ALTLIBRE POLICY PAPER

A UK Digital Sovereignty Act

A policy proposal: the base layer beneath all UK data protection legislation

ADRIAN HOLLISTER · ALTLIBRE · VERSION 1.2, 21 SEPTEMBER 2026

ABOUT THIS PAPER

A UK Digital Sovereignty Act

AUTHOR

Adrian Hollister, founder, AltLibre · altlibre.com

VERSION

Version 1.2, 21 September 2026

STATUS

Policy proposal for discussion, in green paper format.

SUGGESTED CITATION

Hollister, A. (2026). *A UK Digital Sovereignty Act: a policy proposal.* AltLibre policy paper, version 1.2, 21 September 2026.

ALTLIBRE

AltLibre is a European digital sovereignty initiative. It exists to help European organisations keep control of their data, their infrastructure and their choices. This volume follows two earlier papers in the series "Your AI answers to a foreign government": Part 1 examined the documented record of American and Chinese AI providers, and Part 2 set out the European answer. Both are at altlibre.com/blog.

METHOD

Every factual claim carries a dated reference. Annex C lists the sources. Judgement is labelled as judgement.

CONTENTS

In this paper

Foreword

Within four years of Royal Assent, every critical dependency in the public estate could be registered, classified and signed for by a named minister. Every sensitive contract could carry an exit that has been rehearsed rather than assumed. The keys protecting the state's most sensitive data could be held by the state itself. Asked in Parliament who can switch off the health service's data platform, a minister could answer from a register, not from hope.

The benefits arrive in a practical order. Knowledge first: a state that can list what it would lose stops discovering its dependencies in other people's press releases. Negotiating strength next: a buyer who can show a rehearsed exit negotiates differently, and suppliers price that difference into renewals without being asked. Then capability: a published register turns unavoidable public spend into a pipeline that British hosting, custody and evaluation firms can raise money against, while the duties create the skills those firms hire. Accountability throughout: an annual statement to Parliament, signed by name, replacing a silence that has suited everyone except the public.

The larger prize is a place at the rule-making table. The states that set the terms for the next decade of digital infrastructure will be those that can demonstrate, in statute and in operation, what control looks like. Britain has the drafting machinery, the procurement weight and the research base to be one of them. Estonia showed what a small state can do with legal imagination; Britain can do it at a scale that moves markets. None of this requires technology that does not exist, money not already being spent worse elsewhere, or powers Parliament has not granted before. It requires the decision. This volume is the decision, drafted, and chapter 19 lists the points where I most want it challenged.

Adrian Hollister, September 2026.

In brief

38
dated references

Britain's data laws regulate how information is used. None of them regulates who ultimately controls it. The UK GDPR governs processing. The Data (Use and Access) Act 2025 modernises sharing. The Online Safety Act polices content. The Investigatory Powers Act governs interception by British authorities. Every one of them assumes the infrastructure underneath answers to British law, and every one of them is wrong about that, because the infrastructure underneath is overwhelmingly American, rented, and compellable under the CLOUD Act wherever in the world it sits.

This is silent dependence: reliance on foreign-controlled infrastructure that nobody has mapped, nobody has signed for, and nobody has rehearsed losing. Every recent shock in this volume entered through that gap. The £31 billion Tech Prosperity Deal, suspended by Washington as negotiating pressure three months after signature [1][2]. The US federal ban on Anthropic, imposed in February 2026 because an American company declined to permit mass domestic surveillance [3]. The £330 million NHS Federated Data Platform, procured from a foreign-controlled supplier, now urged scrapped by two parliamentary committees, with its break clause due in early 2027 and no rehearsed exit [4][5]. Over £1 billion a year of public cloud spending, concentrated on three American firms [6]. And the EU adequacy decisions on which UK-EU data flows depend, expiring on 27 December 2031, in a Europe that has just tabled its own sovereignty statute [8][9].

This volume proposes the missing layer: a Digital Sovereignty Act, designed as the foundation on which existing and future data legislation rests. Its architecture is six duties, each mapped to an existing institution, each summarised in a sentence:

Register the dependencies. Test the control. Rehearse the exits. Hold the keys. Gate the buying. Report to Parliament.

Register the dependencies. Every public body and operator of essential services maintains a register of critical digital dependencies: provider, parent jurisdiction, hosting, compellable law, data classes, exit provisions. Reported annually to DCMS, audited by the National Audit Office, published in summary. First register within twelve months of Royal Assent.

Test the control. Each dependency is classified S0 to S3 by an effective control test: who owns the parent, whose law can compel them, who holds the encryption keys. A provider that fails a question cannot be classed as sovereign-controlled, whatever its marketing. Microsoft said the quiet part under oath in Paris in June 2025; the Act writes that admission into British law [14][15].

Rehearse the exits. For sensitive and sovereign tiers, contracts must carry data export in open formats, twelve months' notice of withdrawal, escrowed configurations, and portability of AI fine-tunes. Departments run a switch-off exercise for every sovereign-tier dependency at least every two years, reported to the NCSC.

Hold the keys. For the sovereign tier, encryption keys are held by the public body or a UK-controlled trustee, so a warrant served abroad on a provider holding ciphertext yields ciphertext. Regulated finance already works this way; the state meets the standard its own regulators expect of banks [29].

Gate the buying. The Procurement Act 2023 supplies the mechanism; the Act supplies the criteria. Sensitive-tier tenders must answer the control test, carry continuity terms, and, where bids are otherwise equal, prefer the sovereign-controlled bid. Small suppliers get a simplified lane [12].

Report to Parliament. An annual Digital Sovereignty Statement, laid by the responsible Secretary of State: the consolidated register, exercise results, classification movement, and every sovereign-tier dependency where a minister has accepted foreign control, named and justified. Ministers may still choose dependence. They must sign for it in public.

The Act bans nothing, localises nothing by default, creates no new regulator, touches no treaty, and leaves private business alone beyond the essential-services operators already subject to resilience duties. It prices and labels everything. Its precedents are running elsewhere: Estonia's data embassy has operated since 2018 [22][23], Australia's Hosting Certification Framework since 2021 [25][26], France's SecNumCloud corporate-structure tests for years [28], and the EU tabled its Cloud and AI Development Act in June 2026 [9]. Britain is being asked to catch up, not to experiment.

The chapters that follow set out the problem, the design, the deliverability and the engagement. Annex A collects the quotable lines. Chapter 19 asks the questions that need better answers than this volume yet has.

The Act at a glance

TABLE. THE ACT AT A GLANCE

Element	Mechanism	Applies to	Institution
Part 1: Sovereignty register	Annual register of critical dependencies, audited and published in summary	All public bodies, essential-service operators	DCMS, NAO
Part 2: Classification	S0 to S3 tiers via the effective control test: ownership, compellable law, key custody	Every registered dependency	Office for Digital Sovereignty
Part 3: Continuity duties	Data export, notice periods, escrow, fine-tune portability, switch-off exercises	S2 and S3	NCSC, contracting authorities
Part 4: Key custody	Customer or trustee-held encryption keys	S3	Public bodies, NCSC guidance
Part 5: Procurement gates	Control-test disclosure, continuity terms, sovereign tie-break, SME lane	New S2/S3 contracts	CCS, Procurement Act 2023
Part 6: AI and weights	Model registration, behavioural-change approval, open-weights preference	Public-service AI, S2/S3 analytical AI	Cabinet Office, DBIST
Part 7: Accountability	Office for Digital Sovereignty, annual statement, ministerial sign-off	Government-wide	DCMS, ICO, NCSC, NAO
Part 8: Alignment	Tier mapping to EU CADA, treaty carve-outs	International	DCMS, FCDO

The statute book regulates use but not control.

1

The missing layer

Walk the current settlement statute by statute and one absence repeats.

The UK GDPR and the Data Protection Act 2018 constrain how personal data is processed: the purposes, the fairness, the security measures, the rights of the subject. They are deliberately indifferent to who owns the processor, provided the processing itself is lawful and any international transfer has an approved mechanism. A processor owned in a foreign jurisdiction, compellable under a foreign intelligence statute, is entirely compliant, provided the paperwork is in order.

The Data (Use and Access) Act 2025, which received Royal Assent on 19 June 2025 and commenced in stages through early 2026, modernises sharing: smart data schemes, digital verification services, updated legitimate interests, a restructured Information Commission [11]. It is a good statute about flows. It says nothing about control.

The Online Safety Act 2023 regulates content. The Investigatory Powers Act 2016 governs access to communications data and interception by British authorities under British warrants. The Product Security and Telecommunications Infrastructure Act 2022 and the NIS Regulations 2018 address the security of networks and essential services against attackers. The Procurement Act 2023, in force since 24 February 2025, tells public bodies how to buy, with new duties on transparency and supplier performance [12].

Security law asks whether a system is safe from attackers. Data protection law asks whether processing is fair and lawful. Procurement law asks whether the buying was honest. Not one of them asks the question that decided every crisis in this volume: whose law does the operator answer to, who can switch the service off, and who can change what it does without asking us?

That unasked question is the missing layer, and it is why this proposal is drafted as a foundation rather than an amendment. The Digital Sovereignty Act is the substrate those statutes assumed existed, not a patch to the UK GDPR and not a schedule to the Procurement Act: the layer that establishes whether Britain continues, controls and verifies the services beneath everything else.

Three properties define the layer, each testable, none novel:

Continue. The service survives provider withdrawal, whether that withdrawal is commercial, political or compelled. Not "we believe it would survive". Rehearsed, timed, evidenced survival.

Control. Decisions about the service, its data, its behaviour and its future are made under UK law by parties UK law can reach. Not "the UK subsidiary decides". Effective control, traced to the parent.

Verify. Britain can inspect what the service does, including with its data and its models, and can detect material change. Not "the provider attests". Inspection with rights behind it.

A state that has all three is sovereign over its digital estate. A state missing any one of them is a customer hoping the contract holds. Britain today is the second, and the next chapter explains how deliberate choices, individually reasonable, produced that outcome.

2

How we got here

Britain did not lose control of its digital estate. It sold, rented and rationalised the estate away, one sensible decision at a time. Silent dependence was not imposed. It accumulated through four eras, each with its own logic.

The outsourcing era. From the 1990s, government concluded it was bad at running technology and should buy outcomes instead. The logic was fiscal and managerial: transfer risk, pay for results, let specialists specialise. What it produced, documented most painfully by the Post Office Horizon scandal, was a state that could no longer see inside its own systems. The Institute for Government's analysis of Horizon identified the enduring lessons. Public bodies staff contract management more thinly and more juniorly than suppliers staff their side. Proprietary systems cannot be switched off or handed to a competitor, so failing suppliers get renewed because there is no viable alternative. Horizon itself was meant to be replaced in 2023; Fujitsu's separate contract for the Police National Computer was extended in 2022 because, in the Home Office's own words, no viable alternative existed [21]. The lesson generalises: a dependency you cannot exit is a tenancy at the supplier's pleasure, whatever the contract says.

The cloud-first era. In 2013 the coalition government adopted a cloud-first policy for central government: prefer cloud over ownership, public cloud over private. As an antidote to the outsourcing era's bespoke monstrosities, it was right. It also changed the nationality of the state's infrastructure. Within a decade, the default destination for a government workload was an American hyperscaler, procured through frameworks that made the default easy and the alternative effortful. Public cloud spend passed £1 billion a year and kept climbing, overwhelmingly with three US firms [6].

The platform era. By the early 2020s the hyperscalers were no longer selling hosting but platforms: identity, databases, analytics, machine learning, all tightly integrated and deliberately sticky. Exit costs stopped being a contract clause and became an engineering programme. The state of digital government review in January 2025 found fragmentation, duplicated procurement and £45 billion a year in unrealised savings from better digital management [13]. The same fragmentation that wastes the money hides the dependency map: no official can produce, on one page, the list of systems whose loss would stop a public function.

The AI era. The AI Opportunities Action Plan of January 2025, all fifty recommendations accepted by the government, set the ambition in Matt Clifford's phrase: Britain should be "an AI maker, not just an AI taker" [19]. A year on, the delivery ledger shows £68 billion of pledged investment, five AI Growth Zones and a tenfold increase in AI compute capacity from 2024 levels [20]. The energy is real, and so is its direction: almost all of it is investment in capability, and almost none of it is control. The plan's Sovereign AI recommendation produced a unit with £500 million to invest and no powers over who owns, compels or can switch off the resulting services [10]. The December 2025 suspension of the Tech Prosperity Deal, £31 billion of that pledged investment held up as a negotiating lever over the digital services tax, showed what investment without control is worth when the politics turns [1][2]. Capital without control is subsidy, not sovereignty.

Each era made sense on its own terms. The cumulative result did not get chosen at all: a state whose hospitals, tax system, police and armed forces run on platforms owned in other jurisdictions, under contracts written for a world in which suppliers are never used as pressure. That world ended. The next chapter lays out the evidence.

3

The evidence

£31bn
suspended three months after signature

Invisible dependence, not dependence itself, is the sin. The case for the Act does not rest on what foreign states or foreign companies might do. It rests on what they have already done, documented, dated and sourced. The evidence falls into three mechanisms, matching the three properties of the missing layer.

The switch: services can be turned off

December 2025: the Tech Prosperity Deal. In December 2025, three months after signing it, the United States suspended the £31 billion technology partnership with Britain [1][2]. The deal had covered Microsoft's £22 billion AI supercomputer commitment, Google's Hertfordshire data centre and a UK arm of the Stargate programme. Washington cited frustration with the UK's digital services tax, online safety rules and food standards. Number 10 was left briefing that talks remained active. Whatever the deal's merits, the episode established a fact: Britain's technology strategy is now explicitly treated by its closest ally as negotiating stock, and Britain's discovery channel for that fact was a newspaper.

February 2026: the Anthropic ban. The US government ordered every federal agency to stop using Anthropic, an American company, after it refused to strip two clauses from its acceptable use policy: no mass domestic surveillance of Americans, no fully autonomous weapons. The Pentagon designated the company a supply-chain risk and instructed defence contractors to sever commercial ties [3]. The courts pushed back, but the instruction to every dependent, including British ones, is plain: access to American technology is revocable by the American state, at speed, for reasons decided in Washington. If they will do it to their own most safety-conscious lab, they will not pause over a subcontractor in Cheltenham.

The running record. OpenAI cut API access to China with days of notice in July 2024 [31]. Microsoft suspended cloud services to Nayara Energy, an Indian refiner, in July 2025, enforcing EU sanctions that India had not adopted and no law required it to enforce; service returned only after court action in New Delhi [34]. None of these decisions was unlawful. They were contractual and political, and the customers had no say.

The reach: data can be read under foreign law

The CLOUD Act 2018 obliges US providers to produce data in their possession, custody or control regardless of where it is stored. It exists because Microsoft fought a US warrant for emails held in Dublin, and Congress answered by abolishing the geography. The UK-US Data Access Agreement, in force since 3 October 2022, gives law enforcement on both sides a direct channel to data held by each other's providers [7]. In May 2025 a US court ordered OpenAI to preserve every ChatGPT conversation it would otherwise have deleted, EU users' GDPR erasure rights suspended, and later ordered 20 million of those conversations produced to plaintiffs [35].

The most useful evidence is a single sentence. In June 2025, under oath before a French Senate inquiry, Microsoft France's director of public and legal affairs, Anton Carniaux, was asked whether he could guarantee that French citizens' data would never be transmitted to US authorities without French authorisation. His answer: "No, I cannot guarantee it" [14][15]. Microsoft separately advised Scottish police authorities in writing that it cannot guarantee data sovereignty for Microsoft 365 [15]. This is the vendor's own testimony, not a campaigner's claim about American platforms, and the Act's classification rule writes it down.

The dial: behaviour can be changed without asking

AI services introduce a third mechanism. Their behaviour is set by prompts, fine-tuning and filters controlled by the provider, and it can change overnight. At 3:15 in the morning on 14 May 2025, someone modified Grok's system prompt to force a specific political answer. For hours the chatbot answered unrelated questions with a conspiracy theory its owner had personally promoted. xAI called it an unauthorised modification, the second in four months [16]. Two months later, after its owner announced it would be made less politically correct, the same system posted antisemitic material and praised Hitler, weeks before the Pentagon awarded its maker a contract worth up to $200 million [3]. In May 2024 OpenAI's own threat reporting disclosed a covert influence operation by an Israeli political marketing firm using its models to generate pro-Israel content through fake personas [32]. And since July 2025, US federal procurement has required AI suppliers to meet government-defined standards of "truth-seeking" and "ideological neutrality", with the administration defining both [33].

A British public service built on a foreign model is a service whose behaviour can be amended by a foreign owner, employee, contractor or procurement officer, without notice. For a chatbot that is embarrassing. For a model triaging welfare cases it is something worse.

A state that cannot list what it would lose has already lost something.

4

The exposure in numbers

The dependency is not rhetorical. It has figures.

Over £1 billion a year in UK public sector cloud spend, concentrated on three American providers, with official figures showing the total rising year on year [6].

£45 billion a year in unrealised savings identified by the state's own digital review, the same fragmentation that conceals the dependency map [13].

£330 million for the NHS Federated Data Platform with Palantir, a US company whose business is data integration for states, procured at pace, now urged scrapped by two parliamentary committees, with NHS England unable to evidence the benefits and the break clause due in early 2027 [4][5].

£31 billion of pledged US technology investment suspended as a negotiating lever in December 2025 [1][2].

£68 billion of AI investment pledged since January 2025, directed to capability with no accompanying control framework [20].

Over 90 per cent of AI supercomputing controlled by US and Chinese firms; no British frontier model exists [17].

27 December 2031: the sunset on the EU adequacy decisions that keep UK-EU data flows lawful, in a Union that has now proposed its own sovereignty tiers and will judge Britain's exposure to third-country access when renewal is argued [8][9].

2022: the year Fujitsu's Police National Computer contract was extended because the Home Office had no viable alternative, fifteen years after that dependency should have been designed out [21].

Two features of this ledger deserve emphasis. First, none of it is secret: the state itself publishes most of the figures. The problem is not hidden information but the absence of anywhere the information accumulates into a decision. Second, the ledger is currently unpriced. Dependence without an exit is a liability, and it appears on no balance sheet, in no risk register with a minister's signature, and in no statement to Parliament. The Act's first function is to make the ledger official, because liabilities that are measured get managed, and liabilities that are not, mature.

5

Design principles

No bans, no walls, no empire. Six principles govern every clause in Part B. They are what separate a statute that can pass from a gesture that cannot.

1. Proportionate. Obligations scale with sensitivity. A council's website hosting is not the health service's patient platform, and the Act never treats them alike. Most of the public digital estate will attract no duty beyond a register entry.

2. Tiered, not binary. Dependence is a fact of modern computing; the Act's purpose is to make it visible, chosen and survivable, not to abolish it. American hyperscalers will continue to host most government workloads for years, knowingly and by decision, and the Act is designed to make that a defensible choice rather than an accidental one.

3. No bans, no default localisation. The Act names no company and no country. Its tests are jurisdictional and apply as readily to Beijing as to Washington, and to a British company that sells to a foreign parent the day after the sale.

4. Treaty-compatible. Nothing touches the UK-US Data Access Agreement, Five Eyes cooperation, defence arrangements or trade commitments. The Act changes how Britain buys, maps and rehearses, not what Britain promises others.

5. Institutionally light. Powers and duties attach to bodies that exist: DCMS, the ICO, the NCSC, the NAO, the CCS, coordinated by one small office. No new regulator, no licensing empire, no logo and estate. Departments are renamed more often than statutes are amended: digital government has had three Whitehall homes in four years, most recently when DSIT was abolished in July 2026 [38]. The duties therefore attach to the Secretary of State, so the next reshuffle moves the Office without opening the Act.

6. Adequacy-positive. Every measure is chosen to strengthen the UK's position for the 2031 EU adequacy renewal, which will be argued substantially on third-country access [8]. A Britain that can evidence key custody, classified dependencies and rehearsed exits walks into that argument with documents, not assurances.

A seventh principle is enforced by the drafting itself: every clause must survive the question "does this stop anyone doing lawful business?" If the answer is yes, the clause is wrong. The Act constrains the state as a customer, not the market as a supplier.

6

Part 1 of the Act, the sovereignty register

You cannot govern what you have not listed. **The duty.** Every central government department, executive agency, arm's-length body, devolved administration, local authority above a size threshold, and operator of essential services must maintain a register of its critical digital dependencies. A critical dependency is any externally provided digital service whose withdrawal, degradation or hostile alteration would materially impair a public function or essential service.

The entry. Each register entry records: the provider and its corporate parent; the parent's jurisdiction of incorporation and principal place of control; hosting and processing locations; the foreign legal instruments capable of compelling access or interruption (the register names the instruments of compulsion, jurisdiction by jurisdiction); the data classes held and their volumes; the contracted exit provisions; the dependency's classification under Part 2; and the date of the last review. The body's accounting officer signs the entry. That signature is the point: dependencies become owned facts, not ambient concerns.

The reporting. Registers are submitted annually to the Office for Digital Sovereignty (Part 7). The NAO audits a sample each year for completeness and accuracy, as it already audits departmental accounts. The Office publishes a consolidated summary, redacted for security, so that Parliament, industry and the public can see the shape of the state's dependence and watch it change year on year. The first register is due twelve months after Royal Assent.

The design choices that matter. The register rides existing cycles where possible: CAF assessments, annual accounts, Government Security classifications [13][15]. It captures dependence, not systems inventories, which keeps it short; a department's register should run to dozens of entries, not thousands. And it is public in summary, because the discipline of publication is what keeps registers honest. Private registers become stale; published ones get challenged.

What it costs. Clerical effort and accounting-officer time, estimated in the low hundreds of thousands of pounds across central government for the first year, falling thereafter. Compared to the £45 billion a year of unrealised savings the DSIT review identified [13], it is the cheapest reform in this volume, and the one on which everything else depends.

7

Part 2 of the Act, classification and the effective control test

4
tiers, S0 to S3

Labels do not determine classification. Every registered dependency is classified into one of four tiers:

S0, public. Public information and low-impact services. No further duties.

S1, operational. Internal services whose loss is disruptive but recoverable within tolerance. Register entry and a documented exit plan.

S2, sensitive. Personal data at scale, commercially sensitive state functions, services whose failure harms citizens directly. Continuity duties under Part 3 and procurement gates under Part 5.

S3, sovereign. Systems adjacent to national security, critical national infrastructure control, health and biometric platforms, law enforcement core systems, democratic infrastructure. The full regime: Parts 3, 4, 5 and 6.

The test. Classification of control turns on three questions, applied to the provider and every material sub-processor:

01. **Ownership.** Who owns and controls the parent company?
02. **Compellability.** Whose law can compel the provider to surrender data, alter service, or change behaviour, without reference to the customer?
03. **Key custody.** Who holds the encryption keys that protect the data?

A dependency fails sovereign classification if any answer resolves to a foreign state or a party that foreign state can compel. The test is deliberately indifferent to marketing: a US-domiciled parent answers questions one and two against itself regardless of how many British regions, sovereign badges or local subsidiaries it operates. When AWS launched its European Sovereign Cloud in January 2026 with €7.8 billion of investment and a German regulator's endorsement, it built a properly engineered answer to residency. It did not change the answer to question one, and under this Act question one is the one that decides [18]. Microsoft's sworn testimony in Paris settled question two for its entire sector [14][15].

The guidance. The Office for Digital Sovereignty publishes classification guidance, worked examples and an appeals route, because defensible classification needs a place to argue. Some answers will be genuinely arguable. Compellability is a question of legal judgement, not measurement, and a provider with a foreign parent behind an elaborate domestic structure will litigate its classification. The appeals route and the Office's published reasons exist for exactly those cases: a test that admits its borderline is more credible than one that pretends to have none. The Office reviews classifications annually and on trigger events: change of provider ownership, new foreign legislation, merger, or a geopolitical event of the kind Chapter 3 documents. The register therefore moves with the world, not with the contract cycle.

The naming function. The test's deepest purpose is linguistic. Today "sovereign" means whatever a brochure needs it to mean: the EU's own €180 million sovereign cloud tender, awarded in April 2026, accepted a consortium built on S3NS, the Thales and Google Cloud joint venture, at SEAL-2 while its three European rivals reached SEAL-3 [37]. Under the Act, sovereignty becomes a finding of fact with three questions behind it. Suppliers may still sell; ministers may still buy; but nobody may call the purchase something it is not.

8

Part 3 of the Act, continuity duties

A dependency you cannot exit is a tenancy, not a contract. **The duties.** For every S2 and S3 dependency, the contract must contain, as a matter of law and not negotiation skill:

Data export: complete export of the customer's data in documented open formats within thirty days of request, with the schema and tooling needed to use it.

Notice: minimum twelve months' notice of service withdrawal or material degradation, with continued service on existing terms for the notice period.

Escrow: deposit of configurations, deployment scripts and, where feasible, source materials with an independent escrow agent, releasable on defined trigger events. Escrow is mature practice in regulated finance: NCC Group, which describes three decades of escrow operation, builds it into cloud offerings used by banks [29][30].

Portability: for AI services, export of fine-tunes, evaluation suites and configurations in usable form.

The exercise. Every S3 dependency undergoes a switch-off exercise at least every two years: a scored simulation of provider withdrawal, whether commercial, political or compelled, testing detection, decision, data recovery and service restoration against stated objectives. Results go to the NCSC and are summarised in the annual statement. The first exercises should be scheduled where Parliament is already watching: the NHS Federated Data Platform, whose break clause falls due in early 2027, is the obvious first candidate [4][5].

The precedent. The NCSC's Cyber Assessment Framework already obliges departments to meet resilience profiles against attackers [13]. The continuity duty extends the same discipline to a different threat actor: the supplier. This is not a conceptual stretch. The operational resilience regime in financial services, built by the Bank of England and the FCA over a decade, already requires firms to map important business services, set impact tolerances and test exit strategies for third-party providers, with escrow among the recognised tools [29]. The Act holds the state to the standard its own regulators enforce on the private sector.

The limit of the duty. Continuity duties cannot make every dependency survivable; some platforms are too deep, and the answer for those is classification, key custody where applicable, and a ministerial signature under Part 7. The duty is rehearsal and option, not omnipotence. An exercised exit that is never used costs a fraction of an unplanned one, as every organisation that has lived through a provider failure knows.

A warrant served on a provider that holds ciphertext and no keys yields ciphertext.

9

Part 4 of the Act, key custody

48
months to full key custody

For every S3 dependency, encryption keys protecting the data must be held by the public body itself or by a UK-controlled trustee, using external key management, hold-your-own-key architectures or equivalent technical measures, such that the provider cannot read the data it hosts or processes. Where a service cannot function under this rule, for example certain managed analytics, it cannot be classified S3-sovereign-controlled, and the dependence is recorded, and signed for, under Part 7.

Why this clause matters most. Parts 1 to 3 make dependence visible, classified and survivable. Part 4 is the only clause that makes foreign compulsion futile for the most sensitive tier. The CLOUD Act compels production of data within a provider's possession, custody or control; data encrypted under keys the provider does not hold is data the provider cannot meaningfully produce. This converts the legal exposure documented in Chapter 3 into a technical nullity for the workloads that matter most, without amending anyone's law, breaching anyone's treaty or asking anyone's permission.

The practice exists. External key management and hold-your-own-key patterns are shipping features of all three hyperscalers, adopted by regulated finance and insurance precisely for jurisdictional reasons; Microsoft sells the capability as Data Guardian and External Key Management [18]. The NCSC publishes key management guidance. The Act does not ask the market to invent anything; it asks the state to buy what banks already buy.

The governance. Key custody brings its own discipline: key ceremonies, dual control, quorum recovery, audit trails, and a custodian competence the public sector must build or contract. The NCSC guidance that follows the Act should specify patterns, and the trustee market, UK law firms, escrow agents and specialist custodians, will develop as it has in finance [29][30]. Getting key governance wrong loses data permanently, which is why the clause applies to the narrowest tier and phases in over 48 months.

10

Part 5 of the Act, procurement gates

Buyers with criteria get served. Buyers without criteria get marketing. **The mechanism.** The Procurement Act 2023 already gives contracting authorities the tools: award criteria, conditions of participation, exclusion grounds and transparency duties [12]. Part 5 of this Act supplies the sovereignty content. For new contracts above threshold covering S2 and S3 workloads:

- tenders must require disclosure answering the effective control test, for the bidder and material sub-processors;
- contracts must embed the Part 3 continuity terms;
- for S3, key custody compliant with Part 4;
- where two bids are otherwise comparable, the sovereign-controlled bid wins: a tie-break written into law;
- below-threshold and SME suppliers use a simplified disclosure route, so the gate does not become a wall against the British startups it is designed to benefit.

The machine. Crown Commercial Service frameworks incorporate the criteria as they renew, so the existing buying machine does the work rather than a parallel one. Frameworks carry model clauses for continuity, escrow and key custody, shrinking the negotiation from months to a checkbox, which is how policy reaches contracts in practice.

The market effect. The gate leaves American suppliers entirely welcome, on one condition: a hyperscaler can sell anything it likes, but it declares its jurisdictional exposure in the tender, and the sensitive tiers price that exposure in. The precedent is Europe: confronted with sovereignty criteria, the hyperscalers built sovereign offerings to order [18]. The offerings do not pass the control test, but their existence proves the commercial point: criteria move supply. Britain's £1 billion-plus annual cloud spend is negotiating weight the state has never consciously used [6].

The safeguard. A ministerial waiver, published and justified in the annual statement, covers cases where no sovereign-controlled bid exists or capability requires otherwise. The gate channels buying; it does not strangle it.

11

Part 6 of the Act, AI models and weights

A model re-tuned by its owner without notice is a policy change nobody voted on. **Registration.** AI systems used in public services enter the sovereignty register like any other dependency, with three additional disclosures: where the model is hosted, whose law governs the provider, and whether the system prompts, fine-tuning or output constraints can be altered without the public body's knowledge.

Behavioural change control. For citizen-facing AI in the S2 and S3 tiers, the public body must be able to inspect and approve material behavioural changes before deployment, with a duty on providers to disclose them. Chapter 3 documented why this is not hypothetical: a system prompt was modified at 3:15 in the morning to force a political answer, the second such change in four months [16]. A welfare triage model or a police summary tool whose behaviour shifts silently is a policy instrument changed without authority, and the Act treats it as one.

The weights preference. For analytical AI in the S3 tier, public bodies must prefer open-weight models hosted on UK-controlled infrastructure where a suitable model exists, with a published derogation where none does. The rationale is the arithmetic of the earlier volumes: a model whose weights sit on British servers cannot be switched off in Washington or Beijing, mined under foreign law, or re-tuned without the owner's knowledge. Britain holds no frontier model; US and Chinese firms control over 90 per cent of AI supercomputing [17]. The preference converts that weakness into strategy: Britain fine-tunes, evaluates and hosts open models, European, American or Chinese in origin, on infrastructure it controls, building sovereign capability at a fraction of frontier cost.

The money. The Sovereign AI Unit's £500 million and the wider £2 billion AI ecosystem package fund exactly this: domestic fine-tuning capacity, evaluation infrastructure, hosting and skills [10]. The Action Plan said Britain should be an AI maker [19]. The weights preference is the clause that makes "maker" mean something a British engineer can execute this year, not an aspiration for the next spending review.

Transparency for citizens. Public-facing AI services must disclose that they are AI and name the provider and hosting jurisdiction in plain view, extending the logic of the EU's Article 50 transparency duties to the sovereignty dimension [9]. Citizens deserve to know that a machine answered, and whose machine.

Ministers may still choose dependence. They must sign for it in public.

12

Parts 7 and 8 of the Act, institutions, accountability and alignment

A small Office for Digital Sovereignty sits within DCMS, staffed at 40 to 60, owning the register, the classification guidance, the model clauses and the annual statement. DCMS is the present home of digital government: the machinery-of-government changes of July 2026 abolished DSIT and returned digital foundations, digital transformation and the Government Digital Service to a strengthened Department for Digital, Culture, Media and Sport, while AI strategy and the AI Security Institute moved to the Cabinet Office and the science and innovation portfolio to the renamed business department [38]. The Act attaches its duties to the Secretary of State rather than to a departmental name, so a future machinery-of-government order can move the Office without amending the Act. It is a coordination and standard-setting body, deliberately denied an inspection empire: the ICO folds sovereignty exposure into data protection assessments, the NCSC into the CAF, the NAO audits the registers. Three institutions that already exist, one office that joins them.

The annual statement. Once a year the responsible Secretary of State lays a Digital Sovereignty Statement before Parliament: the consolidated register summary, switch-off exercise results, classification movement, waivers granted, and every S3 dependency where a minister has accepted foreign control, named and justified. That final requirement is the discipline that makes the rest real. Accountability in this domain has never meant blame; it has meant that someone with a name and a job has read the risk and signed for it. Horizon taught the country what happens when nobody does [21].

Devolution. The register duty applies to devolved administrations with reporting through their own accountability lines, respecting the devolution settlements; the classification standards and model clauses are shared UK-wide, because a citizen's data does not change sensitivity at the border.

International alignment. The S0 to S3 tiers map onto the four assurance levels in the EU's proposed Cloud and AI Development Act [8][9]. Suppliers then face one coherent European market rather than two diverging ones, and the UK makes its 2031 adequacy argument from a position of demonstrable alignment. Carve-outs protect Five Eyes cooperation and defence arrangements. The Act speaks to dependence, not alliance. Alignment also serves British suppliers: a UK provider certified sovereign at home steps onto the EU's ladder with the paperwork half done.

13

The capability question

£500m
Sovereign AI Unit

Every sovereignty proposal eventually meets the same question from the Treasury bench: where does British capability come from? A register, a control test, continuity duties and key custody all discipline demand. They do not, by themselves, create supply. The Act answers on both sides: it grows the domestic market it regulates, and it admits the limits of that ambition.

Demand is the cheapest industrial policy the state owns. The public sector spends more than £1 billion a year on cloud and digital infrastructure [6], and spends it today with almost no preference structure attached. The classification and gating machinery in Parts 2 and 5 of the Act converts that existing spend into a predictable, published demand signal. A British hosting provider, a UK-key-custody service, a domestic escrow specialist or a sovereign AI builder can read the register, see which systems sit in which tier, and see the published direction of travel for S2 and S3 workloads. That is a pipeline. Pipelines are what investors price. Australia's Hosting Certification Framework reshaped procurement by attaching certification to eligibility: from 2021, suppliers hosting whole-of-government data had to certify, and the market reorganised around the tiers [25] [26]. The signal did the work.

The Act deliberately builds on existing institutions rather than inventing new ones. The Sovereign AI Unit, funded with £500 million [10][19] and housed since July 2026 in DBIST [38], becomes the natural home for the demand-side intelligence the register generates: which capabilities the state repeatedly cannot buy domestically, at which tiers, and at what scale. The AI Opportunities Action Plan committed Britain to being an AI maker, not an AI taker [19], and £68 billion of private investment had been pledged against that agenda by January 2026 [20]. What the plan lacks is a mechanism that steers any of that capital toward sovereign capability specifically. The register is that mechanism. An annual statement to Parliament is a more powerful industrial instrument than any grant scheme. When it says, in public, "the state runs 340 S3 workloads and can source 12 per cent of them domestically", it tells the market exactly where the gap is and how long it will persist.

Skills follow rehearsed responsibility. The continuity duties in Part 3 and the switch-off exercises in Annex E create, for the first time, a statutory reason for thousands of public sector technology teams to understand exit engineering, key management, model provenance and dependency mapping. These are precisely the skills the private sovereign market needs. Regulated finance ran the same cycle over a decade: operational resilience rules created a domestic industry of exit planners, resilience testers and custody specialists, because regulation made the skills mandatory and the market made them valuable [29]. The Act replicates that flywheel across the whole public estate. No training budget is required to start it; the duties themselves generate the demand for the skills, and the people who hold those skills become the seed population of the domestic supply side.

Honesty about what cannot be built quickly. Britain will not manufacture leading-edge semiconductors at scale this decade, and no Act of Parliament changes the physics of that. Britain will not produce a foundation model to rival the largest American or Chinese systems on a public budget, and pretending otherwise would discredit everything else in this volume. What Britain can build, within the life of one Parliament, is the layer where sovereignty is in fact exercised: hosting under UK jurisdiction, key custody, managed continuity, model evaluation, open-weight deployment and fine-tuning capability, and the professional class that runs all of it. Switzerland's Apertus project showed what a mid-sized state can field when it decides openness itself is the

strategy [36]. Britain's research base is deeper than Switzerland's. What it has lacked is a statute that points demand at it.

The market test. The success measure for this chapter is three numbers the register will make visible for the first time, none of them the count of press releases about British AI. They are the share of S3 spend with suppliers passing the effective control test, the share of S3 workloads with a rehearsed, evidenced exit, and the number of UK-headquartered suppliers winning S2 and S3 contracts. If those numbers do not move within four years, the Act has failed as industrial policy, and the annual report to Parliament will say so in terms nobody can spin.

The capability question has a harder edge, and it deserves stating plainly. A country that imports all of its digital infrastructure exports the careers that go with it. The register, the gates and the duties are defensive instruments. This chapter is the offensive one: it uses the state's unavoidable spend to build the domestic layer that makes the defensive instruments credible. Defence without offence is managed decline with better paperwork.

14

What the Act deliberately does not do

The fastest way to kill a sovereignty proposal is to let it be described as what it is not. This chapter pre-empts that.

It does not ban any company. No supplier is excluded from any tier by nationality. Classification records facts about control; ministers may accept those facts, on the record, where capability requires.

It does not localise data by default. Only the S3 tier carries architectural requirements, and they concern keys and exits, not geography. A workload can be sovereign-controlled in an overseas data centre if the ownership, compellability and key questions resolve correctly, as Estonia proved when it placed state data in Luxembourg under a legal architecture that kept control Estonian [22] [23].

It creates no new regulator. The Office for Digital Sovereignty coordinates; the ICO, NCSC and NAO execute within their existing remits. Total new headcount is 40 to 60.

It does not touch the private economy beyond operators of essential services, who already carry resilience duties under existing law. No startup, no ordinary business, no consumer gains a single new obligation.

It does not breach any treaty. The UK-US Data Access Agreement, Five Eyes arrangements, defence cooperation and trade commitments stand untouched [7]. The Act is exercised through British buying decisions and British record-keeping, the least confrontational instruments a state possesses.

It does not pretend Britain is a superpower. There is no chip fab clause, no frontier model programme, no national champion designation. The ambition is narrower and harder: a state that knows, tests, rehearses and accounts.

15

Objections and answers

"This damages the US relationship." The relationship absorbed the EU's CADA proposal, which goes further and names the same risks [9]. It was the United States that suspended the Tech Prosperity Deal over a tax dispute, demonstrating that the relationship is conducted transactionally regardless of British deference [1][2]. Allies negotiate with states that know their exposure. They invoice states that do not.

"It threatens EU adequacy." The 2031 renewal will be argued on third-country access risk, as every adequacy review since Schrems has been [8]. Key custody, classified dependencies and rehearsed exits are the evidence base for that argument. The Act is adequacy's friend, and the tier mapping in Part 8 makes the friendship structural.

"It costs too much." The register and classification are clerical work: hundreds of thousands of pounds across central government in the first year, low millions only when the whole public sector is counted. Continuity terms are contractual, phased with renewals over four years. Key custody is the one real capital item, confined to the narrowest tier. One honest admission belongs here: sovereign-qualified supply prices above standard cloud, as France's SecNumCloud market shows [28]. That premium is the insurance price on the liability this volume sets out, it attaches only to the tiers where the exposure justifies it, and it falls as the gates widen the market that meets the criteria. Set against £45 billion a year of unrealised savings and a £1 billion-plus cloud bill that a documented, option-holding customer can negotiate down, the Act pays for itself in the first hard negotiation it enables [6] [13]. Dependence without an exit is an unpriced liability, and unpriced liabilities mature.

"We lack the capability." True at the frontier, false at the workload. Escrow, external key management, rehearsed exits and open-weight fine-tuning are established engineering practice, running today in regulated finance and in several European states [22][26][29]. The capability that is missing in practice, a register-keeping, exercise-running discipline in departments, is precisely what the Act builds, funded where needed by money already announced [10].

"It chills innovation." The Act regulates buying, not building. It creates a procurement lane for SMEs, obliges government to plan exits, which lowers the lifetime risk of selling to the state, and funds domestic AI capability through the weights preference. The chill runs the other way: a market where one brochure word, sovereign, means anything is a market where suppliers with nothing to hide cannot compete.

"The hyperscalers will refuse the terms." They said so in Europe, then built sovereign clouds to order and accepted SecNumCloud's corporate-structure tests through partnerships [18][28]. Criteria move supply. Britain's £1 billion annual spend, currently an unconscious habit, is the criterion it has never used [6].

"This is protectionism in disguise." Protectionism excludes foreign suppliers to shelter domestic ones. The Act excludes no one, names no country, and applies its strictest duties only where the state itself is the customer. Australia's hosting framework, the closest Commonwealth comparator, made the same distinction and sustained it [25][26].

"Security through obscurity is enough; publishing registers helps adversaries." Registers are published in summary, redacted for security, exactly as the CAF regime balances transparency with protection [13]. A dependency that only exists safely while nobody mentions it is not safe.

"It duplicates existing frameworks." The register rides the CAF cycle, the gates ride the Procurement Act, the audit rides the NAO's mandate [12][13]. What is new is the question they jointly answer: whose law controls the service. No existing framework asks it. That is the gap, and it is one clause deep.

"The timing is wrong; wait for Europe." Europe has moved: the CADA proposal is before Parliament and Council, and its tiers will reshape the market Britain buys from [9]. Waiting means adopting whatever classifications settle elsewhere, as a taker of standards, in the same posture the Action Plan warned against for AI itself [19]. The maker-taker choice applies to rules as much as to models.

16

The legal mechanics

A statute addressed to government must show its working in the legal machinery. This chapter maps the four junctions where the Act meets existing law, and the drafting choices at each.

Data protection law. The Act is drafted as a foundation, not an amendment. The UK GDPR and DUAA continue to govern processing exactly as they do today; nothing in this Act creates a new processing power, a new exemption or a new data right. The interaction is one-directional: the ICO gains a duty to consider registered sovereignty exposure as a factor in its existing assessment and enforcement functions, so that a controller's dependence on a foreign-compellable processor becomes visible inside the regime that already exists [11]. Data protection sits on top of the Act, as the title promises, because the Act supplies the fact base the upper layers have always lacked.

Procurement and trade law. The Part 5 gates operate as conditions of participation and award criteria under the Procurement Act 2023, instruments the GPA and domestic law both recognise [12]. The effective control test is drafted to be origin-neutral: it classifies by jurisdiction of control, not nationality of supplier, applies identically to British and foreign bidders, and a British company acquired by a foreign parent changes classification on the day of the sale. The sovereign tie-break activates only between otherwise comparable bids, the narrowest possible preference. Australia's hosting framework has run on the same architecture since 2021 without trade challenge, which is the strongest available evidence that criteria drafted around control rather than origin survive scrutiny [26][27]. Defence and security procurements rely on the existing exemptions, untouched.

Subsidy control. The Part 6 weights preference is a procurement duty, not a subsidy programme, and raises no Subsidy Control Act issues. Where the Sovereign AI Unit funds domestic hosting, evaluation or fine-tuning capacity, it does so under the existing framework that governs its current investments [10]. No new spending power is created; money already announced is pointed at capability rather than, as at present, at capability alone.

Devolution and delegated powers. Data protection is reserved; procurement is substantially devolved; health, education and policing are devolved in varying degrees. The Act proceeds by setting UK-wide classification standards and model clauses while routing register reporting through each administration's own accountability lines, so no devolved competence is overridden. Classification guidance and tier thresholds are made by regulations under the affirmative procedure, giving Parliament a vote on any movement of the boundaries. A five-year review clause requires the Secretary of State to report on the Act's operation, and the Act contains no Henry VIII powers to amend primary legislation. Powers that reach far attract challenge; powers drafted to reach exactly this far tend to survive.

17

Comparative practice

Four jurisdictions show the pieces of this Act already running.

Estonia: control without geography. After the 2007 attacks took down 58 Estonian websites, the state confronted the question small digital countries cannot avoid: what happens if the territory fails? Its answer, the data embassy, places state data and services in a Luxembourg Tier IV facility under a 2017 bilateral agreement modelled on the Vienna Convention: the resources remain under Estonian control, with something like diplomatic immunity, able to run a government in exile if required [22][23][24]. Monaco followed with its own arrangement in 2021 [24]. The lesson for Britain is the legal imagination, not the building in Luxembourg. Estonia separated sovereignty from geography using contract, treaty and architecture, exactly the instruments Parts 3 and 4 use.

Australia: the certification route and its limit. The Hosting Certification Framework, live since 2021, certifies providers as Assured or Strategic for government hosting, assessing ownership structure, supply chain and change-of-control undertakings, and requires sensitive and PROTECTED government data to use certified hosts [25][26]. It is the closest thing to Part 5's procurement gate in the Commonwealth. Its documented limit is equally instructive: certification does not require Australian ownership, and critics, including ASPI, note that hyperscalers pass while remaining foreign-compellable, leaving the framework short of true sovereignty [27]. Britain should adopt the mechanism and close the gap: the effective control test is the missing question Australia's framework does not ask.

France: the corporate-structure test. SecNumCloud, ANSSI's cloud qualification, pairs technical security requirements with corporate-structure conditions designed to limit non-EU control, forcing US providers into joint ventures with French partners to qualify [28]. It is the bluntest instrument among the four, and the trade-offs show: years of contention, and qualified offerings that are American technology in French governance wrappers. Britain's control test borrows the bluntness where it matters, questions one and two, while avoiding the joint-venture fiction by recording the finding.

The European Union: the tiered market. The Cloud and AI Development Act, proposed on 3 June 2026, defines four assurance levels from EU data location up to full supply-chain transparency with no third-country interference, for phasing into public procurement after adoption [9]. Levels 3 and 4 structurally exclude foreign-controlled providers from the most sensitive workloads. Whatever Britain thinks of Brussels, CADA will shape what suppliers build and offer across Europe. Part 8's tier mapping ensures Britain buys into that market as a rule-maker's neighbour, not a rule-taker's customer.

All four reach the same conclusion: what matters is who controls the service, not where the racks stand. Each has built a partial answer. None has assembled the full stack, register, test, rehearsal, keys, gates, accountability, in one statute. That assembly is this proposal's claim to novelty, and to usefulness.

18

Implementation

The legislative pathway. This volume is the green paper. The natural sequence: a consultation period through autumn 2026, run jointly by DCMS and interested parliamentarians; a white paper in early 2027 with the technical annex (clause-to-statute mapping, in preparation); introduction as a government bill in the 2027-28 session, with pre-legislative scrutiny by the relevant select committee, which the FDP controversy has primed to be receptive [4]. Royal Assent on that timetable lands the first registers in 2029, comfortably inside the EU adequacy argument and in step with CADA's procurement tiers [8][9]. Should the timetable slip, every Part of the Act except the statutory duty itself can be piloted through existing powers: CCS frameworks, CAF profiles and Treasury spend controls already allow the register, the clauses and the exercises. A serious department could start on Monday. For the first live decision, it must: the FDP's break clause falls due in early 2027, before any bill can pass, so the dependency map for that platform has to be built under existing powers this year [4][5]. The Act converts good practice into duty; the practice should not wait for the Act.

First 100 days. Establish the Office for Digital Sovereignty. Issue classification guidance and the control test. Commission registers from the twenty largest public IT estates. Convene ICO, NCSC, NAO and CCS to map the Act onto existing cycles. Schedule the first switch-off exercise for the FDP ahead of its break clause [4][5].

Year one. Registers complete for central government and essential-service operators; first published summary. CCS frameworks amended on renewal. First exercises run and reported.

Years two to four. Continuity duties flow through S2 renewals. Key custody phases into S3 over 48 months. The weights preference takes effect as the Sovereign AI Unit stands up domestic hosting and evaluation capacity [10]. First annual statement at the end of year one, and annually thereafter.

The sequencing logic. Visibility first, then contracts, then the sensitive tier, then accountability. Each stage makes the next cheaper: you cannot price an exit you have not mapped, cannot gate a purchase you have not classified, and cannot sign for a risk you have not rehearsed.

What it costs. Parliament will ask, and the answer should be ready. The Office for Digital Sovereignty is a small institution: on the precedent of comparable arm's-length bodies, a staff of 40 to 60 and a running cost in the low tens of millions a year, absorbed within the DCMS settlement rather than added to it. The register itself is built from data departments already hold; the DSIT review found the problem was never collection but assembly [13]. The continuity clauses cost nothing to draft and are carried by suppliers as a condition of market access, the same mechanism by which the Procurement Act's prompt-payment and exclusion requirements are carried today [12]. Key custody for the S3 tier is the one properly new spend: managed HSM or trustee services for a tier that will number in the low hundreds of systems, not the thousands, at a unit cost the regulated finance market has already commoditised [29]. Set against the exposure side of the ledger, the arithmetic is not close. The state spends more than £1 billion a year on cloud [6]. The National Audit Office and the DSIT review have both pointed to unrealised savings in the tens of billions across the digital estate [13]. A single unrehearsed exit from a critical platform, run in anger during a dispute, would cost more than the entire Act. Estonia, a country of 1.3 million people, built its data embassy and has run it for nine years [23][24]. The question was never whether Britain can afford the Act. It is whether it can afford the alternative, which is the current arrangement: the liability is already on the books, and it is unpriced.

What it saves. Three recoverable costs become visible the day the first register lands. Duplicated exit risk: today every department prices, or fails to price, the same supplier risk independently. Negotiating position: a state that can show a rehearsed exit negotiates renewals differently, and suppliers know it; the FDP procurement demonstrated what negotiating without an exit looks like [4] [5]. Incident cost: the switch-off exercises convert the most expensive category of failure, the surprise dependency, into a drilled routine. None of this requires optimism about behaviour change. It requires only that the state know what it depends on, which is the least a state can know.

19

Consultation questions

This proposal is published for discussion, and the following questions are the ones on which better answers would most improve it. Responses are invited through altlibre.com by 31 December 2026.

01. **Is the S0 to S3 classification the right shape?** In particular, should any category currently proposed for S2, such as education records or welfare case management, sit in S3?
02. **Should the effective control test gain a fourth question?** The strongest candidate is operational: could the service run for ninety days if every person of foreign nationality in its operating chain were withdrawn? We excluded it as unauditable. We are persuadable.
03. **Who should own the Office?** DCMS is our proposal; the Cabinet Office, which now holds AI strategy and the AI Security Institute, and the ICO both have claims. What matters is a single owner with parliamentary accountability, and that the register does not become a consultancy farm.
04. **Should any private-sector duty extend beyond operators of essential services?** Our instinct is no. The counterargument is systemic financial infrastructure, which the operational resilience regime partly covers already [29].
05. **What belongs in the technical annex?** Officials and engineers who will implement this are invited to say which mappings, model clauses and exercise templates would save them the most time.

Register the dependencies. Test the control. Rehearse the exits. Hold the keys. Gate the buying. Report to Parliament.

20

The bottom line

Britain has spent thirty years becoming a customer. Its hospitals, its tax system, its police and its armed forces run on platforms owned in other people's jurisdictions, under contracts written for a world that no longer exists. The evidence of its ending arrived in December 2025, when the ally that built those platforms paused a £31 billion partnership over a tax dispute, and again in February 2026, when it sanctioned its own AI champion over a surveillance clause [1][3].

The statute book has not caught up. It regulates use and ignores control, which is why every crisis in this volume surprised the officials it happened to. A Digital Sovereignty Act expresses no distrust of any ally. It expresses something more basic: that a state's ability to function should never depend on a decision taken in a boardroom or a briefing room beyond the reach of its own law, unmapped, unrehearsed and unsigned-for.

Nothing in these pages is radical. Estonia has run a data embassy for nine years [22]. Australia has certified government hosting for five [25]. France has tested corporate control for longer [28]. The EU proposed its tiers this summer [9]. Regulated finance has rehearsed exits and held its own keys for a decade [29]. Britain is being asked to assemble what works, to write it down, and to sign for it.

What success looks like in 2030. The first annual statement has been laid three times. Every S3 system in the state has a named minister who has signed for it, and the signatures are public in summary. The NHS enters the FDP break-clause window with a rehearsed exit on the shelf, and the supplier knows it, which is precisely why the exit will probably never be needed [4]. Whitehall's productivity suite runs behind keys the state holds, and the annual signature for its configuration is a line in a minister's diary, not a scandal in a newspaper. The share of S3 spend passing the effective control test has moved from a number nobody knew to a number Parliament debates. A domestic layer of hosting, custody and evaluation suppliers, small but real, bids for work the register made visible. And when the next December 2025 arrives, as it will, the officials in the room are reading from a register rather than discovering their dependencies from a press release. That is the whole ambition: a state that knows what it depends on, and can prove it.

The components are on the shelf. What remains is the decision to use them.

Your data. Your rules. Your country.

ANNEX A

Lines to take

32
lines to take

The quotable lines of this volume, collected for speeches, briefings and interviews.

01. The statute book regulates use but not control.
02. Silent dependence: reliance on foreign-controlled infrastructure that nobody has mapped, nobody has signed for, and nobody has rehearsed losing.
03. Register the dependencies. Test the control. Rehearse the exits. Hold the keys. Gate the buying. Report to Parliament.
04. Invisible dependence, not dependence itself, is the sin.
05. A dependency you cannot exit is a tenancy, not a contract.
06. Capital without control is subsidy, not sovereignty.
07. Labels do not determine classification. Three questions are: ownership, compellability, keys.
08. A warrant served on a provider that holds ciphertext and no keys yields ciphertext.
09. Buyers with criteria get served. Buyers without criteria get marketing.
10. A model re-tuned by its owner without notice is a policy change nobody voted on.
11. Ministers may still choose dependence. They must sign for it in public.
12. You cannot govern what you have not listed.
13. A state that cannot list what it would lose has already lost something.
14. Dependence without an exit is an unpriced liability, and unpriced liabilities mature.
15. No bans, no walls, no empire.
16. Security law asks whether a system is safe from attackers. Data protection law asks whether processing is fair. Neither asks whose law the system answers to.
17. The Act constrains the state as a customer, not the market as a supplier.
18. Britain did not lose control of its digital estate. It sold, rented and rationalised the estate away, one sensible decision at a time.
19. Sovereignty is a finding of fact with three questions behind it.
20. The state meets the standard its own regulators expect of banks.
21. Criteria move supply.
22. An exercised exit that is never used costs a fraction of an unplanned one.
23. The maker-taker choice applies to rules as much as to models.
24. Allies negotiate with states that know their exposure. They invoice states that do not.
25. Demand is the cheapest industrial policy the state owns.
26. A country that imports all of its digital infrastructure exports the careers that go with it.
27. Defence without offence is managed decline with better paperwork.
28. The liability is already on the books, and it is unpriced.
29. Open weights on your own infrastructure classify better than a domestic brand on someone else's. Test control, not origin.
30. The question was never whether Britain can afford the Act. It is whether it can afford the current arrangement.
31. A state that knows what it depends on, and can prove it.
32. Your data. Your rules. Your country.

ANNEX B

Glossary

TABLE. GLOSSARY

TERM	MEANING IN THIS PAPER
CADA	The EU's Cloud and AI Development Act, proposed on 3 June 2026, establishing four cloud and AI sovereignty assurance levels.
CAF	The NCSC's Cyber Assessment Framework, the resilience standard for UK government and essential services.
CCS	Crown Commercial Service, the government's central purchasing body.
CLOUD Act	The US Clarifying Lawful Overseas Use of Data Act 2018, obliging US providers to produce data under their control regardless of where it is stored.
DBIST	Department for Business, Innovation, Science and Trade, renamed from the Department for Business and Trade in July 2026.
DCMS	Department for Digital, Culture, Media and Sport, home of digital government since July 2026.
DSIT	Department for Science, Innovation and Technology, abolished July 2026; digital functions to DCMS, science to DBIST, AI strategy to the Cabinet Office.
Effective control test	The three- question classification test in Part 2: ownership, compellability, key custody.
Escrow	Deposit of software, configurations or source materials with an independent agent, releasable on defined trigger events such as provider failure.
FCDO	Foreign, Commonwealth and Development Office.
FDP	The NHS Federated Data Platform, a £330 million data integration programme contracted to Palantir in 2023.
ICO	Information Commissioner's Office, the UK data protection regulator.
Key custody	The question of who holds the encryption keys protecting hosted data; the subject of Part 4.
NAO	National Audit Office.
NCSC	National Cyber Security Centre.
Open-weight model	An AI model whose parameters are published under a licence permitting download and self- hosting, such as DeepSeek R1 (MIT) or Qwen (Apache 2.0).
Silent dependence	Reliance on foreign- controlled infrastructure that nobody has mapped, nobody has signed for, and nobody has rehearsed losing.
Switch-off exercise	A scored simulation of provider withdrawal required for S3 dependencies under Part 3.
UK-US Data Access Agreement	The 2019 bilateral agreement, in force since 2022, enabling direct law- enforcement requests to each other's providers.
Weights preference	The Part 6 duty to prefer open- weight models on UK- controlled infrastructure for sovereign- tier analytical AI.

ANNEX C

Sources

38

dated sources, verified September 2026

01. The Guardian, "US puts £31bn tech 'prosperity deal' with Britain on ice", 15 December 2025.
02. World Politics Review, "U.S. Suspends Tech Partnership With U.K.", 17 December 2025. https://www.worldpoliticsreview.com/united-states-united-kingdom-tech-partnership/
03. Congressional Research Service, "Federal Government and Anthropic: Considerations for AI Innovation and Competition" (IF13217), 31 July 2026. https://www.congress.gov/crs-product/IF13217
04. The Guardian, "MPs urge Labour to ditch £330m Palantir software contract", 9 July 2026.
05. The Bureau of Investigative Journalism, S. Armstrong, "Palantir: NHS England admits data don't prove contentious platform's benefits", 2026.
06. Government Digital Service, "Improving public sector spending with the cloud cost data solution", Government Technology Blog, 17 June 2025. https://technology.blog.gov.uk/2025/06/17/improving-public-sector-spending-with-the-cloud-cost-data-solution/
07. Agreement between the UK and the USA on Access to Electronic Data for the Purpose of Countering Serious Crime, signed 3 October 2019, in force 3 October 2022.
08. European Commission, renewed UK adequacy decisions, adopted 19 December 2025, sunset 27 December 2031; ICO, "Receiving personal information from the EEA", updated 15 January 2026.
09. European Commission, proposal for a Cloud and AI Development Act, COM(2026) 502 final, 3 June 2026. https://digital-strategy.ec.europa.eu/en/library/proposal-cloud-and-ai-development-act-cada
10. UK Government, "New package puts AI at the heart of national renewal", 21 November 2025; "Government to invest over £2 billion in the UK's AI ecosystem", 20 June 2025.
11. Data (Use and Access) Act 2025, Royal Assent 19 June 2025; ICO commencement guidance.
12. Procurement Act 2023, in force 24 February 2025; Cabinet Office, "Transforming Public Procurement".
13. DSIT, State of digital government review, January 2025, cited in "Rewiring the state: Delivering digital government", 3 June 2026; NCSC, Cyber Assessment Framework guidance, 2026.
14. French Senate, fact-finding mission on digital sovereignty, sworn testimony of Anton Carniaux, director of public and legal affairs, Microsoft France, 10 June 2025; Forbes, "Microsoft Can't Keep EU Data Safe From US Authorities", 22 July 2025. https://www.forbes.com/sites/emmawoollacott/2025/07/22/microsoft-cant-keep-eu-data-safe-from-us-authorities/
15. The Register, "Microsoft admits it 'cannot guarantee' data sovereignty", 25 July 2025.
16. xAI statement on the Grok system prompt incident, via X, 16 May 2025; The Decoder, "xAI reverses Grok's prompt changes after racist responses", 21 May 2025. https://the-decoder.com/xai-reverses-groks-prompt-changes-after-racist-responses/
17. Bloomsbury Intelligence and Security Institute, "US-UK Tech Prosperity Deal: Implications for Technology Cooperation", 22 December 2025. https://bisi.org.uk/reports/us-uk-tech-prosperity-deal-implications-for-technology-cooperation
18. Amazon, "AWS Launches AWS European Sovereign Cloud", 15 January 2026, https://press.aboutamazon.com/aws/2026/1/aws-launches-aws-european-sovereign-cloud-and-announces-expansion-across-europe; Microsoft Azure blog, "Microsoft strengthens sovereign cloud capabilities with new services", 4 November 2025.

19. GOV.UK, "AI Opportunities Action Plan", 13 January 2025; Matt Clifford's recommendation of a UK Sovereign AI unit.
20. DSIT, "AI Opportunities Action Plan: 2026 Progress", January 2026. https://delivery.ai.gov.uk/
21. Institute for Government, "Six lessons government should learn from the Post Office scandal", 12 January 2024. https://www.instituteforgovernment.org.uk/comment/lessons-government-post-office-scandal
22. Microsoft EU policy blog, "Diplomatic immunity for data: Estonia creates a virtual embassy", 14 December 2017. https://blogs.microsoft.com/eupolicy/2017/12/14/diplomatic-immunity-data-estonia-creates-virtual-embassy/
23. e-Estonia, "Data Embassy". https://e-estonia.com/service/e-governance/data-embassy/
24. Luxembourg government, "E-embassies in Luxembourg". https://luxembourg.public.lu/en/invest/innovation/e-embassies-in-luxembourg.html
25. Australian Government, Hosting Certification Framework. https://www.hostingcertification.gov.au/framework
26. Lexology, "Data Sovereignty and the Digital Transformation Agency's Hosting Certification Framework", 17 June 2021.
27. The Strategist (ASPI), "A sovereign Australian government data framework", 11 August 2021. https://www.aspistrategist.org.au/a-sovereign-australian-government-data-framework/
28. ANSSI, SecNumCloud 3.2 qualification criteria, including corporate-structure requirements limiting non-EU control.
29. NCC Group, response to the Financial Stability Board discussion paper on third-party risk management, citing the Bank of England and PRA regime (CP30/19) and escrow practice in regulated finance. https://www.fsb.org/uploads/NCC-Group.pdf
30. NCC Group, "Escrow as a Service". https://marketplace.microsoft.com/en-ae/product/ncc.eaas
31. Rest of World, "OpenAI cuts its last and most important link to China", 27 June 2024. https://restofworld.org/2024/exporter-openai-china-api-access/
32. Time, "OpenAI: Russia, China, Israel Use It for Influence Campaigns", 30 May 2024. https://time.com/6983903/openai-foreign-influence-campaigns-artificial-intelligence/
33. The White House, Executive Order 14319, "Preventing Woke AI in the Federal Government", 23 July 2025. https://www.whitehouse.gov/presidential-actions/2025/07/preventing-woke-ai-in-the-federal-government/
34. BankInfoSecurity, "Nayara Energy vs. Microsoft and Compliance-Driven Lockouts", 13 August 2025. https://www.bankinfosecurity.com/nayara-energy-vs-microsoft-compliance-driven-lockouts-a-29203
35. Terms.law, "OpenAI v New York Times: When Your ChatGPT Logs Become Evidence", 12 November 2025. https://terms.law/2025/11/12/openai-v-new-york-times-stopped-being-just-a-copyright-case-the-moment-the-court-turned-to-your-chatgpt-logs/
36. ETH Zurich and EPFL, "Apertus: a fully open, transparent, multilingual language model", released 2 September 2025. https://www.swiss-ai.org/
37. European Commission, "First Commission tender for sovereign cloud", 20 April 2026, https://interoperable-europe.ec.europa.eu/collection/sovereignty/news/first-commission-tender-sovereign-cloud; Reuters, "EU Commission awards 180 million euro cloud contract to four European providers", 17 April 2026.
38. House of Lords, written statement HLWS298, "Machinery of Government Changes", 21 July 2026. https://questions-statements.parliament.uk/written-statements/detail/2026-07-21/hlws298; GOV.UK, "Machinery of Government changes: fact sheet", 22 July 2026. https://www.gov.uk/government/news/machinery-of-government-changes-fact-sheet

ANNEX D

Model contract clauses

Draft clause language for Crown Commercial Service frameworks, in plain form for discussion. Each clause corresponds to a duty in the Act; the statutory versions will be settled by parliamentary counsel.

Clause 1: data export. "On request by the Authority, the Supplier shall within thirty (30) days deliver a complete copy of the Authority's data in the documented open formats specified in Schedule X, together with all schemas, dictionaries and tooling reasonably required to make use of that data, at no charge beyond reasonable media costs. This obligation survives termination or expiry of the Contract."

Clause 2: notice of withdrawal. "The Supplier shall give not less than twelve (12) months' written notice of any withdrawal, sunset or material degradation of the Service, and shall continue to provide the Service on the existing terms throughout the notice period. Material degradation includes any reduction of functionality, performance, support or security maintenance affecting the Authority."

Clause 3: escrow. "The Supplier shall deposit with the agreed Escrow Agent, and keep current on each release: (a) all configuration and deployment materials for the Authority's tenancy; (b) where feasible, source code and build instructions; (c) runbooks sufficient for a competent third party to operate the Service. Release events are: insolvency of the Supplier; withdrawal of the Service; failure to provide the Service for thirty (30) consecutive days; or lawful compulsion preventing the Supplier from performing."

Clause 4: AI portability and change disclosure. "On request, the Supplier shall export all fine-tuning parameters, evaluation suites and prompt configurations applied to the Authority's deployment in a usable, documented form. The Supplier shall give not less than thirty (30) days' written notice of any material change to model behaviour, system prompts, safety filters or output constraints affecting the Authority's deployment, and shall not deploy such change to the Authority's tenancy without the Authority's written approval."

Clause 5: key custody. "All Authority data at rest and in transit shall be encrypted under keys held exclusively by the Authority or its appointed UK trustee, using the external key management arrangement specified in Schedule Y. The Supplier shall have no technical means of accessing plaintext Authority data. The Supplier shall notify the Authority within seventy-two (72) hours of any legal process seeking Authority data, to the extent notification is lawful."

Clause 6: sub-processor transparency. "The Supplier shall maintain a current register of all sub-processors, their parent jurisdictions and the legal instruments capable of compelling each, shall update it within fourteen (14) days of any change, and shall not appoint a sub-processor failing the Authority's notified classification threshold without prior written consent."

Clause 7: exit assistance. "The Supplier shall provide reasonable exit assistance for up to twelve (12) months following notice of termination, including knowledge transfer, parallel running and data migration support, at the rates set out in Schedule Z, which shall not exceed the Supplier's standard rates for equivalent services."

ANNEX E

The switch-off exercise template

The Part 3 exercise, specified so departments run it consistently.

Scope. One S3 dependency per exercise. The exercising body names an exercise director, records the dependency's register entry as the baseline, and notifies the NCSC at least twenty working days in advance.

Scenario classes. Each exercise runs one of four scenarios, rotated across cycles: (a) commercial withdrawal, the provider gives notice on contractual terms; (b) abrupt withdrawal, service ceases without notice; (c) compelled action, the provider is required by a foreign authority to surrender data or alter service; (d) behavioural change, an AI service's outputs shift materially without the body's approval.

Phases and measures. Detect: how the body learns of the event, and how fast. Decide: who has authority to invoke the exit plan, and how long decision takes. Recover: restoration of data from export or escrow, measured against the recovery point objective. Restore: resumption of service on the alternative arrangement, measured against the recovery time objective. Report: findings scored red, amber or green against each objective, with a remediation plan for anything not green.

Reporting. Scores and remediation plans go to the NCSC within twenty working days of the exercise. The Office for Digital Sovereignty summarises results in the annual statement, by department and scenario class, without disclosing operational detail.

Cost discipline. Exercises are desktop simulations with a technical validation component, not full failovers, except where the NCSC judges a live test proportionate. A well-run exercise costs tens of thousands of pounds; an unplanned withdrawal of a sovereign-tier system costs what it costs, and somebody always pays it.

ANNEX F

Worked register entries

6
worked register entries

Six examples showing the register and classification in operation, chosen to span the hardest cases rather than the easiest.

Entry 1: the NHS Federated Data Platform. Provider: Palantir Technologies UK Ltd. Parent: Palantir Technologies Inc, incorporated Delaware, principal control Denver, United States. Hosting: UK regions of US hyperscalers. Compellable instruments: CLOUD Act; FISA 702. Data classes: patient-level health data at national scale. Exit provisions: break clause available early 2027; no rehearsed migration; proprietary data model. Classification: S3. Control test: fails questions one and two. Duties engaged: Parts 3, 4, 5, 6. First action: switch-off exercise scheduled ahead of the break clause; ministerial signature required for continued foreign-controlled S3 operation, or migration initiated [4][5].

Entry 2: a unitary council's website and forms hosting. Provider: a UK SME hosting company. Parent: UK employee ownership trust. Hosting: UK data centres. Compellable instruments: UK law only. Data classes: public content; low-volume contact forms. Classification: S0 for content; S1 for forms data. Duties engaged: register entry and documented exit plan only. Effort: half a day a year.

Entry 3: a police force's AI-assisted evidence triage. Provider: a US frontier AI company, API access. Parent: US-incorporated. Hosting: provider's US and EU estates. Compellable instruments: CLOUD Act; FISA 702. Data classes: evidential material, personal data of victims and suspects. Behavioural control: system prompts and filters provider-controlled, changeable without notice. Classification: S3. Control test: fails all three questions. Duties engaged: full regime. Part 6 consequence: migration path to an open-weight model on UK-controlled hosting within the derogation framework, with the Sovereign AI Unit's evaluation infrastructure supporting the transition [10].

Entry 4: HMRC's tax records analytics workload. Provider: a US hyperscaler's UK regions, under a CCS framework. Parent: US-incorporated, listed. Hosting: UK data centres, UK-resident staff in day-to-day operations. Compellable instruments: CLOUD Act reaches the parent wherever the data sits; the UK-US Data Access Agreement provides a channel for criminal matters but does not displace unilateral compellability [7]. Data classes: taxpayer records at national scale. Exit provisions: contractual data export, untested; egress pricing untested at this volume. Classification: S3. Control test: fails question two (compellability) regardless of where the racks stand. Duties engaged: Parts 3, 4, 5. First action: customer-held keys under Part 4, converting the compellability exposure into a technical nullity for data at rest; the register entry records that the residual exposure is metadata and in-use data, and prices it. This entry is the one the volume's critics should study: the Act does not order HMRC off the hyperscaler. It orders HMRC to hold its own keys and to know, in writing, what remains exposed after it does.

Entry 5: a university's research compute cluster. Provider: mixed. Compute on a US hyperscaler's research credits programme; models fine-tuned from open weights; some workloads on a Chinese open-weight model hosted in the university's own data centre. Compellable instruments: CLOUD Act for the hosted workloads; none for the self-hosted. Data classes: research data, some dual-use adjacent. Classification: S2 for the hosted research workloads; S0 for the self-hosted open-weight workloads, because the effective control test asks who can compel, and on the university's own iron the answer is UK law alone. Duties engaged: continuity clauses on the hosted workloads; register entry only for the rest. The lesson runs counter to the usual assumption: open weights on your own infrastructure classify better than a domestic brand on someone else's. That is what testing control rather than origin buys.

Entry 6: a Whitehall department's productivity suite. Provider: Microsoft 365. Parent: US-incorporated. Hosting: UK and EU data centres under published residency commitments. Compellable instruments: CLOUD Act; the vendor's own testimony before the French Senate in June 2025 established that it cannot guarantee against US government access, under any configuration it sells [14][15]. Data classes: the working record of government, including policy advice, legal correspondence and ministerial submissions. Exit provisions: none rehearsed at departmental scale anywhere in Whitehall. Classification: S3. Control test: fails questions one and two. Duties engaged: full regime, phased over 48 months. First actions: customer-held keys where the architecture permits; a documented, exercised export of the record into open formats under Annex D clause 1; a ministerial signature each year for continued operation in this configuration. This is the hardest entry in the register and the most important. The Act does not pretend Whitehall can migrate off its productivity suite in one Parliament. It insists that the decision to stay is taken openly, annually, by name, with the exposure recorded and the exit rehearsed, rather than inherited silently from a procurement made before anyone asked the question.

The pattern the examples teach: the register prohibits none of these arrangements. It makes each one a recorded, classified, signed-for decision, with the duties following automatically from the facts. Six entries, six different answers: that is what a control test buys that an origin test cannot.

ANNEX G

Mapping to existing statutes

TABLE. MAPPING TO EXISTING STATUTES

Act Part	Existing instrument it rides	What changes
Part 1: register	CAF assessments, annual accounts, NAO audit	Dependency becomes a recorded, signed fact
Part 2: classification	Government Security classifications	Control becomes a testable property
Part 3: continuity	Procurement Act contract terms; financial- sector resilience practice (CP30/19) [29]	Exit becomes contractual and rehearsed
Part 4: key custody	NCSC key management guidance; hyperscaler EKM features [18]	Compulsion becomes futile for S3
Part 5: gates	Procurement Act 2023 conditions and criteria [12]	Jurisdictional exposure is declared and priced
Part 6: AI	Sovereign AI Unit funding [10]; ICO AI guidance	Model behaviour becomes inspectable; weights preference funds domestic capability
Part 7: accountability	DCMS, ICO, NCSC, NAO remits	Parliament receives an annual account
Part 8: alignment	EU adequacy framework [8]; CADA tiers [9]	UK and EU classifications interlock

Your data. Your rules. Your country.

AltLibre Papers, No. 2. Written by Adrian Hollister. Free to quote, republish and translate under CC BY-SA 4.0. altlibre.com