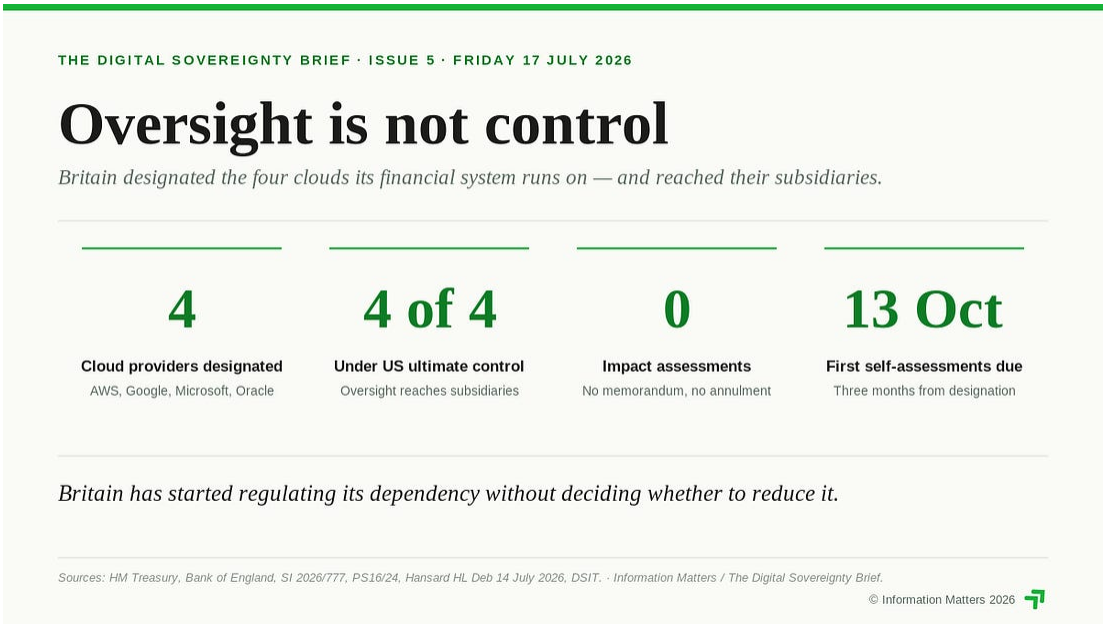
The Digital Sovereignty Brief #5 — "Oversight is not control"

The UK designated the four cloud providers its financial system runs on — and reached their Luxembourg, Irish and UK subsidiaries, not the US parents that control them. Parliament cannot annul it.

MARTIN DE SAULLES
JUL 16, 2026

The Digital Sovereignty Brief · Issue #5 · Friday 17 July 2026 *A weekly read on UK digital sovereignty: who owns the tech, where the data lives, and where it could be cut off.*



> **SOVEREIGNTY WATCH — the first UK Critical Third Party designations.** On 10 July HM Treasury announced its first

> designations under the Critical Third Parties regime, with effect from 13 July. Microsoft Ireland Operations Limited is one of the four. When we scored Microsoft 365 we said we would re-score it if this happened, so we will, and we will publish the working. Our provisional read is that it does not move: the regime covers operational resilience, and changes nothing about jurisdiction or ownership, so the verified score of 3.6 out of 5 should hold.

The week in six lines:

- **The UK designated its first four Critical Third Parties, and all four are US-owned.** On 10 July HM Treasury announced the designation of Amazon Web Services EMEA SARL, Google Cloud EMEA Limited, Microsoft Ireland Operations Limited and Oracle Corporation UK Limited, with effect from Monday 13 July. Joint Bank of England, PRA and FCA oversight began that day. Until then the register had been empty.
- **The regime reaches subsidiaries, not owners.** Three of the four designated entities are incorporated in Luxembourg or Ireland rather than Britain, and every one of them sits beneath a US parent. The Bank of England says in its own notes that "designation under this regime is not the same as authorisation by the regulators".
- **The instrument doing it is two pages long, and Parliament cannot annul it.** SI 2026/777 carries no explanatory memorandum and no impact assessment, and section 429(8) of FSMA excludes designation regulations from the annulment procedure. The

consultees were the three regulators and the four companies being designated.

- **The rules applied from Monday, and the Treasury Committee wants AI firms considered next.** Interim self-assessments are due with the regulators within three months, around 13 October. Dame Meg Hillier says she believes the time may come to designate specific AI firms too.
- **The Lords debated the same dependency four days later.** At the Cyber Security and Resilience Bill's second reading on Tuesday 14 July, Baroness Kidron told the House that "a truly secure cyber policy is a sovereign one", and a digital sovereignty strategy amendment that the Commons never reached is heading for Grand Committee.
- **Britain has started regulating its dependency without deciding whether to reduce it.** Supervising the four is a real improvement. It is not a reduction in exposure, and nothing announced this week was.

The UK now supervises the four cloud providers its financial system runs on. That is a real improvement, and the first time the state has done something about this dependency rather than describe it. But the supervision attaches to the Luxembourg, Irish and UK subsidiaries, under an instrument neither House can vote on, in a regime the regulators themselves say covers resilience rather than authorisation. The cut-off risk we measure sits with the US parents, and a UK regulator has no power to designate those.

Ownership & control

The first four Critical Third Parties are all US-owned. On 10 July HM Treasury announced that it had designated Amazon Web Services EMEA SARL, Google Cloud EMEA Limited, Microsoft Ireland Operations

Limited and Oracle Corporation UK Limited as Critical Third Parties under the Financial Services and Markets Act, by SI 2026/777, with effect from 13 July. The Bank of England, PRA and FCA began joint oversight that Monday. AWS's designated entity is incorporated in Luxembourg, Google's and Microsoft's in Ireland, and only Oracle Corporation UK Limited is a UK company — which Companies House shows is itself 75%-plus controlled by another UK holding company. All four ultimately answer to a US parent. Naming them at all is progress. But the entities named are not the entities that decide.

Why it matters: our test for control has never been where the head office is, and this is the cleanest illustration yet of why. A UK regulator can now require Microsoft Ireland Operations Limited to map its services and file a self-assessment. It cannot require Microsoft's US parent to keep serving a British bank, and nothing in the designation touches the US legal instruments that reach the data. Designation makes the dependency visible and supervised. It does not reduce it. That is not a criticism of the Treasury — it is the limit of what a domestic resilience regime can do, and it is why a resilience answer is not a sovereignty answer. HM Treasury · Bank of England · SI 2026/777

Briefly: Railpen's consortium has until 5pm on Monday 20 July to put up or shut up on IP Group, which holds stakes in Oxford Nanopore and First Light Fusion; the deadline can only be extended with the Takeover Panel's consent. No firm offer had been announced as this issue closed. The board has now rejected four approaches, the most recent a cash-plus-shares-plus-contingent-payment structure implying 69.4p a share excluding the contingent element — against a last-reported net asset value of 110.4p, a 37% discount. If it lands, a portfolio of British deep-tech stakes passes to British pension capital, which is the rare ownership story that moves in our direction. IP Group's response.

The National Security and Investment Act register was quiet: no final orders published between 9 and 16 July, the most recent being 1 July.

Call-ins are not published, so this covers only what the Cabinet Office puts on the record.

Data & infrastructure

Microsoft's EU Data Boundary has not moved in three months, and the last substantive thing it did was widen. We check the change log every week. The most recent entry remains 13 April, a housekeeping removal of a discontinued product. The last substantive change was 3 April, when Microsoft added Copilot experiences across Microsoft 365, Dynamics 365, Power Platform and Copilot Studio to the list of services that transfer a subset of customer data, pseudonymised personal data or professional-services data out of the boundary on an ongoing basis. Before that, on 7 January, Anthropic models within Microsoft's generative AI services were added to a related list — the continuing data transfers that apply to every service inside the boundary.

Why it matters: the EU Data Boundary is the most-cited residency commitment in European enterprise IT, and the direction of its last two substantive entries is outward — the AI layer being bolted onto the productivity stack is the part that leaves. For UK buyers it was never a UK commitment in the first place. Three months of no change does not mean the commitment is weakening. It does mean the only recent movements have been additions to the transfer-out list, which is reason enough to keep reading it. Microsoft EU Data Boundary change log.

Briefly: Xlinks has postponed the public information days advertised for this week on its proposed 850-acre data campus between Great Torrington, Huntshaw and Weare Giffard in Devon — a 1.5GW AI compute site plus a transmission-scale battery project — moving them "to later in the year" as a petition against the scheme passed 23,500 signatures. Worth noting for two reasons. The developer is UK-controlled on the face of the Companies House register, which makes it unusual among schemes of this size. And on Xlinks' own account this is a district-council application to Torridge, with a consultation carrying

no statutory deadline — which is why it can be moved at will, and why "consultation" on a project of this scale is worth reading closely wherever you meet it. Xlinks. · North Devon Gazette.

Nothing to report on data residency itself this week. No UK or EU residency commitment, sub-processor change or AI-supplier change dated inside the window survived checking — several candidates that search results placed in July turned out on reading to be from March 2025 or January 2026.

Reports & analysis

A £1bn cloud-outage number, and an argument about the denominator underneath it. The Cyber Monitoring Centre, a non-profit that categorises cyber events affecting UK organisations, published research on 9 July with Parametrix, an insurance managing general agent, estimating that a 24-hour failure of AWS's Dublin region would cost UK companies around £1bn in direct revenue, and the Northern Virginia region £650m. AWS rejected it on 13 July: the scenario is "unrealistic", a complete 24-hour regional failure "has never occurred for any major cloud provider", real outages are partial and usually resolved in hours, and the model ignores availability-zone failover. AWS also noted that Parametrix sells cloud-outage insurance, and said the interest was not disclosed in the report. Separately, the CMC's own press release and Computer Weekly's account of the document itself give materially different figures for how many UK companies depend on cloud for critical functions — the release states a share of companies, the reporting describes that share as revenue-weighted, with the unweighted number far lower.

Why it matters: all three parties here have a fair point. AWS is right that total regional failure is not the base case, and right that an insurer has an interest in a large number. The CMC is right that region-level concentration is a real exposure UK boards have not priced. But the number we would actually want — how many UK firms would stop

trading if one region went dark — is the one being reported two different ways, and an unweighted count and a revenue-weighted share are the difference between a niche problem and a systemic one. The report sits behind a lead-capture form and we have not read it, so we are reporting the dispute and not adjudicating it, and we are not printing figures we cannot check. Neither the CMC nor Parametrix has publicly answered AWS's disclosure point. Our ask is narrow: whichever basis the headline figure uses, say so in the sentence that carries it. Cyber Monitoring Centre · Computer Weekly · Commercial Risk

Chatham House argues for sovereignty by coalition, and against both autarky and dependence. Alex Krasodomski, who directs Chatham House's Digital Society Programme, published an expert comment on 13 July arguing that "a strategy resting on proximity to the US alone looks less sensible with every passing day", and setting out what he would tell an incoming government. Do not try to out-build the US or China on compute: build enough sovereign onshore capacity for critical inference, and commit the surplus to British start-ups and universities. Do "distinctive things well at home", including digital identity and AI in public services, as "a piece of digital public infrastructure that makes everyday life easier". And "pool what you can" — sovereignty maximised through coalitions with other middle powers rather than "hopeless attempts at autarky" and "rickety national silos", citing David Eaves at UCL on NATO cloud interoperability as a way to pool demand and weaken single-vendor lock-in.

Why it matters: this is an argument rather than a finding — it carries no original data, and it should be read as Chatham House's position. It is also the most serious attempt we have seen this month to answer the question the select committee, the Bank and the Cloud Challenge Book have all now posed and left open. "Enough for critical inference" is a testable proposition, unlike gigawatt announcements, and it is the sort of specification our Sector Exposure work could score against. Where we would push: pooling with middle powers still leaves the question of

who controls the pooled stack, and NATO interoperability has not historically produced non-US infrastructure. Chatham House.

Regulation & policy

The instrument bringing four systemic cloud providers under UK supervision is two pages long, and neither House can vote on it. SI 2026/777 was made on 8 July by two Lords Commissioners of the Treasury. It has no explanatory memorandum and no impact assessment — legislation.gov.uk records no associated documents, and the instrument's own explanatory note says a full assessment "has not been produced… as no, or no significant, impact on the private, voluntary or public sector is foreseen". It carries no date of laying before Parliament, and section 429(8) of FSMA expressly excludes regulations made under section 312L from the annulment procedure. What section 312L does provide is a private safeguard rather than a parliamentary one: the Treasury must consult the Bank, PRA and FCA, and must give written notice to the firms it intends to designate, with a reasonable period for them to make written representations. The recitals confirm that happened. No public consultation was held and no consultation response was published.

Why it matters: we are not alleging impropriety — designation is an executive act, closer to a listing decision than to legislation, and Parliament chose this architecture when it passed the 2023 Act. But the practical shape is worth stating plainly. A decision that four named foreign-controlled companies are systemically important to British finance was taken by a two-page instrument, with no impact assessment, no parliamentary procedure, and a consultation whose only participants were the regulators and the companies themselves. Say the same regime is later pointed at an AI provider, as the Treasury Committee's chair has now suggested it might be: that would be a significant judgement about which foreign firms Britain's financial

system cannot do without, made through the same door. SI 2026/777 as made · FSMA section 312L · FSMA section 429

The rules applied from Monday, and the Treasury Committee has AI firms in mind next. The rulebook the designations activate was finalised in November 2024 and has been in force since January 2025, so it applies on designation rather than after a general grace period — a defined subset of requirements carries a transitional period, listed in the regulators' supervisory statement. Six CTP Fundamental Rules apply from the start. Each designated firm must file an interim self-assessment with the regulators within three months, around 13 October, and must have mapped its services and produced an incident management playbook within twelve. Thereafter the annual self-assessment must be shared, redacted, with the firms it serves — the provision most likely to change what UK financial institutions actually know about their own suppliers. One respondent asked the regulators for a twelve-month implementation period; they declined, and kept the three-month self-assessment deadline over five respondents' objections, conceding it "will be challenging for CTPs". Dame Meg Hillier, chair of the Treasury Committee, welcomed the designations on 10 July — her committee recommended them in January — and added: "I believe there may come a time when the government needs to consider designating specific AI firms under the Critical Third Parties Regime."

Why it matters: the most consequential provision is the shared self-assessment. Firms have spent years unable to get straight answers from hyperscalers about concentration and exit, and a regulator-mandated document landing on the buyer's desk shifts that balance a little. The AI point matters too: designating a frontier model provider would be the first time the British state formally recognised a US AI lab as infrastructure its financial system depends on. Given what the last two months have demonstrated about who controls access to those models, that recognition would be honest — and would make the gap between

supervision and control considerably harder to look away from. Bank of England · PS16/24 · SS6/24 · Treasury Committee

Four days later, the Lords spent three and a half hours on the same dependency. The Cyber Security and Resilience Bill had its second reading on Tuesday 14 July, running to 9.20pm across 31 speeches, and was committed to a Grand Committee whose date has not yet been announced. The Bill brings data centres above a threshold into scope as regulated essential services and captures large and medium managed service providers — these "comprise fewer than one in 10 of the MSPs active in the UK but account for around 97.6% of the UK's MSP revenue", the minister said — with 24-hour and 72-hour incident reporting and powers to designate critical suppliers. The sovereignty argument ran through the debate. Baroness Kidron said the Bill "focuses primarily on what a limited set of companies and service providers should do and too little on the resilience of the wider digital system", and put it directly: "Over the last two years, we have seen the way in which dependencies on US tech have muted our ability to protect children and creatives and made our NHS, government data and our economy vulnerable. A truly secure cyber policy is a sovereign one." Baroness Bennett told the House that Siân Berry had tabled a Commons amendment — never reached — that would require the government to maintain a digital sovereignty strategy assessing, among other things, "extra-territorial legal requirements that may be imposed on non-domiciled suppliers". Baroness Ludford asked why the government had "diverged rather decisively from the EU model".

Why it matters: the Berry amendment is worth tracking. Its second limb is the CLOUD Act and FISA 702 problem written into legislative text — the first time we have seen the extraterritorial-reach risk our framework scores named in a British bill rather than a committee report. It was not debated in the Commons and it now has a second chance in Grand Committee, where the arithmetic is different and Kidron, Bennett and Alton have all signalled intent. A duty to publish a digital sovereignty

strategy would not itself reduce a single dependency. It would force the government to write down which ones it has, which is more than any instrument currently requires. Hansard, HL Deb 14 July 2026, cc565–624.

And on Wednesday, DSIT asked industry whether the government should have a position on the sovereignty of UK data at all. A call for evidence, *Data flows you can trust*, opened on 15 July and closes on 9 September. Theme 4 asks whether there would be "merits or risks in a more explicit position from the Government on the 'sovereignty' of UK data", defining the term as "the level of control and access organisations and governments have over their data". It asks organisations to report "any requests you encounter from public authorities in other countries to access data that you hold, either in the UK or when stored abroad". Elsewhere the paper defines a transfer to include "transfer by access" — where data stays in the UK and is reached from overseas — and asks how "distributed cloud infrastructure impacts your knowledge of where data is transferred to". Two companion calls opened the same day, on data regulation for AI and on public-sector data re-use.

Why it matters: the department is asking because the position is not settled. This is the most direct set of questions Whitehall has put to industry on the subject, and "transfer by access" is the concept most UK buyers get wrong — the belief that data held in a UK region is beyond foreign reach, which is the assumption our Sector Exposure Profiles keep finding underneath sovereignty claims. The department is asking the right questions eight days after Parliament said it had no coherent framework. We intend to respond, and we will publish what we send. Data flows you can trust.

Subscribed