HERBERT SMITH
FREEHILLS
KRAMER

NAVIGATING FOREIGN DIRECT INVESTMENT REGULATION: DATA CENTRES

What are FDI regimes?

Foreign direct investment (**FDI**) regulation is an area of increasing activity and enforcement worldwide. Against a backdrop of heightened geopolitical tensions and associated pressure to keep strategic industries 'onshore', recent years have seen further proliferation of FDI regimes and tightening of existing rules.

Under FDI regimes, national governments or agencies are able to review (and potentially block or impose conditions on) inbound investments, usually on national security or public interest grounds. Mandatory notification obligations may apply, and clearance may be required, before transactions can complete. In other cases, FDI may be regulated via "negative list" arrangements that limit or prohibit, or impose other regulatory requirements on, foreign investment in specified industries.

Mandatory FDI regimes typically apply to specified classes of investments – although agencies often have broad powers to proactively "call in" transactions on national security or other grounds. These rules are increasingly not limited to controlling interests but can capture minority non-controlling investments (eg as low as around 10% – see the table below for a sample of FDI regimes). Often there are no turnover or other materiality thresholds for FDI rules to be engaged, and decision-making can be less transparent than in other regulatory processes such as merger control. This means outcomes can be harder to predict in the absence of regular contact with an FDI agency. Significant sanctions can also be imposed for a failure to notify or completing a transaction without the necessary clearance.

It is possible (and sometimes likely) for multiple FDI regimes to apply to a single transaction – especially in significant cross-border investments. With this in mind, conducting a multi-jurisdictional FDI analysis is now an essential part of any M&A or investment due diligence exercise.

FDI and data centres: key trends

Data centres have fast become the core of modern digital infrastructure. Demand for data centre capacity continues to experience unprecedented growth globally, driven by the relentless computing requirements of generative AI, internet of things (**IoT**) integration, next-generation mobile networks, and other advanced technological applications.

This demand is forecast to outstrip supply, with demand for data centre driven cloud and AI doubling since 2021 in the US and Western Europe, and expected to nearly triple again by 2030. While the US leads the world on overall data centre capacity, other regions such as Africa, the Middle East and APAC are also experiencing unprecedented levels of demand. In turn, the collective frenzy to satisfy demand has fed concerns around compute (underlying semiconductors), energy (electricity and water), and land (planning) bottlenecks, as well as significant environmental threats.

In particular, advances in AI use cases (driven by the proliferation of AI chatbots and AI integration) have accelerated investment in data centres and their underlying infrastructure. This has predominantly been fuelled by US 'big tech' firms, which are anticipated to invest a staggering collective $500 billion in data centres in 2026 alone. However cross-border activity has also thrived, whether driven by financial investments, tapping overseas expertise, or support for government missions to scale up "sovereign AI" capabilities. By some estimates, data centres have accounted for around $170 billion of announced greenfield foreign investment annually since 2022. This momentum has continued apace – with recent reporting by UN Trade and Development (**UNCTAD**) that data centres captured more than one fifth of global greenfield investment in 2025 (making them one of the largest recipients of new investment worldwide). In October 2025 it was announced that a consortium including Abu Dhabi fund MGX alongside BlackRock, Global Infrastructure Partners (**GIP**), Nvidia and Microsoft are to acquire Texas-based Aligned Data Centers, one of the world's largest data centre operators, in a $40 billion acquisition. According to FDI Intelligence, in the first half of 2025, the overall value of data centres and semiconductor projects stood at nearly $300 billion, with 24 individual projects each worth more than $1 billion.

The strategic importance of data centres to governments is multi-fold. Vast swathes of the public and private worlds (including many critical services and capabilities) rely on this infrastructure. What's more, data centres host an enormous amount of sensitive data, while the computing power they underpin (as well as the underlying hardware) are viewed as critical to the global balance of economic and military power. The macro geopolitical significance of data centres is clear: governments worldwide are accelerating investment in data centre infrastructure and the supply chains that underpin them – a push most visible in the intensifying competition between the United States and China, which host 39% and 22% of global data centre power, respectively.

It is therefore not surprising that an increasing number of national governments have included data centres within their FDI regimes. Owners, operators, and investors must navigate evolving regulatory frameworks, with a particular sensitivity toward data centre infrastructure and capacity from a national security and critical infrastructure perspective.

Data centres increasingly in-scope of FDI regimes

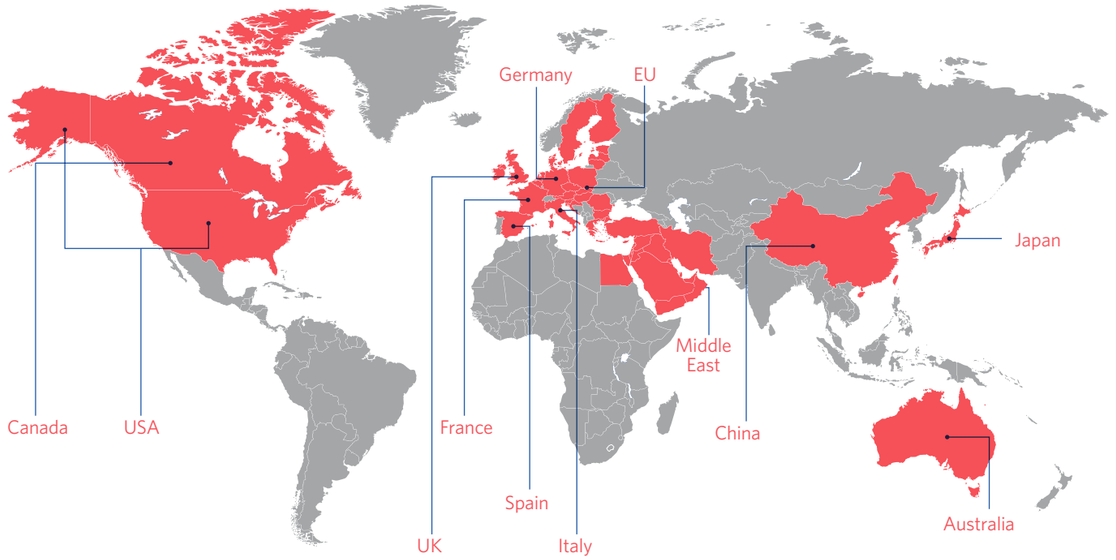
As outlined above, FDI controls are focused on protecting national security interests. While traditionally this has centred on areas such as defence (eg, military and dual-use goods or services), there has been a gradual enlargement of FDI regimes internationally to include critical infrastructure and other areas of perceived sensitivity within their ambits, such as advanced technology, communications, data, and healthcare.

Given the geopolitical, economic and technological trends discussed above, data centres are a key focus area in this expansion of regimes. In their drive to achieve 'data sovereignty', governments and national agencies have been increasingly willing to vet inbound investments in data centres, whether from the perspective of critical infrastructure, sensitive data or advanced technological capabilities.

For example, in several FDI regimes (eg, Australia, the UK, the US and many EU Member States), the processing and storage of data (particularly sensitive or governmental personal data) is itself deemed to constitute critical infrastructure. This means that in many cases, potential investors in such assets are required to obtain mandatory FDI clearance before their transaction can complete.

This regulatory attention is likely only to increase in the future given the scale of investment and strategic importance attached to data centre infrastructure. Further shifts in the regulatory environment can be seen, for example, in the UK Government's recent consultation on changes to its investment screening regime under the National Security and Investment Act (**NSIA**). If carried into effect, these amendments would expand the existing UK mandatory notification regime from capturing data centres that process certain government or public sector data, to potentially covering all third-party operated UK data centres, including certain cloud service providers (**CSPs**) and managed service providers (**MSPs**). This is expected to bring up to an additional 50 businesses within the scope of the UK mandatory filing regime. Meanwhile, the revamp of the EU's FDI Screening Regulation, on which political agreement was recently reached, is expected to include digital infrastructure within its minimum scope of sensitive sectors and key technologies subject to FDI screening by national regimes in the EU Member States.

In sum, data centres are increasingly in-scope of FDI regimes around the world – a trend that is likely to continue. Further, different rules and national priorities have manifested in fragmented FDI filing and review requirements that can lead to multiple differing filing requirements for investors, as demonstrated by the following table summarising rules and features relating to data centres across prominent FDI regimes:



Jurisdiction	Summary of FDI regime	Are data centres captured?
 Australia	Australia has an active FDI regime under the Foreign Investment Review Board (**FIRB**). Mandatory filings are required both for general real estate investments (subject to financial thresholds) and for the acquisition of 10% or more (and in some circumstances less) in "national security businesses" (with a nil financial threshold). National security businesses include businesses that hold assets defined as "critical infrastructure assets".	Yes – both from a general real estate perspective and because the categories of infrastructure assets critical to the economy include data storage and processing.
 Canada	Acquisitions of control of Canadian businesses by non-Canadians are subject to review under the Investment Canada Act (**ICA**). Critical infrastructure is a specifically designated sensitive sector under the current regime. Amendments to the ICA passed in March 2024 will also introduce a mandatory and suspensory notification and review process for foreign investments in certain defined business sectors. The sectors to be included have not yet been finalised.	Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic wellbeing of Canadians and the effective functioning of government. While not explicitly included, data centres are generally viewed as critical infrastructure.

Jurisdiction	Summary of FDI regime	Are data centres captured?
 China	There are two China FDI related approval regimes: (1) the Negative List, which prohibits foreign investment or restricts the maximum foreign shareholding in a Chinese business in specific sectors; and (2) the national security review of FDI, which applies to foreign investment in: • military related industries or entities adjacent to military facilities, or • key industries (including important infrastructure, important information technologies and internet products and services, key technologies, etc.) that concern national security, if the foreign investors obtain "actual control" over the enterprise.	Negative List: Yes, foreign shareholding in data centres in China generally cannot exceed 50%. However, China has recently implemented a pilot programme under which data centres established in certain pilot Chinese cities may be exempted from this shareholding restriction. National security review: Possibly. To be determined on a case-by-case basis.
 European Union (EU)	The EU FDI Regulation does not establish FDI screening at an EU level but creates a framework for pan-EU cooperation on FDI screening which obliges Member States to notify the European Commission (and each other) of FDI in their territory undergoing screening.	Yes – in determining whether FDI is likely to affect security or public order, Member States may consider its potential effects on, inter alia, critical infrastructure, which includes data processing or storage.
 France	France has an active mandatory and suspensory FDI regime. The following types of transactions by a foreign investor are subject to prior approval by the French Ministry of Economy if they involve a sensitive sector: • acquisition of a controlling stake in a company incorporated under French law or a branch registered in France; • acquisition of all or part of the business of a company incorporated under French law; and • transactions resulting in the foreign investor exceeding the threshold of 25% of the voting rights of a company incorporated under French law or 10% of the voting rights if the shares in this company are admitted to trading on a regulated market (except those transactions conducted by an EU Investor).	Yes – French sensitive/strategic sectors cover activities likely to jeopardise national defence interests or public order/public safety. This includes infrastructure, goods or essential services that ensure the supply of certain services – including data processing, transmission or storage activities.

Jurisdiction	Summary of FDI regime	Are data centres captured?
 Germany	Germany imposes mandatory suspensory filing requirements for investments in sensitive sectors, which are triggered if an investor obtains voting rights above specified thresholds. For example: • Obtains voting rights of 10/20% in sensitive sectors, and • Obtains additional voting rights of 20%, 25%, 40%, 50%, 75%.	Yes – various types of data centres trigger a mandatory filing obligation (eg, housing, hosting, cloud computing) when case-specific thresholds (on capacity or users) are exceeded.
 Ireland	Ireland has mandatory and suspensory filing requirements for certain sectors, including critical infrastructure, technologies and dual-use items, supply of critical inputs, access to or control of sensitive information, and media plurality.	Yes – critical infrastructure, whether physical or virtual, includes data processing or storage.
 Italy	Italy has mandatory and suspensory filing requirements. Notifications are required for transactions relating to 'strategic assets' in the sectors of energy, transport, networks, communications, as well as in other sensitive sectors.	Yes – critical infrastructure, physical or virtual, includes the treatment or archiving of data. Moreover, technologies related to on-demand service distribution for computing (servers), storage (databases) and analysis (software), configurable and available remotely, fall within the scope of Italy's FDI rules.
 Japan	Japan has a reasonably active FDI regime. The regime is generally only mandatory and suspensory in respect of certain listed Japanese companies that are active in defined sectors. These sectors include national security and public order (for example telecommunications, transportation, electricity, water supply and railway services). Acquisitions of 1% or more of the shares or voting rights in these listed companies engage the regime.	Data centres are not explicitly included. However, depending on the specific nature of the data centre business and the services it provides, it may still fall within the scope of a designated business. For example, if registration or notification under Japan's *Telecommunications Business Act* is required, the operation of a data centre may fall within the category of the designated business.

Jurisdiction	Summary of FDI regime	Are data centres captured?
 Middle East	FDI regulation in the Middle East is relatively nascent, and the majority of jurisdictions do not have FDI regimes requiring pre-notification and clearance. Although a number of jurisdictions (such as Kuwait and Oman) have a 'negative list', they generally do not expressly include the infrastructure sector nor data centres.	Data centres not explicitly included.
 Netherlands	The Netherlands has a mandatory and suspensory FDI regime applying to investments targeting designated vital providers active in sensitive technology and operate a business campus, or companies active in the field of highly sensitive technologies. The Netherlands also has sector specific FDI rules for Gas, Electricity and Telecommunications.	Data centres are not explicitly included in The Netherlands' primary FDI regime. However, the telecommunications sector specific rules apply to parties with relevant influence in the Dutch telecommunications sector – including data centres. These rules capture data centre services with a power capacity exceeding 50 Mw or providing hosting services for more than 400,000 domain names with a ".nl"-extension.
 Spain	Spain has a mandatory suspensory FDI screening regime, which applies when a foreign investor acquires a shareholding of 10% or more in a Spanish company/asset, or otherwise acquires effective control of the company/asset in certain restricted sectors. The regime also applies for UE/EFTA investors when the investment exceeds EUR 500 million, or if the acquired company is publicly listed.	The Spanish FDI rules do not establish any express reference in relation to data centres. However, they may be included under the FDI regime through other categories (eg if declared as critical infrastructure/fundamental inputs).
 UK	Under the National Security and Investment Act (**NSIA**), a mandatory and suspensory notification obligation applies to investments passing through 25%, 50% or 75% shareholdings in a target entity carrying out activities in the UK in one or more of 17 specified sectors.	Yes – the specified sectors capture a broad range of activities including data infrastructure (for example data centres, cloud storage services and data storage, processing and transmission).

Jurisdiction	Summary of FDI regime	Are data centres captured?
 United States	The USA has an active mandatory FDI screening regime, administered by the Committee on Foreign Investment in the United States (**CFIUS**). Notification under the CFIUS regime is largely voluntary and mandatory filings are generally only required (i) where the US target business produces or develops a product that is subject to US export control regulations or (ii) where a foreign government owns 49% or more of the investor and the investor will acquire 25% of more of a US business, where in both instances the US target business involves certain critical technology, sensitive personal data, or critical infrastructure. Critical infrastructure is assessed on a case-by-case basis.	Potentially – critical infrastructure sectors include assets, systems, and networks, whether physical or virtual, that are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. Not all data centres are treated as critical infrastructure (eg data centres co-located at submarine cable landing points are explicitly mentioned as being critical infrastructure). Whether a data centre is considered critical infrastructure will depend on location, what data is being handled, and whether the operator has access to or control over it.
 Other Countries	N/A	Examples of other FDI regimes that also broadly involve protections for data centres/storage (either explicitly or through the inclusion of 'critical infrastructure' related to data processing/storage) include: Austria, Belgium, Czech Republic, Fiji, Finland, Latvia, Luxembourg, Malta, Moldova, Monaco, Poland, Portugal, and Slovenia. Switzerland's new FDI regime, expected to come into force in 2027, may also capture data centres under critical IT systems/infrastructure – however this regime uniquely applies only to state-controlled investors (ie private foreign investments are not captured).

Conclusion

FDI regulation has been an increasingly prominent factor for cross-border M&A transactions for a number of years. Within this, data centres have become a focal point of attention for FDI agencies due to their strategic importance, turbo-charged by voracious scaling-up as a result of generative AI and other applications.

As technologies and demand continue to develop further, it appears that these trends will only accelerate as governments around the world prioritise secure ownership and operation of data centres to drive economic growth, 'data sovereignty', and support for critical capabilities.

Timely assessment and consideration of multi-jurisdictional FDI filing requirements has never been more important for data centre investors to mitigate these multi-fold threats to deal timelines and deliverability. With careful planning and expertise, complemented by effective advocacy and (where appropriate) thoughtful government relations strategies, these challenges can be successfully navigated without becoming ensnared in the broader geopolitical web.

Contacts

UK, US, EMEA

Veronica Roberts
Partner, Global Foreign Direct Investment Group Lead, London
T +44 20 7466 2009
veronica.roberts@hsfkramer.com

Joseph Falcone
Partner, New York
T +1 917 542 7805
joseph.falcone@hsfkramer.com

Kyriakos Fountoukakos
Global Head of Competition, Brussels
T +44 7920 455 155
kyriakos.fountoukakos@hsfkramer.com

Dr Marius Boewe
Partner, Düsseldorf
T +49 211 975 59066
marius.boewe@hsfkramer.com

Iria Calvino
Partner, Madrid
T +34 91 423 4022
iria.calvino@hsfkramer.com

Christopher Theris
Partner, Paris
T +33 1 53 57 65 54
christopher.theris@hsfkramer.com

Francesca Morra
Partner, Milan
T +39 02 3602 1371
francesca.morra@hsfkramer.com

Jean Meijer
Partner, Johannesburg
T +27 10 500 2642
jean.meijer@hsfkramer.com

Chris Walters
Partner, Dubai
T +971 4 428 6338
chris.walters@hsfkramer.com

Laurence Bary
Partner, Paris
T +33 6 18 11 47 83
laurence.bary@hsfkramer.com

APAC team

Stephen Dobbs
Partner, Sydney, Australia
T +61 2 9225 5511
stephen.dobbs@hsfkramer.com

Nanda Lau
Partner, China
T +86 21 23222117
nanda.lau@hsfkramer.com

Adelaide Luke
Partner, Hong Kong
T +852 21014135
adelaide.luke@hsfkramer.com

Graeme Preston
Partner, Tokyo
T +81 3 5412 5485
graeme.preston@hsfkramer.com

For a full list of our global offices visit **HSFKRAMER.COM**