers of personal data outside the European Economic Area, which require specific conditions to be met for international transfers rather than mandating data storage in any particular country.

The hosting of health data requires both HDS certification and a specific contractual framework with the data controller. Defence-classified data is subject to requirements of a materially higher order, which have direct implications for the physical security architecture, access control design, and choice of technology providers at affected facilities.

Data centre operators that process or transit personal data flows across EEA borders should be aware that the competent authority (the "CNIL") has the power to suspend international transfers in cases of non-compliance with applicable transfer mechanisms. This power should be reflected in the standard contractual frameworks governing cross-border data flows, and operators should ensure that their transfer impact assessments and supplementary measures remain current in light of the CNIL's evolving enforcement posture.

Planning classification: the "warehouse" problem and reform prospects

Data centres do not occupy a discrete category in the French urban planning system. They are generally classified under the "warehouse" sub-category, which restricts their location to suitable business parks and may lead to restrictions that are inappropriately calibrated to the operational and spatial requirements of modern data centre facilities. Certain projects, particularly those specifically dedicated to the roll-out of network coverage by electronic communications operators, may be reclassified as "facilities of public interest and public services"; others may benefit from a more permissive interpretation under local planning regimes, depending on the applicable case law in the relevant jurisdiction. Proposed legislative reforms aim to resolve this ambiguity.

All projects must comply with the hierarchy of national and local planning documents: the regional spatial planning scheme ("**SRADDET**" or "**SDRIF**"), the territorial coherence scheme ("**SCoT**"), and the local urban plan ("**PLU/PLUi**"). Compliance with this hierarchy is a condition of planning permission and must be verified at the outset of any site selection process.

PINM designation and accelerated permitting

Data centres require both planning permission and authorisation under the regime for installations classified for environmental protection ("**ICPE**"). The ICPE regime is not specific to data centres, but applies to a wide range of industrial and high-impact facilities. Data centres are generally subject to the full authorisation procedure, which is consolidated under the single environmental authorisation (encompassing ICPE, water, Natura 2000, protected species assessments). In addition, data centres are subject to the Zero Net Land Take ("**ZAN**") law, which imposes binding quotas on the consumption of undeveloped land. With this, ZAN compliance is an increasingly significant constraint on greenfield site selection and should be addressed during the earliest stages of site identification, before committing substantial development costs. In the Paris region, data centre projects exceeding 5,000 m^2 of floor area are also subject to the commercial property approval procedure. The overall lead times for a greenfield project remain in the region of five years or more, reflecting the cumulative demands of planning, environmental, and ICPE procedures, although several recent reforms aim to accelerate pathways for strategically significant projects.

The most important of these is PINM status, which is being extended to data centres on the basis of qualitative criteria (sovereignty, ecological transition, power, and investment), rather than a fixed power threshold, making it accessible to a broader range of projects than a purely capacity-based test might allow. PINM designation carries several procedural advantages: firstly, centralisation of building permit processing at prefectural level; secondly, accelerated harmonisation of applicable planning documents; thirdly, facilitation of exemptions for protected species ("**RIIPM**"); and fourth, priority treatment for RTE connection applications.

ENVIRONMENTAL OBLIGATIONS

The ICPE regime and single environmental authorisation

The obligation to carry out an EIA stems mainly from the ICPE regime, with the applicable thresholds determined by reference to the installed power of generators and other equipment. The single environmental permit consolidates the various environmental consents (covering ICPE, water, Natura 2000, and protected species), but does not merge with, or replace, the building permit. The two authorisations proceed on separate tracks, and a project may obtain one before, or independently, of the other. Large-scale projects located in sensitive areas, particularly those raising water management or biodiversity concerns, are subject to stricter requirements.

More generally, recent years have been characterised by a tension between procedural acceleration, reflected in the single environmental authorisation and the PINM fast-track, and tightening substantive environmental requirements, which are likely to become even more stringent in the coming years.

Efficiency disclosure: PUE transparency without mandatory thresholds

France imposes transparency obligations, rather than mandatory regulatory thresholds: data centre operators are required to make annual declarations of efficiency indicators, including PUE (as well as potentially WUE and CUE), on the national platform, but no minimum PUE or equivalent regulatory floor has yet been enacted. This position distinguishes France from jurisdictions that have moved to mandatory efficiency thresholds, and reflects a policy choice, still under review, to drive performance improvement through disclosure and fiscal incentive rather than direct regulation.

Non-compliance with reporting obligations attracts administrative penalties. More significantly, reported efficiency performance determines access to certain tax benefits (notably the reduced excise duty rate) and the implementation of a certified energy system (ISO 50001 certification being the most relevant standard) is a condition of access to the deepest available tariff reductions under TURPE. Energy performance is also taken into account in the context of the cost-benefit analysis required for the waste heat recovery obligation, and influences the outcome of the environmental authorisation process. Sponsors should additionally be aware that energy performance requirements intersect with the RTE fast-track procedure and sustainable building design requirements, including the greening and solarisation of rooftops under applicable construction standards. Managing these intersecting obligations as a coherent operational and compliance programme, rather than addressing each in isolation, will be essential for operators seeking to optimise both their regulatory position and their cost base.

Mandatory heat recovery: the ERF requirement and ADEME support

Since 2025, data centre operators with an installed capacity of 1 MW or above have been subject to a statutory obligation to recover waste heat, with a minimum Energy Reuse Factor ("**ERF**") of 0.20, which is set to increase over time. An exemption is available where a cost-benefit analysis, conducted in accordance with the methodology specified by the competent authority, demonstrates that heat recovery is not technically feasible or economically viable in the project's specific circumstances, for example due to the data centre located at a geographical distance from heat networks, district heating infrastructure, or other facilities capable of utilising the recovered heat. A transitional regime applies to data centres where a planning application was submitted before 1 January 2026. Under this regime, the operator must carry out the cost-benefit analysis and submit it to the competent administrative authority by 1 October 2027.

ADEME's Heat Fund provides financial support for qualifying heat recovery investments. It is a potential value-creation lever for greenfield projects, where recovered heat can be supplied to adjacent users. It is also an increasingly major point of scrutiny in environmental assessments and relations with local authorities which are acutely aware of both the environmental and economic value of waste heat utilisation.

ESG disclosure, extended producer responsibility, and greenwashing risk

Beyond the European rules on CSRD and taxonomy, data centre operators must publish detailed annual energy performance information on the national platform described above. These transparency obligations, combined with 'green' tax criteria, local authorities' expectations, and lender ESG requirements all focus on the performance trajectory over time (not just the initial PUE) as central to the project's acceptability and bankability.

The French Extended Producer Responsibility ("**EPR**") regime under Article L. 541-10 of the French Environmental Code, requires 'producers' of electrical and electronic equipment (defined broadly as any person who manufactures or has manufactured under their brand, sells under their brand, imports, places on the market, or sells at a distance in France) to contribute to the prevention and management of waste from these types of equipment. However, this framework is not intended to apply to operators of data centres, who do not qualify as 'producers' for these activities.

As of [June 2026], no enforcement action had been taken against a data centre operator in France specifically for greenwashing. However, the Competition Authority's study of December 2025 identified material risks of biased data and non-disclosure in the sector's environmental communications, whilst the CRE's March 2025 report on PPAs calls for greater transparency regarding the additionality of both CAPNs and PPAs.

REAL ESTATE AND SITE STRUCTURING

Site identification: land policy and the ZAN policy

France has launched a national land strategy for data centres, combining the identification of 'ready-to-use' sites, which are already connected or have a mechanism of pre-reservation of electricity capacity, prioritising the use of brownfield sites, and the establishment of regulated allocation procedures for strategic public land. Site choice is the project's primary determining factor. It must take into account the urban context of the site. Under current legislation, premises housing data centres are, in principle, classified under the 'warehouse' sub-category, which may affect their eligibility in certain areas of the local authority's local urban development plan ("**PLU**") or inter-municipal plan ("**PLUi**") and lead to restrictions that are not always suited to the specific characteristics of these facilities.

Added to this is the authorisation process, as noted above. Data centre projects require planning permits and frequently fall under the regime for classified facilities for environmental protection. In Île-de-France, projects exceeding 5,000 m^2 of floor area are subject to a commercial property approval procedure, which underscores the importance of the initial site selection. From an operational perspective, brownfield sites or former industrial sites can offer real advantages as they may already be located in areas compatible with intensive use. They are often situated in areas already designated for economic activities, are less exposed to the risk of land-use conflicts, and may benefit from prior assessments or studies that facilitate the processing of permits.

They are part of the zero net land take ("**ZAN**") policy, which encourages the re-use of already developed land and brownfield sites rather than the consumption of natural, agricultural or forest land. This policy requires that data centres must be accounted for within local or regional land take quotas.

Grid proximity as a site selection criterion: RTE and Enedis Connectivity

Electricity connection is also a major real estate consideration. In France, a site's suitability depends on its proximity to a suitable substation operated by the transmission system operator ("**RTE**") or distribution operator ("**Enedis**"), the available capacity in the area in question, and the possibility of securing a connection schedule compatible with the project. The 'connectability' or 'easily connected' nature of the land is a property selection factor, on an equal footing with the buildability or availability of the plot.

The French government has begun to develop a proactive approach to electricity capacity for sites considered to be strategic. A capacity pre-reservation procedure for certain sites was introduced in 2025 by the French Energy Regulatory Commission ("**CRE**"), combined with fast-track connection mechanisms for sites identified as priorities, with a target timeframe of 3 or 4 years (instead of 6–9 years) for high-power sites (up to 400 MW).

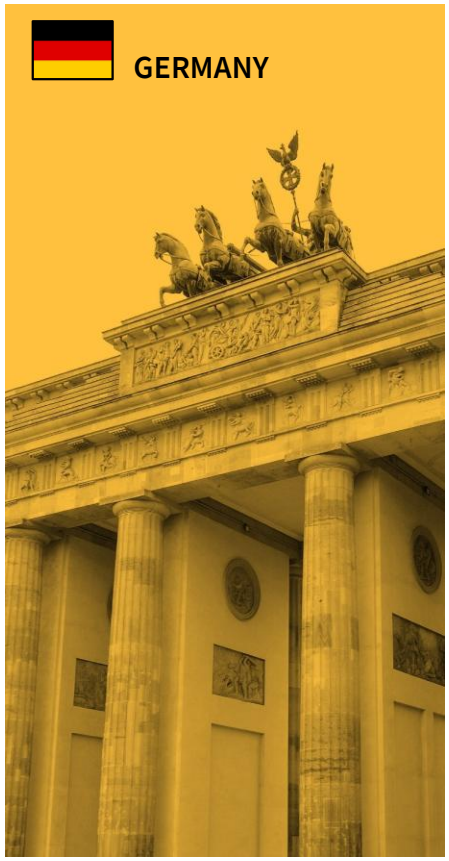
Fibre access, routing rights, and securing network easements

A data centre must have access to a reliable connection to electronic communications networks. This involves checking not only the proximity of fibre networks, interconnection points and data transport infrastructure, but also the feasibility of routing the necessary wires and other equipment to the site and then within the site. Where a site is detached from a larger property complex, or where a campus is developed in successive stages, care must be taken to ensure that deeds of sale, leases or partition agreements expressly provide for the rights of way and use for electricity networks, fibre, internal roads, water and other utilities.

Industrial classification and the property tax consequences

The French Council of State has ruled that data centres cannot be classified as storage premises within the meaning of the provisions applicable to the tax on the creation of offices, commercial premises or storage premises in the Île-de-France region. This exclusion means that, depending on the scale and predominant role of technical installations, the data centre may be considered an industrial establishment for the purpose of assessing its property rental value. Consequently, the property structuring of a data centre project must incorporate, from the outset, an analysis of the potential implications regarding property tax, the CFE (business property tax) and, more generally, rental value.

Country Chapters



Germany is the EU's largest data centre market with approximately 3 GW of installed capacity distributed across around 100 large-scale facilities (each greater than 5 MW), 2,000 mid-sized data centres (100 kW to 5 MW), and 50,000 smaller IT installations (less than 100 kW). Surging demand for high-performance computing, AI infrastructure, and sovereign data storage is consolidating that position. Germany's ambition, as set out in the *Rechenzentrumsstrategie* ('the Data Centre Strategy') published on 18 March 2026, is to become the EU's prime hub for sustainable, resilient, and sovereign data centre infrastructure.

The German Government plans to double Germany's general computing capacity, and quadruple the AI computing capacity, by 2030, to which end the Federal Government intends to implement short-term measures designed to improve the framework for inward investments in data centre projects.

GRID CONNECTION

Operators and applicable voltages

The German electricity grid comprises various voltage levels, from low voltage (up to 1 kV) through medium and high voltage (up to 110 kV) and extra-high voltage (at least 220 kV). Over 800 distribution system operators ("**DSOs**") operate the low-, medium-, and high-voltage networks. Four main transmission system operators ("**TSOs**") operate the extra-high-voltage transmission system. The federal regulator is the Federal Network Agency (*Bundesnetzagentur*).

Data centres usually own the assets necessary for their grid connection. For larger data centres, these assets typically include the data centre's switchgear bay and the connection line to the cable end seals in the grid operator's switchgear bay. The operator of a hosting data centre (in which the operator also operates the servers) qualifies as a mere consumer of electricity. By contrast, the operator of a co-location data centre can qualify as an electricity supplier, subject to certain regulatory requirements.

From "first come, first served" to "maturity" test

German grid operators face an increasing number of grid connection requests, in particular from battery storage and data centre projects. In many regions, the demand exceeds the available capacity for the foreseeable future, resulting in a significant backlog for data centre projects. Grid operators are required by law to provide non-discriminatory grid connection unless doing so is technically or commercially impossible or unreasonable. Most DSOs in Germany currently process grid connection requests in the order of their submission (under a "first come, first served" principle). To address the backlog, the German TSOs changed their grid connection procedure in 2026 to a maturity-based procedure (so-called *Reifegradverfahren*). Under this procedure, the TSOs assess applications based on a set of verifiable criteria and their likelihood of realisation. Applicants earn points based on the maturity of their project and the documents submitted and the TSOs process all applications collectively in fixed cycles, lasting approximately ten months.

To connect to and use the grid, data centre operators must normally conclude the following agreements with the relevant grid operator: a grid connection construction agreement, a grid connection agreement, a grid connection usage agreement, a grid usage agreement, and a grid management agreement. To decrease waiting times for a grid connection, data centre operators may use flexible grid connection agreements and cable pooling. Flexible grid connection agreements allow for take-off and feed-in restrictions, while cable pooling allows generation and consumption assets to share a single connection point.

Grid connection applicants bear the costs for the construction of the grid connection assets in their ownership. In addition, grid operators are entitled to charge a construction cost contribution (*Baukostenzuschuss*). This is a one-time payment made by the connecting customer for the construction or expansion of the grid. Grid operators calculate the construction cost contribution by multiplying the individual connection capacity (in kW) by the average capacity price (in € per kW) that grid users in the grid operator's area have paid over the preceding five calendar years for the relevant voltage level. Additionally, TSOs reduce the construction cost contribution by up to 80% to account for regional differences in grid management costs.

Network tariffs and the 2029 Reforms: from rewarding steady load to pricing flexibility

Grid operators charge network tariffs and other levies for the offtake of electricity from the grid. Under the current regulatory regime, large electricity consumers, such as data centres, may benefit from reduced network tariffs if they have a steady and high electricity consumption profile. The Federal Network Agency is currently revising the regulatory framework for network tariff calculation and allocation, which is set to apply from 2029. As part of this regulatory revision, the Federal Network Agency aims to incentivise flexible electricity consumption instead of a steady and high consumption.

POWER ACCESS AND PROCUREMENT

Corporate PPA structures in one of Europe's largest markets

In Germany, data centre operators can choose from a wide range of electricity procurement models. Traditional options include full-service supply contracts, typically with fixed prices, tranche-based portfolio models under which suppliers manage price risks, and direct market access where operators trade electricity themselves. To meet renewable energy sourcing requirements, several renewable sourcing models are used. These include standard supply contracts combined with guarantees of origin, off-site (physical) PPAs, and on-site generation arrangements. Increasingly, operators are adopting hybrid strategies that combine traditional supply with corporate PPAs.

Germany has one of the most developed PPA markets in Europe. It draws on a diverse pipeline of underlying assets: projects from new renewable assets, plants that have voluntarily exited subsidy schemes, and older installations which are no longer eligible to receive subsidies. Physical PPAs, where electricity is delivered from a renewable plant to the balancing group of the data centre or its services provider, are the most common structure. On-site PPAs and self-generation offer greater control and can reduce grid costs, but are constrained by space and scalability. Virtual PPAs are also structurally possible in Germany, but remain less widely used.

Corporate PPAs with nuclear generators are not commercially available for data centre operators in Germany. Following completion of the shutdown of the last three nuclear plants in April 2023, Germany took its remaining nuclear power plants offline.

Evidencing renewable supply without an additionality requirement

The relevant renewable energy certificate system is based on GOs. These certificates evidence the renewable origin of electricity. Germany participates in the European certificate system, with mutual recognition across most EU Member States (refer to Section 4: EU-wide regulatory overview). Certificates can be freely imported and exported, producing a liquid and interconnected market.

GOs can be issued for both new and existing renewable assets, including plants that have exited subsidy regimes. Data centre operators are moving towards "high-quality" certificates linked to new-build renewable projects, typically procured through PPAs. This trend is reinforced by regulatory and policy developments, on the one hand, and corporate commitments such as those under RE100 and Science Based Targets, on the other hand. For example, the draft industrial electricity price support scheme requires that only PPAs financing new or modernised renewable assets qualify as eligible decarbonisation measures.

Nuclear power does not qualify for GOs and cannot be used to meet renewable energy requirements under the German Energy Efficiency Act. As a result, cross-border PPAs linked to nuclear power plants do not provide a recognised "green" attribute in Germany.

NATIONAL STRATEGY, INVESTMENT INCENTIVES, AND PLANNING

Ambition to double compute and quadruple AI capacity by 2030

On 18 March 2026, the German government published its Data Centre Strategy. The Strategy's stated aim is to recalibrate the German policy and regulatory environment so that investments in data centre infrastructure can keep pace with the demand generated by accelerating digitalisation and AI deployment across the economy. As noted above, the German Government is aiming to double Germany's general computing capacity, and quadruple its AI computing capacity, by 2030. The government has identified three key areas of action, in which it plans to take 28 measures in the following 12 months:

i. energy and sustainability,

ii. location and land, and

iii. technology and sovereignty.

The Strategy proposes a range of measures, such as:

- changing grid access rules to improve capacity allocation and transparency;
- easing regulatory requirements governing energy efficiency and usage of waste heat;
- the acceleration and harmonisation of planning and permitting procedures, including by developing a concept for preferential site designations; and
- the introduction of special provisions for the allocation of the trade tax base (*Zerlegung*) where data centre operators maintain permanent establishments in multiple municipalities.

It should be noted that the Strategy is non-binding on both the German Government and the legislator, and further legislative steps are necessary to implement the proposed measures. It does not provide for any direct subsidy programmes for data centre projects, although data centre operators may be eligible for support under existing subsidy programmes for climate protection, heat utilisation, or energy efficiency measures.

How legal form and site selection drives the effective tax rate

German tax law does not provide for sector-specific tax incentives applicable to data centres. However, data centre operators can benefit from tax incentives available for renewable energy installations and battery storage, where they install and operate self-generated renewable energy facilities to power the data centre.

The applicable tax regime depends on the legal form of the operator. Corporations are subject to corporate income tax (currently 15%, but scheduled to be gradually reduced to 10% by 2032) plus a solidarity surcharge of 5.5% on the corporate income tax (giving a combined rate of 15.825%) and trade tax (minimum effective rate of 7%, averaging around 15% depending on the applicable municipality). Partnerships are subject to trade tax at the partnership level, while personal or corporate income tax is levied at the level of the individual partners depending on their respective legal form. There are no sector-specific tax rates or special economic zones in Germany, but the trade tax burden can vary significantly depending on the municipality in which permanent establishments are maintained.

Dual NIS2 and CER Directive implementation

Data centres in Germany are subject to the critical infrastructure regulatory regime. The German legislator has implemented the NIS2 Directive and the Critical Entities Resilience Directive through the German Act on the Federal Office for Information Security and on the Information Security of Facilities (*Gesetz über das Bundesamt für Sicherheit in der Informationstechnik und über die Sicherheit in der Informationstechnik von Einrichtungen*) and the Umbrella Act for Critical Infrastructure Protection (*Dachgesetz zur Stärkung der physischen Resilienz kritischer Anlagen*) (refer to Section 4: EU-wide regulatory overview). In Germany, data centres with at least ten racks and an IT-capacity of 3.5 MW classify as critical facilities. Server farms with at least 10,000 physical or 15,000 virtual server instances are also classified as critical facilities. The Federal Office for Information Security (*Bundesamt für Sicherheit in der Informationstechnik*) is the competent regulatory authority.

Operators of critical facilities are required to take appropriate, proportionate, and effective organisational and technical measures to prevent incidents affecting the information technology systems, components, or processes used by the operators for their facility. The measures must be based on an "all-hazards" approach, covering both IT-related and physical risks. Additional registration, reporting, and disclosure obligations apply. Non-compliance may result in penalties. A penalty can reach up to €10,000,000 and, where the operator's annual revenue exceeds €500,000,000, up to 2% of that annual revenue.

Foreign investment screening: the 10% threshold and how to clear a German data centre deal

Data centre acquisitions or investments may trigger a filing obligation under Germany's foreign investment screening rules. The Federal Ministry for Economic Affairs and Energy (*Bundesministerium für Wirtschaft und Energie, "BMWE"*) may review certain acquisitions of voting rights in a German company by a non-EU acquirer. Where the target company operates critical facilities or provides certain cloud computing services, notification is mandatory.

The non-EU acquirer must file the acquisition with the BMWE without undue delay after signing. Data centres with at least ten server racks and an IT-capacity of 3.5 MW, and server farms with at least 10,000 physical or 15,000 virtual server instances, qualify as critical facilities for these purposes. Acquisitions of target companies that provide cloud computing services are subject to a notification requirement where the facilities used for that purpose (e.g., data centres or server farms) reach or exceed the same thresholds on the basis of their use for the respective cloud computing service.

The filing obligation applies where an investor directly or indirectly acquires at least 10% of the voting rights in the target company through a share deal. The authorities also count certain control rights – such as board seats or veto rights over strategic decisions – toward this threshold, where applicable. German FDI law does not permit investors to offset diluted voting rights when calculating an indirect acquisition. Even a minority stake at an intermediate holding level can therefore push the acquirer above the 10% threshold. Asset deals can also trigger a filing obligation. An investor who acquires a data centre's key operational assets – rather than shares in the owning company – may also need to file with the BMWE. Greenfield investments are generally not caught by the German investment screening regime.

The transaction is subject to regulatory clearance by the BMWE. If the acquisition requires an FDI filing, the share transfer remains legally ineffective (*schwebend unwirksam*) until the BMWE clears the acquisition or clearance is deemed granted. Until clearance, the acquirer must not exercise any voting rights attached to the acquired shares (so-called "gun-jumping"). Violations may be sanctioned. The BMWE may also grant clearance subject to remedies, or, in the last resort, prohibit the transaction.

Data localisation in practice: GDPR transfers and German health and tax data constraints

German law does not impose a general data localisation requirement and does not prohibit non-European cloud services. Certain risk-based legal obligations may nonetheless operate as de facto localisation constraints. The GDPR permits transfers of personal data to countries outside the EU or EEA (so-called "third countries") where they ensure an adequate level of data protection, as demonstrated by an adequacy decision of the European Commission, or where appropriate safeguards are in place between the parties to the transfer, such as standard contractual clauses.

German sector-specific rules can also create de facto data localisation obligations. These include, among other things:

- the cloud processing of personal health and social services data, which is only permitted in EU Member States, EEA countries, Switzerland, or countries with an EU adequacy decision; and
- the storage of accounting records relevant for tax purposes, which may only be stored in third countries under certain conditions and requires prior approval from the competent tax authorities.

Consents that set the German build timetable

German zoning law follows a three-tier system (state, regional, and municipal levels), with no provisions governing the permissibility of data centres. Permissibility is determined on a case-by-case basis, by reference to the zoning permissibility and the permits required.

Where a zoning plan applies, the permissibility of a data centre development depends on the designated specific land use areas under the Federal Land Use Ordinance (*Baunutzungsverordnung*). Data centres are commercial areas and industrial areas, depending on a case-by-case determination, with the decisive criterion typically being the level of noise and air emissions caused by the specific data centre. A key indicator for the classification of a project as materially disturbing (and therefore permissible only in industrial areas) is whether the installation requires a permit under the Federal Emission Control Act (*Bundes-Immissionsschutzgesetz*). To avoid such complex delineation, which may also be subject to legal challenges, municipalities and developers often opt for so-called special areas that can be tailored specifically to allow for data centres.

Where no zoning plan exists, fall-back provisions apply. Within a contiguous built-up area (*im Zusammenhang bebauter Ortsteil*), a project must fit with the character of its immediate surroundings, which is rarely the case for large-scale data centres. In outer areas (*Außenbereich*), data centres currently do not qualify as privileged projects, making permissibility particularly difficult to establish for large-scale projects. There is no settled case law addressing the zoning classification of data centres with large emergency power generators, a point of legal uncertainty that the Data Centre Strategy proposes to address through clarifying legislation.

A data centre does not, in itself, require an emission control permit. However, fuel- or gas-powered emergency power generators with a rated thermal input exceeding 50 MW do, in line with the IED's implementation into German law. This permit has a concentration effect (*Konzentrationswirkung*), replacing most other permits for the emergency power generator (but not the data centre as such). The permit review process, which involves a public participation, typically takes around seven months, provided the submitted permit application documents are complete and accurate. The permitting authority may accelerate the process by approving early commencement of construction works while the review is still pending.

In addition, the data centre itself generally requires a building permit, governed by state law, with a process duration of approximately up to six months. Further permits may be required depending on the project design, including for transformer substations or cooling water supply. The competent authority is determined by state law. Germany has no unified consenting framework or fast-track permitting pathways for data centres, resulting in heterogeneous requirements and, in some cases, protracted proceedings.

In practice, close alignment with the involved municipalities (zoning) and state authorities (permitting) has proven key to expedited approval and implementation.

ENVIRONMENTAL REGULATION AND SUSTAINABILITY

An indirect Environmental Assessment trigger through large generators

Certain projects require an EIA prior to approval under the Environmental Impact Assessment Act (*Gesetz über die Umweltverträglichkeitsprüfung*), which forms part of the relevant permit procedure, and requires the applicant to report on the project's significant environmental effects. Data centres are not directly subject to an EIA, but an EIA requirement may arise indirectly from auxiliary installations, such as emergency power generators qualifying as combustion engine installations. Emergency power generators with a rated thermal input exceeding 200 MW are subject to a mandatory EIA; a pending draft bill proposes raising this threshold to 300 MW. Below these thresholds, a case-by-case screening may be required. There are no proposals to extend mandatory EIA requirements to data centres.

At the EU-level, the European Commission has published a proposal for a regulation to accelerate EIAs (refer to Section 4: EU-wide regulatory overview), to which the German Federal Council (*Bundesrat*) has lodged objections in several respects. More broadly, a recent draft amendment to the Federal Building Code proposes simplifying environmental assessment requirements for zoning plans generally.

A separate habitat compatibility assessment may be required where the site affects a Natura 2000 area under the Habitats Directive or nature conservation areas protected under state law, adding further complexity and timeline risk to the consenting pathway. In addition, environmental offsetting requirements may apply on a case-by-case basis, particularly under the Federal Nature Conservation Act (*Bundesnaturschutzgesetz*). To date, no successful judicial or administrative challenges to data centre planning decisions on environmental grounds have been identified.

Hard targets for energy efficiency and reuse

Data centres in Germany must comply with a tightening energy efficiency regulation regime. The German legislator implemented the EED through the Energy Efficiency Act (*Energieeffizienzgesetz*) (refer to Section 4: EU-wide regulatory overview), which sets quantified targets going well beyond the EED's minimum harmonisation requirements. Under the Energy Efficiency Act, operators of data centres commissioned after 30 June 2026 must achieve a power usage effectiveness ("PUE") factor of 1.2 or lower.

Data centres must also comply with an energy reuse factor ("ERF"), targeting the proportion of waste heat that is recovered for use. The applicable ERF depends on the commissioning date and ranges from 10% to 20%, with 20% applying to data centres commissioned on or after 1 July 2028. The Energy Efficiency Act allows for exceptions to the ERF, including where the data centre operator has a written agreement with a nearby municipality or heating grid operator for waste heat utilisation. The data centre operator can be subject to administrative fines of up to €100,000 for at-fault non-compliance with the PUE or ERF requirements.

Furthermore, data centres must use 100% electricity from renewable sources, with effect from 1 January 2027. Virtual supply is sufficient to meet this requirement (meaning that physical supply from a renewable source is not required, and the requirement can be satisfied through contractual or certificate-based mechanisms). No administrative fine is currently provided for non-compliance, which leaves the obligation enforceable, in practice, principally through reputational and contractual channels.

CSRD transposition pending

The German legislator has not yet implemented the CSRD into national law (refer to Section 4: EU-wide regulatory overview). A first draft of the CSRD Transposition Act (*CSRD-Umsetzungsgesetz*), first adopted by the Federal Government on 3 September 2025 is still being debated in parliament. Pending implementation, national non-financial reporting obligations transposing the Non-Financial Reporting Directive (Directive 2014/95/EU), which the CSRD supersedes, continue to apply. In addition, the Energy Efficiency Act (refer to section 6.4.2) requires data centre operators to publish information on the data centre annually, disclose energy consumption to customers, and publish energy-saving implementation plans.

As far as can be seen, no greenwashing lawsuits have to date been brought against German data centre operators or their energy suppliers. The risk is, however, growing. The German Act against Unfair Competition (*Gesetz gegen den unlauteren Wettbewerb*) prohibits misleading environmental claims. Organisations such as *Deutsche Umwelthilfe* have pursued greenwashing cases against energy suppliers, setting precedents that could extend to data centres. In addition, the German legislator transposed the Empowering Consumers Directive (cf. Section 4: EU-wide regulatory overview) into national law in February 2026, with effect on 27 September 2026.

REAL ESTATE

Site control and structuring

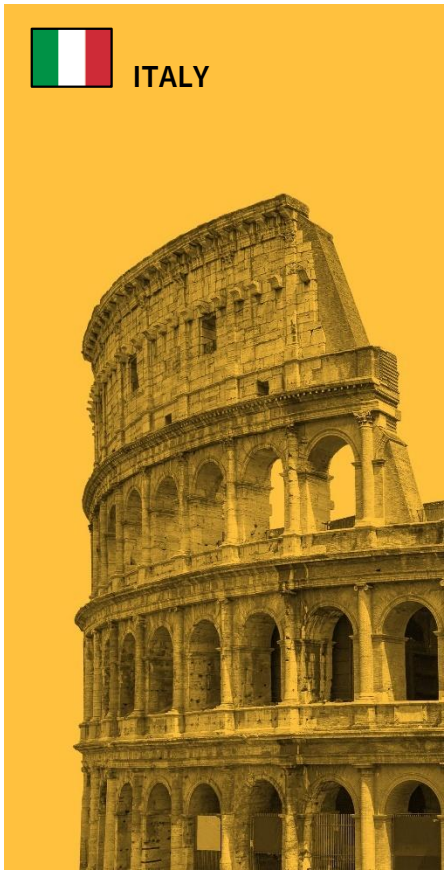
Under German law, the real estate set-up for a data centre is a key value driver and demands careful structuring from the outset. Investors focus on legal certainty, long-term site control, and full bankability. Due diligence centres on title, encumbrances, third-party rights, contamination, and ground conditions, as statutory liability for contamination can attach to the owner regardless of fault. These aspects are typically addressed through a combination of tailored representations and warranties, specific indemnities, purchase price mechanisms, and, where appropriate, warranty and indemnity insurance.

Site control structuring is one of the most consequential decisions in any data centre project. Freehold acquisition, heritable building rights (*Erbbaurecht*) and commercial leases each determine the level of control, capital efficiency, and financing flexibility available throughout the asset's lifecycle. Each structure carries its own risk profile and lender requirements, including step-in rights, assignability, and protection against termination, that must be carefully calibrated to the project. Where operators sub-let capacity to customers, an additional layer of structuring is required. German tenancy law provides strong statutory protections for tenants that can restrict operational flexibility if not properly anticipated and addressed at the outset.

Registered easements for power and fibre

Securing reliable grid connection and fibre connectivity requires enforceable rights to install and operate infrastructure across third-party land. From a real estate perspective, the key question is whether these rights are registered in rem in the land register, and are therefore binding on future owners, or whether they are merely contractual and thus significantly less protective. Where connections cross multiple properties, coordination and timing add further complexity. Early route planning, robust documentation, and a clear strategy for securing registered easements are therefore essential to ensure long-term operational continuity.

Country Chapters



Italy's data centre market sits at an earlier stage of development than Europe's established hubs, but it is moving quickly. Connection demand on the transmission grid reached approximately 66 GW by the end of 2025, concentrated overwhelmingly in the north, and the legislative response has gathered conspicuous pace: a national investment-attraction strategy published in November 2025, a unified fast-track authorisation procedure for data centres enacted in 2026, a dedicated regional law in Lombardy, and siting guidance in Apulia designed to draw development southward. Italy does not yet have a national law governing data centres as a distinct category of infrastructure but only stand-alone provisions referring to, among others, the authorisation procedure. What exists instead is an accumulated body of targeted interventions whose common purpose is to close the gap with Europe's leading markets.

GRID CONNECTION

Grid architecture and market structure

Italy operates a strict unbundling model. Transmission at high and extra-high voltage is the exclusive responsibility of Terna S.p.A., the Transmission System Operator ("**TSO**"), which manages the national grid, dispatching, and system balance independently of generation and supply interests. Distribution at medium and low voltage is carried out principally by E-Distribuzione S.p.A., alongside a number of smaller distribution system operators ("**DSOs**") responsible for local grid operation, maintenance, the connection of new users, and meter management. The sector is regulated by the Italian Regulatory Authority for Energy, Networks and Environment ("**ARERA**"), the independent national regulator.

As a consequence of the unbundling framework, data centre sponsors may not own or operate public network infrastructure. Grid connection works (*impianto di rete per la connessione*) built by a sponsor to connect a data centre to the grid are, as a rule, transferred to and operated by the relevant network operator.

Connection, queue reform, and the geography of capacity

The connection process is the point at which Italy's institutional ambition meets its physical constraint. Connection to the grid is governed by the Terna Grid Code, which applies, among others, to consumption unit (*unità di consumo*) with a power capacity of 10 MVA or more. Smaller data centres connect under the technical rules of the relevant DSO.

The standard Terna connection procedure comprises the following stages: (i) submission of a connection request; (ii) issuance by the TSO of a general technical solution (including a connection estimate), which is later replaced by the detailed technical solution; (iii) acceptance of the connection estimate; (iv) execution of a connection agreement covering dedicated works, milestones, and security; and (v) completion of the works, commissioning, and activation of the connection. Overall connection timelines vary considerably, depending on the voltage level, the scale of the connection works (including whether network reinforcement works are needed), the project's location, and the planning and authorisations procedures applicable to the relevant infrastructure.

Whilst cost allocation depends on the specific rules of the grid operator, as a general rule, data centre sponsors bear the costs – as envisaged under the connection agreement – for: (i) submitting the connection request and the technical solution and the review of these documents by the grid operator; (ii) the grid connection works; (iii) the testing and acceptance by the grid operator of the grid connection works.

As of late 2025, there is approximately 66 GW of demand from data centres for connection to the Terna grid, although this figure does not include demand from small scale data centres whose connection procedures are handled by DSOs. Data centre projects are heavily concentrated in the north of Italy, with only 20% of demand coming from the south of Italy and approximately 20 GW in the metropolitan area of Milan alone.

There are no fast-track or priority mechanisms currently envisaged under the Terna Grid Code for particular categories of data centre. The government is, however, currently actively encouraging the installation of data centres and has sought to simplify the authorisation process. Recent legislative reforms have introduced a single authorisation procedure for certain categories of data centres and relevant user connection works (*opere di connessione di utenza*) regardless of their voltage, helping to coordinate planning, environmental, and sectoral clearances under one unified procedure.

As noted, availability of capacity remains uneven across the country: demand (and, as a result, connection backlogs) is heavily concentrated in northern regions with strong industrial grids and fibre backbones, notably Lombardy. Whilst there are currently no national legislative measures designed to rebalance the geographic allocation of data centres, it is possible that the Italian government will seek to address this imbalance legislatively in the coming years.

Meanwhile, the "Strategy for Attracting Foreign Investment in Data Centres" - published on the website of the Ministry of Enterprise and Made in Italy in November 2025 – has promoted the development of data centres in Southern Italy. Regional governments have taken note of that policy signal: the Apulia Region has adopted high-level siting guidance to attract data centre investments, leveraging (among other factors) its logistics capacity, its central Mediterranean location, good connectivity to data networks (including several major submarine cables), low seismicity, and high renewable energy production that can help lower net electricity consumption and emissions.

Flexibility, charging and electricity supply

Large electricity consumers such as data centres are not mandatorily subject to flexibility requirements. Large consumers may, however, voluntarily participate in Terna's auctions concerning the interruptibility (now instantaneous peak demand response service – *servizio di modulazione straordinaria istantanea in aumento*) and demand response services, with remuneration defined under ARERA-approved mechanisms.

Usage tariffs for large electricity consumers such as data centres are set periodically by the ARERA through a system that protects the interests of users and consumers and aims to ensure the promotion of competition, the efficiency of public utility services and adequate levels of quality in those services. Connection charges are envisaged for (i) transmission and dispatching services; (ii) distribution service; (iii) metering service; and (iv) the general costs associated with the electricity system (such as research costs, incentives for the use of renewable energy sources, social tariffs for customers in financial difficulty, concessions for high-energy-consumption customers, the decommissioning of nuclear power stations, etc.). or additional network costs (such as equalisation mechanisms and measures to improve service quality).

Data from late 2025 shows that smart meters account for almost all of the total number of meters (approximately 97%). Furthermore, the replacement of first-generation smart meters with second-generation smart meters is under way.

POWER ACCESS AND PROCUREMENT

Power procurement and corporate PPA structures

In Italy, data centres may procure electricity through a range of contractual structures, including traditional retail supply agreements, physical or sleeved PPAs, virtual PPAs and, subject to the applicable regulatory framework, self-consumption and onsite generation arrangements. Private wire and direct supply structures are also allowed and are most commonly implemented through regulated self-consumption configurations, including systems qualifying as SSPCs (*Sistemi Semplici di Produzione e Consumo)* where the generation plant and the consumption unit are directly connected and the transfer of electricity is treated as self-supply rather than transmission or distribution activity.

Data centre operators may also develop onsite renewable generation, battery storage, and backup generation facilities, subject to the relevant permitting, environmental, grid connection, and fire-safety requirements. This is increasingly relevant given the rapid growth of data centre electricity demand, grid-connection constraints, and the need to secure stable, competitive, and low-carbon supply. Hybrid and multi-technology arrangements combining offsite PPAs, onsite renewable generation, BESS, and other flexibility solutions are therefore becoming particularly attractive for hyperscale and energy-intensive data centre projects.

Where electricity is supplied through the public grid, ordinary transmission, distribution, dispatching, and general system, charges apply. By contrast, self-consumption and private wire arrangements may benefit from a different tariff treatment, provided that the relevant configuration qualifies under the applicable regulatory framework. In practice, the principal benefit of these arrangements is the ability to reduce overall energy supply costs by decreasing reliance on electricity purchased from the grid and, depending on the applicable regulatory regime, reducing the amount of network tariffs, system charges, and other regulated costs associated with electricity withdrawn from the public grid. In addition, under the Italian Excise Code, electricity produced from renewable energy plants with a capacity exceeding 20 kW and consumed by self-producing undertakings in non-residential premises located on the same production site may benefit from an exemption from electricity excise duties, provided that the producer and the final customer coincide and the electricity is used for non-domestic purposes.

Renewable electricity is increasingly the preferred source of supply for large energy consumers, including data centre operators, as a result of decarbonisation targets, ESG commitments and long-term price stability considerations. The Italian corporate renewable PPA market has grown significantly in recent years, particularly for solar PV projects, and Italy is now regarded as one of the more active PPA markets in Southern Europe. More precisely, in the Italian market, the most common PPA structures adopted by data centre operators are long-term off-site corporate renewable PPAs, predominantly based on solar PV assets and typically implemented through physical or sleeved arrangements. Virtual PPAs are also used, although less frequently than in other jurisdictions. As data centre loads typically require a near-baseload supply profile, operators are increasingly exploring hybrid procurement strategies combining renewable PPAs, onsite generation, battery storage and other flexibility solutions capable of better matching round-the-clock electricity demand. Although liquidity remains generally lower than in more mature European jurisdictions, the number and size of transactions continue to increase, and corporate PPAs are becoming an increasingly common route to market for renewable energy developers and large industrial and digital infrastructure consumers.

Renewable energy certificates

Italy operates within the European guarantees of origin ("**GO**") system, administered by the Gestore Servizi Energetici ("**GSE**") and the Association of Issuing Bodies ("**AIB**"). Unlike several other jurisdictions, Italy does not recognise RECs, REGOs, or I-RECs. GOs are interchangeable across the European system.

GOs are decoupled from the physical sale of electricity and may be purchased separately on the market, which is managed, on a national level, by the Gestore dei Mercati Energetici S.p.A. ("**GME**"). GOs are tradable even on the international exchange platform managed by the AIB and accessible through the Certify Platform. One fundamental exception applies to generation assets that have received public support including the withdrawal of energy by the GSE: in those cases, GOs are issued and simultaneously transferred free of charge to the GSE which made available GOs through public auctions (Aste GO), rather than passing to the producer or being available for bilateral purchase.

For the purposes of issuing and granting GOs, producers must apply to, and obtain IGO qualification from, the GSE subject to an assessment carried out by this latter authority. If IGO qualification is requested jointly with the application to receive public support, the GSE communicates the outcome of the assessment within the term of conclusion of the assessment procedure for the public support application.

The IGO status is valid for five years, unless significant modifications are made to the production plant, in which case the status must be updated before the expiry of that period.

Each GO certifies 1 MWh from a qualifying renewable source is tradable for 12 months and can still be cancelled for a total of up to 18 months (no later than 31 March of year n+2). After that date, any GO still held by GO operators will be deemed "expired" and can no longer be used. No GO may be issued more than 12 months after the production period.

Nuclear power procurement

A bill delegating authority to the Italian Government to establish a regulatory framework for "sustainable nuclear energy" is currently under parliamentary consideration. The bill – A.C. 2669, presented by the Government on 17 October 2025 – is intended to enable the adoption of legislative decrees governing, among other things, the development of a national nuclear programme and related aspects. According to the Chamber of Deputies (*Camera dei Deputati*) materials, the bill was approved by the Chamber of Deputies (*Camera dei Deputati*) on 4 June 2026 and must still be examined and approved by the Senate before becoming law.

Whilst the bill does not expressly refer to data centres, the development of nuclear generation in Italy could have indirect implications for data centres, particularly in relation to the availability of stable, low-carbon electricity supply for energy-intensive infrastructure.

That said, nuclear energy remains a highly sensitive political and legal issue in Italy, particularly because Italian voters previously rejected nuclear power in dedicated referenda. Therefore, even if the bill is ultimately approved – reportedly within the Government's target of the end of the legislature (i.e. by the end of 2027) – the matter may be subject to a further referendum.

NATIONAL STRATEGY, INVESTMENT INCENTIVES AND PLANNING

National strategy, investment policy, tax and subsidies framework

Italy's policy framework is in active development. In November 2025, the "**Strategy for Attracting Foreign Investment in Data Centres**" was published on the website of the Ministry of Enterprise and Made in Italy. The strategy aims to strengthen Italy's role as a European and Mediterranean digital hub, promoting the widespread development of data storage and cloud infrastructure to serve businesses, public administration and citizens. Italy's strategy on AI and data centres was further delineated by the Minister of Enterprise and Made in Italy in the context of the G7 ministerial meeting on Digital and Technology held in France.

To date, the Italian government has concentrated on providing a clear permitting and localisation framework rather than on a grant and incentive mechanism. In any case, there is growing national awareness that data centres are not only critical infrastructure for the digital transition but could also evolve into new hubs for energy system flexibility (e.g. onsite storage and grid support services). This momentum is visible both at a national level and regionally: recent regional measures such as Lombardy's new law on data centres and the Apulia guidelines evidence an increasingly coherent policy push across Italy.

Critical infrastructure designation and cybersecurity

Data centre service providers fall within the digital infrastructure sector under the NIS2 framework, as implemented in Italy by Legislative Decree No. 138/2024. Depending on their size, activities and relevance under the applicable criteria, operators may qualify as essential or important entities and thereby become subject to cybersecurity risk-management and incident-notification obligations. The Italian framework is supervised by the Agenzia per la Cybersicurezza Nazionale ("**ACN**") - which acts as the national NIS authority and single point of contact - and CSIRT Italy. In addition, where the relevant networks, information systems or IT services support essential State functions or essential services for civil, social or economic activities, and their disruption or misuse could prejudice national security, the operator may fall within the Italian National Cybersecurity Perimeter. Sponsors and operators should therefore assess, at an early stage, both their NIS2 classification and any potential inclusion within the National Cybersecurity Perimeter, and should build ACN-facing cybersecurity governance, incident reporting and compliance procedures into the development and operational planning of the facility.

National security and foreign investment screening

Data centres may fall within Italy's foreign investment screening regime if the relevant assets or services involve the processing, storage, access to or control of strategic or sensitive data. The assessment will depend on the specific features of the infrastructure, the services provided, and the type of customers or sectors served. In particular, cloud services, cybersecurity, critical technologies, communications infrastructure, or services supporting regulated or sensitive sectors such as finance, healthcare, energy, transport, or public administration may also be relevant. Where applicable, the regime may result in notification obligations.

In case of failure to comply with the notification obligation, the Presidency of the Council of Ministers may apply an administrative fine equal to twice the value of the transaction and, in any case, not less than 1% of revenue.

Data localisation and cross-border data flows

There is no general obligation to localise private-sector data in Italy. Localisation or quasi-localisation requirements arise principally in relation to public-sector cloud migration and sensitive public data, where Italian rules and policy require public administrations to use qualified cloud services and, for the most sensitive categories of public data and services, infrastructure meeting enhanced security and resilience requirements. Outside those specific regimes, cross-border transfers of personal data are governed by the GDPR: transfers outside the European Economic Area require an adequacy decision, appropriate safeguards such as standard contractual clauses, or another valid transfer mechanism, rather than storage in Italy as such. Data centre operators handling personal data flows should ensure that their contractual framework, transfer impact assessments and supplementary measures remain aligned with GDPR requirements and the Italian Data Protection Authority's enforcement approach.

Land use classification and default consenting route

There is no national land-use or zoning classification specifically dedicated to data centres which, in any case, are generally considered compatible with the productive/industrial or tertiary land uses, depending on local plans and case-by-case assessments. All projects, including data centres, must comply with the hierarchy of national urban planning law, regional and provincial planning documents and the local urban plans which divide into general planning instruments (PRG, PUG, and PSC) and implementation planning instruments (PUA). Compliance with this hierarchy is a condition of planning permission and must be verified in the context of the issuance of the building title for data centre projects.

However, regional initiatives are emerging to provide specific instructions for the localisation of data centres. Lombardy has recently enacted regional law 11/2026 on data centres with the aim of taking a comprehensive approach that goes beyond permitting mechanics alone. This is consistent with Lombardy's longstanding position as Italy's leading region by number and capacity of data centre sites.

The law prioritises siting in areas identified by local authorities for urban and territorial regeneration, including brownfields (such as disused or inactive quarries and mines), contaminated sites (including orphan sites), degraded, unused, and underused areas, as well as areas potentially contaminated under applicable legislation. The law also requires proximity and compatibility with existing electrical infrastructure so as to minimise the territorial impact of new connection works. The Municipality has committed to identify abandoned, contaminated, degraded, unused, and underutilised areas within the municipal territory and areas affected by existing data centres, newly constructed data centres, or data centres undergoing expansion, within one year from the enactment of the regional law.

Locating data centres in these priority areas triggers incentive measures (for example, reductions in the construction contribution and priority access to regional funding streams for digital innovation and the digital transition). Conversely, to discourage greenfield development, significantly higher urbanisation charges apply to projects to be installed on agricultural areas.

Moreover, on 22 October 2025, Apulia Region enacted "*Guidelines for the localisation and realisation of data centres in the Apulia Region*" with the aim of making clearer the existing permitting framework to authorise construction and operation of data centres, as well as providing instructions for the localisation of data centres taking into account possible territorial constraints and the wide presence of "suitable" areas, meaning dismissed industrial areas, brownfield sites, contaminated sites.

National/fast-track consenting pathways

The recent Law-Decree 21/2026, as converted by Law 49/2026, ("**Decreto Bollette**") introduced a unified, simplified authorisation procedure for data centres and relevant user connection networks, of any voltage, intended to bundle planning, landscape, environmental and sectoral clearances in a sole authorisation procedure, including EIA/EIA screening and those environmental permits encompassed within the sole environmental authorisation (*autorizzazione integrata ambientale*). The sole authorisation procedure for data centres has only been recently enacted so is still untested, however, the relevant provisions of the Decreto Bollette set a maximum term of duration of ten months from the conclusion of the preliminary assessment on the completeness of the documentation, extendable for a maximum of three months depending on the complexity and the scale of the project.

Data centre projects carried out on Italian territory with a total value of €1 billion and higher could be declared of strategic national interest pursuant to Law-Decree 104/2023 (converted by Law 136/2023). In such case, the data centre project must be authorised via a single authorisation handled by an extraordinary commissionaire. The single authorisation for strategic interventions replaces any approval, consent, permit, authorisation, however named, necessary for the project, including those from an environmental, health, and fire prevention perspective.

In parallel, since 1 January 2024 Italy has established the single Special Economic Zone for the South ("**ZES Unica**") covering Abruzzo, Basilicata, Calabria, Campania, Molise, Apulia, Sicily, and Sardinia (Law Decree 124/2023, as converted by Law 162/2023). Within the ZES Unica, projects are filed through the Sportello Unico Digitale ZES, which exercises the same functions as the Sportello Unico Attività Produttive for productive activities, and are subject to a simplified "single authorisation" pathway issued following a fast track, simplified steering committee convened by the ZES Mission Structure. The single authorisation replaces all other permits and consents otherwise required (including the variation to the urban-planning instrument).

Finally, it should be noted that the Senate is currently considering a draft of a delegated law (*legge delega*) aimed at introducing an all-encompassing framework for data centres, which would cover, amongst other matters, ATECO classification, security, resilience and recovery, and energy efficiency. Whilst no concrete steps have followed yet, this initiative should be monitored by stakeholders in order to understand how it will interact and combine with the recent legislative reform.

ENVIRONMENTAL REGULATIONS AND SUSTAINABILITY

Environmental impact assessment

The EIA trigger in Italy is not the facility housing the computer equipment itself, but its ancillary infrastructure. In other words, it is the emergency generation fleet that – as a thermal power installation – engages the regime. Data centres whose emergency generators have a thermal power capacity of between 50 and 150 MW are subject to EIA screening, while those exceeding 150 MW are subject to a full EIA. Where a project incorporates renewable generation – an increasingly common configuration – the separate screening and EIA thresholds applicable to such plans must also be applied.

Two further regimes overlay the EIA position. A habitats incidence assessment (*Valutazione di incidenza ambientale*) is required if the project directly or indirectly affects Natura 2000 areas, and, where the thermal capacity of the emergency power units exceeds 50 MW, the activity falls under the IPPC framework and requires an Integrated Environmental Authorisation ("**AIA**"). Practice has consolidated quickly. In 2024, the Ministry of the Environment and Energy Security ("**MASE**") adopted Guidelines for Environmental Assessment Procedures of Data Centers, outlining the aspects of projects subject to assessment, the applicable methodologies, and the means of compliance. The guidelines – together with the practical instructions MASE provides through the environmental inquiry procedure (*interpelli ambientali*), under which operators may submit questions that MASE is required to answer – now constitute the principal practical reference for structuring the environmental workstream, and they should be consulted before the generator and cooling configuration is fixed.

Energy efficiency: PUE and mandatory standards

Italy imposes no mandatory energy efficiency performance standards on data centres: there are no binding maximum thresholds for PUE, WUE, or CUE. Nonetheless, Italy has implemented Article 12 of the recast EED in advance of full transposition, through Article 16 of Decree-Law No. 131 of 2024 (the so-called "*Decreto Salva Infrazioni*"): a measure adopted precisely to forestall infringement proceedings for missing the transposition deadline. The obligations apply to operators of data centres with an IT power demand of at least 500 kW, who must publish, by 15 May of each year, prescribed information including the facility's identity, ownership, commissioning date, and municipality; its floor area, installed power, annual inbound and outbound data traffic, and stored and processed data volumes; and its performance against key performance indicators set out in Commission Delegated Regulation (EU) 2024/1364. Facilities used exclusively for defence or civil protection are excluded, and information protected by commercial or corporate secrecy need not be disclosed. Practical experience remains limited to the establishment of the reporting framework itself.

Energy efficiency does not currently operate as a condition of grid connection or operating licenses. Efficiency is nonetheless assessed indirectly within the permitting process. The MASE guidelines require the EIA to address the project's energy performance, consumption, and resource use. The AIA includes measures controlling emissions to air, water, and soil that bear on environmental efficiency without setting a sector-specific indicator. All water discharges also require prior authorisation subject to emission limit values, so that water resource availability conditions the cooling design even in the absence of a WUE target. The prudent assumption, in Italy as elsewhere in Europe, is that disclosure will harden into prescription, and that designing to anticipated rather than current standards is cheaper than retrofitting compliance.

Heat recovery and waste heat obligations

There is currently no mandatory obligation under Italian law requiring data centres to supply or utilise waste heat, and the matter has not been comprehensively regulated at national level. However, Lombardy's regional framework already designates recovery and use of residual heat from data centres, through district heating networks and other efficient applications for the benefit of renewable energy communities and public users, as a priority.

Practical implementation has begun. On 25 June 2025, A2A inaugurated at its Lamarmora plant in Brescia the first Italian project recovering waste heat from a data centre into an urban district heating network, developed in partnership with Qarnot and using liquid-cooled technology to recover thermal energy at temperatures of up to 65°C. The heat is fed into Brescia's district heating network – among the largest in Europe, comprising more than 684 km of pipelines and serving approximately 22,000 customers – and the project is expected, once fully operational, to satisfy the heating demand of more than 1,350 apartments and to avoid approximately 3,500 tonnes of CO_2 emissions annually. The Brescia precedent matters commercially as well as technically: it demonstrates that heat offtake is bankable in the Italian market, and sponsors of northern projects proximate to district heating should assess recovery potential at the design stage, both as a hedge against future regulation, and as a source of local authority goodwill in the consenting process.

Sustainability reporting

Italy has transposed the CSRD, so that in-scope companies report under the ESRS. The Italian decree establishes no additional sector-specific obligations for data centres: the data centre-specific disclosure burden derives instead from the EED, as implemented by the *Decreto Salva Infrazioni*.

As of June 2026, no greenwashing claims or investigations appear to have been brought against data centre operators or their energy suppliers in Italy. Consistent with the position across the surveyed jurisdictions, that absence should be read as a matter of timing rather than of principle. Environmental claims – particularly unqualified renewable supply chains – should be substantiated to the standard required by the GO framework and the operator's reporting obligations.

REAL ESTATE CONSIDERATIONS

Real estate considerations are a key factor influencing the feasibility, timing, and bankability of a data centre project in Italy. Site selection cannot be treated as a stand-alone land acquisition or leasing exercise; it must be assessed together with title to the land, cadastral status, urban planning designation, existing agreements affecting possession or use, easements, rights of way, utility corridors, grid connection land requirements, and the physical ability of the site to host an energy-intensive infrastructure.

In the Italian market, the real estate analysis is focused on the legal availability and development-readiness of the land. This includes verifying, among other things, full and exclusive ownership, continuity of title, absence of mortgages, prejudicial registrations, liens, privileges, pre-emption rights, agrarian rights, and other encumbrances, as well as identifying any existing easements, urban planning agreements, leases, agricultural tenancies, or third-party rights that could affect construction, access, interconnection, or operation of the data centre.

Italy does not currently have a comprehensive national real estate regime specifically dedicated to data centres. Accordingly, the legal analysis must be carried out through the ordinary Italian real estate, planning, environmental, and grid-connection framework, with particular attention to the rules applicable in the relevant Region and municipality. In Lombardy, recent regional guidance and the new regional legislative initiative approved by the Regional Council (*Consiglio Regionale*) on 26 May 2026 reinforce the importance of brownfield, dismissed, contaminated, degraded, unused, or underused areas, and seek to provide greater certainty on the urban planning treatment of data centres. However, for investment and diligence purposes, the decisive exercise remains a site-by-site review of title, land availability, planning designation, and existing burdens on the property.

Land availability, title, planning designation and operational constraints

The first level of analysis is ownership and legal availability. Italian practice requires a full review of the acquisition deeds, notarial reports, cadastral identification, the twenty-year title chain, continuity of registrations under Article 2650 of the Italian Civil Code, and the absence or presence of mortgages, seizures, prejudicial registrations, real estate liens, tax and agrarian privileges, easements, indivisibility restrictions, pre-emption rights, and other third-party rights. The assessment should extend beyond bare ownership to whether existing servitudes, planning prescriptions, agricultural leases, telecom leases, and prior urban planning agreements could prejudice the construction, development, or operation of the facility: a discipline of particular importance in Italy, where development frequently involves assemblages of several cadastral parcels, historical industrial land, agricultural land, or land already affected by planning conventions or infrastructure rights.

The second is possession and freedom to develop. Existing agricultural leases, even where temporary, must be reviewed to confirm expiry, termination rights, waiver of renewal, or consensual early termination. Existing leases or surface rights granted for telecom or utility infrastructure must be assessed for their compatibility with the planned facility, for any restrictions on buildability or the economic exploitation of adjoining areas, and for any automatic termination or modification rights triggered where authorisations are refused, revoked, or affected by changes in law.

The third is urban planning compatibility, which requires review of the applicable municipal planning instrument – in Lombardy, the territorial government plan (*Piano di Governo del Territorio*) – its technical implementation rules, and any applicable implementation plans, subdivision plans, single desk procedures, or planning agreements. Under the Lombardy approach, data centres may be treated as compatible with productive and directional uses, so both greenfield sites with compatible zoning and existing buildings or industrial sites capable of conversion may be suitable, provided that the planning rules allow the use, and that any required implementation plan is approved.

Brownfield and former industrial sites may offer significant advantages – location within areas already designated for productive uses, reduced land-use conflict, and alignment with the policy preference for the reuse of developed land that both the Lombardy law and the Apulia guidelines now reward – but they demand enhanced diligence on contamination, remediation obligations, previous planning conventions, existing infrastructure easements, and environmental prescriptions affecting the soil and subsoil.

Electricity grid connection as a real estate issue: land, easements and infrastructure corridors

Grid connection is itself a real estate question in Italy. One feature of Italian practice deserves particular emphasis: the connection agreement is closely linked to land control, and may be signed only after the necessary authorisations have been obtained and ownership or equivalent rights have been secured over the land required for the transmission facilities.

Existing electrical easements require careful assessment. An easement in favour of the network operator is not necessarily incompatible with a data centre, but its wording, location, duration, and operational restrictions may materially affect the development layout, so legal title review should be combined with technical mapping of the easement corridor, clearance requirements, access rights, and limitations on building or excavation. New easements and rights of way should be addressed in the acquisition documents, easement deeds, development agreements, or other land instruments, and should cover installation, access, inspection, maintenance, replacement, and upgrading; for campus-style or phased developments, those rights should be drafted broadly enough to support future capacity increases and additional phases, rather than only the first energisation of the site.

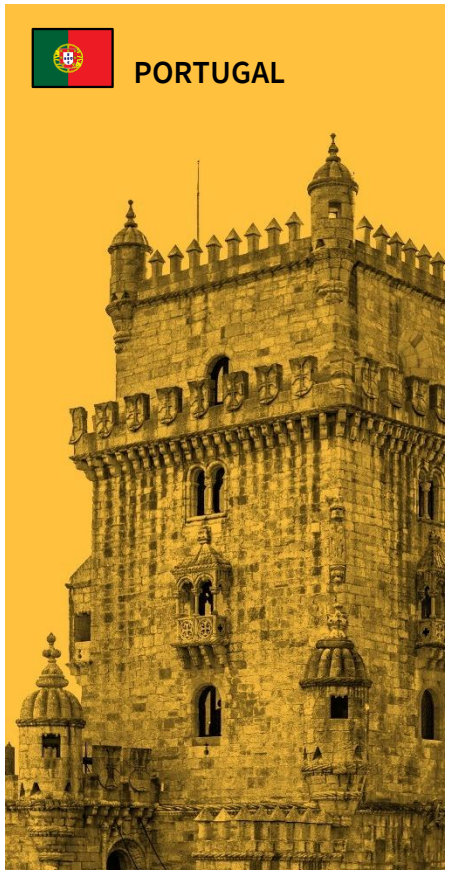
Connectivity, utilities, access and securing property rights

A data centre requires more than legal ownership of a plot. For example, it depends on robust and enforceable rights for road access, internal circulation, construction logistics, fibre routes, electricity corridors, water and drainage networks, cooling infrastructure, and fire safety systems. Those rights matter most where the site forms part of a wider industrial estate, a former development area, a multi-parcel assemblage, or a phased campus.

The deeds of sale, leases, partition deeds, planning agreements, and easement deeds should expressly regulate access, utility corridors, fibre routes, electricity lines, internal roads, maintenance and step-in rights, restrictions on interference by neighbouring owners, and the ability to carry out future upgrades. Where the data centre depends on rights over land it does not own, those rights should be registrable, durable, and binding on successors in title.

Review of the notarial reports, together with the underlying contractual and planning documents, is therefore essential, and should identify urban planning prescriptions, telecom and agricultural leases, existing servitudes, electrical easements, and any prior planning convention connected to a former productive development, each of which may affect legal availability, access, construction sequencing, infrastructure routing, or the delivery timetable. Particular attention should also be paid to agreements that prevent the tenant or occupier from creating passive easements, subletting or granting use rights to third parties. These provisions may be useful where the developer needs to clear the land before construction, but they may also reveal constraints that must be resolved before new utility rights, grid connection rights or access arrangements can be granted. The closing discipline is the one in which this chapter began: in Italy, the property workstream, the planning workstream, and the connection workstream are a single, independent sequence, and the projects that proceed fastest are those that treat them as such from the first day of site identification.

Country Chapters



Portugal has emerged as a compelling destination for data centre investment in southern Europe, combining strategic geographic positioning, abundant renewable energy resources, and a regulatory environment increasingly oriented towards the facilitation of digital infrastructure. The country serves as a natural gateway to both the Iberian Peninsula and the wider European market, whilst its Atlantic coastline provides direct access to transatlantic and African submarine cable routes, existing industrial grid connections, and available land suitable for hyperscale development.

The sector has attracted a substantive pipeline of investment proposals, driven principally by hyperscalers and AI-focused infrastructure investors seeking to capitalise on Portugal's renewable energy endowment and its position outside the capacity-constrained markets of northern Europe.

GRID CONNECTION

Securing grid access in a capacity-constrained market

One of the key constraints for data centre investors and developers in Portugal is securing grid access for large-scale consumption. The rapid growth in demand for grid connection capacity – driven in significant part by an influx of data centre investment projects – has placed considerable strain on the Portuguese public electricity supply network and has prompted a substantive regulatory response from the Portuguese Government.

In Portugal, there are two key network operators. Rede Elétrica Nacional, S.A. ("**REN**") is the holder of the transmission system public service concession and serves as the Portuguese transmission system operator ("**TSO**"). E-Redes – Energia S.A. ("**E-Redes**") is the holder of the distribution system (medium and high voltage) concession and serves as the Portuguese distribution system operator ("**DSO**"). E-Redes is also the holder of a significant majority of the low-voltage municipal distribution grids. On the regulatory side, the Energy Services Regulatory Authority (Entidade Reguladora dos Serviços Energéticos, "**ERSE**") acts as the independent regulator of the energy sector.

The Portuguese national electricity system is built upon a clear model of unbundling network activities from competitive activities. These unbundling rules mean that the ownership and operation of transmission and distribution network assets are activities exclusively reserved for the concession-holders and are not open to third parties (including data centre developers) on a standalone basis. While the developer may be responsible for the construction of connection infrastructure connecting a consumer installation to the grid, the connection infrastructure may become the property of the relevant network operator and be integrated into the public grid. This means that a data centre developer with significant connection requirements could, in principle, co-finance grid reinforcement works, although the infrastructure itself could remain under the concession-holder's ownership and control.

The connection queue: reform, priority pathways, and capacity allocation

The standard framework on grid access and connection of consumption installations is mainly set out in the ERSE Commercial Relations Regulation, which governs the conditions for the connection of electricity consumption installations to the public grid. As a general rule, the connection process works on a "first-come, first-served **"** basis and is initiated by the developer submitting a request to the relevant network operator. Developers must provide the technical information requested by the operator to perform studies to evaluate whether it can grant the requested grid connection and if any grid reinforcement works are necessary. For connections above a certain capacity and voltage, construction conditions and timelines are agreed between the developer and the relevant network operator.

The Portuguese National Data Centre Plan ("**PNCD**"), approved by the Resolution of the Council of Ministers no. 2/2026, of 8 January ("**RCM 2/2026**") and Resolution of the Council of Ministers no. 70/2026, of 13 April ("RCM 70/2026"), acknowledges that grid connection times in Portugal are typically between 2 to 5 years, a range that reflects not only the complexity of technical works but also the length of administrative and licensing procedures as well as grid works and availability.

The PNCD explicitly identifies constraints on access to the electricity grid as one of the key challenges affecting project execution in Portugal. The combination of a rapidly growing demand pipeline – driven by hyperscale and AI-related data centre projects – and the relatively long timelines for both grid reinforcement and administrative procedures has created a de facto queue for large consumption connections, particularly in areas of concentrated demand (for example the town of Sines, which is considered attractive to developers due to its port infrastructure, existing industrial grid connections, access to submarine cable landing stations and available land). Submarine cable connectivity is itself now the subject of EU-level resilience policy and dedicated funding under the Commission's February 2026 Action Plan on Cable Security, a consideration relevant both to the durability of Sines's locational advantage and to the structuring of any cable consortium participation.

The Government's response to this congestion was through the implementation of an exceptional regime developed to allocate interconnection consumption capacity in areas of high demand (excluding low voltage connection requests), as set out in Decree-Law no. 80/2023, of 6 September ("**DL 80/2023**"). The procedure is intended to be open, transparent, equitable, and competitive, and encompasses multiple potential phases: (i) manifestation of interest and posting of a performance bond, combined with identification of unused capacity; (ii)evaluation of demand and network reinforcement; (iii) making unused capacity available and, where applicable, mandatory waiver and assignment of dormant capacity; and (iv) auction procedure if necessary.

In February 2026, the Portuguese Government launched a public consultation for the manifestation of interest in the allocation of consumption-connection capacity in a high demand area composed of the entirety of the continental territory for medium and high voltage connections with a capacity above 20 MVA.

Within the DL 80/2023 mechanism, priority treatment is available to priority projects. Priority project status is available to projects with project-of-national-interest ("**PIN**") status in certain at-risk sectors (as defined under EU State aid guidance) or to projects funded under specific innovation agendas under Portugal's Recovery and Resilience Plan ("**PRR**"). While there is no explicit fast-track category reserved for data centres as such, the combination of PIN or PRR status and the priority project regime under DL 80/2023 provides the most direct pathway to preferential capacity allocation for strategically significant projects.

Grid connection capacity constraints in Portugal are not geographically uniform: they are most pronounced in areas of concentrated data centre demand. In response, extending the DL 80/2023 exceptional procedure to the entirety of the continental grid territory in 2026 represented a recognition that localised capacity for consumption constraints are becoming a nationwide challenge, rather than one confined to a single area.

Within the DL 80/2023 mechanism, the legislator seeks to satisfy the demand for connection capacity of electricity consumption installations required, through network reformulation or reinforcement, as well as redispatch measures and the introduction of flexibility measures. Measures currently being developed under the PNCD include the identification and enabling of pre-licensed zones with early-stage licensing and coordinated planning for grid connection, as well as a review and simplification of licensing procedures to ensure more efficient processing within maximum statutory decision deadlines, while maintaining applicable legal, technical, and environmental requirements.

Flexibility obligations, connection charging, and the use-it-or-lose-it discipline

Portugal does not currently impose sector-specific mandatory demand response or interruptibility obligations on large consumers such as data centres. There is, however, a form of capacity-specific "use-it-or-lose-it" discipline embedded in the exceptional connection capacity-allocation framework established by DL 80/2023, under which holders of allocated but unused grid connection capacity for consumption are notified and required either to present evidence of their need for the allocated capacity with a corresponding use timetable, or to voluntarily make the capacity available to meet demand from incoming applicants, with the warning that failure to do so may result in mandatory assignment.

Looking ahead, the PNCD's Energy and Infrastructure axis includes an initiative, which aims to integrate energy efficiency criteria and demand flexibility mechanisms in planned grid connection infrastructure, promoting more efficient network use and greater resilience of the energy system. This initiative signals that the Government intends to formalise demand-side flexibility requirements as a structural element of future data centre grid connections, though the precise legal instruments and financial incentive mechanisms remain to be defined in implementing legislation.

The connection charging framework applicable to large electricity consumers – including data centres – is set out principally in ERSE Commercial Relations Regulation. As a general principle, the costs associated with a new connection are structured around the four main components: (i) costs of connection elements (the physical infrastructures linking the installation to the grid); (ii) a standardised network contribution, calculated by multiplying the ERSE-published unit value in €/kVA by the requested power, with the applicable unit value varying by voltage level and published periodically by ERSE; (iii) connection service charges, which cover items such as site visits, design documents, budgeting, and construction supervision; and (iv) third-party costs, which reflect costs incurred by the operator in connection with works carried out by third parties necessary to implement the connection. In relation to metering, large electricity consumers connected at medium, high or very high voltage are subject to mandatory remote metering under the applicable ERSE regulatory framework and network operator's technical specifications, enabling both the network operator and suppliers to access such data for billing, settlement and network management purposes.

POWER ACCESS AND PROCUREMENT

Power procurement: a mature PPA market with strategic cost levers

Portuguese law permits data centre operators to use a range of power procurement structures. Physical PPAs – long-term bilateral agreements under which a producer supplies electricity from a specified renewable generation asset to a consumer, with delivery effected through the public grid – are a well-established instrument in the Portuguese market. Virtual, or synthetic, PPAs are similarly available: under such structures, the data centre operator continues to procure electricity at market prices through a power supplier, whilst the PPA counterparty provides a financial settlement mechanism (typically structured as a CfD) by which the parties exchange the difference between an agreed strike price and the relevant market reference price. Virtual PPAs do not constitute regulated electricity supply contracts under Portuguese law and are generally structured as private law commercial agreements, however, where the arrangement qualifies as a commodity derivative under Directive 2014/65/EU (MiFID II) as implemented in Portugal, the requirements of the applicable financial markets framework will apply accordingly. As regards direct supply arrangements, Decree-Law no. 15/2022, of 14 January ("**DL 15/2022**") provides for individual and collective self-consumption of electricity from renewable sources, under which a data centre operator may develop or commission on-site or proximate renewable generation capacity and consume the output directly, subject to applicable technical, environmental and administrative licensing requirements. Co-located backup generation, including different types of power generation and energy storage systems, is similarly permitted subject to the applicable licensing regimes.

From a cost perspective, the interaction between the chosen procurement structure and regulated network charges is a material consideration. Where electricity is consumed from the public grid – as is the case with physical and virtual PPAs – access tariffs and general economic interest charges ("**CIEG**") apply on the volume consumed. Electricity generated and self-consumed on-site without injection into or import from the public grid is, in principle, exempt from access tariffs on the self-consumed portion, which may represent a meaningful cost advantage for operators able to optimise on-site generation against load. As noted in section 6.3.1 below, operators qualifying for electro-intensive consumer status may additionally benefit from significant reductions in CIEG charges, irrespective of the procurement structure adopted. The Portuguese corporate renewable PPA market is active and benefits from the country's abundant renewable assets. Portugal has been active in terms of executed corporate PPAs, with a growing number of hyperscale and infrastructure investors having concluded long-term renewable supply agreements, particularly in connection with utility-scale solar and onshore wind projects.

Portugal currently has no operational nuclear power plants and, unlike several of its European neighbours, has not historically pursued nuclear energy as part of its electricity generation mix. Absent a fundamental shift in Portuguese energy policy, in-country nuclear power generation is not expected to be available in the short to medium term.

Guarantees of Origin: European interoperability and the approaching granularity standard

Portugal operates a guarantee of origin ("**GOs**") scheme for the certification of the electricity produced from renewable energy sources, including GOs for renewable electricity and for renewable heating and cooling, and GOs for renewable gases and low-carbon gases. Each GO represents one megawatt-hour (MWh) of energy produced from a qualifying renewable source. The Portuguese GO framework does not impose a mandatory additionality requirement as a condition of GO issuance; that is, there is no general rule restricting the issuance of GOs exclusively to newly commissioned generation facilities. GO issuance is therefore implemented irrespective of the age of the installation.

For GO issuance, the system operates by reference to a period tied to the production period recorded on the GO, with the default reference period for production declarations being one month. For cancellation – the mechanism by which a consumer claims the renewable attribute of a GO – the relevant consumption period must be continuous, cannot exceed twelve months, and cannot span different civil years, meaning that in practice GO matching in Portugal operates on an annual or sub-annual basis. The GOs framework does not currently prescribe hourly certificate matching, nor does Portugal seem to be moving towards a more granular certificate matching. However, with Renewable Energy Directive (Directive (EU) 2023/2413, "**RED III**") introducing provisions designed to encourage more granular – including hourly – matching of renewable energy consumption with production, it is reasonable to expect that Portuguese implementing legislation will progressively align with those requirements in the coming years.

Portugal's GO framework is designed to operate within the European Energy Certificate System ("**EECS**"), administered by the Association of Issuing Bodies ("**AIB**"), with cross-border interoperability facilitated through the AIB as GOs are mutually recognised across the AIB member network (encompassing most of Europe's electricity markets). International transfers of GOs – both imports into Portugal and exports from Portugal – are, where possible, carried out through the AIB in accordance with the EECS framework and AIB rules. GOs from other EU Member States are recognised unless there are well-founded doubts as to their accuracy, reliability, or veracity, and any refusal of recognition, together with the reasons therefor, must be communicated to the competent authorities. Portugal is accordingly fully aligned with the EU GOs framework established under the Renewable Energy Directive and its successors. This mutual recognition is particularly relevant for data centre operators operating across multiple European jurisdictions, as it allows GOs sourced in one EU Member State to be cancelled and claimed by a consumer in another, facilitating European renewable energy procurement strategies.

NATIONAL STRATEGY, INVESTMENT INCENTIVES, AND PLANNING

AI data centre policy architecture, tax levers, and tariff benefits

The Portuguese Government's national AI strategy is structured around two pillars.

The first is the National Agenda, approved by the RCM 2/2026, which sets forth several key measures and actions to be carried out by the Portuguese Government in the field of AI between 2026 and 2030, foresees key measures including the implementation of the PNCD, the creation of zones with simplified licensing procedures, and the establishment of a centralised investor support structure.

The second pillar is the PNCD, approved by RCM 70/2026, which outlines the Portuguese State's strategy for strengthening the country's computational capacity and digital infrastructure, spread into four strategic areas: the economic axis, the digital and technological axis, the energy and environmental axis, and the governance and administrative simplification axis.

Portugal does not have a specific tax regime for data centres, nor government-designated zones with specific incentives to be awarded upon the construction or operation of data centres. Nevertheless, Portuguese law provides a range of tax benefits relevant to data centre development. These include tax benefit regimes for productive investment, such as Decree-Law no. 162/2014, of 31 October ("**DL 162/2014**"), which allows deductions from corporate income tax liability based on eligible investment under the provisions of DL 162/2014, as well as exemptions from or reductions in municipal property tax, municipal property transfer tax, and stamp duty. Furthermore, these benefits are supplemented by contractual investment incentive regimes negotiated with the Portuguese State on a case-by-case basis, which may include tax credits and property tax benefits. Finally, subsidies and support may also be granted in the future under European-based investment programmes such as Portugal 2030 and the Portuguese Recovery and Resilience Facility.

Regarding energy tariffs benefits, obtaining the electro-intensive customer status under the provisions of DL 15/2022 allows for reductions of between 75% and 85% on general economic interest charges levied for using the electricity grid. This regime may be particularly relevant for data centre operators with high energy consumption, although it does not constitute a sector-specific incentive.

NIS2 obligations and supervisory architecture

In Portugal, data centre service providers are expressly designated as essential entities pursuant to Decree-Law no. 125/2025, of 4 December ("**DL 125/2025**") and may be designated as critical entities after a national risk assessment under the terms of Decree-Law no. 22/2025, of 19 March ("**DL 22/2025**"). These providers are subject to the supervision of the Portuguese National Cybersecurity Centre ("**CNCS**") which is the competent regulatory body with supervisory authority over the sector.

The supervisory regime applicable to data centres depends on whether their respective managing entities are classified as "essential entities" or "important entities" under DL 125/2025, which is determined by whether they have more than 250 employees, and whether their annual turnover or annual balance sheet total exceeds EUR 50 million or EUR 43 million respectively (in case of certain categories of entities, those are in scope regardless of their size). While essential entities are subject to continuous ex-ante supervision (including inspections, regular audits and information requests), important entities are subject to ex-post supervision, which is triggered in the event of evidence of non-compliance with applicable legal obligations.

Data centre service providers must adopt enhanced cybersecurity and operational resilience measures, including technical, organisational, and risk management measures aimed at preventing, responding to, and recovering from incidents. These measures also require the appointment of responsible internal officers and impose duties of cooperation and notification with regard to the relevant authorities, including the CNCS.

Foreign investment screening: narrow scope, cumulative triggers, and third-country acquirers

Portugal does not have a specific foreign investment screening regime exclusively applicable to data centre acquisitions or investments. However, pursuant to Decree-Law no. 138/2014, of 15 September ("**DL 138/2014**"), Portugal has established a foreign direct investment screening regime for acquisitions of control over strategic assets in the energy, transport, and communications sectors. For these purposes, "strategic assets" are defined as the main infrastructures and assets devoted to national defence and security, as well as to the provision of essential services in the energy, transport, and communications sectors.

Under DL 138/2014, the Portuguese Government has the power, in exceptional circumstances and through a reasoned decision, to oppose the acquisition, by persons from third countries outside the European Union ("**EU**") and the European Economic Area ("**EEA**"), of direct or indirect control over such strategic assets, where such transactions may jeopardise national defence and security or the security of supply of essential services to the national interest.

The application of DL 138/2014 to any particular transaction is, however, subject to the cumulative satisfaction of the following requirements: (i) the relevant asset must fall within one of the covered sectors: namely, energy, transport or communications; (ii) the asset must qualify as a "strategic asset" within the meaning of the regime; (iii) the asset must be operational at the time of the transaction; and (iv) the acquirer must be a person from a third country, that is to say, a country outside the EU and the EEA. Where any of these conditions is not satisfied, the provisions of DL 138/2014 will not apply.

Where all of the above conditions are met, the Portuguese Government may initiate an assessment procedure on its own motion within 30 days of the transaction's signing or from the date on which it was publicly disclosed. Furthermore, entities involved in the transaction may request confirmation from the Portuguese Government that no assessment procedure will be initiated and no decision to oppose the transaction will be adopted. In both cases, the absence of a decision by the Portuguese Government indicates non-opposition to the transaction in question. Should a decision of opposition be adopted, any legal acts and transactions relating to the operation in question shall be null and void, including those concerning the economic exploitation of or exercise of rights over the assets or the entities controlling them.

Accordingly, an investment in a data centre would be subject to a case-by-case analysis as it may be subject to DL 138/2014 – but only to the extent that the data centre in question is operational, qualifies as a strategic asset within the relevant sectors, and the acquirer of control is an investor from a third country outside the EU and the EEA.

Data localisation: a permissive general regime with sectoral exceptions

Portugal does not impose a general mandatory data localisation requirement for personal or non-personal data. As an EU Member State, Portugal is subject to the directly applicable framework established by Regulation (EU) 2016/679 (the "**GDPR**"). The Portuguese data protection framework, including Law no. 58/2019, of 8 August (which ensures the implementation of the GDPR in the Portuguese legal order), does not introduce any additional data localisation obligation beyond those arising from the GDPR itself.

Notwithstanding the absence of a general data localisation obligation, certain sector-specific rules and guidance from the relevant supervisory authorities may, in practice, constrain the location of data processing and storage. In the financial sector, prudential supervisory requirements – including those arising from the European Central Bank's supervisory framework and the European Banking Authority's guidelines on outsourcing – impose conditions on the outsourcing of critical or important functions, including requirements relating to data access, auditability, and supervisory oversight, which may effectively favour the retention of certain data within the EEA or within jurisdictions subject to equivalent regulatory standards. In the health sector, while there is no express statutory requirement mandating that health data be stored in Portugal, the processing of health data is subject to enhanced protections under the GDPR and Law no. 58/2019, and sector-specific rules governing the national health system may impose conditions on the hosting and accessibility of patient data. As regards government and classified data, the Portuguese national security classification framework – governed by the applicable SEGNAC regulations (National Security Department) – imposes restrictions on the handling, storage, and transmission of classified information, which may require that certain categories of government workloads be processed and stored within national territory or in facilities meeting specific security accreditation standards.

The practical impact of data localisation and security classification requirements on data centre siting decisions in Portugal is, at present, relatively limited for private-sector operators, given the absence of a general localisation mandate and the free movement framework applicable within the EEA. Portugal's position as an EU Member State, combined with its geographic location makes it an attractive jurisdiction for operators seeking to serve European and transatlantic markets without encountering cross-border data transfer restrictions within the EEA. However, for operators seeking to host government workloads or data subject to national security classification, the applicable SEGNAC requirements and any future implementing measures under the PNCD may influence siting decisions in favour of facilities located within Portuguese territory and meeting the requisite security accreditation standards. The PNCD acknowledges the importance of aligning Portugal's digital infrastructure strategy with applicable data sovereignty and security requirements, and future regulatory developments in this area may further shape the conditions under which data centre operators are able to host public-sector and security-sensitive workloads.

Planning classification: municipal variability and pre-licensing uncertainty

Portugal does not have a land use or zoning classification specifically for data centres. The applicable planning framework depends on the relevant municipal master plan (*plano diretor municipal*) and the classification assigned by the licensing authority. Municipal practice varies depending on whether the data centre is intended for industrial, storage, tertiary, or technology services use. This lack of a uniform classification creates uncertainty during the pre-licensing stage and has been identified as an obstacle to sector development in the PNCD.

The applicable licensing process is governed by Decree-Law no. 555/99, of 16 December, which controls building operations at a municipal level.

Fast-track consenting: the PIN regime and the PNCD's pre-installed zones

Currently, Portugal does not have a national or fast-track infrastructure regime applicable to data centres specifically. There is also no centralised licensing mechanism that would combine all the planning, environmental, and sectoral consents required for such projects in a single authorisation, which only exists at the environmental licensing level.

Against this backdrop, the PNCD identifies the simplification and rationalisation of licensing procedures as a strategic priority, proposing the establishment of "pre-installed zones" - areas with a pre-prepared planning and environmental framework, as well as coordinated planning of connections to essential infrastructure, including energy and telecommunications networks. However, this remains a programmatic policy direction that has not yet been implemented in legislative terms.

Moreover, as stated above, the PIN (*Projeto de Interesse Nacional*) regime is a Portuguese legal framework, established to attract and facilitate large-scale investment projects considered to be of potential national interest. Under the regime, projects meeting certain eligibility thresholds – typically relating to investment volume, job creation, technological innovation, export capacity, or contribution to regional development – may apply for PIN status, which grants them a streamlined and expedited treatment by public authorities. Once classified as PIN projects, investors benefit from a coordinated, single-point-of-contact approach with the public administration, priority handling of licensing and permitting procedures, and dedicated support from relevant government agencies, including AICEP (*Agência para o Investimento e Comércio Externo de Portugal*).

ENVIRONMENTAL REGULATION AND SUSTAINABILITY

Case-by-case EIA screening

In Portugal, data centres are not automatically subject to an environmental impact assessment ("**EIA**") under Decree-Law no. 151-B/2013, of 31 October. Whether they are subject to this regime depends on a case-by-case screening decision by the relevant public authority (namely, the Portuguese Environmental Agency or the entity responsible for the project's licensing procedure), which is responsible for granting the necessary administrative authorisation for the project, and depends on the project's characteristics and size.

Energy efficiency: a transitional regime moving towards European alignment

Portugal does not currently impose mandatory energy efficiency standards on data centres, but rather a layered framework of EU-derived reporting obligations, tariff conditionality, and forthcoming implementing legislation. The present regime rests on Directive (EU) 2012/27 and Directive (EU) 2013/17, together with the Portuguese instruments that transpose them.

Two domestic instruments operate at different levels. On one hand, Decree-Law no. 68-A/2015, of 30 April addresses energy consumption at the company level: mandatory four-year independent energy audits (unless a certified energy or environmental management system is in place), energy management systems, and incentives for technological modernisation. On the other hand, Decree-Law no. 84/2024, of 4 November, which partially transposed Directive (EU) 2023/1791 and gives effect to Commission Delegated Regulation (EU) 2024/1364, addresses data centres as a specific asset class, imposing reporting and public disclosure obligations on facilities with an installed IT power capacity of 500 kW or above across energy consumption, renewable energy use, waste heat reuse, water consumption, and other efficiency indicators. The regimes are cumulative, and operators caught by both must reconcile divergent reporting cycles, indicator sets, and supervisory channels.

Transposition of Directive (EU) 2023/1791 remains incomplete, and there is no meaningful administrative or case law experience to draw upon. However, once the EU Data Centre Energy Efficiency Package is adopted, it is expected to introduce harmonised thresholds applying directly across Member States, converting disclosure into substantive performance standards.

The most immediate point at which energy efficiency is already a binding commercial condition lies in the electro-intensive customer regime under DL 15/2022: maintaining that status requires implementation of an EN ISO 50001:2018 certified energy management system within three years of joining the scheme. The ISO 50001 condition is the gating criterion for access to the most valuable tariff reductions available under Portuguese law.

Finally, in Portugal, energy efficiency is not yet a standalone requirement for grid access or prior control permits, but that is an artefact of regulatory lag. Data centre operators assume that mandatory thresholds will be introduced within the current investment horizon, that retrofitting compliance is materially more expensive than designing to anticipated future standards, and that the current electro-intensive status and PNCD eligibility already track performance levels that are likely to be mandated in due course.

Waste heat recovery: an emerging frontier with structural constraints

Currently, Portugal imposes no mandatory obligations on data centre operators regarding the supply or utilisation of waste heat, placing it at the permissive end of the European spectrum, which is shifting rapidly towards ever-greater prescription. The structural constraints on the Portuguese regime are real: limited district heating infrastructure, a climatic profile that reduces the marginal heating value of recovered heat, and a geographic distribution of likely clusters at distance from concentrated industrial offtakers.

There are currently no known reference projects in Portugal involving the use of waste heat from data centres in district heating networks or industrial processes. The PNCD does, however, identify waste heat recovery as a relevant technological solution for the sustainability of the sector.

Sustainability reporting: a European framework awaiting domestic implementation

The sustainability reporting obligations applicable to data centre operators in Portugal arise principally from EU law, with no national instruments specifically targeting the sector. The Portuguese position is defined by the interaction between the directly applicable elements of the EU framework, the ongoing process of domestic transposition, and the sector-specific reporting introduced by Decree-Law no. 84/2024.

The CSRD has not yet been transposed into Portuguese law, but that is not equivalent to non-application. The obligation to prepare and publish a sustainability report within the scope and timeline specified in the CSRD is sufficiently precise and unconditional to engage direct effect; the substantive content of that report is separately governed by the ESRS adopted under Commission Delegated Regulation (EU) 2023/2772, which as a directly applicable delegated regulation requires no transposition. In-scope operators cannot defer compliance pending domestic implementation, although the practical enforceability of those obligations remains incomplete: Portugal has not yet designated the competent supervisory authority or established the administrative penalty regime required under Articles 34 and 51 of CSRD. Operators subject to both the CSRD and Decree-Law no. 84/2024 face real friction in the interim: their reporting cycles do not align, their indicators differ, and the audiences to whom each instrument's disclosures are directed have different expectations. That coordination burden is transitional, rather than permanent – once CSRD is transposed, it will largely supersede the domestic regime – but it is presently unmitigated by any consolidated Portuguese guidance.

No publicly relevant greenwashing investigations or enforcement proceedings have targeted data centre operators or their energy suppliers in Portugal to date. That absence reflects regulatory lag rather than low risk. The Portuguese Consumer Directorate – (*Direção Geral do Consumidor*) has demonstrably intensified its attention to environmental claims: in 2024, it reviewed more than 250 advertising messages in the energy sector and intervened to require the withdrawal of a 'fly greener' claim, following a complaint by DECO Proteste (Portugal's principal consumer protection association).

REAL ESTATE

Site acquisition

Due diligence in the real estate sector should focus on reviewing land registry certificates for properties on which data centres are located, as well as verifying relevant unregistered matters. Key aspects to examine include the chain of title, registered encumbrances, unregistered third-party rights, compatibility of the use permit with intended use (i.e. as a data centre), exposure to environmental risks (including soil contamination) and the land's physical and geotechnical conditions. The allocation of risk between the seller and the buyer is governed by the general rules of the Portuguese Civil Code and is typically supplemented by contractual warranties and representations, specific indemnities, and, in some cases, price retention or escrow mechanisms in line with market practice for real estate transactions.

In Portugal, the main structures for securing the right to use a property for a data centre are freehold acquisition, surface rights and commercial leases. Freehold acquisition provides maximum operational flexibility, significantly reducing the risk of third-party interference whilst facilitating financing through the granting of security interests over the property. The surface right enables infrastructure to be constructed or maintained on third-party land and is frequently used in project finance structures. It is a transferable and encumberable real right (including by way of mortgage) and may be constituted for a fixed or indefinite term. Upon expiry, ownership of the constructions reverts to the landowner, and the parties may agree on compensation or indemnity mechanisms. This structure offers an intermediate risk profile: it is less exposed to landlord insolvency than a lease, but dependent on the stability of the constituted right.

Non-residential leases must be in writing and may only be agreed for a maximum term of 30 years. Leases exceeding six years are mandatorily subject to land registration, which reinforces their enforceability against third parties and purchasers of the property. In the event of a property transfer or landlord insolvency, the lease generally remains in force under applicable civil and insolvency legislation. However, the tenant's position depends on the lease's enforceability and the insolvency proceedings' specific circumstances. Portuguese law does not provide for statutory step-in rights for lenders in lease agreements. These are usually addressed in the contract and, if necessary, through tripartite agreements between the lender, operator, and landlord.

Space provided to third-party tenants may be offered as a sub-lease, which is subject to the non-residential lease regime. Alternatively, service agreements can be used to avoid the mandatory lease regime. In the latter case, care must be taken to ensure that the arrangement is not reclassified as a lease, particularly by granting exclusive and stable use of a defined area. Where a head lease is in place, it is essential that the agreement expressly authorises the transfer of use to third parties; otherwise, the subletting will be invalid. The fit-out obligations, service levels, operator access for installation and maintenance of equipment, allocation of preventive and corrective maintenance responsibilities, and reinstatement of the space at the end of the term should be expressly regulated in the contract.

Securing power, fibre, and water access across third-party land

The routing of power, fibre optics, and water connections across third-party land may require the establishment of predial servitudes (easements), or the use of administrative mechanisms as set out in sector-specific legislation.

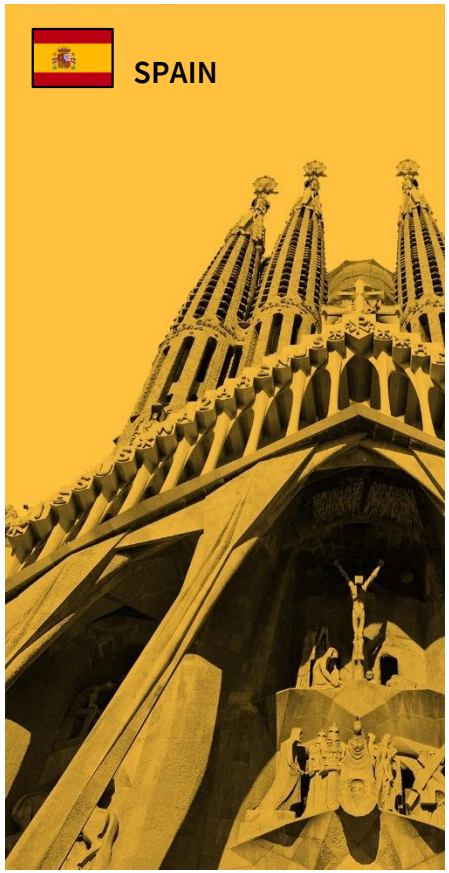
These servitudes may be established by operation of law, contract, will, usucaption or pursuant to the doctrine of the common owner, or as a result of a judicial or administrative decision. Two particularly relevant examples are the statutory right of way, which applies when a property lacks adequate access to a public highway and must be established via the route and means that impose the least burden on the servient tenement, and the statutory water channel easement, which allows water to be conveyed across third-party land for agricultural or industrial purposes. In both cases, the establishment of these servitudes requires the payment of compensation to the owner of the affected property.

In the energy and telecommunications sectors, administrative servitudes and other statutory rights to install infrastructure on third-party land are particularly relevant, specifically in relation to electricity and electronic communications networks. These provide more structured mechanisms where it is not possible to obtain the consent of the affected landowners.

In practice, obtaining these rights often requires negotiation with affected landowners along the infrastructure route. This can introduce significant delays to the project timeline and increase implementation costs, especially where there is no applicable framework of administrative servitudes or public utility regimes to allow for the coercive imposition of the burden.

Predial servitudes are subject to land registration and once constituted and registered they attach to the burdened property and bind subsequent owners in the event of a transfer. However, outside the cases expressly provided for by law, there are no general mechanisms to unilaterally impose servitudes on landowners who refuse to encumber their properties. This leaves the operator dependent on obtaining private agreements, identifying alternative routes, or, where there is a legal basis, resorting to the courts to recognise the rights arising from such servitudes.

Country Chapters



Spain has emerged as one of southern Europe's most dynamic data centre markets. The country possesses abundant renewable generation and a mature corporate PPA market. The government intends to increase installed IT capacity from approximately 500 MW to around 2,500 MW by 2030, with total investment potentially exceeding €60 billion. The Aragón region has emerged the country's leading hyperscale hub, followed by Castilla-La Mancha, Extremadura, Navarra, and the Basque Country, whilst Madrid and Barcelona remain the principal colocation markets. What follows is a thematic analysis of Spain's position across the principal dimensions of the comparative framework applied throughout this publication.

GRID CONNECTION

Grid architecture and market structure

Access and connection to the electricity grid is probably the greatest roadblock to develop data centres in Spain today. As electricity consumers, obtaining demand-side grid access and connection rights, and maintaining their validity, is a critical factor for the success of data centre projects.

The Spanish electricity sector operates under a strict unbundling model. Transmission is carried out exclusively by Red Eléctrica de España ("**REE**"), the sole transmission system operator, under full ownership unbundling. Distribution is carried out by a limited number of distribution system operators subject to legal and functional unbundling.

As a result, data centres can only access physical electricity supply through: firstly, obtaining grid access and connection permits to the transmission grid (high voltage: 220 kV or higher) or distribution networks (medium or low voltage) ("**A&C Permits**"), which represents the primary route for connecting to the grid; or secondly, implementing behind-the-meter arrangements, although it should be noted that these are typically insufficient on their own for large-scale facilities. Spanish law does not currently allow for alternative grid access arrangements, such as microgrids, closed distribution networks, or energy communities.

In line with EU regulations, grid operation in Spain is a regulated activity, subject to exclusive or special rights and strict unbundling conditions. Therefore, no other operator rather than the authorised grid operators is permitted to provide grid access arrangement. Recent legislative reforms allow alternative grid access arrangements for certain specific cases (such as microgrids, closed distribution networks, or energy communities), but data centres do not qualify to participate in any of these alternatives. In other words, A&C Permits are their main mechanism to secure energy supply.

Limited grid capacity remains a major constraint on data centre development in Spain. According to recent surveys, it is estimated that the total grid connection requests for data centres reached approximately 8.7 GW, of which only around one in four MW had been awarded. To tackle this lack of grid capacity, the Spanish government approved targeted amendments to the transmission grid development plan in April 2024 and July 2025, and a new transmission grid plan is expected during 2026 (to be applicable until 2030). This plan will include mandatory developments of the grid, in order to attend new capacity needs (from both generation and demand sides). A&C Permits for data centres or other consumers can only be obtained at existing or planned grid nodes in positions designated for demand purposes. Recent regulatory amendments have sought to make node planning more flexible and to allow, in certain cases, grid extension or change of purpose of existing node positions to supply new demand facilities deemed strategic investment.

Connection queue: reform, maturity milestones, and competitive tenders

Grid capacity availability varies materially by location, making node selection a critical early step. Capacity maps published by grid operators are a key reference. The forthcoming 2025-2030 grid plan formally incorporates a 2,500 MW data centre target and is expected to identify the transmission reinforcements needed to accommodate projected demand. Although the 2025-2030 grid plan should have been approved by the end of 2024, its processing has been delayed due to, among other reasons, the emergence of new electricity-intensive demand facilities. However, said forthcoming grid plan would consider the demand needs of the years 2025 and 2026, while interim amendments of the previous grid plan were implemented as a bypass measure to attend to urgent grid capacity needs.

Spain's grid access and connection framework for large consumers is comprehensively regulated through a single electronic process at national level, under standardised timelines and before the grid operator responsible for the relevant node. End-to-end timelines from A&C Permits request to energisation may range between 30 and 40 months under an optimistic scenario, assuming no tenders are called and depending on the scope of connection works required.

A&C Permits applications were historically processed on a "first come, first served" basis. To address speculation risk, competitive tender procedures can now be activated at overloaded nodes, though these procedures are yet to be thoroughly tested in practice. A&C Permits holders are now subject to binding project maturity milestones over a five-year window – including a grid works' down-payment, execution of a grid reinforcement agreement and grid access contracts – with automatic permit lapse in case of non-timely compliance. In addition, with effect from June 2026, each sponsor is required to make monthly capacity reservation payments. During the first year, 100% of such capacity reservation payments will be credited against future tolls; thereafter, this proportion will reduce to 80%, with the remaining 20% being non-recoverable.

Sponsors must bear the full cost of private connection infrastructure and any required grid reinforcements. A structural constraint applies to campus or multi-tenant configurations: any connection infrastructure shared by more than one consumer is legally deemed part of the public distribution grid and must be transferred to the local DSO for no consideration, with a right of partial cost recovery if subsequently used by additional consumers.

Flexibility, charging, and electricity supply

Data centres in Spain are not subject to any mandatory sector-specific demand response or interruptibility obligations by virtue of their nature or size. As a general rule, A&C Permits in Spain are granted on a firm basis, meaning the contracted capacity is guaranteed at all hours of the year. A flexible access regime is currently being developed by the Spanish Markets and Competition Regulatory Authority (Comisión Nacional de los Mercados y la Competencia, "**CNMC**"), which in July 2026 released a revised draft resolution for public consultation outlining the conditions under which demand facilities may hold flexible A&C Permits. Under this regime, the degree and nature of the flexibility afforded will vary depending on the type of permit granted, ranging from restrictions on the hours during which consumption is allowed to more active real-time interventions by the grid operator, such as remote disconnection or power reduction. However, this flexible regime allows one to obtain grid access connections where the available access capacity is scarce. Data centres are not obliged to opt for flexible A&C Permits, and in practice, are unlikely to do so given their operational requirement for uninterrupted power supply (unless otherwise mitigated with BESS facilities or other behind-the-meter alternatives). In respect of the electricity sector balance markets, although they are not obliged to participate in them, data centres may participate voluntarily in the interruptibility service or in demand response programmes managed by REE.

POWER ACCESS AND PROCUREMENT

A mature and liquid PPA market

Spain has a mature and liquid corporate PPA market, particularly attractive for large electricity consumers such as data centres. The market benefits from a stable regulatory framework, significant renewable generation capacity and strong participation from utilities, IPPs, traders, financial institutions and hyperscale technology companies. Spain has consistently ranked among the leading European jurisdictions by contracted renewable PPA volumes.

Consumers connected to the grid – including data centres – generally require an electricity supply agreement with an authorised supplier, which acts as intermediary responsible for supplying electricity to the consumer, either through purchases in the wholesale electricity market or through bilateral physical PPAs. Spanish regulation allows substantial contractual flexibility regarding pricing, tenor, delivery of GOs, balancing liabilities and other commercial terms.

Large consumers may also enter into direct physical PPAs with generators, though these arrangements generally require a supplier acting as a "sleeving" intermediary. Consumers may also enter into financial PPAs, without the need for a sleeving structure, to hedge exposure to variations in electricity prices. Both physical and financial PPAs may provide for the sale of the GOs associated with the volume of electricity contracted.

As an alternative to supplier intermediation in physical arrangements, large consumers may apply to become a "direct market consumer", allowing them to carry out direct wholesale market or bilateral PPA purchases. In practice, this structure is used in limited cases only due to extensive technical, operational, and financial compliance obligations.

Spanish regulation also allows proximity-based and behind-the-meter structures connecting generation directly to consumers. These structures are particularly favourable to large consumers because renewable electricity consumed on-site generally avoids a significant portion of regulated costs (i.e., grid tolls and charges). Shared self-consumption schemes and surplus compensation mechanisms are also permitted and increasingly relevant for data centres, particularly in areas facing grid access constraints.

Given their constant consumption profile, data centres are expected to accelerate deployment of hybrid PPA structures – combining solar, wind and/or BESS – as well as more sophisticated power procurement models combining corporate PPAs with tolling agreements engaging BESS operators.

Renewable energy certificates

Spain operates a fully EU-compliant Guarantees of Origin ("**GOs**") system administered by the CNMC, under which one GO is issued per MWh of renewable electricity injected into the grid. Spanish GOs are fully aligned with the EU Renewable Energy Directive and mutually recognised across interconnected European markets. Under the current regulatory framework, GO matching between renewable generation and electricity consumption is performed on an annual basis, in line with prevailing practice across most European jurisdictions. However, market participants increasingly expect a gradual transition towards more granular temporal correlation, including monthly or hourly matching standards, particularly for large electricity consumers.

At present, data centre operators in Spain are generally not subject to a legal obligation requiring a minimum percentage of their electricity consumption to originate from renewable sources, nor are they required to demonstrate that such electricity is sourced from newly commissioned renewable projects (i.e. the so-called "additionality requirement"). Nevertheless, sustainability and traceability requirements applicable to data centres are expected to become significantly more stringent over the coming years as a result of the implementation of the EED, Delegated Regulation (EU) 2024/1364, and recent Spanish regulatory and policy developments. In particular, Royal Decree-Law 7/2026 expressly contemplates the future development of specific sustainability requirements applicable to large data centres, including potential obligations relating to renewable energy additionality and temporal correlation.

Nuclear power procurement

No explicit legal prohibition on entering into PPAs with nuclear generators (including SMRs) currently exists, but the current regulatory and policy framework provides very limited incentives for doing so. Even though several nuclear reactors still provide a significant share of electricity generation, the Spanish government has approved a moratorium on new nuclear construction which still continues and maintains its phase-out strategy. All operating plants in Spain are scheduled to shut down progressively between 2027 and 2035, notwithstanding ongoing discussions regarding possible lifetime extensions.

NATIONAL STRATEGY, INVESTMENT INCENTIVES, AND PLANNING

National strategy, investment policy, tax, and subsidy framework

Spain aims to increase installed data centre IT capacity from approximately 500 MW to around 2,500 MW by 2030, with total investment potentially exceeding €60 billion. The regulatory framework is still evolving: the government has proposed a sustainability and energy-efficiency regime for data centres, but implementing regulation remains in draft form following a 2025 public consultation. Similarly, Spain's 2026 Digital Sovereignty Roadmap reaffirmed digital infrastructure and "green" data centres as strategic national priorities. While data centres are not yet expressly classified as "high priority" projects under the access and connection regime, the regulatory trend points towards greater recognition of strategically relevant digital infrastructure.

Like many other European jurisdictions, regional planning tools for projects of strategic interest have accelerated permitting for large-scale data centre developments. Aragón has emerged as the leading hyperscale hub (AWS, Microsoft), followed by Castilla-La Mancha (Meta), Extremadura, Navarra, and the Basque Country. Madrid and Barcelona remain the main colocation markets.

The most relevant support schemes available for data centres are energy-related, particularly programmes managed by the Instituto para la Diversificación y Ahorro de la Energía (IDAE), and financed through EU and FEDER funds supporting BESS. Spain's Energy Storage Strategy targets over 20 GW of installed storage by 2030 and 30 GW by 2050.

Aligned with EU regulations, data centres are not yet legally treated as "electro-intensive consumers" and therefore cannot benefit from rebates on regulated electricity costs available to qualifying industrial consumers. Additionally, no sector-specific tax regime applies to data centres. Projects are subject to the standard 25% corporate income tax rate, although general incentives – including accelerated depreciation and R&D deductions – may be available depending on the investment structure.

Critical Infrastructure designation and cyber security

Spain has yet to transpose NIS2. The government published a Draft Cybersecurity Law in January 2025, with parliamentary approval widely expected in the second half of 2026. However, the current framework in Spain remains the NIS1 regime, under which data centre operators are not automatically covered, and only become subject to regulatory cybersecurity obligations if they are formally designated as operators of essential services or cloud computing providers. Once in force, the Spanish transposition will also introduce several jurisdiction-specific features: a traceability requirement in incident management, a mandatory information security officer with coordination responsibilities, and potential liability for individual board members for regulatory infringements. On the physical resilience side, transposition of the EU Critical Entities Resilience Directive is also pending, with a draft Critical Infrastructure Law published but yet to complete the legislative process. Notable proposed features include a new intermediate category of "strategic entities" subject to lighter-touch obligations than critical entities, a mandatory periodic certification scheme, and enhanced obligations such as compulsory drills with law enforcement and extended background checks.

Under the current NIS1 framework, the main obligations for covered entities are to implement proportionate technical and organisational security measures, designate an information security officer, and notify significant incidents to the competent authority ("**INCIBE-CERT**"). Incident reporting is channelled through INCIBE-CERT for private-sector operators of essential services, with notification triggered when an incident reaches a "critical", "very high", or "high" impact level under a five-tier severity taxonomy (i.e. "critical", "very high" "high", "medium", "low"). Reporting timelines require an initial notification immediately upon detection, intermediate updates within 24 to 72 hours depending on severity, and a final report within 20 to 40 days. Supervisory competence is distributed across several Ministries (Defence, Internal Affairs and Digital Transformation) and key governmental bodies (mainly CNPIC and CCN), depending on the nature of the entity and the sector in which it operates. Sector-specific regimes may displace or supplement these general obligations; most notably, the Digital Operational Resilience Act (DORA) applies to financial entities and their critical ICT third-party service providers or the telecom sector that subject to its own security and incident-reporting requirements under the Spanish General Telecommunications Law 11/2022.

Data centres providing services to public entities are additionally subject to the National Cybersecurity Scheme, which sets mandatory security requirements calibrated to the risk category of the relevant system. Sector-specific regimes – most notably in telecoms and financial services – may displace or supplement these general obligations. Carve-outs exist for entities supporting national security or defence functions (Instituto Nacional de Ciberseguridad).

National security and foreign investment screening

Spanish FDI legislation has not been modified to explicitly designate data centres as a distinct category subject to FDI screening. However, data centres may fall within the scope of the FDI authorisation regime where the Spanish authorities determine that they constitute critical infrastructure – whether physical or virtual (including data processing or storage facilities) – or where the operator has access to sensitive information. Spanish FDI authorities have subjected transactions involving data centres to screening on this basis.

Under the Spanish national regime, prior authorisation is required where certain conditions of the investors and the target are satisfied. Both non-European Union, or non-European Free Trade Association investors ("**Non-EU/EFTA**") and non-Spanish EU/EFTA investors ("**EU/EFTA Investors**"), the latter of which on a temporary basis until 31 December 2026, are deemed to be foreign investors for the purposes of the Spanish FDI regulations. In general terms, prior authorisation is required where the following conditions are satisfied:

1. the investor is either: (a) a non-EU/EFTA resident, OR (b) an EU/EFTA resident investing more than €500 million in a non-listed Spanish company, OR (c) an EU/EFTA resident acquiring a stake in a listed Spanish company;
2. acquires at least 10% of the share capital or control of a Spanish company; and
3. the target operates in a strategic sector or meets certain conditions, or that the investor falls within one of the specified categories under the regime.

Investments in companies with annual turnover below €5 million are generally exempt, subject to exceptions in the energy, communications, and strategic raw materials sectors. Other less relevant conditions should be analysed on a case-by-case basis. Failure to obtain the required authorisation may result in the transaction being declared null and void, and administrative penalties of up to the value of the transaction may be imposed. Given this risk, investors typically elect to submit a formal prior consultation to the FDI authorities – which must respond within 30 business days and whose determination is binding – in order to obtain clarity on whether an authorisation is required.

Data localisation and cross-border data flows

Spain has not adopted general mandatory data localisation requirements distinct from the EU-wide framework. The Spanish regime aligns with the GDPR without adding Spain-specific geographical storage obligations. International transfers of personal data from Spain follow the standard GDPR mechanisms. Sector-specific legislation governing electoral rolls, population registers, tax data, and health system data imposes strict purpose limitation, access control, and confidentiality requirements, but does not mandate that such data be stored exclusively within Spanish or EU territory.

Whilst it may be argued that certain data centre service providers, particularly those offering colocation or housing services, do not directly process the data stored therein and therefore may not qualify as data processors, the Spanish data protection supervisory authority's position is that data centre providers should be treated as data processors and are subject to personal data protection regulations.

Land use classification and default consenting route

Land use classification is a critical factor in data centre development. Data centres are typically located in urban or suburban areas, close to their clients and with ready access to essential infrastructure – in particular, electricity grids, but also water supply, fibre optic connectivity and transport links. Urban planning matters are predominantly managed before the authorities at the regional and municipal levels, with divergences in zoning rules, permitted uses and procedural requirements across Spain's 17 regions and over 8,000 municipalities.

There is no specific land use or zoning category for data centres under Spanish law. Projects are typically located on urban land and classified under conventional use categories – most commonly industrial or, in some cases, tertiary (services) – which do not adequately reflect the operational profile of modern data centres. In many cases, data centre projects are not compatible with existing municipal urban planning instruments, thus requiring amendments to regional or municipal planning frameworks. At the national level, the government's 2024 AI Strategy signalled its intention to develop a regulatory framework to foster the sustainable installation of data centres. However, no standalone national legislation addressing data centre planning or accelerated consenting has been enacted, and the sector continues to rely on regional instruments and urban planning procedures.

National/fast-track consenting pathways

Spain has no dedicated national significant infrastructure regime for data centres. No single authorisation bundles the planning, environmental, and grid consents a project requires. Acceleration is instead delivered through two distinct layers – a mature set of regional strategic-interest instruments, and an emerging national framework – each resting on a different constitutional competence and offering a different package of benefits.

At the regional level, most of Spain's 17 regions have established instruments for declaring qualifying projects to be of strategic or regional interest, on the basis of criteria such as investment volume, job creation, sustainability impact, and contribution to economic development. These instruments are not designed specifically or exclusively for data centres, but a project that satisfies the applicable criteria can secure designation and the procedural advantages that follow. The criteria, procedure, and effects of such declarations vary from one community to the next, yet they tend to converge around a common set of benefits: firstly, automatic compatibility of the data centre – including its ancillary and connection facilities – with existing land-use classifications; secondly, streamlined administrative procedures and reduced timelines; thirdly, land expropriation rights; and fourth, exemption from certain permits or procedural steps. The practical value of a regional declaration to a given project therefore turns on the rules of the specific community in which the site is located, a matter that should be assessed at the site-identification stage, rather than assumed.

At the national level, Royal Decree-Law 7/2026 introduced a new and independent category of "Strategic Investment Projects", with implementing criteria to be set out in a Royal Decree currently in draft form. The national regime reaches the matters that fall within State competence, and on which the regions are not competent – grid connection foremost among them – and so addresses the principal constraint that regional instruments cannot. Although the regime applies to large-scale demand facilities generally, the current version is specifically designed in part to accommodate data centre developments. Projects are declared by the Government's Delegated Commission for Economic Affairs on the basis of criteria, including investment volume and creation of highly qualified employment, with digitalisation a positively weighted factor.

Designation may carry several advantages: institutional support and facilitation of administrative and permitting procedures (including different permits to be granted at all administrative levels); facilitated grid access and connection (including temporary capacity reservations and priority in the permitting process queue); inter-administrative coordination; and streamlined access to public funding. Royal Decree-Law 7/2026 also introduces a related category of "Preferential Energy Projects", under which associated energy facilities benefit from facilitated processing. The implementing Royal Decree is expected to be approved during the course of 2026, at which point the national fast-track route – today still in formation – will become operative alongside the established regional instruments.

ENVIRONMENTAL REGULATION AND SUSTAINABILITY

Environmental Impact Assessment

Spanish legislation does not list data centres as a standalone project category subject to mandatory EIA. Whether a given facility requires one is determined case by case, by reference to both the national and regional regulations applicable to the data centre's location, and the assessment may follow either an ordinary or a simplified procedure depending on the project's characteristics. Where an EIA is required and concluded favourably, the competent authority issues an environmental impact statement (*declaración de impacto ambiental*) ("**DIA**"), which is a precondition to construction and commissioning.

In practice, the EIA obligation is triggered not by the data centre as such, but by its associated infrastructure. The most common triggers are backup generators, electrical substations, cooling systems, and combined heat and power installations, each of which may bring the project within a screening category under the applicable legislation. Beyond the EIA itself, a project may require further environmental permits calibrated to its specific configuration, including permits for atmospheric emissions, for water abstraction and discharge, and for waste management.

A DIA is accordingly required for many data centre projects, on grounds that include: firstly, atmospheric emissions from backup generators and combustion equipment; secondly, the need to obtain a prior urban planning instrument; thirdly, the environmental characteristics of the site or surrounding area; fourth, the integration of the data centre within a broader development (such as co-located on-site renewable generation); and fifth, the cumulative effects of the project taken together with others in the vicinity. The practical consequence is that the EIA question turns on how a project is configured and sited, rather than on its scale alone, so sponsors should resolve the screening position – and the procedure that follows from it – at an early stage, before the design of ancillary infrastructure is fixed.

Energy efficiency: PUE and mandatory standards

Spain is in the process of transposing Article 12 of the EED through the forthcoming Royal Decree on energy efficiency and sustainability for data centres (the "**Draft RD**"), whose public consultation period expired on 15 September 2025. The Draft RD is broader and stricter in certain respects than the requirements of the EED. For example, aside from submitting an annual report to the energy authorities covering the indicators set out in the Regulation (EU) 2024/1364, the draft RD additionally requires operators to report on socio-economic indicators, including estimates of direct and indirect jobs created, the qualification level of such employment, territorial impact, and an analysis of expected economic impact at local and national level. These socio-economic reporting requirements go beyond the EED's disclosure obligations.

Spain has not yet introduced mandatory regulatory thresholds for Power Usage Effectiveness ("**PUE**"), Water Usage Effectiveness ("**WUE**"), or other efficiency metrics. However, the Draft RD adopts a best-practice approach, requiring data centres to report on their level of compliance with the EU Code of Conduct on Data Centre Energy Efficiency and, for data centres with an IT demand exceeding 100 MW, to demonstrate that they are among the top 15% of facilities with the best sustainability indicators. Relevant key performance indicators include PUE, WUE, the Energy Reuse Factor ("**ERF**"), and renewable energy coefficients, with the applicable metrics varying depending on the size of the data centre. Significantly, the Draft RD links compliance with these obligations directly to grid access: access and connection permits for new projects are conditional on demonstrating such compliance, and existing permit holders must provide proof of compliance when executing the technical grid access agreement. Non-compliance with the energy efficiency and sustainability requirements may result in loss of grid access and connection permits. .

Heat recovery and waste heat obligations

Spain is also in the process of transposing the EED through the Draft RD by requiring data centres with a total rated energy input exceeding 1 MW to utilise their waste heat for heating, cooling, or other heat applications, unless a cost-benefit analysis (CBA) demonstrates that this is not technically or economically feasible. New projects (and substantially renovated facilities) must prepare a CBA report as a prerequisite for project implementation. The CBA report must be approved by the competent regional authority where the project will be located. For the purposes of obtaining municipal building permits and A&C Permits, the sponsor must demonstrate that the CBA report has been approved. The approved CBA report has a validity period of five years and must be renewed following the same procedure. The waste heat reuse measures identified in the CBA must be implemented during this five-year period. If the sponsor implements the CBA measures within the first three years, the Draft RD contemplates that they may benefit from certain support mechanisms (such as Energy Saving Certificates).

Sustainability reporting

The Draft RD imposes annual reporting obligations on data centres with an IT power demand of 500 kW or above, covering energy performance, water consumption, heat reuse, and renewable energy share. The mechanism by which these obligations bite is the feature that distinguishes the Spanish regime from a conventional disclosure duty: if the Draft RD is adopted in its current form, compliance will be tied to the grant and maintenance of A&C Permits, so that a reporting failure threatens the operator's grid access itself rather than merely exposing it to an administrative penalty.

The CSRD has not yet been fully transposed into Spanish law, although a draft bill (Proyecto de Ley de información empresarial sobre sostenibilidad) is progressing through the parliamentary process. In the interim, the Spanish authorities have confirmed that Spanish companies may prepare their 2025 sustainability reports under the ESRS. Distinct from the CSRD process, Royal Decree 214/2025 of 18 March 2025, in force since 12 June 2025, establishes a mandatory carbon-footprint calculation and reporting regime for large companies and public sector entities, replacing the previous voluntary registration system. Obligated entities must calculate their organisational carbon footprint annually and prepare a greenhouse gas emission reduction plan with a minimum five-year time horizon. Direct emissions (Scope 1) and indirect emissions from purchased energy (Scope 2) are mandatory; value-chain emissions (Scope 3) remain voluntary for private sector companies at present, although the regulatory trajectory points toward an extension of Scope 3 obligations from 2028.

No greenwashing claims or investigations against data centre operators or their energy suppliers in Spain have been publicly reported as of June 2026.

REAL ESTATE

Project site

Due diligence on a Spanish data centre site starts with the search in the Land Registry (*Registro de la Propiedad*) and must be cross-checked against the Cadastre (*Catastro*) to identify discrepancies. Beyond registered charges, due diligence should cover unregistered rights, administrative licences, existing leases (which bind purchasers), easements, and soil contamination (particularly for brownfield sites). A separate zoning analysis should confirm that the intended use is permitted from an urban planning perspective. Risk allocation is primarily contractual: through title warranties, price adjustments, environmental indemnities, and W&I insurance.

Three structures are available for securing a campus site. Freehold acquisition (*pleno dominio*) is the preferred route: it carries no reversion risk, supports full mortgage security, and affords the greatest flexibility – including multi-PropCo structures where each module sits in its own special purpose vehicle, ring-fencing liabilities and simplifying future disposals. Where a campus comprises multiple buildings, a real estate complex (*complejo inmobiliario*) or a horizontal division (*división horizontal tumbada*) allows each module to hold its own land registry status and to be financed or sold independently, while shared infrastructure is governed and funded collectively. The surface right (*derecho de superficie*) is the closest Spanish equivalent to a long-term ground lease, granting the right to build and own constructions on another party's land for up to 99 years; it is registrable, mortgageable, and transferable, but the buildings revert to the landowner on expiry without compensation. A commercial lease is viable where neither ownership structure is attractive: term and renewal are freely negotiated (without statutory minimum or renewal right), and land registry protection is available – and advisable – to protect the tenant against a sale or the enforcement of third-party security. Both leasehold and surface-right structures require direct agreements with lenders to protect their enforcement position.

Where an operator sub-lets space to customers, colocation arrangements are almost universally structured as service agreements, under which the operator supplies a full range of services – power, cooling, security, and connectivity – and retains control of the facility throughout. Provided an arrangement is genuinely constituted on that basis, rather than as a lease, the statutory tenant-protection regime does not apply. A requalification risk arises where a customer is given exclusive physical control of a self-contained space with no meaningful service overlay; fit-out obligations and maintenance responsibilities should therefore be allocated explicitly in the customer contract, since each either reinforces or undermines the characterisation as a service.

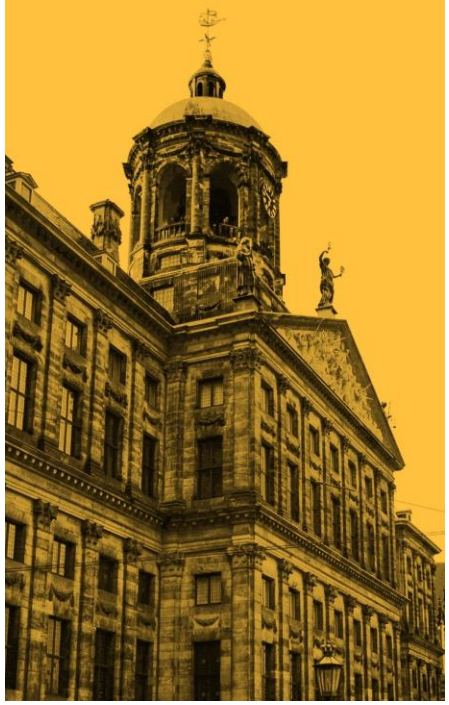
Grid connection and connectivity

The standard tool for securing rights of passage for utilities across third-party land is an easement (*servidumbre*), which must be granted as a notarial deed and registered with the land registry to bind successors and be fully effective against third parties. An easement may attach to the land itself (*in rem*), or to a specific beneficiary such as a grid operator (personal), and it may be agreed voluntarily or imposed by law against compensation. What determines its security in every case is registration, which is the step that carries the right across a future sale of the burdened land.

A major consideration for a data centre sponsor is whether the route can draw on the statutory regime for regulated electricity infrastructure. Transmission and distribution grids are declared as public utilities under Spanish law, which allows grid operators – and, in certain cases, sponsors of self-consumption or on-site PPA arrangements – to invoke the compulsory expropriation procedure to obtain the necessary easements where voluntary agreement cannot be reached. Outside that regime, an easement cannot be demanded: unless the project has been approved as one of regional interest – which may trigger an equivalent public utility declaration over the affected plots for any utility infrastructure – the sponsors must rely entirely on voluntary agreements with each landowner along the route. That dependence is a critical risk and timeline driver, because a single holdout can delay or block a connection, which makes early engagement and adequate programme contingency essential.

Country Chapters

THE NETHERLANDS



Today, with almost 200 data centres – including two hyperscale centres – the Netherlands is one of Europe's leading co-location data centre hubs. Between 2021 and 2023, installed capacity expanded from 1,489 MW to 1,638 MW. Despite its growth, the sector increasingly faces constraints: most notably, spatial scarcity and grid congestion. Since 1 January 2024, a nationwide restriction exists for new hyperscale data centres exceeding 10 hectares and requiring a connection capacity of 70 MW or more, with exceptions applying only in a small number of government-designated locations. Despite these current practical restrictions, the Dutch government has expressed strong support for AI infrastructure development, including market-funded AI gigafactories, and has signalled its intention to encourage private capital and streamline the applicable permitting framework. Therefore, the long-term demand fundamentals – digitalisation, AI adoption, and the Netherlands' position as a European connectivity hub – remain strongly in the sector's favour.

GRID CONNECTION

Grid architecture

The Dutch Energy Act, which entered into force on 1 January 2026, represents a landmark reform in the Dutch energy sector. Its aim is alleviating grid constraints by modernising the gas and electricity market and aligning Dutch law with the EU Clean Energy Package. The act distinguishes the high voltage transmission system, operated by TenneT ("**TSO**"), and the local distribution systems, operated by several distribution system operators, such as Enexis ("**DSO**"). The Netherlands Authority for Consumers and Markets ("**ACM**") is the independent national regulator.

As in other European jurisdictions, the Dutch system is founded on the principle of unbundling. In practice, this means that ownership and operation of transmission and distribution network assets are not available to third parties, such as data centre developers, on a standalone basis.

Grid connection, charging, congestion and queues

System operators are in principle required to offer a grid connection within a reasonable time – as ultimately determined by the ACM – and to realise it once accepted. Where insufficient capacity is available, an operator may refuse the request until constraints are resolved, though it remains obliged to expand the grid in the meantime – such refusals are increasingly giving rise to litigation, making careful review of the associated contracts ever more important. Customers can access the electricity grid through three main routes: firstly, transmission-level connections (typically at least 110 kV, for projects of around 100 MW or more); secondly, distribution-level connections (generally no more than 66 kV, for smaller-scale projects); or thirdly, alternative private network arrangements, such as a closed distribution system or a direct line. Data centre operators are increasingly turning to alternative arrangements to mitigate congestion and secure more flexible or faster access to capacity. System operators charge customers for the realisation of new connections, typically in stages under a milestone scheme. Once a connection is in place, customers are charged periodically for its maintenance, operation, and the transport of electricity. The associated tariffs are set by the ACM on the basis of each system operator's total allowed revenues, reflecting pooled system costs that cannot be traced to an individual customer.

Grid congestion remains the most significant obstacle to data centre development in the Netherlands. As of 2025, queues are substantial: DSO applications number approximately 14,000, representing around 9 GW of demand, whilst more than 200 TSO requests account for around 38 GW. In some regions, new or upgraded connections have been temporarily suspended pending capacity expansions, with connection times in severely congested areas reaching up to ten years. Northern regions retain more available capacity, though this advantage is gradually eroding as electrification and industrial growth accelerate.

Allocation of scarce grid capacity

In congested areas, the default first come, first served ("**FCFS**") allocation model no longer applies. In its place, the ACM has established a priority framework under which priority is given to congestion alleviators, safety-critical infrastructure, and essential public services – with priority among congestion alleviators determined by objective effectiveness. Within all other categories, and between parties without priority status, capacity is allocated on an FCFS basis. Data centres do not hold independent priority status but may qualify indirectly where capacity is used exclusively for a priority-sector party through a joint application.

The priority framework is still evolving and subject to ongoing litigation, with further clarification expected in 2027.

Flexibility mechanisms

Grid access in the Netherlands is actively managed to prevent overload, with system operators relying on flexibility mechanisms that require or incentivise large users – including data centres – to adjust consumption patterns. Three principal instruments are currently in use:

- *Capacity steering contracts:* Agreements under which users commit to reducing or increasing electricity consumption or supply depending on grid conditions, in exchange for financial compensation.
- *Capacity limitation contracts:* A specific form of capacity steering contract under which users commit only to reducing consumption or supply at specified times in exchange for financial compensation. These are the primary tool for securing ongoing grid access at congested nodes.
- *Redispatch (via GOPACS):* A short-term mechanism to adjust consumption or generation in near real time, operating through either voluntary participation or mandatory bids. Businesses with a connection of 60 MW or more are always required to offer flexible capacity.

Alternative transmission rights

In response to grid congestion, three types of non-firm transmission rights are available, each offering a different level of supply certainty:

- *Fully variable transmission right:* Provides grid access only when sufficient transport capacity is available, typically confirmed one day in advance. Supply is not guaranteed and operators must be capable of absorbing interruptions at short notice.
- *Time-block transmission right:* Grants access during predefined periods – such as off-peak or night-time hours – with no entitlement to capacity outside those windows. Offered by DSOs, this product suits operations that can be scheduled around fixed availability periods.
- *Time-duration transmission right:* Ensures grid access for a minimum proportion of time (typically around 85%), with advance notification of unavailable periods. Offered by the TSO, this is the most operationally predictable non-firm option and is generally the most relevant for operators requiring a baseline level of supply certainty.

These variants may be combined to construct a tailored solution aligned with a data centre's operational model and flexibility requirements. Single-owner data centres are generally better placed to participate in flexibility arrangements, as they can adjust aggregate consumption without contractual constraint — particularly where operators can shift or modulate workloads such as AI training to periods of greater grid availability. Co-location data centres face greater structural complexity: the presence of multiple tenants with distinct load profiles and service level commitments limits the operator's ability to curtail or shift consumption unilaterally.

Additional policy measures

As part of the National Action Programme on Grid Congestion, additional measures are being developed to enable more efficient use of existing grid infrastructure. These include a "use-it-or-lose-it" regime — allowing system operators to reduce contracted capacity where utilisation consistently falls below the contracted threshold — and group transport agreements, which allow multiple large customers to contract and allocate capacity collectively. For larger data centre campuses or operators running multiple co-located facilities, group transport agreements may offer a practical route to securing aggregate capacity unavailable to individual applicants.

Although no sector-specific interruptibility obligations currently apply to data centres, participation in flexibility arrangements is in practice increasingly a de facto prerequisite for securing and maintaining grid access, rather than a purely optional commercial choice.

POWER ACCESS AND PROCUREMENT

Procurement structures and legal framework

Unable to rely on timely or adequate grid access, data centre operators in the Netherlands are increasingly securing renewable energy through PPAs concluded directly with generators. Beyond providing price certainty and a guaranteed renewable supply, PPAs concluded by larger data centres can materially strengthen the investment case for new solar and wind projects by offering the long-term offtake certainty that project finance structures typically require.

A growing number of operators are also reportedly participating in grid balancing programmes – offering demand flexibility in exchange for revenue or preferential access terms – or exploring on-site generation to reduce dependence on congested grid infrastructure. Corporate PPAs, on-site generation, and grid balancing participation are increasingly viewed as complementary components of an integrated energy strategy rather than discrete alternatives. To alleviate grid congestion, some industries are also considering hydrogen as part of their broader solution to secure long-term energy supply.

Renewable procurement and certificates

The principal renewable energy certificate scheme in the Netherlands is the GO scheme, administered by VertiCer. The Dutch scheme imposes no mandatory additionality requirement, meaning GO certificates may be issued from both new and existing generation capacity. This diverges from the more demanding additionality standards increasingly embedded in voluntary corporate sustainability frameworks – including the 24/7 carbon-free energy matching methodology adopted by a number of hyperscalers – and from the broader direction of travel in EU disclosure policy.

The Dutch GO scheme complies with the European standard for guarantees of origin and operates in accordance with the standards set by the AIB, through which cross-border interoperability is facilitated.

Nuclear incentives

The Netherlands currently operates one nuclear reactor that generates electricity. However, its nuclear footprint is set to expand materially: a new state-owned entity has recently been incorporated with a mandate to develop additional nuclear generation capacity. That said, this project remains in its initial stages and it will be some considerable time before any new capacity comes online.

In parallel, certain operators are actively considering direct supply arrangements from SMR facilities, although the commercial framework governing such arrangements remains at an early stage of development.

NATIONAL STRATEGY, INVESTMENT INCENTIVES, AND PLANNING

National strategy, investment policy, tax, and subsidy framework

Data centre policy in the Netherlands has evolved incrementally across a range of instruments – including spatial planning documents, economic strategy papers, and sectoral legislation – and at different levels of government. To date, these have not been consolidated into a single overarching framework. The result is a duality that operators and investors must navigate carefully:

- On the one hand, data centres are recognised as a key component of the Netherlands' digital infrastructure and as playing an important role in safeguarding the country's digital open strategic autonomy. This recognition is reflected in the 2025 draft spatial planning memorandum – which sets out the spatial planning framework for the Netherlands through to 2050 and is expected to be adopted later this year – as well as in the Dutch government's broader support for AI infrastructure investment.

- On the other hand, national, regional, and local authorities have in practice progressively introduced stricter regulations and policies governing data centre development, driven by concerns over energy consumption, spatial planning pressure, and environmental impact. In a number of cases, this has resulted in moratoria on the construction of new data centres, or of specific categories thereof.

These constraints are expected to persist in the short term. In the longer term, however, the demand drivers – digitalisation, AI adoption, and the Netherlands' established position as a European connectivity hub – support the expectation that the sector will continue to grow, albeit within an increasingly regulated framework.

On the fiscal and incentive side, various Dutch subsidies and tax incentives may be available for qualifying investments aimed at stimulating the use of renewable energy, reducing CO_2 emissions through amongst others improvement of efficiency rather than asset relocation, re-using residual heat, and funding research to improve upon the foregoing. The headline Dutch corporate income tax rate is 25.8%. Additional or accelerated depreciation allowances may be available for qualifying data centre investments, including related battery storage. Dutch real estate transfer taxes are a point of attention, but should not apply to the sale of an entity that owns and actively operates data centres located in the Netherlands.

Critical National Infrastructure designation

Under the current regime, multi-tenant data centres exceeding 50 MW of aggregate connection capacity are designated as “other vital providers” under the Network and Information Systems Security Act, carrying an incident reporting obligation to the National Security Centrum and, in certain circumstances, to the Minister of Economic Affairs.

The cybersecurity landscape is, however, undergoing significant reform. The Cybersecurity Act (transposing NIS2) and the Critical Entities Resilience Act (implementing the CER Directive) have both been adopted by Parliament and will enter into force on 15 August 2026. The Cybersecurity Act will supersede and expand the current framework. Data centres exceeding the medium-sized enterprise threshold and/or designated as a “critical entity” under the Critical Entities Resilience Act will be designated “essential entities”, whilst small-sized data centre entities will be designated "important entities". Both categories will be subject to a duty of care – already applicable to many operators, but extended in scope – enforced by the Dutch Authority for Digital Infrastructure. Administrative fines may be imposed on the entity for breaches of the notification requirements and the duty of care – as prescribed by NIS2 – as well as non-cooperation with the supervisory authority, or other violations. Apart from that, administrative fines of up to €25,000 may be imposed on managing directors personally for breaches of training/qualification criteria. The Critical Entities Resilience Act will operate in parallel. Once formally designated a "critical entity" by the relevant Minister, a suite of resilience obligations applies; however, providers of data centre services as defined in NIS2 are exempted from certain key obligations, including the duty of care.

Operators should verify carefully whether their specific activities and designation status engage or exclude requirements under each regime.

National security and foreign investment screening

Foreign investment in Dutch data centres is subject to a sector-specific screening regime under the Telecommunications Act, operating independently of general merger control and without any turnover-based or deal-value threshold. Data centre operators – and entities holding a controlling interest in such an operator – may fall within scope; single-tenant facilities are excluded. A notification is required where a party intends to acquire “predominant control” – which includes holding at least 30% of voting rights, having the ability to appoint or dismiss more than half of the board or the supervisory board, or holding shares with statutory control rights – in a relevant operator resulting in “relevant influence” in the Dutch telecommunications sector, meaning that abuse or deliberate disruption of that operator – or any other relevant operator in which the holder or acquirer (or their group) holds or acquires predominant control – could interrupt the availability or verification of data centre services with a power capacity exceeding 50 MW (assessed at the group level), or disrupt the availability, reliability, or confidentiality of data centre services delivered to the AIVD, the Ministry of Defence, the MIVD, the NCTV, or the National Police.

Multiple activities within the Dutch telecommunications sector – such as fibre networks and data centres – are aggregated when determining whether this threshold is met. A party that has already reached the threshold of relevant influence, whether through pre-existing activities or a previous transaction, need not notify further transactions.

The consequences of non-compliance are material: failure to notify may result in an administrative fine of up to €900,000. No standstill obligation applies, meaning completion before clearance is technically permissible but entirely at the parties' own risk. A transaction completed in contravention of a prohibition decision is in principle null and void, and the Minister may additionally order unwinding, suspension of control rights, or conditional clearance requiring divestiture or restrictions on network access.

Where a transaction falls outside the scope of the Telecommunications Act, the general foreign direct investment screening framework may nonetheless apply.

Data localisation and cross-border data flows

The Netherlands imposes no general statutory data-localisation requirements, and as of May 2026, no sector-specific localisation requirements exist beyond those arising under EU legislation. The principal relevant instrument is the Dutch central government's Rijksbreed cloudbeleid 2022, which requires government departments procuring public cloud services to conduct risk analyses addressing the geographical spread of data flows and associated security risks. In practice, this directs government and government-adjacent workloads towards EU or Netherlands-based cloud regions. Operators serving public sector clients, or entities in regulated sectors subject to equivalent data governance expectations, should factor this into their infrastructure planning and contractual positioning.

Land use classification and default consenting route

New hyperscale data centres – defined as facilities exceeding 10 hectares with an electrical connection capacity of at least 70 MW – are subject to a nationwide development prohibition under the Environmental Quality Decree. A narrow carve-out exists for Hogeland and Hollands Kroon in the north of the Netherlands, where existing hyperscale facilities may expand. Outside those designated locations, the prohibition should be treated as effectively absolute in the near term. Sub-hyperscale data centres are governed by the applicable environmental plan; a specific permit is required where a proposed development departs from it.

Additional regional and municipal policy frameworks will often apply and should be identified early in the development process. Decision-making authority rests in principle at the provincial or municipal level, including for hyperscale facilities within the designated northern municipalities.

National/fast-track consenting pathways

The Netherlands has no fast-track or nationally significant infrastructure regime for data centres, distinguishing it from several comparable European jurisdictions.

The most effective procedural tool available is the coordination scheme, which consolidates the preparation, adoption, and challenge of related decisions into a single unified procedure. This avoids sequential permitting and reduces the risk of delays arising from inconsistency between decisions. While not equivalent to a dedicated fast-track regime, the coordination scheme is the best mechanism currently available and should be considered for any project requiring multiple (environmental) permits.

ENVIRONMENTAL REGULATION AND SUSTAINABILITY

Environmental Impact Assessment

Data centres do not constitute a separate designated category under Annex V of the Environment and Planning Decree, which lists the project types requiring either a full EIA report or an EIA evaluation on the basis of their potential for significant environmental effects. An EIA obligation can nonetheless arise where a data centre project meets the thresholds or criteria set out in Annex V by virtue of its ancillary infrastructure; most commonly where emergency power generators with a total thermal capacity exceeding 300 MW are installed. A Council of State ruling in 2024 confirmed that the 300 MW threshold applies to the combined capacity of all combustion installations at a single data centre, rather than to each individual generator separately.

Where a data centre project is preceded or enabled by a plan or programme – for instance, a spatial planning instrument or zoning amendment – an EIA may also be required at the plan or programme level.

Environmental regulations

Data centres in the Netherlands are subject to the general national rules set out in the Environmental Activities Decree. The operation of a data centre supporting data traffic or data storage constitutes an environmentally harmful activity within the meaning of that Decree, engaging a suite of general environmental rules. Additional provisions may apply depending on the facility's technical configuration — including rules on combustion, cooling installations, or large-scale energy generation — and locally established environmental rules should be identified at the planning stage.

Two permits merit particular attention. An environmental permit is required for cooling water discharge where the heat load on a surface water body exceeds 50 MW, a threshold routinely met by hyperscale and large co-location facilities. A nature permit may also be required where a project could significantly affect one of the Netherlands' 162 Natura 2000 areas; in practice, such permits can be difficult to obtain given the country's ongoing nitrogen crisis, which continues to generate litigation and policy uncertainty at the national and local levels.

Energy efficiency: PUE and mandatory standards

PUE requirements are set at local rather than national level and may therefore vary by location. The greater Amsterdam area requires a PUE of 1.2 or below for new data centre projects. As not all authorities have defined a specific threshold, operators should verify the applicable local requirements at the site-selection stage.

With regards to energy saving obligations, pursuant to the Environmental Activities Decree and the Environmental Buildings Decree, data centres consuming 50,000 kWh or more annually must implement all energy-saving measures with a payback period of five years or less, or apply the relevant measures from the Recognised Energy Saving Measures List. Those consuming 10,000,000 kWh or more are additionally required to assess measures with a payback period of up to five years. The Recognised Measures List has attracted criticism for not being consistently suitable or cost-effective across all data centre types and configurations. An extension of the payback period to seven years is under consideration, which, if adopted, would increase the compliance burden for operators.

Operators subject to the energy-saving obligations must also report every four years on their implementation of the required measures; this information is published subject to redaction of confidential business data. Compliance can be operationally complex where operators do not control their clients' IT infrastructure, a challenge particularly acute for co-location providers. Data centres with an installed IT capacity of at least 500 kW must additionally report annually on PUE and further performance indicators, including water use, waste heat reuse, and renewable energy consumption. Larger operators may also be subject to energy audit requirements under the EU Energy Efficiency Directive, which are not fully aligned with the domestic reporting obligation.

Heat recovery and waste heat obligations

There is currently no mandatory obligation on data centres in the Netherlands to supply waste heat to external recipients. However, certain provinces have moved ahead of the national framework: Noord-Holland, for instance, has introduced permit requirements within its Environmental Regulation requiring data centres to configure their systems to enable the transfer of waste heat to a heating company or end user. As of March 2026, 28 active waste heat projects involving data centres have been reported in the Netherlands, reflecting both commercial interest and local regulatory expectations.

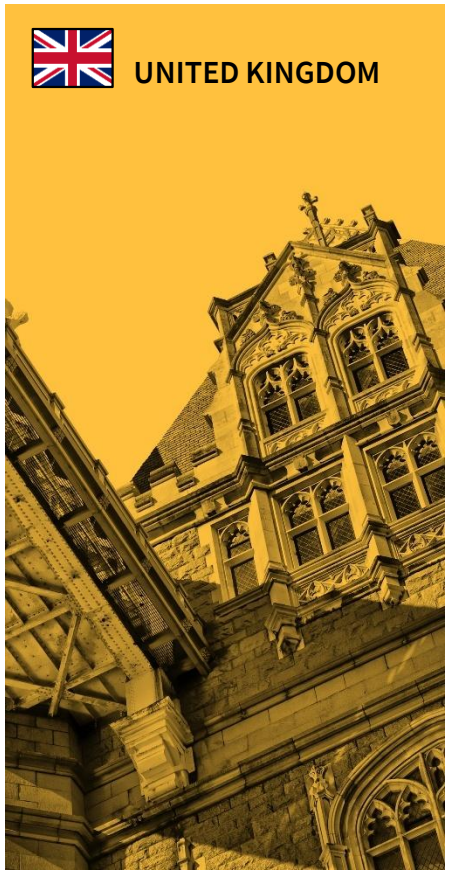
The recently adopted Collective Heat Act, expected to enter into force on 1 January 2027, will empower heat companies to require waste heat producers – including data centres – to make waste heat available upon request, with associated costs regulated rather than commercially negotiated. Whilst the Act supports the integration of waste heat into district heating networks and the broader energy transition, its practical reach is constrained by a structural limitation: commercially viable supply requires geographic proximity to existing heat network infrastructure, a condition not universally met across the Netherlands. Operators assessing sites should therefore treat network infrastructure as a relevant locational factor, both for compliance purposes and in anticipation of the Act's obligations.

Sustainability reporting

In addition to European rules on CSRD and taxonomy, most data centre operators must report on their energy savings obligations and may be subject to annual reporting requirement (see above).

No greenwashing complaints had resulted in sanctions against data centre operators by June 2026.

Country Chapters



The UK is, by installed capacity, the largest data centre market in Europe and the third largest globally. More than £45 billion of private investment has been announced since July 2024 and, in September 2024, data centres were designated as Critical National Infrastructure ("CNI"), the first new CNI sector in nearly a decade. The government's ambition is to make Britain an "AI superpower", as set out in the AI Opportunities Action Plan of January 2025, and it has committed to at least 6 GW of AI-capable data centre capacity by 2030 under the UK Compute Roadmap. These aspirations are, however, colliding with a severely congested electricity grid, an evolving planning regime, tightening environmental obligations, and new cybersecurity requirements. What follows is a thematic analysis of the UK position across the four principal dimensions of our comparative framework.

SECURING GRID ACCESS: OBSERVING THE UK'S CAPACITY CONSTRAINTS

Grid access is the single greatest constraint on data centre investment in the UK today. The queue for new connections is long, and the rules governing how grid capacity is allocated are undergoing significant reform. For sponsors, investors, and lenders evaluating new developments, understanding when and at what cost grid connection can be secured is a fundamental first step to assess viability.

In Great Britain, customers seeking grid access can connect: firstly, at the transmission level (275kV in England & Wales; 132kV in Scotland) directly by applying to the National Energy System Operator ("**NESO**"); or secondly, at the distribution level by applying to the relevant Distribution Network Operator ("**DNO**") covering the area within which the customer is located. Independent Distribution Network Operator ("**IDNO**") and private networks also exist (outside of the general scheme).

Queue reform and prioritising grid capacity

Historically, UK grid connections operated on a "first-come, first-connected" basis. However, the surge in connection applications produced long and congested queues against an already pressured system. That experience is driving fundamental and ongoing reforms, with the UK now transitioning to a "first-ready-and-needed, first-connected" approach, under which projects are assessed on their readiness and strategic alignment, rather than solely on the order in which they applied. The ongoing queue reform process has already filtered out generation and storage projects that failed to meet the relevant criteria, with a consequent meaningful reduction of the generation queue.

The rapid increase in demand-side connection applications, which had not faced the same scrutiny during the initial filtering process, means that further steps are necessary. The Department for Energy Security and Net Zero ("**DESNZ**"), Ofgem, and NESO are considering a number of significant proposals, including: financial commitment requirements for data centre projects, designed to encourage withdrawals of speculative projects from the queue; reservation and reallocation by DESNZ of grid capacity for strategically important projects; and a Connections Accelerator Service providing engineering and technical support for priority projects. There is no formal statutory fast-track mechanism for data centres, though the proposed capacity reservation and Connections Accelerator Service may in practice prioritise qualifying projects. Separately, the government's AI Growth Zones programme aims to provide pathways to timely connections for strategically important demand users located in designated Growth Zones.

Flexibility connections, charging structures, and supply options

Demand connections at the transmission level may be offered on either a firm basis (which is contractually guaranteed and not subject to curtailment), or a non-firm basis (which is conditional, and subject to curtailment during system constraints, outages, or pending reinforcement works). DESNZ, Ofgem, and NESO are currently considering whether to expand the use of flexible or non-firm capacity agreements as a mechanism for enabling projects to connect more rapidly.

Taken together, UK grid access for large demand users is becoming more structured, but also more selective. Continuing reforms are designed to prioritise projects that are both ready and strategically important. Nevertheless, those reforms will also require developers to demonstrate greater upfront commitment, and a clearer case for strategic alignment, than the previous first-come first-served regime demanded.

POWER PROCUREMENT: STRUCTURING SUPPLY IN A MATURE MARKET

The UK offers data centre operators a mature and flexible power procurement regime, with a range of plausible structures and a well-developed market in long-term renewable contracts. Yet, a principal issue for most operators is how to navigate the network charging and regulatory classification consequences that flow from each choice.

Selecting procurement models: structural considerations

Data centre operators in the UK can obtain electricity from the public network under a standard supply contract with a licensed electricity supplier, source electricity directly from one or more grid-connected generators via a bilateral power purchase agreement ("**PPA**"), or procure power from on-site generation assets or via private wire arrangements from facilities which do not supply them through the grid.

In practice, most operators that rely on the grid go further than standard supply contracts, either by entering into PPAs ("sleeved" by a licensed supplier) to gain price certainty and to ensure green benefits, or as a financial hedging mechanism. Operators opting for virtual PPAs may fall within the definition of a "commodity derivative" under the UK Markets in Financial Instruments framework, meaning that actions in relation to the virtual PPAs may constitute a "regulated activity", requiring certain authorisations or exemptions. It is, however, possible to structure virtual PPAs so that they fall within the available exemptions and are not considered commodity derivatives.

In January 2026, the government announced a call for evidence on corporate PPAs, in which it sought views from market participants as to how the UK's corporate PPA market can be developed and improved in order to help industrial and commercial offtakers (including data centre operators) secure stable, competitively priced low-carbon electricity. The government has suggested that its strategy in this area is likely to be informed by international best practice in order to improve competitiveness, increase efficiency, and remove barriers to growth.

There are no material legal restrictions on developing on-site generation assets, although the usual planning consents and environmental permits apply.

Managing network charges: the private wire opportunity

Where power is delivered through the grid, licensed suppliers bear a range of charges: Transmission Network Use of System ("**TNUoS**") charges or Distribution Use of System ("**DUoS**") charges (as applicable), Balancing Services Use of System ("**BSUoS**") charges, and Supplier Obligation levies (including policy costs passed through under the Renewables Obligation and Contracts for Difference ("**CfD**") schemes), which they typically pass through to their customers as "non-commodity" components of the supply bill. The Climate Change Levy is also payable on supplies of energy in full unless an exemption or discount applies: renewable electricity no longer attracts a blanket exemption, though a reduced rate may be available in certain circumstances. A principal advantage of using private wire arrangements is that TNUoS, DUoS, and BSUoS charges are not typically payable by customers.

Renewable energy procurement and the UK certificate regime

Data centre operators have become a driving force behind demand in the UK's corporate PPA market for renewable or low carbon electricity, and often require certificates to be provided by the counterparty to the relevant PPA to demonstrate these low carbon or renewable credentials.

The principal renewable energy certificate scheme is the Renewable Energy Guarantee of Origin ("**REGO**") regime, administered by Ofgem under the Electricity (Guarantees of Origin of Electricity Produced from Renewable Energy Sources) Regulations 2003 (as amended), under which one REGO is issued per MWh of eligible renewable electricity generated. There is currently no mandatory additionality requirement, meaning REGOs may be issued in respect of existing as well as new generation, though offtakers may impose contractual additionality criteria in their PPAs (such as requiring that the relevant generation facility achieved grid connection after a specified date). Annual matching remains the standard, but Ofgem and DESNZ have both expressed interest in developing more granular – potentially hourly – matching standards and have consulted on the future architecture of the scheme: a direction of travel that several large technology companies – including Google and Microsoft – have actively advocated. UK REGOs are no longer mutually recognised with EU Guarantees of Origin: the UK is not a member of the European Energy Certificate System, meaning UK REGOs cannot be used to demonstrate renewable origin for EU regulatory purposes, and EU Guarantees of Origin cannot be imported into the UK REGO registry. No bilateral recognition arrangement is currently in place, although discussions remain ongoing.

Large nuclear and SMR developments

In relation to nuclear, there is no regulatory prohibition on bilateral PPAs between data centre operators and nuclear generators. However, in practice, the existing fleet has historically sold output through the wholesale market. Hinkley Point C – the 3.2 GW nuclear power station currently under construction in Somerset – is supported under a bespoke CfD arrangement with a UK government-owned counterparty whose terms limit the scope for direct PPAs during the CfD term. Corporate PPAs with small modular reactor ("**SMR**") projects are areas of active commercial interest, with developers including Rolls-Royce SMR and GE Hitachi highly engaged in the UK market.

AI SUPERPOWER AMBITIONS, FISCAL INCENTIVES, AND PLANNING CONSENT

The UK has aspirations to become a global hub for AI infrastructure. The AI Opportunities Action Plan, published in January 2025 with all 50 recommendations accepted by the government, gives formal expression to that ambition. The investment case for data centre sponsors turns, in practice, on whether planning consent can be secured in reasonable time. This position has improved materially over the past 18 months, although important risks remain.

Fiscal incentives and AI Growth Zones

On fiscal incentives, the permanent full expensing regime (in force from April 2023) allows a 100% first-year deduction for qualifying main-pool plant and machinery, with up to 80-90% of new-build data centre expenditure potentially eligible. Special rate pool assets also attract a 50% first-year allowance. Five AI Growth Zones – at Culham, Blyth Cobalt Park, North Wales, South Wales, and a fifth currently under review – each target at least 500 MW of capacity by 2030, with bespoke electricity price discounts for constrained regions, and further designation expected on a rolling basis.

Critical National Infrastructure designation, cybersecurity obligations, and foreign investment controls

The security and ownership-scrutiny framework has tightened considerably. The Critical National Infrastructure ("**CNI**") designation of 12 September 2024 affords data centres prioritised access to the National Cyber Security Centre and emergency coordination mechanisms, but imposes no direct security obligations of its own. That changes with the Cyber Security and Resilience Bill, introduced November 2025 and expected to receive Royal Assent in 2026, which will designate data centres as essential services under amended NIS Regulations: applying to colocation and other non-enterprise facilities at or above 1 MW of rated IT load, and to enterprise facilities at or above 10 MW, with penalties of up to £17 million or 4% of worldwide turnover. Two features warrant particular attention. The first is the incident-notification cadence – an initial notification within 24 hours and a full report within 72 – which broadly tracks NIS2 but diverges from it in definitional detail, leaving operators with both UK and EU sites to run parallel rather than unified reporting playbooks. The second is the Bill's supply-chain dimension: operators will need to embed security testing, audit, and incident-cooperation duties into supplier and colocation contracts.

Alongside this, the National Security and Investment Act 2021 designates "data infrastructure" as one of 17 mandatory notification sectors. In the latest reporting year, the sector accounted for 14% of all notifications, making it the joint fifth most common notification basis. Foreign investment of data infrastructure is not prohibited, but CNI designation has heightened government scrutiny of cross-border acquisitions. UK GDPR imposes no data localisation requirement, although sector-specific rules—including NHS frameworks, FCA/PRA outsourcing and operational resilience rules in the financial sector, and defence networks—support or reinforce demand for UK-sited capacity.

Planning pathways: NSIP reform, fast-track routes, and judicial review risk

The two most consequential recent planning developments concern the NSIP regime and environmental challenge risk. From January 2026, data centres became eligible projects under section 35 of the Planning Act 2008, creating an opt-in route to the NSIP process, through which a Development Consent Order can consolidate planning permission, compulsory acquisition powers, and ancillary authorisations into a single instrument. The thresholds triggering mandatory NSIP treatment are to be set in a forthcoming National Policy Statement for Data Centres, with no consultation having commenced as at the date of this publication. The Planning and Infrastructure Act 2025 supports the introduction of a new fast-track route for certain NSIPs, intended to shorten the acceptance-to-decision stage from an average of around 17 months under the standard process to a non-statutory target up to 12 months for eligible projects.

Sponsors of large-scale projects should weigh the NSIP route with care: although the consolidated consent mechanism offers genuine advantages, uncertainty as to the threshold and the nascent National Policy Statement leave significant questions unresolved. The Foxglove-led judicial review of January 2026 – in which the government conceded that a 90 MW facility had been consented without adequate EIA screening – marks the first successful environmental challenge to a UK data centre consent and indicates that EIA compliance may attract heightened scrutiny. Below the NSIP threshold, the revised National Planning Policy Framework of December 2024 requires planning policies to “pay particular regard” to data centre needs, and Green Belt policy has been materially relaxed through the “grey belt” concept: three recovered appeals determined by the Secretary of State in 2024-25 each approved hyperscale campuses on Green Belt land, though one (Woodlands Park) remains subject to a live judicial review.

ENVIRONMENTAL OBLIGATIONS, EFFICIENCY, AND DISCLOSURE

The most striking structural feature of the UK's environmental framework for data centres is what it lacks: unlike the EU, which imposes mandatory power usage effectiveness and energy performance reporting on data centres through Article 12 of the recast Energy Efficiency Directive, the UK has no equivalent regime. This is a significant point of divergence for global operators and investors. The UK framework is instead built upon a combination of voluntary participation, sectoral fiscal incentives, as well as general environmental regulation and licensing, overlaid by an evolving and diverging corporate sustainability disclosure regime that may continue to tighten through to 2028 and beyond.

Energy, emissions, and water: operational constraints and incentive structures

The primary energy efficiency mechanism is the Climate Change Agreement for data centres, administered through techUK, in which over 170 sites participate. Participation delivers an approximately 93% discount on the Climate Change Levy against a 14.5% efficiency improvement target measured from a 2022 baseline to 2030. While the Climate Change Agreement applies on a voluntary basis incentivised by the discount, the UK also has a general energy efficiency regime – the Energy Savings Opportunity Scheme – which applies to any undertakings with an annual turnover in excess of £44 million and an annual balance sheet total in excess of £38 million. In-scope undertakings are required to collect information relating to their energy consumption, carry out energy audits and implement action plans to improve energy efficiency.

While the UK ETS does not traditionally apply to the data centre sector, it does apply to power generation activity, which means that installations ancillary to data centres with thermal combustion capacity at or above 20 MW (a threshold typically triggered by aggregate backup diesel energy generation of around 7.5 MW) may nonetheless fall within scope of the UK ETS, which carries significant potential cost implications.

Water is an emerging operational constraint: generally, abstraction exceeding 20 m3 per day requires an Environment Agency licence under the Water Resources Act 1991. Moreover, the first AI Growth Zone at Culham sits within a "seriously water stressed" catchment, a consideration that sponsors of large AI facilities in that zone must address from the outset. Additionally, an Ofwat consultation in August 2025 relating to water efficiency and wholesale charges for business customers has indicated that the government intends to revise the current charging structure for wholesale water supply which currently discounts charges for large-scale water users, a policy direction affirmed by the more recent Water White Paper released in January 2026. This suggests a high likelihood of increased costs for water usage in the foreseeable future, intended to drive a focus on water efficiency.

Alongside these requirements, the UK heat network and waste frameworks contain further latent obligations. The Heat Networks (Market Framework) (Great Britain) Regulations 2025, in force from 27 January 2026, regulate the supply of waste heat, including by data centres. Primary legislation, notably the Energy Act 2023, will also enable future heat network zoning that could require large non-domestic buildings to supply waste heat into local networks. No such supply obligation currently applies. Operators may also be subject to the waste duty of care under the Environmental Protection Act 1990 in respect of certain electrical equipment once it becomes waste. No data centre-specific circular economy obligations currently exist, although the Environment Act 2021 carries enabling powers for extended producer responsibility schemes that could eventually reach IT hardware.

The trajectory of sustainability disclosure

While the UK imposes no sector-specific sustainability disclosure requirements on data centres, UK requirements are likely to compel increasingly detailed and demanding disclosure over time. UK Sustainability Reporting Standards S1 and S2, adopted on 25 February 2026 and based on the International Sustainability Standards Board's International Financial Reporting Standards S1/S2 framework, adopt a single materiality approach. They also encourage disclosure in accordance with the SASB standards, including the Technology & Communications standards. This diverges from the Corporate Sustainability Reporting Directive's double materiality approach, an important difference to note for operators with reporting obligations in both jurisdictions.

Under Financial Conduct Authority ("**FCA**") proposals, mandatory climate disclosure under UK Sustainability Reporting Standard S2 (Climate-related Disclosures) is expected for listed companies from accounting periods beginning 1 January 2027, with the UK government intending to consult later this year on introducing similar disclosure requirements for large unlisted companies. The Streamlined Energy and Carbon Reporting framework already applies to quoted and large unquoted companies, while the parallel energy use reporting obligations under Phase 4 of the Energy Savings Opportunity Scheme fall due by December 2027.

The UK imposes no sector-specific sustainability disclosure requirements on data centres. As we have seen in previous chapters, the EU adopts a different approach to the data centre sector. For data centre sponsors and investors operating across both markets, this asymmetry creates an immediate practical question: whether to voluntarily align UK reporting with EU standards, or to maintain distinct frameworks. As the UK's disclosure regime matures and diverges further from EU requirements, that issue may become harder to defer.

SITE SELECTION AND REAL ESTATE STRUCTURING

The real estate workstream of developing a data centre may determine the timetable for a UK data centre project, with the acquisition of appropriate land one of the primary considerations.

Securing development land

Selecting an appropriate site for a data centre project is not an easy task. As discussed in the foregoing sections, the site must fit a number of physical and regulatory constraints that are largely outside a developer's control: firstly, proximity to a suitable grid offer, substation with available capacity or some other form of power; secondly, sufficient cooling water for operating the data centre; and thirdly, a land area large enough to house the scale of the planned project, and any potential expansion plans in the future. Consideration as to whether planning consent would be granted for the area is also required. In general, suitable land for data centre development in the UK is scarce, with competing demands from housing, energy infrastructure, farming, and other industry. Brownfield and other former industrial sites may be fruitful ground for developing data centres, however they may bring heightened risk of environmental remediation work requirements, which will require additional due diligence and potentially increase costs.

Freehold, leasehold, and long-term control

Many large data centre sites are held as freehold properties, meaning the developer owns both the building and the land it stands on, for an unlimited period of time. There is no landlord, and no expiry date. The primary alternative way to hold land in England and Wales is through leasehold structures, where the proprietary right is derived from a lease, which grants exclusive possession of a property for a defined term, subject to conditions. Ultimate ownership remain with the owner of the freehold, and, unless extended, the property reverts to the freeholder when the lease expires.

The choice between freehold acquisition and leasehold structures is rarely a pure legal question: it turns on the developer's capital strategy, the landowner's willingness to dispose, the availability of debt finance against each tenure, and the long-term operational flexibility required. Freehold ownership maximises operational autonomy, provides security of tenure and preserves residual asset value for developers, which is significant given typical 25 to 30 year operational lives for hyperscale facilities. Long leasehold structures (commonly 125 years or longer, at peppercorn or geared rents) are nevertheless prevalent where the underlying landowner is a public body, a strategic landowner, or an institution unwilling to dispose of the freehold; in such cases, particular attention should be paid to provisions of the lease so it provides the desired flexibility for the data centre project and the necessary security of tenure.

Securing easements and managing restrictive covenants

Data centre sites depend on a network of third-party rights over neighbouring land for power, water, drainage, fibre, and vehicular access, all of which are essential for their daily operations. To enact these rights, careful consideration of easements may be needed. An easement, in English law, is a non possessory property right giving its holder a defined right of use over land owned by another person. The land subject to the easement remains fully owned by the landowner, but the use of that is limited by the terms of the easement. Typical examples include a right to use water pipes or drains, use gas pipes or electricity wires, or pass over a path, road, or way.

Developers should therefore ensure that any selected site has the necessary easements and other access rights required for the data centre to function and, if not, how likely it would be for neighbouring landowners to grant the necessary access rights. Where a site is being acquired out of a larger estate that will become the neighbouring land, the developer should ensure that the transfer of the site grants these rights. In such circumstances, the developer should also consider whether it needs to restrict the use of the neighbouring land – for example, to prevent uses that could disrupt its operation as a data centre – and, if so, seek to include restrictive covenants in the transfer.

Key Contacts

BONELLIEREDE

GIORGIO FRASCA
+39 06 84551 279
Giorgio.Frasca@belex.com

GIOVANNA ZAGARIA
+39 06 84551 275
Giovanna.Zagaria@belex.com

BREDIN PRAT

FRÉDÉRIC SALAT-BAROUX
+33 1 44 35 37 76
fredericsalat-baroux@bredinprat.com

BARTHÉLÉMY COURTEAULT
+33 1 44 35 35 72
barthelemycourteault@bredinprat.com

GABRIELLE REDDÉ
+33 1 44 35 27 41
gabrielleredde@bredinprat.com

DE BRAUW

MARTJE DE VRIES LENTSCH
+31 20 577 1384
martje.devrieslentsch@debrauw.com

BAS BOUTELLIER
+31 20 577 1442
bas.boutellier@debrauw.com

JASPER VAN UDEN
+31 20 577 1576
jasper.vanuden@debrauw.com

HENGELER MUELLER

THOMAS LANG
+49 69 17095 646
thomas.lang@hengeler.com

MICHAEL SCHRAMM
++49 211 8304 723
michael.schramm@hengeler.com

JÖRG MEINZENBACH
+49 211 8304 784
joerg.meinzenbach@hengeler.com

SEBASTIAN SCHNEIDER
+49 69 17095 120
sebastian.schneider@hengeler.com

SLAUGHTER AND MAY

MIKE CORBETT
+44(0)20 7090 3431
mike.Corbett@slaughterandmay.com

SIMON BARTLE
+44(0)20 7090 3563
Simon.bartle@slaughterandmay.com

JAMES COOK
+44(0)20 7090 4216
james.cook@slaughterandmay.com

AARON WU
+44(0)20 7090 3328
Aaron.wu@slaughterandmay.com

DANIEL MEWTON
+44(0)20 7090 5909
Daniel.mewton@slaughterandmay.com

URÍA MENÉNDEZ

IGNACIO ÁLVAREZ COUSO
+34915860381
ignacio.alvarez@uria.com

JAVIER RUIZ-CÁMARA
+34915860680
javier.ruiz-camara@uria.com

BLANCA ARLABÁN
+442072601800
blanca.arlaban@uria.com

RITA XAVIER DE BRITO
+351210308643
Rita.xbrito@uria.com

CATARINA TAVARES LOUREIRO
+351213515362
catarina.loureiro@uria.com

JOÃO LOURO E COSTA
+351210308613
joao.lourocosta@uria.com

ACKNOWLEDGEMENTS

Slaughter and May - The editorial development of this report and UK chapter was led by the Slaughter and May team, comprising Mike Corbett, James Cook, Daniel Mewton, Simon Bartle, Aaron Wu, Kathryn Emmett, Ivo Trice, Faatimah Zamir, Josh von Stutterheim, and Jezneel Durogene, with support from Natalie Donovan, Emily Bradley, Annalisa Tosdevin, Bryony Bacon, Lisa Sabbage, Roshan Gulati, Julian Wong, Beckie Dean and Douglas Fraser.

Hengeler Mueller - The EU and German chapters were prepared by the Hengeler Mueller team, comprising Anouk Ludwig, Christine Hofherr, Dimitri Krupp, Jens Wenzel, Jonas Els, Jörg Meinzenbach, Luca Bellotti, Michael Schramm, Sebastian Fernkorn, Sebastian Schneider, Thomas Lang, Ursula Dahmen, and Vera Jungkind.

De Brauw Blackstone Westbroek - The Dutch chapter was prepared by the De Brauw Blackstone Westbroek team, comprising Martje de Vries Lentsch, Jasper van Uden, Josefien Vreeken, Annabel van Schaik, Max Kaumo, Welmoed Willemsen, Youri Pluis, Geertje Creijghton, Bommel van der Bend, Daniël van der Nat, Bas Boutellier, Michael Schouten, Fleur Hazewinkel, Stephanie The, Davine Roessingh, Henk van Ravenhorst, Lennart Vos and Annemijn Prakken-Versteegh.

Bredin Prat - The French chapter was prepared by the Bredin Prat team, comprising Gabrielle Reddé, Gaïane Polard, Barthélémy Courteault, Frédéric Salat-Baroux, and Leeloo Bernard.

Bonelli Erede - The Italian chapter was prepared by the Bonelli Erede team, comprising Giorgio Frasca, Giovanna Zagaria, Giovanni Guglielmo, Marilù Martoriello, Pietro Canale, Giorgia Racini, Silvia Jachia and Enrico Gaetano.

Uría Menéndez - The Spanish and Portuguese chapters were prepared by the Uría Menéndez team, comprising Blanca Arlabán, Catarina Tavares Loureiro, Ignacio Álvarez, Javier Ruiz-Cámara, Leticia López, João Louro e Costa, José Miguel Egea, Juan José Serrano, Jill de Soet Palmeiro, María Trinidad Cabrera, Miguel García, Guillermo Bermejo, Pedro Lluch, Ricardo Costa Amaro, Rita Xavier de Brito, and Esteban Avendaño.

OFFICES

BONELLIEREDE
www.belex.com
Milan, Genoa, Rome, Addis Ababa*, Brussels, Cairo*, Dubai, London
*: *in cooperation with local law firm*

BREDIN PRAT
www.bredinprat.com
Paris, Brussels

DE BRAUW
www.debrauw.com
Amsterdam, Brussels, London, Singapore

HENGELER MUELLER
www.hengeler.com
Frankfurt, Berlin, Dusseldorf, Munich, Brussels, London

SLAUGHTER AND MAY
www.slaughterandmay.com
London, Beijing, Brussels, Hong Kong

URÍA MENÉNDEZ
www.uria.com
Madrid, Barcelona, Bilbao, Bogotá, Brussels, Lima, Lisbon, London, Porto, Santiago, Valencia