Institute *for the* Future of Work

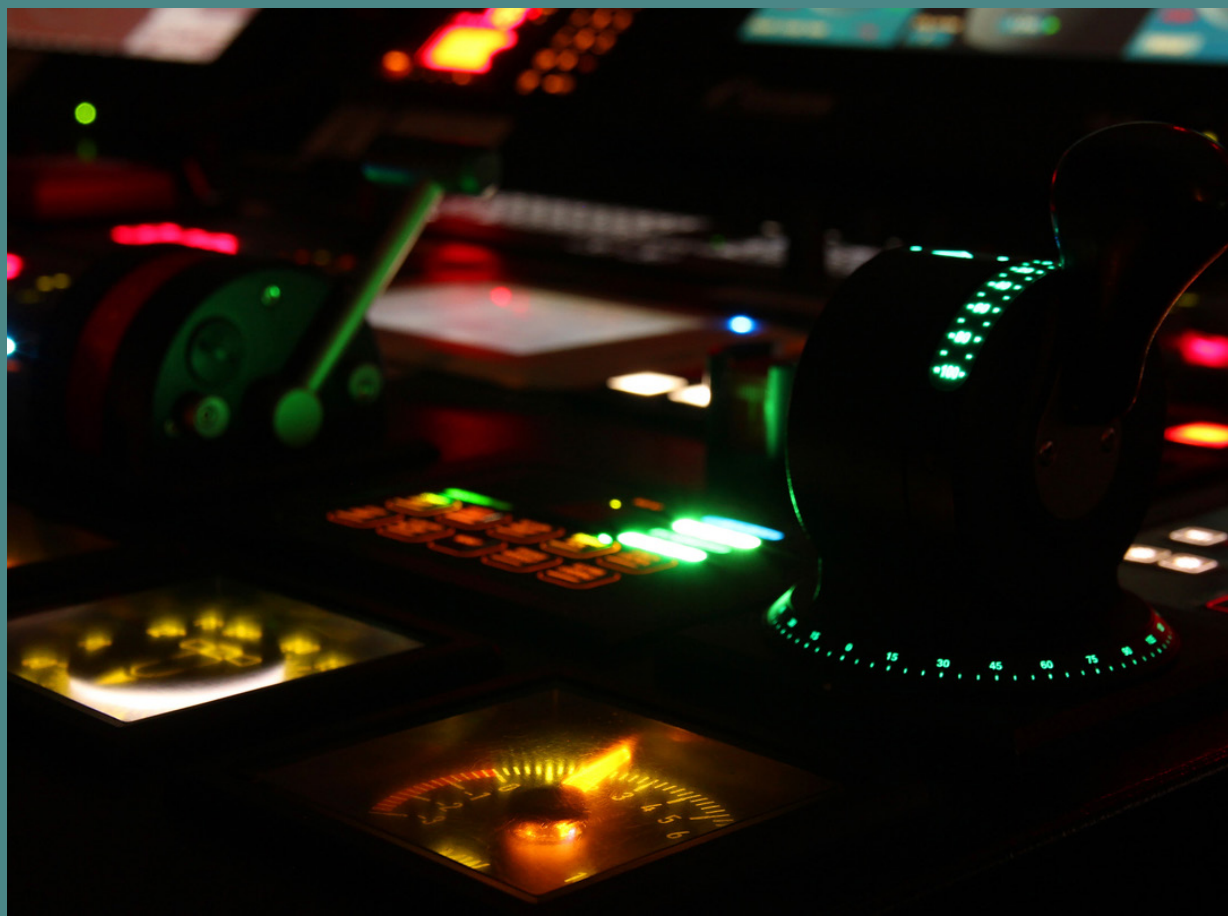
Report

Economic Sovereignty and the Question of Post-Deployment Training

First research report of initial findings from the IFOW Sandbox

Abigail Gilbert, Noam Shemtov, Philip Treleaven, Patricia Shaw, Steven Rolf, Christopher Foster, Edward Challis, Carlos Filipe Balcazar, Swee Leng Harris, Joseph Baines, Julian Germann, Tom Peters

April 2026



Funded by

Friends Provident Foundation

Contents

Funded by:

Friends Provident Foundation

Fair economy. Better world.

The Friends Provident Foundation is an independent charity that makes grants and uses its endowment towards a fair and sustainable economic system that serves people and planet. It connects, funds, supports and invests in new thinking to shape a future economy that works for all.

We are grateful for support from:

ESRC Centre for Digital Futures at Work

This work was supported by the UKRI Economic and Social Research Council [grant number ES/Z504713/1] as part of the ESRC Centre for Digital Futures at Work.

Citation

Gilbert, A., Shemtov, N., Treleaven, P., Shaw, P., Rolf, S., Foster, C., Challis, E., Balcazar, C., Harris, S., Baines, J., Germann, J., Peters, T., *Economic Sovereignty and the Question of Post-Deployment Training.* London: Institute for the Future of Work.
DOI: 10.5281/zenodo.19388140

Permission to share

Executive Summary

This report examines how AI foundation models have transformed the value of workplace data, with significant implications for the structure of the UK and wider global economy.

As AI systems become increasingly embedded in enterprise software, workplace data has emerged as a strategic economic asset. This includes not only personal data, but also tacit and explicit, individual and collective know-how: the processes, decisions, methods, and expertise that underpin workflows, specialisms and competitiveness.

Our research finds foundation model providers may capture valuable business intelligence through ongoing interactions with enterprise users, directly or via intermediaries, enabling the codification (and potential extraction) of firm-specific knowledge that can later support automation, market concentration, and competitive displacement. In many cases, UK businesses remain insufficiently aware of the economic value of this data or the risks to their own organisational success and longevity associated with the extraction and reuse of this valuable data.

The report argues that existing governance frameworks – including data protection, human rights, employment law, intellectual property, trade secrets, competition policy, and trade regimes – offer important but fragmented protections. No single regime adequately addresses how workplace knowledge is captured, processed, and redistributed across the AI value chain. As a result, economic sovereignty must be understood not solely as national technological capability, but as a multi-level governance challenge involving workers, firms, markets, and the state.

Three core implications follow. First, workplace data should be recognised as a strategic national resource. Second, governance responses must operate across multiple levels, combining legal, institutional, and industrial policy measures. Third, sovereign AI sandboxes and hybrid regulatory environments should be developed to test practical safeguards, procurement standards, and governance mechanisms.

Ultimately, the UK's long-term economic resilience and prosperity will depend on whether British firms and workers can retain meaningful control over the value generated from their workplaces in an increasingly AI-mediated economy.

Disclaimer:

Quotations used in this report - taken from roundtables and interviews with professionals working across the AI Value Chain in UKPLC - reflect the individual perspectives of participants, and should not be taken as representing the views of IFOW, nor those of Friends Provident Foundation or ESRC Centre for Digital Futures at Work.

Glossary of key terms

API: Application Programming Interface; a set of rules and protocols that allows different software systems, applications, or services to communicate and exchange data with one another.

Foundation Model: A general-purpose AI model trained on large-scale datasets that can be adapted for multiple downstream tasks and applications.

GPT: Generative Pre-trained Transformer; a class of large language model based on transformer architecture, trained on large-scale text data to generate and interpret language.

GPU: Graphics Processing Unit; a specialised computer chip designed to process large volumes of data in parallel, widely used for AI model training and inference.

Hyperscaler: A large-scale cloud infrastructure provider that delivers compute, storage, networking, and AI services at global scale.

Know-How: Explicit or tacit knowledge of the tasks, processes, or mechanisms for value creation. This can be captured in workplace data and data which may also be personal data.

Large Language Model: A type of foundation model trained on large-scale text datasets to generate, analyse, and predict language outputs.

Workplace Data: All data generated within and collected from activities by workers, as they operate within workplace environments, digital or embodied.

Open Source: Software or AI models made available under licences that permit access to source code, model weights, or architecture for use, modification, and redistribution, subject to licence terms.

Personal Data: Data governed under existing privacy regimes.

Post Deployment Training: The use of workplace data to refine foundation models after release.

RPA: Robotic Process Automation; software designed to automate repetitive, rules-based digital tasks and workflows.

SaaS: Software as a Service; software applications delivered and accessed over the internet rather than installed locally.

Small Language Model: AI models with significantly fewer parameters (typically millions to low billions) compared to large language models, designed to be lightweight, efficient, and capable of running on devices with limited computing power, such as laptops or smartphones.

UK PLC: The commercial community of the United Kingdom considered as a single entity. For the purposes of this report, the particular focus is on UK employers who are adopting and deploying new technologies.

1. Introduction

At the core of any national economy is know-how.

As the American economist Thomas Sowell once suggested, '*while market economies are often thought of as money economies, they are still more so knowledge economies*'.[1] In short: those who hold information about the methods and processes that underpin activities of value creation define the winners and losers in struggles over value – be that amongst competing nation-states, businesses, or between capital and labour.

Today, Artificial Intelligence (AI) is fundamentally changing how know-how is collected, retained, and transferred, raising questions around who will be the new winners and losers. As AI facilitates new means of creating, transmitting, and storing know-how, we foresee very significant disruption to established firms, professions and the UK economy more widely.[2] Understanding and anticipating these effects must be addressed when AI is adopted.

The topic is an urgent concern for organisations and their workforces. Microsoft claimed in 2024 that 75% of global knowledge workers use AI at work.[3] McKinsey research suggests that agentic AI – systems that can reason, decide, and act autonomously – is rapidly evolving from an experimental technology to a parallel digital workforce.[4] Salesforce project a 327% growth in AI agent adoption by 2027, with Chief Human Resources Officers expecting to redeploy a quarter of their workforce.[5]

The real ability of these novel technologies to deliver such outcomes is contested, with different academic studies delivering wildly different estimates.[6] Equally as contested is whether to see these capabilities as 'intelligence'. What cannot be denied, however, is that access to data underpins performance and the evolving inferential power of cognitive technologies.

The value of workplace data – data which encodes the methods and practices of work – has increased exponentially with the arrival of foundation models, and more specifically LLMs, which allow inferences about workplace methods to be generated from this data, allowing for subsequent automation.

Foundation model providers are aware of this potential and, alongside other techniques to improve model performance, describe this new realm of training as 'post-deployment training'. Rather than pre-training, before release, these systems are now training on data as they are used. This means that, in essence, their capability needs to be understood not just as what they can do now, but in the context of their developmental nature over time as they aggregate more and more data.

As Scott Guthrie, executive vice president of Cloud and AI at Microsoft, said in response to a question about whether LLMs would improve from their current, often disappointing state, in terms of accuracy and application in different enterprise contexts:

> *'If you look at training broadly, you'll continue to see more value from more training… but that won't always be pre-training, lots of post-training activities will significantly change the value of the model… very specific to an application or a use case… What's nice about post-training is you don't have to do it in one data centre in one location, part of the technique we've been focused on is how do we take this inferencing capacity across the world… and a lot of it is idle at night, as people go to sleep, then post-training in a distributed fashion across many sites, then when employees come to work, we serve the application'.*[7]

The impacts of this are wide-reaching. In recent months, Anthropic has released CoWork, an agentic AI assistant for knowledge worker tasks, wiping billions off European data stocks.[8] In the days preceding publication of this work, new models from the same provider have been shown capable of breaching Britain's most high-securitised, best resourced in terms of cybersecurity, industry, finance, by the UK Government's own AI Security Institute.[9]

Foundation model providers offer their enterprise clients a service which commits not to use their data for training, unless permission to do so is granted. While this clause requires further investigation, the lengths some providers have gone to in capturing data protected by copyright[10] and other regimes[11] is eroding trust in the rule of law to manage market dynamics. Even the world's greatest technologists have expressed doubt as to the ability to protect their commercially sensitive data from being used for 'post-deployment' training.[12]

These risks are further heightened by recent court rulings, which may mean models are patentable. This fundamentally shifts landscapes of power and legitimacy in these processes of data collection, inference generation, and value chain transformation.[13]

This report presents emerging insights about these risks from interviews and a roundtable with actors from across the AI value chain within British industry. It is structured as follows:

1. We set out how workplace AI sits within the AI value chain
2. We present evidence on how this is being negotiated and understood by UK PLC
3. We discuss the findings in light of interacting regulatory regimes
4. We present a new framework for an integrated conception of sovereignty which connects worker, firm and system levers.

Key Insights and Areas for Policy Development and Inquiry

Here we present key findings and policy insights. These each provoke further work and investigation. As a team, we hope to continue, in an interdisciplinary way and with the wider ecosystem, to develop key recommendations at later stages with relevant parties across the ecosystem.

Market Transformation, Market Power and Market Intelligence

Initial findings:

Foundation models have fundamentally restructured the value which can be derived from workplace data by allowing inferences to be sourced from this data, which can underpin future automation.

This has the potential to radically restructure markets in ways which require careful and conscious attention both at the firm and system level.

Know-how, which represents individual knowledge, skill and capability and the collective intelligence of firms, is being transferred out of the hands of UK firms, without awareness or risk management. While personal data, contract law, intellectual property law, and trade secrets may apply to the distribution of value between UK PLC and AI providers, there is little attention to this in practice.

While not all workplace data should be considered as valuable to those individual firms, or to the UK economy, better awareness of where value is created, transferred and the implications of this is critical.

Post-Deployment Training could threaten the economic sovereignty of UKPLC in the following ways:

- Some foundation model providers, working to avoid becoming commodities, are

incentivised to engage in data collection overreach, exacerbated by perceived social licence resulting from the non-enforcement of earlier, relevant regimes such as copyright.

- While equity investment in early-stage AI firms sees significant UK investment, as firms mature there is a shift towards the US: just 1% of firms are acquired by UK investors, vs 71% by the US. In turn, where these intermediaries collect valuable workplace data, this value can be lost from the UK economy.
- Software as a Service (SaaS) and Agentic AI providers integrating foundation models into products for their customers are not incentivised to safeguard workplace data, owing to weak demand for transparency on collection, use and processing from their enterprise customers, and or their own pursuit of 'Strategic Acquisition' by hyperscalers.

Areas for Further Policy Insight and Research:

- **Approaches to disruption need to look beyond and above the level of jobs,** to consider implications and transformation at the level of firms, and systems.
- **Deeper understanding of the categories and types of business model in relation to workplace data across different SaaS and Agentic Solution providers would assist in better governance of the digital ecosystem.** Identifying and categorising how SaaS and Agentic business models approach workplace data, potentially through formal classification and certification mechanisms, could assist firms in procurement and in considering which practical and contractual measures should be implemented to mitigate such risks and protect commercially sensitive knowledge.
- **Upskilling of UK PLC** in (a) the adaptation and development of Open Source solutions, (b) Federated Computing and (c) Edge Computing solutions could be explored to reduce market asymmetries in capability.
- **Further inquiry into the role of unions as representatives of collective data subjects should be explored and considered, beyond the domain of personal data.** The role of collective bargaining in (a) identifying what is valuable know-how within firms, (b) overcoming the limitations, at a national level, in governing the preservation of know-how could be further explored.
- **Further research into which professional, or systemic, know-how is critical at the sectoral, and national levels should inform further industrial strategy in this field.**

Legal and Regulatory

Initial findings:

Market power is perceived to be more relevant than the rule of law in shaping negotiations between businesses around workplace data in many contexts.

Legal regimes governing workplace data can shape the AI value chain in important ways. Yet they are not consistently regarded in defining approach or business model, and understanding of application is weak in relation to themes of workplace data. This leads to uncertainty or operational friction rather than clarity.

Existing regimes contain relevant and necessary foundational instruments to respond to these challenges. The Data Use and Access Bill, as relating to Business Data and Smart Data, could be explored further in relation to governing workplace data in the interests of UK PLC.

The potential to govern competition risks of post-deployment training is supported by recent developments in our competition regime. However, core principles are not being clearly abided by, and application of relevant enforcement measures is too little tested. In turn, fear of penalty may not be functioning as intended.

Areas for Further Policy Insight and Research:

Sovereign AI Sandboxes could further interrogate the application, interpretation and interoperability of law in the following areas:

- **Trade:** Cross-border data flows enable AI systems trained on worker know-how in one jurisdiction to be deployed globally, creating regulatory arbitrage opportunities that could undermine workforces in the UK and worldwide.
- **Know-How:** Current law does not adequately address how these changes intersect with the boundary between an employer's protectable know-how and an employee's personal skill, knowledge, and experience when that knowledge is extracted for AI training purposes.
- **Data Protection:** Know-how retained in an employee's mind, when systematically extracted and processed for AI training, may constitute personal data or even sensitive mental data under data protection frameworks, yet current regulatory guidance provides insufficient clarity on its categorisation and links to economic risks. As the Information Commissioner's Office takes on a growth mandate, pursuing these connections is increasingly pertinent.
- **Human Rights:** The extraction of mental data and knowledge contained within an employee's or worker's mind engages emerging concerns regarding inalienable human rights of privacy and potential questions around what should be protected from commodification.

Sovereignty

Initial findings:

The challenge of AI sovereignty is not only technological but institutional: it concerns how societies organise the governance of knowledge in an economy increasingly shaped by machine learning systems.

Decisions taken now - by workers, firms, regulators, and policymakers - will play a significant role in determining whether the benefits of this transformation are broadly shared or increasingly concentrated.

Sovereignty in practice involves a distributed set of capabilities within and beyond the state. Practical negotiations and coordination shape sovereignty at various scales, with even highly local or small-scale transactions between worker and firm, or firm and SaaS company, contributing to and shaping global processes.

Areas for Further Policy Insight and Research:

Our work invites:

- An approach to technology regulation, governance and development which begins with and from understanding of the AI Value Chain.
- A review of the adequacy of 'consumer pricing' as an organising principle for the governance of competition;
- A move away from cybersecurity focus on 'malicious actors' to cybersecurity as a route to the protection of value within digital ecosystems.

Sovereign AI Sandboxes are critical to ensuring effective adoption; and should take a 'full stack' approach. Sandboxes could investigate the conditions under which users of foundation models may 'give permission' for data use for training; the ways in which API integration may lead to data collection beyond 'input and output' interaction; and use combined operational and regulatory approaches to develop, and test innovate approaches to value preservation and sharing.

History and Methodology

This project represents the culmination of six years of work at IFOW exploring the codification of work methods. This began in 2021, with a review of the way connected worker platforms were codifying the know-how of essential workers across the economy during the coronavirus pandemic. It was here we first saw firms seeking to elicit work methods and processes.

This paper builds on that work, using recent data from the IFOW Sandbox (for which we've produced a separate methods report), with supplementary roundtables and interviews.[14]

2020/2021 and The Rise of Connected Worker Platforms

During the pandemic we interviewed eight connected worker platform providers as part of a wider project.[15] Connected Worker Platforms (CWP) are Software as a Service (SaaS) providers looking to become 'Microsoft for the 80% of the world's workforce who don't sit at a desk'. These solutions saw rapid expansion and uptake during the pandemic for essential workers, such as those in manufacturing, maintenance, logistics, mining, telecoms, energy and food production. CWP developers we spoke to were explicit about their intention to elicit work methods, practices and processes from the workplaces they serviced in order that this could form the service they provided to firms at a later date.

During this phase, work method elicitation came through either (a) employers inputting work instructions or (b) workers uploading their work methods, adding pictures to support future instructions in real-time or, otherwise, (c) extensive surveillance in the name of deducing work methods through Machine Learning. At this time, before foundation models were established, option (c) was seen as the least effective.

2023: Foundation Model Integration in SaaS

Foundation Models are AI models trained on massive, often unlabelled datasets. LLMs can then be used to generate inferences about workplace methods from this data In 2023, we re-engaged two of the Connected Worker Platform developers we spoke to in 2021. We learned that they perceived LLM integration within their platforms to be rapidly advancing their ability to elicit work methods, overcoming the barriers to strategy (c) outlined above.

2024: Generative AI in the Creative Industries

From 2022 and the launch of Generative AI concern began to arise about automation of non-routine tasks and work. The focus of these debates was on web-scraped data, copyright, and creative work. As part of a wider study, we found that neither workers nor firms knew that - or how - their data was being used to train these models.[16]

We conducted a survey of UK creative workers, who, when asked whether they think their work had been used to 'train' Generative AI systems, the most commonly responsed that they didn't have enough information to know, didn't know where to find information (33%), or suspected it had been used but did not know for certain (30%). Only 5% said that they knew their work had been used to train Generative AI and had given permission.

2024/2025 Sandbox Activities

In 2024, our Sandbox Open call sought out businesses that were looking to integrate new solutions which could be used to achieve the codification of work methods and processes. In 2025, a case study conducted within the IFOW Sandbox highlighted the risks stemming from economic and informational imbalances within the AI value chain, particularly concerning the collection, usage, and processing of workplace data.

Our Sandbox uses a methodology which surfaces interactions between different actors in the AI Value Chain, while focusing on the workplace or enterprise adopting new technologies. Our Open Calls focus on technological use cases which allow us to explore broader conceptual challenges. Through three cases within a first Open Call, this research brought to light risks and issues in the value chain relating to workplace data.

Through one of three cases, we found that SMEs are not thinking about the value of, or risks associated with, allowing others to secure value from the codification of methods within their workplace. Furthermore, those SaaS providers offering services with integrated GPTs were not confident that the technical or legal solutions they had in place to preserve access to that data (and therefore the value to be derived from it) were effective.

Our Sandbox Methodology is published as a separate report, IFOW Sandbox: Phase 1 Methodology Report.

2025/2026 Validation Activities

To check the reach and cross-sectoral relevance of findings from the IFOW Sandbox, we co-convened a roundtable with Automate UK in late 2025, hosting nine industry representatives. We then supported this with a series of five interviews with wider industry actors.

2026 Novel AI Value Chain Analysis

This report also includes a novel assessment of investment in the UK AI Value Chain. Our data on investment in UK AI firms is gathered from S&P Capital IQ Pro. We gathered data on all equity deals involving self-declared AI firms headquartered in the UK, a total of 2704 transactions. Percentages represent relative share of overall deal value by nationality of buyer.

2026 Legal and Policy Review

We have undertaken an extensive legal and policy review to understand how regimes at the individual, firm and system level apply to these questions and how these currently work to manage the distribution of value and associated risks.

2. Introducting Workplace data and the AI value chain

"If you're not able to embed the tacit knowledge of the firm in a set of weights in a model that you control, by definition, you have no sovereignty. That means you're leaking enterprise value to some model somewhere."

S. Nadella, Interview at World Economic Forum, Davos, January 2026[17]

2.1 The Development of Cognitive Technology

'Things have evolved a lot. In the late 90's, we had to work out what expert knowledge was and import it into expert systems – and quiz people about how they did their work. Now with LLMs and ML (machine learning), together, agents – in theory they can learn the rules and come up with the approach you need'

Director of AI Ethics, UK Based MNC

'If you are any Silicon Valley company you're in a situation where you want to get as much access to data as you can...'

Interview, AI Governance Director, MNC

'When a VC (venture capitalist) comes, they'll ask: where is the value and who captures it?'

UK RPA CEO, Interview

Codifying work methods is core to the history of automation. In practice this has relied on a range of approaches to collecting and processing data (see Table 1). Platforms, which operate as business models designed to maximise the collection of data, and exclusivity of access and subsequent rental value of that data, have been highly effective in the collection of this primary resource – turning the structure of the global economy on its head. While the tech sector jumped from 16% to 56% of market capitalisation, oil and gas plummeted from 36% to 7%. [18]

The scale of this automation impact could be significant. McKinsey notes, 'AI agents could now be the evolution and the creation of a digital replica of the entire workforce of an organisation'.[19] This digital replication requires capturing the know-how that makes human workers effective - their understanding of processes, their ability to handle exceptions, and their judgment in ambiguous situations.[20]

As the Competition and Markets Authority notes in its recent review of foundation models, there has been a trend toward integration of these tools in wider, commonly used digital products and services, such as AI Agents. This builds on a history of leveraging behavioural data as a business model within the digital economy.

With access to worker outputs, decisions, processes, methods, and ways of working over long periods, this work can now be codified. Employee inputs, corrections, and feedback on AI outputs can become training data used to improve these systems. This creates a continuous extraction of tacit knowledge: the AI learns not just what decisions were made but how they were made, including the contextual judgments, information about process decisions, choices, and experiential knowledge.

Workplace data can be collected from a range of sectors and serve different kinds of value proposition. Collecting it requires hardware of varying kinds, supportive software processes to support access to data, and firm-level practices of adoption of these processes.

Table 1 - History of Workplace Data Applications[21]

Class	Inferential Power	Data Dependencies (Sources, Types, Collection Hardware)	Function	Infrastructural Dependencies
Robotic Process Automation (RPA)	0 / 10	Sources: Enterprise software interfaces Types: Structured inputs (forms, spreadsheets, records) Collection: APIs, stable UIs, databases	Follows fixed rules, no learning	Legacy IT systems, workflow engines, rule engines, enterprise software with stable schemas
Expert Systems (Rule-Based AI)	1 / 10	Sources: Human experts Types: Codified rules, decision trees, logic statements Collection: Knowledge engineering, manual encoding	Follows fixed rules, no learning	Rule engines, symbolic logic systems, domain-specific software
Narrow Machine Learning	3 / 10	Sources: Behavioural & operational datasets Types: Labelled tabular data, time series Collection: Databases, logs, sensors (limited)	Learns patterns for one task	CPUs, statistical ML libraries, data pipelines, feature engineering stacks
Deep Learning	5 / 10	Sources: Large-scale datasets Types: Images, audio, video, text, sequences, transactions Collection: Cameras, microphones, sensors, scraped datasets	Learns complex high-dimensional patterns	GPUs, cloud compute, CNNs, RNNs, LSTMs, training clusters
Generative AI (LLMs, Diffusion Models)	6 / 10	Sources: Public web, code repositories, media corpora Types: Text, images, audio, code (unstructured) Collection: Web scraping, digitisation pipelines	Creates text, images, code and can generate 'ideas' through novelty if not creativity	GPUs / TPUs, massive training datasets, distributed storage
Agentic AI	7 / 10	Sources: Workplace systems, tools, APIs Types: Workflow logs, emails, action traces, databases Collection: Sensors, enterprise software telemetry, API instrumentation (needs real time feedback loops)	Plans tasks, uses tools, interacts with systems	LLMs + planners, tool orchestration layers, execution environments, distributed inference

Table 2: Types, Value Proposition and Accelerants of Workplace Data as Post Deployment Training Data[22]

Class	Sectors	Data Type	Value Proposition	Technological Accelerants
Knowledge Work Data	Desk-based (professional, managerial, administrative)	Work outputs (documents, messages, code) Processes and workflows Methods, rationales, decision traces	Codification of cognitive workflows allowing for full displacement of roles, or their augmentation	LLM integration into productivity suites Autonomous & semi-autonomous agents Digital twin of individual workers Workflow logs, agent traces Retrieval-augmented generation (RAG) Enterprise platforms (Teams, Zoom, Slack, O365, Notion) Synthetic data generation Post-deployment training
Embodied Work Data	Essential, physical, logistics, fieldwork, service work	Sensor-collected data (audio, video, motion, proximity, wearables) Biometric signals (in some regimes) Task sequences and physical action traces	Codification and automation of physical workflows; allowing for displacement, augmentation, or prediction and optimisation of human labour	IoT infrastructure Computer vision & edge AI Wearables & biometrics (where permitted) Workplace digital twins & simulation Robotics and cobots Environmental sensing (Lidar, RFID, telemetry)
Business Data	Whole economy (infrastructure, logistics, supply chains, procurement practices, markets)	Supplier/ provider records Transactional data Spatial & geolocation data Machine logs Network structures	Modelling market structure, price dynamics, supply chain resilience; agent-based simulations	Large-scale databases & cloud infrastructure Geospatial data Enterprise resource planning (ERP) data streams Digital twins of supply chains Autonomous decision systems (pricing, routing, scheduling)
Workforce Data	Whole economy (HR, performance management, labour allocation)	Work patterns Productivity traces Behavioural data Allocation, scheduling and availability data	Predictive models of workforce behaviour; optimisation of task allocation and labour deployment	Behavioural AI Enterprise HR platforms Reinforcement learning from human feedback (RLHF) in workplace settings

This table was iterated in dialogue with ChatGPT and reviewed by domain experts.

2.2 Introducing the AI Value Chain

> *'In economic terms, machine learning algorithms are self-improving means of production; they appreciate instead of depreciate when used. The result is that they operate as a self-reinforcing monopoly mechanism.'*[23]

At London Tech Week earlier this year, Prime Minister Keir Starmer said he wants the UK to become an "AI maker, not an AI taker". Indeed, a recent report published by the Government Department for Science, Innovation and Technology (DSIT) finds that the UK is developing a vibrant AI business ecosystem with over 5,800 specialist firms – a 58% year-on-year increase.[24]

Firm and equity ownership is one important component of sovereignty. Another is location in the network of interfirm relations through which AI technologies are designed, delivered and enhanced – what we call the 'AI value chain'.

AI, as an evolving and phased technological field, is not merely a General Purpose Technology - i.e. one with economy-wide impact – but a generalising and adaptive infrastructure. Its economic power compounds through increasing control over data, learning and deployment environments. Each successive increase in inferential capability has been enabled not by model improvements alone, but by access to new and exclusive datasets, and the power to process that information. A critical question when looking at any developmental technological process is who will benefit from data collection, use and processing – and who will stand to lose. These discussions are often framed around questions of the AI Value Chain (the interconnected set of firms and services involved in the development, deployment, and iterative improvement of AI models).[25]

When thinking about workplace data it is important to consider that this value chain is not only compute power, models and SaaS solutions – but also includes:

(a) Workers, who create the enterprise level data which encodes processes of work

(b) Enterprises, which are a portal to access workplace data for post-deployment training.

Recognising these actors introduces new questions about value distribution, applicable regulatory regimes, and power dynamics within the marketplace as this relates to transparency and knowledge about how value is being restructured.

Infrastructure Layer

Hardware - Chips

A GPU is a special computer chip designed to process high volumes of data. NVIDIA, a US-based company, has an 81% market share for data centre chips according to recent research.[26] The UK has been core to developing new IP for GPUs via a company working on strategic semiconductor development, but this is now majority owned by foreign capital.[27]

The supply of silicon chips has become a site of geopolitical tension and bargaining. As the Secretary of State for Science, Innovation and Technology suggested in a recent speech: 'Semiconductors have literally become bargaining chips amongst competing nations, and in some cases the AI supply chain is being weaponised for national advantage'.[28] The White House has floated 100% tariffs on imported semiconductors (with carve-outs for companies manufacturing in the US).[29]

Compute

Compute – also known as 'cloud infrastructure' (Infrastructure as a Service - IaaS) – is the collection of hardware and software that allows services like storage, computing, and networking to run over the internet rather than on your personal computer. The cloud market, 'where the internet lives', is dominated by three providers: Google Cloud (13%), Microsoft Azure (20%), and Amazon Web Services (29%). Two are dominant in the UK, with Amazon Web Services (AWS) and Microsoft each having around 40% of market share.[30] Oracle and IBM have considerably smaller market shares, only up to around 5% of UK IaaS.[31]

A Parliamentary Office of Science and Technology (POST) note recorded that.... 'some stakeholders have expressed concerns about storing data belonging to UK organisations and individuals in jurisdictions where the UK has no legal control.'[32]

It is estimated that 92% of the Western world's data are stored in the United States.[33] An estimated 89% of the UK's larger organisations use at least one cloud-based service. According to the US International Trade Administration, the UK is the largest cloud market in Europe and the second largest ICT market in the world, right after the United States.[34] Cloud providers have begun to offer private instances to manage business concerns about this.

The Workplace AI Value Chain

Data Creation Layer

Workers

- Generate raw data through labor, decisions, and interactions
- Apply tacit and explicit knowledge within digital systems
- Train systems, not only producing but also validating systems

Enterprise Adopters (Employers / Operators)

- Procure and integrate technologies
- Define workflows, incentives, and governance that make worker knowledge usable

Inferential Layer

SaaS Providers

(e.g. agentic platforms, digital twins, enterprise solutions)

- Surface, classify, and operationalize data
- Act as the interface layer between firms and AI capability
- Increasingly embed GenAI capabilities into their software

Model Providers

(E.g. LLM vendors, foundation model providers)

- Reason, synthesise, predict, and generate data, predominantly integrated for text-based analysis
- Available either directly or via SaaS (bundled into applications), or directly

Infrastructure Layer

Compute

- Store and manage data at scale, can provide networking, and security
- Enable training, inference, and real-time deployment
- Often vertically integrated with Generative AI providers

Chips

- Supply specialized chips that make large-scale AI feasible
- Set the physical constraints and economics of model training and inference

In 2023 the British Government reviewed compute provisions, disclosing that as of November 2022, the UK had only 1.3% share of global compute capacity.[35] Research by the UK's communications regulator in 2023 suggested that dominant cloud providers generate profits of around 20-40% suggesting a weak competitive environment.[36]

In September 2024 the UK designated data centres as critical national infrastructure, comparable with water and energy. The National Planning Policy Framework was updated in 2024 to consider the need for data centres as part of modern economic infrastructure. Data centres are defined as Nationally Significant Infrastructure Projects, streamlining consent and making decisions centrally rather than through local authorities.

In November 2025 the AI Growth Zones Policy set out the aim of fast-track, investment-friendly regions for large-scale AI-capable data centres.[37] This offers investment incentives and planning support for data centres in designated regions of the UK with reduced

electricity costs and accelerated grid connections. With the UK's Tech Prosperity Deal these initiatives sought to foster greater collaboration in AI with the US, including NVIDIA announcing that it will be building several new 'AI factories' as advanced data centres in the UK, with OpenAI and NVIDIA establishing Stargate UK. This aims to offer a threefold increase in UK data centre compute by 2030.

Inferential Layer

Models

An AI model is a computer program that learns patterns from data so it can make predictions, decisions, or generate responses. In simple terms an AI model is a system trained on data to perform tasks that normally require human intelligence.

Foundation models are AI models trained on massive amounts of data, that can be adapted to different tasks. These are 'general purpose' and can provide a base for many different applications (and so are 'foundational').

All the infrastructure-layer compute 'hyperscalers' (e.g. Amazon Web Services) offer a foundation model, each of which is integrated into services and markets in different ways. However, not all model providers are part of an integrated stack. Notably, OpenAI and Anthropic do not own significant hardware or compute capability directly, but instead rely on partnerships with hyperscalers for training and inference.

There are 'open' and 'closed' model providers. In this report, open models are defined as those with downloadable weights (including those with restrictive licences), while 'closed' models can only be accessed via an Application Programming Interface (API) or a hosted service. Where an open model is used, it can be hosted locally, assuming the entity has sufficient compute capacity. Among the most notable open models are China's DeepSeek and US-based Meta's Llama.[38]

The relationship between Model Providers and Compute Providers is important. Where these providers are not part of an integrated or 'vertical' stack (an integrated stack being where the model provider is also a compute provider) model providers are intermediaries in value chains, with powerful players on both sides – hyperscalers upstream, and enterprise customers downstream.[39]

At present, Generative AI model providers are competing on the basis of brand and quality. However, models could become commodities – interchangeable, largely undifferentiated, and competing on price. Such an outcome would ultimately be good for infrastructure companies, but bad for model providers who are not vertically integrated. While it is near inevitable that model capabilities improve, the question is which firms will dominate in this space. Where models improve, this is a positive for multiple parties: infrastructure firms, integrated infrastructure and model firms, and the model providers. In turn, model-only providers have a particularly strong structural interest in ensuring continual improvements to performance and utility within new domains.

SaaS and Agentic AI

According to DSIT, the UK's AI sector has grown 150 times faster than the broader economy since 2022. Between 2022 and 2024, AI company revenue grew from £10.6 billion to £23.9 billion, a 125% increase. Employment in the sector rose 72% to 86,139 jobs.

Of the companies surveyed in the AI Sector Study by DSIT, 35% reported they were engaged in model training and development; 25% said they were working on sub-frontier models; 3% were working on LLM development; and 2% on foundation model training. In contrast, 51% were working on knowledge synthesis: the largest of any cohort. The second largest cohort was perceptual systems – involved in anomaly detection, computer vision, image processing,

signal detection, multi-modal integration, and audio processing. These capabilities are core to the development of useful and meaningful training data.[40] In this sense, they can be seen as enablers of value creation for the integration of foundation models into wider work processes.

However, our novel and primary analysis (Figure 1) also demonstrates that despite its successes in fostering AI startups, the UK's relatively weak capital markets render its firms vulnerable to acquisition by US investors. Of equity investment in early-stage AI firms, 38% derives from UK investors – a similar quantity to US investors (35%). However, as firms mature and require more capital, US investors come to the fore. During later financing rounds, just 16% of equity issued is purchased by UK investors, and 62% by US investors. And the picture in Mergers and Acquisitions activity is especially stark: just 1% of firms are acquired by UK investors, and 71% by those based in the US. These data imply that far from being an 'AI maker', the UK's AI startup ecosystem functions as a pipeline for acquisition by US firms.

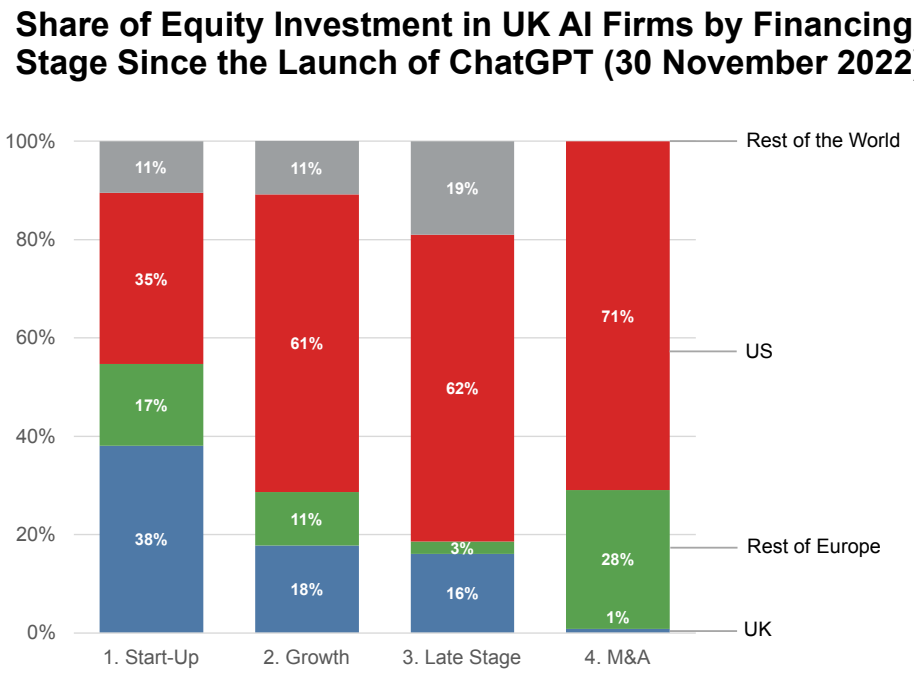
This may mean that inferences generated by these intermediaries are ultimately acquired by US hyperscalers, concentrating insights rather than seeing greater market plurality.[41]

Data Creation Layer

Enterprise

Studies reporting UK business adoption report varied figures. One study found up to 79% of UK firms – with the same rate across large and SME businesses – had adopted AI to automate a cognitive or manual task by 2023.[42] In contrast, the ONS reported in September 2025 that just 23% of all UK businesses (knowingly) report the use of AI tools, up from just 9% in September 2023. For medium-sized enterprises (50 to 249 employees) adoption was found to be significantly higher, at 65%. This difference could well reflect differential confidence and competence in adoption.

Figure 1: Share of Equity Investment in UK AI Firms by Financing Stage Since the Launch of ChatGPT (Nov 2022)



Using S&P transaction type classifications, start-up investment includes accelerator, pre-seed, angel, crowd-funding, seed, pre-series A, and series A. Growth stage investment includes series B, series C, and growth. Late stage investment includes mature and series D, E, F and G. Dataset ends in June 2025.

Source: Authors' elaboration of data from S&P Capital IQ Pro (2026)

More consistent is evidence that, overwhelmingly, firms procure these tools rather than build them: 78% of businesses report accessing, buying, listening to or using third-party AI tools. More than half (53%) rely exclusively on third-party AI tools.[43] 80% of firms say they will commit 10% or more of their total AI budget to meeting regulatory requirements by 2024, with 45% planning to spend at least 20%. However, firms overwhelmingly lack knowledge of how to adopt responsibly. Only 19% said their organisation had implemented a responsible programme or capability, and 27% report inability to recruit talent with knowledge of AI regulation as one of their top three concerns.[44]

A study released in early 2026 by DSIT and DCMS (Department for Culture, Media and Sport) found that among the general workforce, 56% of employers whose businesses are currently using or planning to use AI rate the level of knowledge in their business overall as 'beginner' or 'novice'.[45]

There is sectoral variation in adoption too. IT and telecoms leads at 56% to 93%, followed by finance at 83% and marketing/media at 53%. Manufacturing trails at 19%. The Financial Times reports that half of retailers are adopting Agentic AI solutions, despite the absence of infrastructural or contractual competency to do so safely.[46] This is a serious issue, as 49% of UK businesses cite data privacy and security as their top concern.

However, these concerns are commonly reported to relate to processing of personal data, (GDPR breaches) client data (reputational breaches) or secure data for Critical National Industries as this may be impacted by malicious actors. We suggest that the UK debate around cybersecurity has not yet paid sufficient attention to risks relating to the leakage of know-how.

Workers

A 2026 study by DSIT and DCMS found that 97% of members of the public they surveyed had heard of AI, with 73% reporting having used or consumed AI in the past month. While the British public is highly engaged in using AI in personal and workplace life, trust is low. This may reflect understanding of how it works in practice.

Only 17% said they can explain AI in detail; 28% feel confident using AI in daily life; and 21% feel confident using AI at work. Despite this, there is growing evidence of employees' use of AI outside of their organisational policies, with Microsoft reporting 71% of UK employees using unapproved consumer AI tools at work.[47]

In 2024, 6.67 million employees were trade union members.[48] In terms of negotiating the impacts of adoption, union membership among UK employees fell to 22% in 2024, according to official statistics.

Nevertheless, trade unions are pursuing collective responses to AI adoption within enterprises, thereby shaping value chains. The Trade Union Congress has developed legislation to address the use of AI models for automated decision-making in the workplace through transparency, worker consultation and a union right to data, for example.

3. Lessons from Practice on Workplace Data as New Source of Value

Here we share insights from our conversations with UK PLC about how workplace data features within the value chain, and how different economic and technical frictions shape business strategies and outcomes. This begins with a review of different 'moats' (commonly used to refer to the commercial advantage a company has in relation to protection from competitive threats) and then considers how these business strategies are shaped by geopolitical factors.

The strategy of many agentic solution providers is to learn how to perform a narrow function in a business by accessing workplace data from their first clients. This is often secured through a lower rate for the service.

> *'If I was setting up a company now, I'd want to be able to ingest all the information required to substitute a function. So, let's say it's payroll – I would need to know all the inputs and outputs. Let's say I'd provide a solution from the first ten clients of my SASS company, by the eleventh customer I want to be able to perform like someone who has worked in payroll for fifty years.'* **CEO, UK Robotic Process Automation (RPA) company**

Yet data that is chaotic, and not classified, is not in and of itself valuable. How data is archived and organised determines its quality and utility for effective training.

> *'Partners have a tonne of knowledge. You need that to be accessible. That information is all there but systematising what's recorded in a cogent way is the challenge. I can create a human in the loop step. So if someone asks a question to digital Abby - then if someone tries to ask me, you can [give] permission [to] them seeing it. Abby is someone to trust.'* **Digital Twin Provider, Roundtable**

> *'A company is a multitude of different things… if you're getting data across the piece that could break down into a thousand different agentic SaaS solutions, I don't think that's ridiculous… You can make money by bundling or unbundling in tech'* **UK RPA CEO, Interview**

The providers of bespoke, industry-specific workplace agents are also helping to clean workplace data, through a range of measures. This can include recognising what primary data is to be trusted, or by enrolling workers in editing and refining content.

> *'Rather than human in the loop, it's more like reinforcement training by workers using these systems in real time: the data they edit helps improve the system'* **Roundtable Participant, UK Digital Twin company**

At a foundational level, the data which encodes worker know-how, expression, choice and creativity across many cases is what constitutes a firm.[49]

> *'What is a company? It's a bunch of brains and keyboards… the workforce changes, it's the collective know-how, the brand, the customers, and the systems and processes that persist… people accrue learning and take it elsewhere… that's just on scale with these systems'* **CEO, UK RPA company**

3.1 Differentiated 'Moats'

In discussing workplace data, it became clear that businesses are operating on very different models, with different strategies in terms of their moats and workplace data, shaped also by their position in the value chain. The firms we spoke with conceived the requirement for security of workplace data in different ways, reflecting their specific business model.

To capture the value of these inferences, firms rely on technical approaches to design which can prevent data use and processing by third parties. However, firms also rely on a business model which sees exclusive access to these inferences as its value proposition.

SaaS Provider: Our Moat is Relational

SaaS services integrate foundation models to their products via API, to support accessibility and use of their product, or to support other functions, such as the development of digital twins for enterprise clients. The Commercial Director of a UK RPA provider told us they had recently adopted a range of models to aid delivery. They had trained Claude on their own codebase, incorporating tacit knowledge of their developers to increase speed and performance of workflows:

> *'What used to take three weeks now takes three hours, but it relies on us inputting ten years of our codebase, work we've developed, into Claude'*

When asked if this was seen as a risk, the firm did not feel this knowledge was their moat:

> *'We don't pay much attention to our competition anyway, whether it's another business or an AI trying to compete – a big part of what we do is getting to know a business's pain points, spending time with them to understand what the problems are'.*

In sum, this business model is best understood as one in which the firm's value lies in diagnosing and articulating the client's problem, rather than in the intrinsic originality of the solution. Accordingly, once the issue has been properly identified, the development and execution of a solution may demand time, expertise, and resources, but it is not the primary locus of competitive advantage. The firm differentiates itself at an earlier stage, through analytical insight, problem framing, and strategic judgement.

For that reason, sharing knowledge relating to the solution phase is not typically regarded as commercially sensitive. Because competitive edge rests in problem identification rather than solution delivery, this 'sharing' does not compromise the firm's position. However, this firm also disclosed that they do not include in their contracts with clients explicit mention of their integration of foundation models, or terms on the collection, use and processing of data. When asked, they disclosed that nothing in their contracts prohibits this and clients do not ask them such questions. In this sense, this business model is ambivalent to the outcome of workplace data collection from clients, and could be hostile to raising this as it may impact sales to customers.

Some felt the entire SaaS model was undermined by recent developments with open source, enabling firms to develop bespoke solutions easily, manage their data, and make a shift to localisation:

> *'People are thinking maybe we need to start looking at a market shift from SaaS to ownership, because that seems to be, I mean, you know, the market is rattled. And I think that's part of the reason why investors now are starting to feel, you know, well, the whole SaaS model might be in trouble.'* **AI Adoption Consultant**

Agentic Provider: Looking for Aqui-Hire

Agentic solutions rely on model providers to deliver solutions.[50] Agentic AI solutions, by design, feature environmental learning – i.e. the development of inferences from interactions within an enterprise environment. This can lead to the substitution of a function (learning from across many workers), but where expertise is significant, agentic solutions can also work as the architecture to support recognition of what data, or persons, are trustworthy to use for training a model. An example of this is in law. Not all emails and exchanges are of equal value within a law firm. An Agentic AI solution could be deployed to simultaneously (a) identify whose data is trusted within a business (e.g. a senior barrister) and (b) undertake permissioning of access to this data.

In this sense, an Agentic solution could be used to clean and organise workplace data, reducing noise for training.

> *'Databases are as valuable as the LLM in our product – to only focus on LLMs, which people are [doing] at the moment, overlooks the rest of the foundational technology that's enabling these tools'* **Agentic AI provider, Roundtable**

Generative AI needs use cases, customisable interfaces, and knowledge of domain-specific innovations. To this end, OpenAI has been using 'Forward Deployed Engineers' to go to OpenAI customers and work on downstream applications. A recent job description suggests that '*OpenAI's Forward Deployed Engineering team partners with customers to turn research breakthroughs into production systems. We operate at the intersection of customer delivery and core platform development*'.[51]

As one Digital Twin provider suggested, as they provided a new agentic solution through the Microsoft architecture, it was in their view inevitable that they had access to the data, despite the provider using an independent Azure instance for processing. This acceptance may be linked to an ultimate strategy for aqui-hire.

> *''Everything comes down to user experience and user interface. And for user experience to be any good now, you need an LLM so that people can interact with a system in natural language… Is there a cheaper way to do it? Yes, but no one wants to do that, because the hype cycle we are in means you need to get ahead fast. At the end of the day, Microsoft own the entire stack – they have access to whatever they want….'* **Digital Twin Developer, Interview**

Hyperscalers are underpinning this market – precisely because their future value is reliant on it. As one roundtable participant shared:

> *'If the AI bubble bursts tomorrow it's the end of free tokens… our business model works because we have cheap tokens, funding so we can develop and use the LLM's, the next ingredient is the data from the companies – this has always been there, we aren't automating knowledge creation just knowledge retrieval and dissemination'* **UK Digital Twin SaaS, Roundtable Participant**

Enterprise Level: This is existential risk

In contrast, at the enterprise adoption level, as suggested by a Director of AI Ethics at an FMCG MNC, the codification of organisational know-how was seen as a major risk to their own moat:

> *'The agent is gathering the know-how of the business… and our competitive advantage is potentially being let out of the door. If you were to price it, it would be something you'd have a lot of trouble pricing. But if you did try and price it, you'd come up with a very big number for what is the value of, you know, all the data that encapsulates how a big company like [us] does procurement, logistics, advertising, deployment – all the areas where agentic AI is being proposed… our competitive advantage is really in our ways of doing business – and that's what these systems are learning… it's an incredibly valuable resource, and its compared to brand building.. if someone has access to it, then you know there would be little you'd have to do to operate as we operate.'*

Above, we explained that a UK RPA-SaaS provider may not perceive client workplace data, or the inferences from this, as their 'moat'. This is the first disincentive to design for security. However, this has an impact on the firm they provide to. With that in mind, we asked the same organisation whether, given that they integrate a mainstream LLM into their product for clients, those clients had asked about data collection use and processing. Their response, as shown in that of others, was that enterprises are not aware of risks relating to data collection use and processing beyond personal data.

> *'No clients have ever asked us whether we're using whatever [data], our customers have trust in us that we can reassure, but there's only so much you can know or do… We don't have a policy in place to say that our clients have to agree to us using an AI, they just think it's useful and can help with the business. It's generally protected by data protection, but nothing specific on that wider piece.'* **Director of Commercial, Automation Process Provider, Interview**

> *'SMEs don't understand and aren't aware of the obligations on them, or the ways to be more cyber-resilient.'* **Sandbox Participant, SaaS provider**

Perhaps reflecting the scale of governance capacity unique to a Multinational Corporation (MNC), the Director of AI Ethics at a MNC specialising in fast moving consumer goods (FMCG) highlighted that it was procurement which first brought these risks to light:

> *'It was actually someone in procurement who brought it to my attention, rather than us in the AI Ethics Team… We started to see these very terms in contracts a few years ago: companies that used to provide data services saying 'you can have this but it can only be consumed by humans, and you're not allowed to feed it into your own models'… Now we have a clause that suggests a firm needs to prove it will only be retaining our data for the delivery of our services and no other purposes... but there's no way to prove they are compliant with it; we just have to take them at their word'.*

The potential for future deals, once firms recognise the extent of this potential value transfer was raised from an acquisition perspective:

> *'Almost every company you've heard of is piloting this. And I'd be surprised if any single one of them had made a kind of board level decision to run on it, and more surprised if*

they had thought through the consequences about the sovereignty of their data. And perhaps if they did, they'd think about this as a whole firm transformation and say: 'let's put this on the table as something someone can buy, as an eight-figure sum or whatever; this is us, this is our value.' I've not heard anyone coming out and saying: 'you need to provide me a solution that guarantees security against this.'

While this is a long way off, the potential implications for market concentration are significant and worthy of consideration from a systems-level perspective.

3.2 Value Chain Geopolitics

Conversations about what could preserve the value of workplace data at the enterprise or even SaaS level highlighted the inherently socio-technical nature of this challenge, with politics, power and ideas as important as technical safeguards or measures. While technical security does sit on a spectrum reflecting both system design and human behaviours (such as compliance with organisational cybersecurity practices), when working with hyperscalers, trust was seen as the most critical factor. Factors shaping trust included (a) aligned market interests, such as in the context of a SaaS business strategy that is working towards sale to a vertical provider, and (b) aligned geopolitical interest.[52]

Data Collection, Use and Processing

Research on federated computing highlights architectures in which data remains under the control of the organisation that generates it, while analytical models or computations move across distributed systems to integrate insights.Rather than pooling raw data centrally, federated approaches allow organisations to participate in collective learning while retaining control over underlying datasets.

Related approaches – including edge computing and local model deployment – operate on similar principles. In edge or local architectures, data is processed close to where it is generated (for example, within enterprise systems or on-premise infrastructure) rather than being transferred to external cloud environments. These approaches can reduce exposure of sensitive information while still enabling AI functionality.[53]

However, such solutions have not been relied upon, with cloud storage, offshore, having become a common aspect of the UK industry operating model. In a 2024 survey, 74% of UK businesses reported that they had adopted cloud computing in almost all areas of business operation.[54]

'Industries have been collecting data around process for many years: it's just where it's stored. In the past it was always on premise. Now it's changing – where it's stored and who gets access. If you look at cloud providers, they might not be in the locale, and those providing services might ask to sign out of GDPR because it's costly.' **Roundtable Participant**

The use of Generative AI shifts risk because for data to be processed via an LLM, it cannot be encrypted. Furthermore, several interviewees reported that it wasn't possible to run models on their own compute:

'To access the large models you don't really have the choice to run the software on your own compute (they're too big) so you have to transfer it to the large cloud providers and ultimately at the point the LLM model is reading it its unencrypted and so that has a certain degrees of risk associated with it.. I wouldn't give all of my sensitive commercial information in an unencrypted way to any other company. So why would I give it to these?' **AI Consultant, Interview**

Rather than an absolute risk, several participants understood this as just elevating the need for good cybersecurity protocols.[55]

> *'The thing is the encryption just has to be done in a manner that doesn't allow somebody to come in and put patterns together, and we can argue about that once you get into quantum computing and how well the encryption data keys will work…'* **CTO for multiple UK SaaS firms, Interview**

Open Source and Design Alternatives

Foundation Models typically operate as a service, being hosted remotely and accessed via API. In contrast, Open Source solutions allow for the weights, parameters and run file of an LLM to be downloaded, for local use and, potentially, hosted on a more secure service of a firm's choosing. Using an open source model is a strategy which might be adopted by those who are looking to have exclusive access to inferences developed from workplace data, have the skills to work with such systems, believe they can achieve their commercial objectives with a small language model and, as we now see, can afford independent access to the required amount of compute. Some large firms with higher technical capacities in areas such as chatbots already implement such approaches, to reduce costs and preserve control of data.

A more 'open source' strategy was commended by some we spoke with as a solution to risks relating to the collection of workplace data:

> *'OpenAI and Anthropic are absolutely shaking in their boots right now, that Deepseek is releasing a new model... They seem to be nervous because what Deepseek are doing is the opposite of the hyperscalers. They're saying: 'actually, we don't need these massive data centres. We don't need all of that centralized approach of hosting people's data. You can just download the model, keep it within your computer or within your local servers, and everything stays within your ecosystem'.. We need the AI models to be sitting on our local servers... That's really, I think that's what the enterprises are looking for. But like you said as well, the executives, they're a little bit hyped up about AI and they want to, you know, they've got the FOMO effect, which is a problem.'* **AI Adoption Consultant, Interview**

For many SaaS providers, there was an intangible sense of urgency and pressure from investors and clients to use only the 'top' models. An engaging interface (i.e. one that allows interaction in natural language and is effective) is now seen as a prerequisite of doing business.

> *'Everything comes down to user experience and user interface. And for user experience to be any good now, you need an LLM so people can interact with a system in natural language.'* **Connected Worker Platform Developer, Roundtable**

While the difference in quality between leading open source models and service models is marginal, adopting anything which offers less than the top capabilities was seen, by some, as unacceptable:

> *'Is there a cheaper way to do it? Yes, but no one wants to do that, because the hype cycle we are in means you need to get ahead fast' '[while we have a legal agreement] at the end of the day, Microsoft own the entire stack – they have access to whatever they want.'* **Digital Twin Provider, UK Interview**

'You can't afford to build out your own solutions – you're inevitably going to be reliant on this. So you have to find ways to build trust.' **Global Counsel, Major Technology Company Roundtable**

'I think it's very unlikely google enter the legal space [using data accessed]. But from a data security perspective, it's just kind of crazy. If I ran a large company, I would not allow all my data to be processed by a single GPT provider.' **AI Strategist, Interview**

Some perceived reputational and, so too, commercial risks in using open weight models. This included, but was not limited to, the performance of small language models being seen as incomparable:

'With DeepSeek we would think about it longer. And it's red listed for us because of the possibilities of using it in a scary way... the organisational risks of us using a Chinese model are too high. If we built our own LLM the chances of it being better than ChatGPT are about 10% – big models are too good, it's too tempting. Small models just aren't as good; it's impossible to comprehend how massive these are; it's meaningless to say how big their training dataset is. If you have a discrete use case you can use a small model, but not that many discrete use cases exist.' **Director AI Ethics, UK Based MNC**

'If you're a Silicon Valley company you're in a situation where you want to get as much access to data as you can – the value is what you collect. And you won't get to collect it unless you've got the best service. To give that, you need to rely on the big guts for the backend – it's a cycle' **Roundtable Participant**

While MNC's felt they couldn't legitimately use DeepSeek, the fractional CTO of a number of UK SaaS start ups told us they had been using DeepSeek because – when it was the only open source model – it was their only route to retaining the value of inferences from workplace data with confidence. Now, however they reported they had shifted to Llama3 which was higher performing but they had the same confidence in. However, this requires a level of technical competency which was considered to be narrowly held.

Market Solutions vs Market Power

Pre-empting state-led intervention or assurances of data security, several major compute providers have begun to offer commercial solutions to 'sovereignty as a service'.[56]

Microsoft offer a downloadable version of their cloud service, the Azure suite.

'Microsoft offer a private cloud; they will give you Azure – the Azure suite – this can run on machines entirely owned by you in a room that is owned by you, on your soil. So you can have sovereignty over that stuff, right – it is yours, you own it. And so, you know, a company like UBS would have that, on Swiss soil, owned by the bank…' **AI Consultant, Interview**

Ultimately, market forces may shape the perceived utility, necessity and sufficiency of these solutions. At the roundtable, some expressed that making sovereignty price-dependent, or a commercial option, may lead intermediary businesses, for whom it was not essential, to overlook core privacy requirements, let alone wider data protection. This creates vulnerabilities within the value chain where these risks are not understood or appreciated.

Table 3: Sovereignty as a Service[57]

Company	Programme Name	Launch Date	Target Audience	Core framing of Sovereignty	Main features/ Tools
Amazon	Digital Sovereignty Pledge	Late 2022	Enterprise customers	Control over digital assets	Data location, access control, encryption, hardware level security
Microsoft	Microsoft Cloud for Sovereignty	July 2022	Governments, Public Sector	Data sovereignty governed by local law	Azure public cloud, policy and auditing layers, GDPR compliance
Google	Digital Sovereignty Explorer	March 2023	Enterprise, Governments	Sovereignty as digital transformation and resilience	Diagnostic tool, customized reports, geopolitical risk mitigation

> *'If people can't get the right cost for storage, they'll go somewhere else to find it.'* **General Counsel, MNC Technology Provider**

The security of such separate cloud environments is critical, and underpins trust inn some of the firms who are working as SaaS or AgenticAI intermediaries, as this seems to ensure 'diversification' of investment of workplace data:

> *'People are happy transferring this data to our cloud, so the twin lives in Slack or Teams and they are already paying for that service.'* **Digital Twin Solution Architect, Roundtable**

However, some were sceptical as to the efficacy of such private instances - owing to market related factors:

> *'Many people in business believe their business has a private instance of GPT but what they actually have are some architectural logical guarantees and some legal guarantees... This is not the same as a private instance...' This gets companies like large US banks over the edge to accept it. And I believe they are making those decisions in probably quite robust ways, and getting to a point of comfort with, you know, the legal and technical proposition. In contrast, if we're talking about a large European firm or bank those guarantees are not enough'* **AI Integration Consultant, Interview**

This individual went on to explain their lack of trust that such environments were genuinely exclusive was based on economic and resource factors:

> *The problem then becomes that GPT5 requires so many GPUs – these firms with private cloud, they just couldn't afford to do it. And so, I think that the adoption of AI within certain areas of finance is going to be incredibly delayed, because they just, they just can't get approval to put the client data into that stuff…*
>
> *'There will be some fuse proposition – technical and legal solutions where you could say at any moment it is only handling [enterprise adopter] solution traffic, or something, I don't know how they do it – but there will be some combination of statements which are getting those firms over the line.'*
>
> *'Some firms in Europe definitely see US tech companies as commensurate with the US state, and maybe those closer to the US state do trust these sort of 'solutions' more than others.'*

Another interviewee explained this from practice. For bigger companies the simplicity of integrated solutions – combined compute and foundation model - was inevitable:

> *'When you think about global companies, every global company works with every large contracting firm, and every global company works with every hyperscaler… Companies like ours are just set up to work with the hyperscalers… You see it even with the government… Trying to streamline things and be efficient means inexorably getting pulled towards working with multinationals.'* **Director AI Ethics, UK Based MNC**

However, many believe they have a genuinely private instance of GPT5. Whether this is technically feasible requires further investigation given the above resource intersections.

Nonetheless, access to chips was recognised as a barrier to 'sovereign' AI at the firm level for one MNC we spoke to:

> *'You really saw it in terms of the bandwidth of the hyperscalers to support frontier models... Unless we were prepared to significantly put money where our mouth was, we've felt we aren't getting the access to the limited resources those guys are...'*
>
> *'And if we take our business elsewhere, it's not irrelevant, but it's not a bargaining chip. We don't have that power... Perhaps our leaders will meet their leaders at DAVOS and negotiate something.'* **Director AI Ethics, UK Based MNC**

The sense of an imperative to adopt, at the same time as there was low trust in protections registered as defeatism in some cases. The narrative that 'we need them, they don't need us' was reinforced by UK SaaS providers suggesting low confidence in contract terms, and their ability to enforce.

Table 4: Major Model Provider Statements on Use of Customer Data

Provider	Official page	Key Statement
OpenAI	OpenAI Enterprise privacy page	"By default, we do not use your business data for training our models."[58]
Anthropic	Anthropic Privacy Center – model training policy	"Anthropic may not train models on Customer Content from Services. "Inputs" means submissions to the Services by Customer or its Users and "Outputs" means responses generated by the Services to Inputs (Inputs and Outputs together are "Customer Content")[59]
Microsoft (Azure OpenAI)	Azure OpenAI data privacy documentation	"Your prompts (inputs) and completions (outputs), your embeddings, and your training data: are NOT available to other customers; are NOT available to OpenAI or other Azure Direct Model providers; are NOT used by Azure Direct Model providers to improve their models or services; are NOT used to train any generative AI foundation models without your permission or instruction; Customer Data, Prompts, and Completions are NOT used to improve Microsoft or third-party products or services without your explicit permission or instruction"[60]
Google (Gemini / Vertex AI / Workspace)	Generative AI privacy commitments for Google Workspace	"Your data is your data. The content that you put into Google Workspace services (e.g., emails, documents) is yours. We never sell your data, and you can delete your content or export it. Your data stays in Google Workspace. We do not use your Google Workspace data to train or improve the underlying GenAI and large language models that power Gemini, Search, and other systems outside of Google Workspace without permission."
Google (Vertex AI service)	Vertex AI training restriction documentation	"Google won't use your data to train or fine-tune any AI/ML models without your prior permission or instruction. This applies to all managed models on Vertex AI, including GA and pre-GA models."

All major foundation model providers have explicit contract terms suggesting that customer data will not be used for training, often 'unless permission is given'. However, 'inputs' and 'outputs' are not all data accessible by API. And how exactly 'permissions' work in practice requires further investigation.

Companies may feel wary about adoption, or 'defeated' in these interactions, because:

1. They feel unable to negotiate these clauses with providers to increase security;
2. There is a perception of incomparable financial resource to support legal action later;
3. A successful case even with a clause of this kind would rely on being able to prove use of a given enterprise's data, which is very difficult; or
4. Even if this evidence threshold was met, the legal and regulatory climate seems supportive of those providers.

All major model providers offer enterprise solutions which promise not to use company data for training. Even the world's greatest innovators have expressed doubt as to their ability to protect their enterprise data from being used for such 'post-deployment' training.[61]

Ultimately, following the widespread acceptance, use and normalisation of Foundation Models, known to be created using illegally scraped material,[62] faith in the rule of law seems to be eroding.[63]

This brings us to the next section.

4. Legal and Regulatory Systems Governing the AI Value Chain

In this section we present insights from our engagement with UK PLC as to the relevance, interpretation and consequences of different legal regimes. We then unpack this in relation to legal analysis and context.

Law is often conceived as the formal expression of sovereign will: the mechanism through which states define the rules governing economic activity and the distribution of rights and obligations. In practice, however, legal frameworks operate within complex socio-technical systems in which multiple actors – workers, firms, software providers, and infrastructure providers – interact across jurisdictions and regulatory regimes. In such contexts, law functions not only as a system of governance but also as a source of friction, shaping design choices, procurement decisions, and patterns of adoption across the AI value chain.

For policymakers seeking to understand the economic potential and risks of workplace data use, it is important to recognise that law does not operate as a single, unified framework. Rather, workplace data sits within a set of overlapping legal regimes that collectively shape how such data can be collected, used, and shared, but also how governance of this data is understood by different actors, shaping their behaviour and decisions.[64]

Systems-oriented legal scholarship highlights that law functions as one institutional system among others – alongside markets, organisations, and technological infrastructures – helping to structure expectations and define acceptable practices.[65] In practical terms, this means that the governance of workplace data emerges from the interaction of multiple areas of regulation, including data protection, employment law, trade secrecy, contractual rules, and competition policy. Some of these operate primarily at the level of the firm, shaping how employers gather and manage data about workers, while others operate at the system level, influencing how data can move between organisations or markets. Reviewing these regimes together can signify how their combined effects create the conditions – and sometimes the frictions – that influence whether and how workplace data can be translated into broader economic and social value.

Our review suggests that legal regimes governing workplace data already shape the AI value chain in important ways. Yet they do so unevenly, often generating uncertainty or operational friction rather than providing clear guidance for firms seeking to adopt AI technologies responsibly. *Note: the content of this section does not constitute legal advice.*

4.1 Worker Level

Here we present what we heard from UK PLC about worker-level protections influencing design, development, and deployment, and intersections with the collection, use and processing, of workplace data.

What We Heard

Data protection law – particularly the UK GDPR – was the most known and cited regulatory regime. Participants described GDPR as both a constraint and a driver of architectural choices when developing or adopting agentic solutions, with one explaining their product was in effect to overcome these challenges as faced by digital giants:

> *'Google tried to do this and were sued… It needs consent – you must be careful to design with consent in place… this is a key part of our sales process and onboarding'* **Roundtable Participant, UK Digital Twin Provider**

At the same time, several participants highlighted persistent uncertainty about the allocation of responsibilities within AI value chains, particularly where enterprises adopt software delivered through SaaS or agentic platforms. In practice, SME adopters can assume that software providers bear responsibility for compliance with data protection obligations, even where they remain the legal data controller.

> *'AI needs regulation and guidance. Guidance is needed'* **UK Automation Provider, Roundtable**

> *'There is a widespread lack of understanding about compliance'* **Roundtable Participant, Global Technology Consultant**

This confusion is not limited to industry practice. The UK Information Commissioner's Office (ICO) has itself recognised the difficulty of identifying data controllers and allocating responsibilities within complex digital ecosystems.[66] In turn, some SaaS providers are 'filling in' the governance gap for data controllers (enterprises). While some reported doing 'the responsible thing' others told us that they just follow the clients asks, regardless of their compliance implications, or reading these as their own compliance obligations.

> *'Whenever AI enters the conversation, things are turned up to eleven in terms of what you have to consider... the best we can do when building for a firm is to mimic the processes the system already has. So what we end up doing, before we deploy anything to a customer, is check with their IT – in some cases these are very small organisations and we have to do the responsible thing...'* **Roundtable, UK Digital Twin SaaS Provider**

The Law in Practice

There are a range of applicable individual rights which could apply to worker-led efforts to protect or secure rights to the value arising from workplace data. Beyond this, collective bargaining is a mechanism to negotiate and secure collective rewards or protections

Individual Rights

Know-how refers to technical or practical knowledge derived from experience or research relating to knowing how, when and why to do something - the methods or processes involved in accomplishing a task. Know-how is often not written down, only tacit, which can make it difficult to define. Know-how which is communicated and documented (in forms such as operating manuals) would likely attract intellectual property rights, such as copyright. However, in the context of copyright protection, it is not the underlying know-how itself that is protected against copying or appropriation, but rather the specific form in which that know-how is expressed. Accordingly, a third party would generally remain free, from a copyright perspective, to make use of the underlying knowledge or ideas, provided that doing so does not involve reproducing the particular expression through which those ideas were originally embodied. Know-how which is not communicated nor documented and is retained in the tacit knowledge of an individual would therefore not be considered protectable under copyright law, as it would lack an expression or form which is required for copyright protection.

In general, under UK law, know-how developed and used within a business may constitute a trade secret where it satisfies the legal criteria for protection. In particular, pursuant to the Trade Secrets (Enforcement, etc.) Regulations 2018, information will qualify as a trade secret if it is secret (in the sense that it is not generally known or readily accessible), has commercial value because it is secret, and has been subject to reasonable steps by the person lawfully

in control of the information to keep it confidential. In practice, this means that technical knowledge, methods, processes, or other forms of operational know-how developed within a business all fall within the scope of trade secret protection, provided these conditions are met.

There are three legal terms that need to be considered in the present context: confidential information, know-how, and trade secrets.

- Confidential information is the broadest category. It is protected under the law of confidence where information is secret and disclosed in circumstances giving rise to a duty of confidence.
- Know-how refers to practical technical or commercial knowledge developed within a business. Some know-how may be confidential, while other know-how may be widely known or learned through experience.
- Trade secrets are a specific subset of confidential information that meet the statutory criteria under the Trade Secrets (Enforcement, etc.) Regulations 2018: secrecy, commercial value because of that secrecy, and reasonable steps taken to maintain secrecy.

In short, trade secrets, confidential information, and know-how may fall inside or outside confidentiality depending on the circumstances. The intersection of intellectual property ownership, control and confidentiality of know-how and knowledge gained 'on the job' or in the course of employment, and the protection of data – particularly so-called mental data and cognitive privacy – is an under-explored intersection of law in scholarly literature, as well as in case law. In addition to constituting trade secrets, the codifying capture of know-how has the potential to collect personally identifiable information, to encroach upon mental data, overreaching into the private spheres of individuals, mental integrity, and to infringe upon inalienable human rights.

The intellectual property and employment law question has often been explored through the lens of Faccenda Chicken Limited v Fowler [1987] and subsequent case law, which distinguishes an employer's trade secrets from an employee's general skill, knowledge and experience. Courts have recognised that an employee can 'use to the full any personal skill or experience even if this has been acquired in the service of [their] employer'. While an employee taking documents containing workplace data could be protected by an organisation's Intellectual Property (IP) rights, the same employee walking out the door with knowledge contained in methods and capabilities 'in their head' may not be afforded the same protections. It should also be noted that the fact that the relevant information is retained solely in an employee's memory, rather than recorded in a document or other tangible medium, is not determinative for the purposes of trade secret protection.

If the know-how in question satisfies the substantive requirements of trade secrecy, it may still qualify for protection against misappropriation. This remains the case irrespective of whether the information has been formally recorded or exists only as knowledge internalised by the employee. The critical inquiry is therefore not the medium in which the information is stored, but whether the information itself satisfies the legal criteria for trade secret protection and whether its unauthorised use or disclosure would amount to misappropriation. In addition, depending on 'what' is in the mind of the individual may also determine how it is protected and to what extent it engages rights of the individual, including data protection, privacy, and human rights. The means of extracting such knowledge from the individual may also cause rights-dependent concerns.

In many cases, especially in the context of day-to-day employment where there is not a technology transfer or highly sensitive trade secret, know-how falls outside the realms of

IP and would be considered 'confidential information'. Where know-how does not meet the threshold required to qualify as a trade secret and therefore does not benefit from protection under the Trade Secrets Regulation, it may nevertheless still receive protection either under common law principles or through contractual arrangements. For common law protection, it must have the necessary 'quality of confidence' and be imparted in a 'situation imposing an obligation of confidence'.[67] Know-how that is not generally known or easily accessible and is significant for the use or sale of products or services may be protected as confidential information, regardless of where the employee works – at home, on a factory floor, warehouse, or in an office. What is 'known' can be data, information (processed data) and/or knowledge (information applied through understanding).[68] In an employment relationship, this might be something known by a key employee, senior staff member, or someone who has worked in an organisation for a long time. It is often considered valuable due to its utility in production or business operations.

The limitations of protection afforded by confidentiality are therefore known; it is also generally understood from case lawxi that employees retain the right to use their skill, experience, know-how, and general knowledge for their own benefit or in service of a competitor after their employment ends. Courts have ruled that the employee retains freedom to utilise their personal skills and experience, recognising that an employee "*is entitled to use to the full any personal skill or experience even if this has been acquired in the service of his employer*" and that taking information away in documentary form implies fairly strongly that it is not 'inevitably' in one's head.

In the same case it was reported:

> *"For while it may be true that an employee is entitled - and is to be encouraged - to build up his own qualities of skill and experience, it is equally his duty to develop and improve his employer's business for the benefit of his employer. These two obligations interlock during his employment: after its termination they diverge and mark the boundary between what the employee may take with him and what he may legitimately be asked to leave behind to his employers."*[69]

In a similar case, the court said:

> "... when I use the word 'information', I mean something that can be traced to a particular source and not something which has become so completely merged in the mind of the person informed that it is impossible to say from what precise quarter he derived the information which led to the knowledge that he is found to possess."[70]

It may be more accurately characterised as an employee's personal skill and knowledge, as opposed to information that belongs to the employer and is capable of classification as confidential information or, in certain circumstances, as a trade secret. Personal skill and knowledge typically refer to the experience, expertise, and general competencies acquired by an individual through their work and professional development, which the law generally recognises as remaining with the individual rather than the employer.

By contrast, information that is proprietary to the employer, such as confidential business information or trade secrets, may be subject to legal protection and restrictions on use or disclosure, particularly where it satisfies the relevant legal thresholds or is protected through contractual obligations. In some circumstances, elements of an individual's personal skill and knowledge may also intersect with personal data, particularly where the information relates to identifiable individuals. In such cases, the handling and use of that information may also engage obligations under relevant UK and EU data protection legislation.

If know-how qualifies as personal data, it is treated differently in law. In the EU (subject to the Charter of Fundamental Rights), personal data protection, along with privacy, is an

'inalienable right' that cannot be given away, sold or transferred. In the UK, data protection and privacy are afforded protection under the European Convention of Human Rights, Article 8. Furthermore, Data protection is further enshrined in national laws such as through the EU GDPR for EU member states, and UK GDPR and Data Protection Act 2018, providing personal data protection through horizontally binding legal rights. Whilst know-how is often closely related to confidential information and trade secrets, it can take on characteristics similar to industrial data on one hand and personal data on the other.

One of the main aims of Data Protection law is to provide the possibility for individuals to control the information that concerns or is about them. According to European Data Protection Board Guidelines, personal data cannot be considered as goods; individuals cannot alienate their fundamental human rights.[71]

Personal data is deeply steeped within the framing of privacy. It is not currently a product or something in which property rights vest because it is inherently linked to inalienable rights of the person, such as through privacy and data protection and other personality rights. It is, therefore, necessary to observe certain restrictions aimed at preventing the risk of violation of the personal sphere.[72] In contrast, workplace data is rivalrous and can be exclusively controlled by a specific person in a specific period of time, befitting know-how in the technological transfer or trade secret sense, and is able to be a product or subject to commoditisation.[73]

Several European states have introduced additional protections for personality. Denmark has introduced amendments to its copyright legislation to prohibit imitations of performers or natural persons without their consent. German law also protects the 'sphere of personality', including an individual's voice and likeness from intrusions affecting the individual's economic life or dignity. This remains a gap in UK law, though one which the Secretary of State for Science, Innovation and Technology has committed the government to consulting upon. The trade union Equity is proposing that the UK introduce a 'hybrid' model of personality protection which includes a property right, capable of assignment, license, transfer, to permit the commercial exploitation of personality, and a personal right, grounded in human dignity, which protects moral interests and cannot be overridden by assignment of the property right.

Mental data is any data that can be processed to make inferences about a person's mental states, including cognitive states (thinking, memory, and perception), affective states (emotions and moods), and conative states (intentions and desires).[74]

Mental data can be derived from two sources: (1) neural data (direct brain measurements via EEG, Computer-Brain Interfaces) and (2) non-neural data (behavioural and phenotypic information like voice patterns, facial expressions, written text, and smartphone usage patterns).[75] The way this kind of data or information might be extracted could be through (1) direct neural extraction, digital phenotyping, affective computing and inferring emotion or mood states from facial recognition or crowd analysis, or through so-called "exploitation scenarios" including micro-targeted advertising, lie detection, cognitive assessment for employment, credit scoring or manipulation.

Many of these exploitation scenarios are either being prohibited for use by AI systems or considered High-Risk AI under the EU AI Act. The current state of such technologies cannot decode the semantic content of thoughts themselves but can merely establish statistically significant correlations between data patterns and mental state categories. These 'best guesses' raise serious privacy concerns.

UK law protects the right to privacy through Article 8 of the European Convention on Human Rights, which protects 'respect for private and family life, home and correspondence'. The primary cause of action is misuse of private information, developed in Campbell v Mirror

Group Newspapers [2004] as concerned with 'the protection of human autonomy and dignity - the right to control the dissemination of information about one's private life'.[76]

Courts apply a two-stage process: first assessing whether there is a reasonable expectation of privacy, then balancing competing rights (in the Campbell case, this was the publisher's right to impart information against the claimant's privacy rights and could similarly be considered in the context of an employer wanting to 'publish' know-how for training of AI). This framework could apply to the extraction of worker know-how where that know-how constitutes private information about the individual.

These complex and overlapping rights frameworks have clear implications for where an enterprise can place its 'moat' (as discussed above). Enterprises should carefully consider which frameworks apply to their workplace data in consultation with relevant stakeholders, including their workforce.

Collective Bargaining

It is now widely recognised that many impacts on work and people of AI are 'relational'. Conventionally, this is understood most in relation to the limit of tort law models, those which require individuals to make a claim of wrongdoing after an injustice to them, rather than collective, systemic review of impacts.

However, these impacts are also relational and systematic when thinking about workplace data. Data collected from one individual, reflecting the codification of their work methods, can act back upon and impact others.

Unions, representing cohorts of individuals, are also able to offer a more powerful, collective voice for workers, as data subjects of various kinds (personal, and otherwise). Furthermore, they are well placed to ascertain changes to work. A union can help both individuals and groups respond to collective risks, and to steer towards greater collective benefits, while also holding the 'countervailing power' to ensure there is meaningful contestability and redress where any agreement is not followed.[77]

Collective bargaining is the process by which unions negotiate with employers on behalf of members. An agreement falls within the statutory definition to the extent that it relates to the terms and conditions of employment; or how technology is used to recruit or dismiss workers; or to allocate tasks and duties (See Trade Union and Labour Relations (Consolidation) Act 1991 section 187 (2)). Schedule A1 (paras 3 and 31) highlights the right to enter into collective bargaining over terms and conditions related to the core issues of pay, hours and holidays, as well as to the information that is necessary for the purpose of collective bargaining (TULCRA, section 181). Although this does not amount to general coverage of all uses, algorithmic technologies that could be used to determine or impact pay, as could foundation models via the codification of work methods could, may be covered.

The nature of the agreement between the union and employer about the scope, process and information required for bargaining is key: the agreement is only binding if it is in writing and states that it is intended to be enforceable (s 179). Taken together, this means that union officials could propose oversight of data collection, use and processing at work as part of collective bargaining, and responsible employers should welcome the opportunity and process of assessment.

Other legal mechanisms available to unions exist independently of the collective bargaining infrastructure and include:[78]

- Existing collective agreements, contracts and workplace policies, including those that already deal with some aspects of digital systems.
- Existing provisions on digital systems in contracts of employment or contracts for service.

- Data protection rights of individual workers, as well as consultation rights under the UK General Data Protection Regulation (UK GDPR)
- Data Protection Impact Assessments required under data protection law
- Equality Impact Assessments required for public bodies and recommended for private bodies
- Health and Safety consultations with appointed trade union health representatives
- Information and Consultation of Employees requiring negotiation on matters for consultation by large and medium-sized employers
- The Directors Report for large and medium-sized employers.

4.2 Enterprise Level

Here we present some of the key firm-level legal considerations presented by those we spoke to, and then consider the relevant and existing legal frameworks which apply in practice.

What we Heard

Among those we spoke to, there was a lack of confidence in terms of how Trade Secrets, Intellectual Property and Know-how would apply to interactions between different actors in the value chain in terms of the collection and processing of workplace data.

> *'People are worried about their personal data and client data somehow causing a compliance problem; they aren't thinking about data relating to their processes.'* **Roundtable Participant**

> *'I'm not sure if anyone is really thinking about the business know-how.'* **Director AI Ethics, UK-based MNC**

When speaking to the domains of activity within which Agentic AI was being proposed for deployment and, in turn, the inferences an agentic solution could generate about business operations, the Director AI Ethics at a UK-based MNC suggested:

> *'It's not really patentable, or a trade secret – it's more just the case that if you do these things at scale and you've got a big history of doing it, you just have the first-hand knowledge of doing that, and you have the expertise, you've built the processes that might not even be explicit necessarily'.*

This point should, however, be qualified. Even where individual operational activities or data points may appear routine in isolation, the systematic operation of processes at scale and over extended periods may nonetheless generate valuable insights. The accumulation and analysis of operational information can reveal patterns, efficiencies, or optimisation strategies that may inform decision-making and improve business processes.

The commercial value in such cases often lies not in the underlying data itself, but in the knowledge derived from its sustained use and analysis. Over time, organisations may develop refined methods, improved workflows, or operational strategies based on these insights, which may contribute to greater efficiency or competitive advantage.

While the individual activities or data involved may appear unremarkable, the insights generated through long-term and large-scale operational practice may acquire independent commercial significance. In appropriate circumstances, the knowledge and processes informed by these insights may therefore be capable of protection as trade secrets.

Further, SaaS providers who are looking to develop models based on these inferences lack confidence that they will have legitimacy at a later date:

> *'If you have built a model, how can you be sure you can protect it? If you've got original IP – how can you even be sure if it's yours? If you've used a lot of proprietary data to develop it, you might want to sell it but secure the background IP you used to train it – which is a challenge given how this data is being collected.'* **UK SaaS Provider, Roundtable Participant**

It is noteworthy that the manner in which data is collected - whether from one source or another, and by one method or another - does not determine whether protection is available. The more pertinent issue is whether the structured selection of data sources, and the relative weighting attributed to each within the overall training corpus, amounts to confidential information of commercial significance.

In practice, the configuration of a training dataset is rarely arbitrary. Decisions as to inclusion, exclusion, balance, and proportional emphasis often reflect technical judgement and investment. That 'recipe' may disclose how a system has been optimised, how bias has been managed, or how performance has been calibrated for particular use cases. Where those choices are not publicly known, they may confer a competitive advantage.

Under UK law, information will qualify as a trade secret where it is secret, commercially valuable because of that secrecy, and subject to reasonable steps to preserve its confidentiality. A curated and strategically weighted dataset architecture is capable of meeting that standard, even if some of the underlying data sources are publicly available. The protectable interest may lie not in the individual ingredients, but in their deliberate combination and calibration.

However, the application of this is untested:

> *'My sense is there hasn't been any case law cases on this yet… People are bringing lawsuits but it feels like a whole new era. It's different, though, because in confidentiality agreements, I'm one person- but what's the capacity of the human mind to remember these things? Whereas you know, it's very different if you've got an all-seeing eye which remembers everything it's ever seen.'* **Director AI Ethics, UK-based MNC**

Under EU and UK law, information will qualify for protection where it is secret, in the sense that it is not generally known or readily accessible to persons within the relevant circles; has commercial value because it is secret; and has been subject to reasonable steps, in the circumstances, to maintain its secrecy. Importantly to our present context, 'information' is not limited to a single document or dataset. A compilation, structure, or deliberate combination of elements, each of which might appear innocuous in isolation, may constitute a protectable trade secret, provided that the assembled body of knowledge is not generally known and derives value from its confidentiality. Against that background, incremental acquisition may amount to trade secret misappropriation. The gradual nature of acquisition does not, in itself, preclude liability. The relevant question is whether the cumulative result constitutes the unlawful acquisition, use, or disclosure of protected information.

The potential for indemnity-based solutions to this uncertainty was highlighted by one interviewee:

> *'This might be comparable to about two years ago when we were pushing for 'hey, Mr Big Frontier Model, you need to assure us that you own the rights to the data used to build this' – and they got around it by saying, 'we'll indemnify you for any legal action brought against Unilever for plagiarised work'… It wouldn't surprise me if something like that*

> *was introduced: 'we can't guarantee that data won't be used, but we will indemnify you against any losses' – that type of thing.'* **Director AI Ethics, UK Based MNC**

In the US context, Professor Elizabeth Rowe has convincingly argued that data governance is shaped by contract and intellectual property lawin the absence of a regulatory regime. This point is particularly important in light of the dominance of US firms in many of these transactions. Contracts in this context may include choice of law and jurisdiction clauses that designate the law of a US state as the governing law of the agreement and identify US courts as the preferred forum for the resolution of disputes. However, it should be noted that both in the EU and in the UK, parties cannot contract out of data protection law by selecting the law of another jurisdiction. In her article "Private Law in Unregulated Spaces", Rowe explains:

> *'The way in which contract law and intellectual property law have coalesced to define and control data ownership is striking. As a threshold matter, it is property ownership that allocates control of and access to data resources and ultimately enables monetization and value in the marketplace. This control extends to both the public and private spheres, and the attendant implications are far reaching… Contracts have come to facilitate property rights in the management of data resources in almost unbounded fashion. In so doing, contracts effectively yield an even stronger property right than that associated with tangible property.… owners, through contractual provisions, reserve for themselves very broad powers to control a wide range of activities and behaviours relating to data, particularly its accessibility. As such, contracts create de facto property rights, even though contracts themselves are not property. Thus, the declaration of ownership, coupled with courts' broad enforcement of such contract terms, creates a property right or, at a minimum, a quasi-property right, that then coalesces with and augments the accompanying intellectual property rights'*

The intersection of these domains – including UK law on data ownership - is discussed further in relation to the law, in fact, below.

The Law in Practice

Employers can manage risks relating to workplace data vis-a-vis their employees and their rights and entitlements via employment contracts. In the other direction, their mechanisms to manage gov-ernance and protection of value associated with workplace data with software providers is via dif-ferent forms of contractual term and intellectual property law.

Employment Contracts and Intellectual Property

The employment relationship creates a unique context for understanding know-how. Unlike other commercial relationships, employment involves an ongoing, dynamic exchange of knowledge between employer and employee. This exchange is fundamental to the employment contract but creates complex questions about ownership and control of the resulting knowledge.

Within the employment relationship, know-how is created, transferred, and accumulated in several ways. Employers invest in training, provide access to proprietary systems and processes, and create environments where employees develop skills and knowledge. Simultaneously, employees bring their own prior knowledge, skills and understanding as well as develop new insights through experience, and contribute to organisational learning - all of which bring benefit to an employer.

As noted in Stenhouse Australia Ltd v Marshall William Davidson Phillips: '*For while it may be true that an employee is entitled - and is to be encouraged - to build up his own qualities of skill and experience, it is equally his duty to develop and improve his employer's business for the benefit of his employer. These two obligations interlock during his employment: after its*

termination they diverge and mark the boundary between what the employee may take with him and what he may legitimately be asked to leave behind to his employers.'

In the knowledge economy, contracts are often used by businesses to ensure that they own the IP created by employees, contractors and consultants.[80] This is largely achieved by incorporating IP clauses into employment and consultancy agreements. Confidentiality clauses in contracts can form part of a business's protection of its trade secrets, and more broadly provide a business with a contractual right of confidence.[81] Employers typically seek to preserve the confidentiality of know-how through confidentiality provisions in employment contracts or separate Non-Disclosure Agreements. Under English law, workplace information may be protected as confidential through express contractual obligations, such as express confidentiality clauses, imposing a clear obligation on the employee to maintain the confidentiality of specified information and ensuring no disclosure, use, or otherwise except for the proper performance of the employee's duties; definitions of confidential information, such as: business operations and strategic plans; software, technical information, and know-how; relationships with clients and suppliers; pricing structures, financial information, and commercial arrangements; internal processes, documentation, and research activities; restrictions on use and disclosure, such as prohibiting disclosure to third parties without prior authorisation; limiting use of the information to the performance of employment duties; preventing copying, removal, or retention of confidential materials except where required for work purposes; obligations on termination of employment, typically requiring the employee to employee to return or delete documents and materials containing confidential information, cease any further use of such information, confirm compliance with relevant contractual obligations, and reduce the risk of misuse after the employment relationship has ended.

Confidentiality obligations are often supported by additional contractual provisions, including intellectual property clauses clarifying ownership of works created during employment, non-disclosure agreements in relation to particularly sensitive information, post-termination restrictions, such as non-compete or non-solicitation clauses, where appropriate and enforceable. In assessing whether information is confidential, courts may consider whether the employer has treated the information as such in practice. Employers therefore commonly implement measures such as restricting access to sensitive information, marking documents as confidential, adopting internal policies governing the handling of information, and maintaining secure IT systems and access controls. This may confer that adoption of Agentic Solutions without due regard to data collection use and processing could have employee-employer legal consequences at a later date.

Where know-how is communicated and formalised in written agreements, rights to that know-how may remain with the disclosing party, and the receiving party may be restricted in its use and disclosure.xvii The main purpose of enforcing protections afforded by confidentiality is intentionally to preserve existing business and trade and protect from competition for the benefit of potential future business and trade. This is often exercised through restrictive covenants or other restraint of trade contractual clauses.

The fact that work is carried out in a particular location, for example, from home, does not, in itself, affect the legal status or ownership of know-how. Questions of entitlement to know-how typically arise from the employment relationship and the legal obligations attached to it, rather than from the physical environment in which the work is performed.

That said, the circumstances in which know-how is developed or acquired may be relevant when determining how it should be legally characterised. Considerations such as the employee's role, the context in which the knowledge was created, and any contractual or organisational limits placed on its use or disclosure may influence whether the information is properly regarded as belonging to the employer. These factors may also affect whether the

information should be treated as confidential information or, in some instances, as a trade secret.

A further distinction must be drawn between information that belongs to the employer and the employee's own skill, knowledge, and experience. The latter generally remain with the individual and may be used by them in the course of their professional activities. At the same time, information relating to an employee's abilities or professional profile may, in certain situations, fall within the scope of personal data, particularly where such information is recorded, assessed, or otherwise processed in a way that relates to an identifiable person.

In this sense, the location from which work is performed is largely irrelevant from a legal standpoint. What matters instead is the context in which the know-how arises, how it is documented or controlled, and whether legal or contractual obligations attach to it. These factors will ultimately shape whether the information is regarded as personal expertise, employer-owned confidential information, or information subject to additional legal protections.

The rise of remote work, digital collaboration tools, and AI-assisted work creates new contexts in which know-how is developed and shared. These changing work patterns may affect the traditional boundaries between employer and employee knowledge, particularly when digital tools capture and process worker inputs in ways that were not contemplated in existing legal frameworks.

Intellectual Property and Contracts with Software Providers

In the case of software providers, including instances involving bespoke software development, it is extremely uncommon for the commissioning party to obtain contractual terms that transfer ownership of the copyright in the software. In the vast majority of cases, the provider retains copyright in the underlying software, while the commissioning party is granted a licence permitting use of the software in accordance with the agreed terms.

Such licences may vary in scope and may be exclusive or non-exclusive, perpetual or time-limited, and may include restrictions on modification, distribution, or sublicensing. However, absent an express contractual assignment, the intellectual property rights in the software will ordinarily remain with the developer or supplier. Accordingly, the commissioning party typically acquires rights of use, rather than ownership of the copyright itself.

Data Ownership[82]

Domestic legal frameworks governing data access, ownership and rights do exist (such as rights of confidence; copyright; database rights and contractual rights) but may be inadequate in the context of this new systemic challenge.

(1) Rights of confidence

Under English law, the equitable duty of confidence plays a significant role in safeguarding confidential information and workplace know-how. The doctrine operates independently of contractual obligations, although in practice it often functions alongside confidentiality provisions contained in employment contracts and commercial agreements. Its underlying purpose is to restrain the unauthorised use or disclosure of information that has been communicated in circumstances giving rise to an expectation of confidentiality.

The modern approach to actions for breach of confidence is commonly traced to the decision in Coco v A N Clark (Engineers) Ltd. In that case, the court set out three elements that generally need to be established. First, the information must have the necessary quality of confidence; it must not be trivial or already in the public domain. Second, the information must have been communicated in circumstances importing an obligation of confidence. Third, there must be an unauthorised use or disclosure of that information, resulting in detriment to the party to whom the information relates.

Within the employment relationship, the doctrine frequently applies to forms of commercially valuable knowledge encountered or developed in the course of work. This may include technical know-how, operational methods, internal business processes, or information relating to customers and suppliers. The law, however, draws an important boundary between information that properly belongs to the employer and the employee's own skill, experience, and general knowledge. The latter is generally regarded as part of the individual's professional capacity and may ordinarily be used by the employee after the employment relationship has ended.

This distinction has been clarified in a number of decisions, including Faccenda Chicken Ltd v Fowler. In that case the Court of Appeal recognised that information encountered in employment may fall into different categories. At one end are trade secrets and information of a particularly sensitive character, which remain protected even after termination of employment. At the other end are the employee's general skills and accumulated experience, which are not subject to post-employment restrictions. Between these two poles lies a category of information that may be confidential during employment but does not necessarily remain protected afterwards unless specific contractual provisions extend that protection.

For employers, the equitable doctrine therefore provides a foundational level of protection for confidential workplace information. It ensures that information disclosed in circumstances of trust cannot be misused without legal consequence. At the same time, the doctrine seeks to maintain an appropriate balance by avoiding undue constraints on employee mobility and the legitimate use of professional expertise.

In practice, organisations rarely rely on the equitable obligation alone. It is commonly reinforced through contractual confidentiality clauses, intellectual property provisions, and internal policies governing the handling of sensitive information. Such measures help to clarify the categories of information that are regarded as confidential and demonstrate that reasonable steps have been taken to preserve its secrecy.

It is noteworthy that the remedies available where an equitable right of confidence exists are generally more flexible than those that arise following a breach of contract.[83]

Furthermore, contractual rights may only be enforced against another contracting party whereas rights of confidence may be enforced against anyone who receives information in circumstances that give rise to an obligation of confidence. This does not require the recipient to have actual knowledge that they are under an obligation of confidence and is assessed from the viewpoint of a reasonable person in the position of the parties.[84] While rights of confidence provide a powerful and flexible basis for the protection of data and databases in data-sharing deals, they are subject to several limitations:

- Rights of confidence cannot be enforced with respect to information in the public domain.[85]
- Enforcement will not be possible against 'innocent' recipients of the data who could not be expected to know that they were under an obligation of confidence, for instance because they were reasonably entitled to rely on reassurances from the party who supplied the data that the provision was lawful.[86]
- Rights of confidence may be subject to several public policy and public interest based restrictions on their enforcement, including fundamental rights such as freedom of expression, the exposure of fraud or dishonest conduct, and cases involving public safety and wellbeing.

Although a limited degree of harmonisation in the protection of undisclosed information was achieved in Europe by way of Directive (EU) 2016/943 (the EU Trade Secrets Directive),

the Directive only specifies the minimum protection that Member States (including the United Kingdom, prior to its departure from the Union) are required to provide. International harmonisation is also limited to Article 39 of TRIPS, which requires World Trade Organization members to ensure the protection of certain categories of undisclosed information against acquisition, use or disclosure contrary to honest commercial practices.[87] The circumstances in which data and databases can be protected as undisclosed information and the protection that arises can vary significantly, therefore, between jurisdictions and local advice is recommended whenever relying on this form of protection in a data-sharing deal.

(2) Copyright

Copyright can potentially protect both data and databases. Where copyright arises, the owner is provided with a powerful right to prohibit further dealings with the data or database, including the creation of copies and communicating the data or database to the public. Although copyright is a national right, the creation or publication of a copyright work in one country will generally give rise to a copyright in most other countries.[88] However, copyright will only arise when the work is original or if a sound recording or film has not been copied from an earlier sound recording or film:[89]

- Data (other than sound recordings or films) will only qualify for protection by copyright in relation to subject matter that is original in the sense that it is its author's own intellectual creation.[90] This requires a reflection of the author's personality where the author is able to express his or her creative abilities in the production of the work by making free and creative choices.[91] The existence of technical constraints on the possible forms of expression is a factor that can reduce the scope for originality,[92] such that the more restricted the choices, the less likely it is that the the work will be considered original within the meaning of copyright law. (or the expression of the intellectual creation).[93]
- A database may be protected by copyright as an original literary work when it is an author's intellectual creation by reason of the selection or arrangement of its contents.[94] As with copyright in data, copyright in a database will not arise if the selection or arrangement of the contents is entirely dictated by technical function, such that the author has no freedom to express creativity. The requirement for originality prevents copyright applying to all data and databases. When individual data is captured to provide a record of objective facts, there is little scope for each datum to reflect an author's intellectual creation. Data capture through automated processes is therefore unlikely to qualify for copyright protection. The selection and arrangement of data in many databases will also be dictated solely by technical function, limiting the application of database copyright. Copyright is partially harmonised through several international agreements[95] and at the EU level through various directives.[96] The United Kingdom continues to reflect, in its national law, the EU copyright directives and the jurisprudence of the Court of Justice of the European Union up to the point at which the UK departed from the European Union.[97]

(3) Database rights

Within the European Union, the database right constitutes a sui generis form of intellectual property protection designed to safeguard databases that involve a substantial investment in the obtaining, verification, or presentation of their contents. The right was established under Directive 96/9/EC on the Legal Protection of Databases with the aim of encouraging the creation and maintenance of databases by protecting the economic effort required to compile and manage them.

The database right is distinct from copyright protection. Copyright may apply to a database

where the selection or arrangement of its contents reflects the author's own intellectual creation. The sui generis database right, by contrast, is not concerned with originality in this sense. Instead, it protects the investment involved in assembling and organising the data, even where the structure of the database itself does not meet the threshold required for copyright protection. The focus of the regime is therefore on preserving the value of the resources expended in building and maintaining the database rather than rewarding creative expression.

For protection to arise, the database must reflect a substantial investment in obtaining, verifying, or presenting its contents. The right is conferred upon the "maker" of the database, typically the person or organisation that takes the initiative in creating the database and bears the associated financial and organisational risks. The holder of the right is entitled to prevent the extraction or reutilisation of all or a substantial part of the contents of the database without authorisation. In certain circumstances, even repeated or systematic extraction of smaller parts may be restricted where this undermines the normal exploitation of the database.

The duration of protection is generally fifteen years from the date on which the database is completed, although significant updates or additional investment in the database may trigger a new period of protection.

In the workplace, database rights frequently arise in relation to structured collections of business information, such as customer and supplier databases, repositories of technical data, internal research datasets, and operational or analytical information systems. Organisations may commit considerable financial and organisational resources to compiling, verifying, and maintaining such collections of data.

These datasets may also contain elements of technical or commercial know-how, particularly where they reflect accumulated operational experience, research outcomes, or market intelligence. Although know-how as such may not always be protected as a proprietary right, its systematic compilation within a database may fall within the scope of the database right where the necessary level of investment can be demonstrated. For a database right to arise in the United Kingdom in relation to a database created before 1 January 2020, the maker of the database must be either a national or habitual resident of a Member State of the European Economic Area (EEA) or a company (1) formed in accordance with the laws of an EEA Member State and (2) having its central administration or principal place of business in an EEA Member State, or a registered office in an EEA Member State with a genuine link and continuing link to the economy of an EEA Member State. For databases created after 1 January 2020, references to a EEA Member State are replaced with the United Kingdom (i.e., makers based in the EEA will no longer obtain protection for their databases in the United Kingdom, and vice versa).

Database rights are harmonised in the European Union by way of the Database Directive, which continues to be implemented in UK national law.[98] An equivalent right has not been implemented outside the European Union, although other jurisdictions may offer similar forms of protection through a broader application of their copyright law or through laws relating to unfair competition.

(4) Contractual rights

Contracts can be used to define the scope of a permission granted under another right, such as a copyright or database right or to impose (and define the scope of) an obligation of confidence on the recipient.[99] Contracts can also be used to impose direct obligations on a party in receipt of data or a database regarding access, use and dissemination. They may operate to reinforce and broaden the protection available to the proprietor under the relevant proprietary or equitable right. Where several legal bases apply concurrently, they

can function in a complementary manner, strengthening the overall protection afforded to the information and providing the proprietor with additional means of addressing unauthorised use or disclosure.[100] However, contractual obligations regarding access, use and dissemination of data can be imposed on a recipient even when the data is not subject to an IP right.[101] In these circumstances, a contractual obligation restricting access, use or dissemination of data or a database is a negative covenant for consideration that the court will enforce 'provided only that the covenant itself cannot be attacked for obscurity, illegality or on public policy grounds such as that it is in restraint of trade'.[102] Subject to the limitations on contractual terms discussed below, contractual restrictions are therefore commonly imposed in relation to data that is in the public domain and cannot be made the subject of an obligation of confidence. The flexibility of contractual rights to protect data irrespective of any underlying legal rights and to impose fine-grained controls on the access, use and dissemination of that data makes them a crucial tool in any data-sharing deal.

However, contractual rights are subject to two key limitations:

- They are rights in personal and can only be enforced against specific persons.[103]
- The remedies available for breach of contract are generally more limited than those available for infringement of an IP right or a breach of confidence.[104] Other than some limited areas (e.g., prohibitions on anticompetitive agreements), contract law is not harmonised between different jurisdictions and local advice under the governing law of the contract is recommended. It is noteworthy that this is also the case in the United States, where contract law is not harmonised at the federal level. Instead, it is primarily governed by state law, and the applicable legal rules may vary significantly from one state to another within the United States.

Whatever form a data-sharing deal takes, there are four 'dimensions' of control that a party sharing data can use to protect their interests: Who can access the data? What data can they access? How can they access the data? What can they use the data for? Decisions regarding each dimension of control will ultimately be informed by a range of commercial, legal and technical factors, including the value and sensitivity of the data, the benefit each party hopes to realise through the arrangement, the legal rights that protect the data and the technical infrastructure that will facilitate the sharing.

4.3 System Level

This section reviews the system level legal frictions shaping workplace data and the AI Value chain with relevance to post-deployment training. Recent policy relating to the UK's development of the UK AI stack is set out in 2.2. Here, we consider how legal regimes which operate at the national level may shape different outcomes of post-deployment training in the UK economy.

Data Use and Access

The Data (Use and Access) Act ("the Act") received Royal Assent on 19 June 2025. The Act does recognise a new category of data, 'business data'. This does not explicitly mention know-how, but does cover domains which may cover it: information about goods, services and digital content supplied or provided by the trader; information relating to the supply or provision of goods, services and digital content by the trader (such as, for example, information about: where goods, services or digital content are supplied or provided; prices or other terms on which they are supplied or provided; how they are used, or their performance or quality); information relating to feedback about the goods, services or digital content (or their supply or provision), and information relating to the provision of information described in paragraphs (a) to (c) to a person in accordance with data regulations; "customer data" means information relating to a customer of a trader, including (a) information relating to goods,

services and digital content supplied or provided by the trader to the customer or to another person at the customer's request. These clauses appear to offer the potential for better sight of b2b market interactions within the digital economy, which could support governance of post-deployment training data.

The Act also makes provisions for smart data, building on the success of Open Banking and extending this to other sectors and industries. This can apply to business data. This could see significant innovation in terms of cultivating UK 'know-how' datasets for innovation from UK enterprises for UK AI. However, such applications have not yet been raised or discussed in relation to these provisions.

The Act also, inversely, advanced two changes to data protection law as was, which could encourage post-deployment training. This includes changes to the use of personal data for 'commercial' scientific research, and changes in the requirement for balancing tests where there are legitimate interests. Many of the Act's provisions will be implemented via further regulation. While a plan is set out for further activity, when the most relevant provisions – those relating to 'business data' - will be clarified is not specified.[105]

Data transfer regulation also changed under The Act. Under Art. 44 of the United Kingdom General Data Protection Regulation (UK GDPR), it is required that international transfer of personal data should only take place under certain conditions and with certain safeguards in place. The 2018 Data Protection Act allows personal data to flow from the UK to other countries on the basis of an adequacy decision, appropriate safeguards (such as standard data protection clauses and binding corporate rules), or other conditions specified under the Data Protection Act. The Data Use and Access Act of 2025 simplified rules on transferring personal data internationally ensuring adequacy can be granted if the destination's protection is "not materially lower" than the UK's. This effectively increased the legal breathing room to maintain data flows with trade partners like the US.

For organisations that rely on cloud computing, these changes are significant. Workplace data, including employee information, operational datasets, and technical logs, may be processed through distributed cloud systems that store or analyse data in multiple jurisdictions. The revised framework seeks to accommodate this reality by enabling more pragmatic transfer mechanisms, while still requiring organisations to assess and manage risks associated with overseas processing. The Cyber Security and Resilience Bill would add stricter reporting rules relating to data centres and managed service providers to enhance cybersecurity if it passes.

Competition

The Digital Markets, Competition and Consumers Act (the Act) received Royal Assent on 24 May 2024. The legislation introduced a new regulatory regime for digital markets to be enforced by the Digital Markets Unit (DMU) of the Competition and Markets Authority (CMA), and gives the CMA new powers to impose large fines. It covers three broad categories of reform: (a) introducing an ex-ante regulatory regime for businesses that have "Strategic Market Status" (SMS); (b) develops behavioural antitrust prohibitions relating to abuse of dominance, merger control and market investigations; and (c) gives the CMA powers to impose civil penalties of up to 10% of a business group's worldwide turnover, without having to seek a court order in some instances.

Under the digital markets competition regime, the CMA may designate firms with "Strategic Market Status" (SMS) in relation to a particular digital activity where they have substantial and entrenched market power. Once designated, the CMA can impose conduct requirements or introduce pro-competition interventions to achieve positive outcomes for UK consumers and businesses. The DMU requires fair dealing, open choices and trust and transparency, and to treat users fairly and interact on reasonable terms to make free choices between services

and make informed choices. These requirements can extend to not using data 'unfairly' with breaches allowing a penalty of up to 10% of global turnover, with third party follow on claims for damages and disqualification of directors.

Further, The Final Order Mechanism seeks to set terms of trade between a body with SMS and one or more third parties, where it considers that the existing terms of an SMS are not fair or reasonable.

These provisions clearly have relevance to the findings of this work. However, as our research suggests, businesses are not experiencing these provisions in practice (trust and transparency, for instance).

Trade

The UK government may be restricted from legal intervention relating to the protection of workplace data by obligations in trade agreements. This renders mechanisms at the individual and firm level more important.

Digitally delivered services made up more than 60% of total UK exports of services and around 45% of total UK imports of services between 2016 and 2024.[106] These are services supplied from the territory of one country into the territory of another, where only the service itself crosses the border, and services involve the electronic transmissions of data.[107] Most policies associated with the governance of data flows from and to the UK are part of free trade agreements (FTAs).

Many trade agreements (CPTPP, Australia-UK FTA, Japan CEPA) restrict governments from developing requirements to access source code as a condition of market access. This acts as a barrier to regulatory scrutiny. Moreover, many agreements have restricted data localisation, or efforts to shape this, unless relating to personal data, which has itself been a source of contention.

The United Kingdom also participates in the World Trade Organization's (WTO) E-commerce Joint Statement Initiative, and has joined several FTAs with binding commitments to "free flows of data" across borders.[108] The purpose of these agreements has been to promote inter-operability among different systems and trust in how data is transferred, managed and used, and to uphold intellectual property rights, banning mandatory disclosure of source code to gain market access.[109] This requires trade partners to commit to establishing or maintaining domestic legal frameworks that protect both personal data and intellectual property rights.

These agreements attempt to create consistent commitments to avoid "unjustified restrictions" – as they must be "legitimate public policy objectives" and not be arbitrary or discriminatory. More encompassing agreements such as the CPTPP also subject digital provisions to the CPTPP's formal dispute settlement mechanism, which is governed by chapter 28. In it, when no agreement is reached between the parties, a panel of experts reaches a binding decision. However, the complaining party can retaliate by suspending "equivalent" benefits usually by increasing trade barriers on a non-compliant party. Others similar to the TCA are governed by the EU's "Adequacy Decision," which confirms the UK's data protection standards (GDPR) are equivalent to the EU's.

Overall, commitments around data within FTAs have often been less binding in terms of law. However, the UK has recently sought to push binding rules more strongly in their agreements. For example, recently concluded and ongoing agreements with Singapore, Ukraine, Iceland, and Lichtenstein contain high-standard rules and deep coverage of digital trade issues, including commitments to open transfers of data across borders, personal data protections and intellectual property rights protection. For Iceland, Ukraine and Lichtenstein, data protection standards are governed by the EU's "Adequacy Decision." Recent negotiations with India, however, have created exceptions to this model, as the FTA contains fewer binding

prohibitions on data localisation. It instead includes clauses to promote cross-border data flows, but allows for more domestic flexibility regarding data localization for national security and public policy, as India has traditionally maintained a "sovereign" stance on data.[110]

Despite a few exceptions (like India), the UK has sought out the free flow of data between business relations and customer-business relations. This is evidenced in a decline in the Digital Trade Integration Project's cross-border data policies score from 0.25 in 2020 to 0.17 by 2024, which indicates a reduction in barriers to data flows.

At a more international scale, the UK's participation in the World Trade Organization's (WTO) E-commerce Joint Statement Initiative seeks to influence the creation of standards on regulations and dispute mechanisms to facilitate the flows of data, while protecting personal data and intellectual property rights. This initiative, which has 71 WTO-country members as co-sponsors, representing most of world trade, includes developing digital customs and logistics processes, barriers to inter-operability between different systems, and the limited availability of certain digital services. These can facilitate the flows of data necessary to support digitisation of customs and border processes. This includes paperless trading, electronic contracts, electronic authentication, and electronic trust services. This creates a digital trail of every modification, approval, and timestamped action taken by companies and their employees, to facilitate auditing and fraud prevention. Furthermore, the digital customs can facilitate taxation of digital services, although the UK often adheres, though not fully, to the moratorium on imposing customs duties on electronic transmissions – except for a 2% Digital Services Tax (DST) on specific multinational tech revenue.

5. Reflections for the Economic Sovereignty of UKPLC

> *'I think this is happening over the next three years, we aren't there yet. I don't believe there are any companies who have fully deployed agentic systems that could be harvesting this data yet'* **Director AI Ethics, UK-based MNC**

This report has examined how the arrival of foundation models, as integrated by SaaS and Agentic solutions within British enterprises, creates a new imperative to understand the value and significance of workplace data. Historically, shifts in automation have depended on the codification of human knowledge and work processes. What distinguishes the current moment is the scale, speed, and organisational reach within which such codification can occur.

Evidence gathered through interviews, roundtables, and the IFOW Sandbox indicates that UK organisations are not yet fully aware of the value of their workplace data, or the risks arising from impact post-deployment training. Concerns about AI adoption have largely centred on personal data protection, cybersecurity, and copyright. Far less attention has been paid to the possibility that enterprise know-how – embedded in documents, communications, and workflows – may be extracted and incorporated into AI systems that are owned and controlled elsewhere or that are currently UK-owned but with structural market incentives to be bought out elsewhere.

The British Government does have strong existing bases to manage market-related risks arising from this critical danger, in competition and data laws. However, such mechanisms are untested and under-discussed. Moreover, voluntary mechanisms are not working in practice, and we find evidence of non-compliance with existing regimes.

Workplace data sits at the intersection of employment law, data protection, human rights, intellectual property, trade secrets, contract law, competition policy, and international trade agreements. None of these frameworks alone provide comprehensive governance of how workplace knowledge may be captured and redeployed through AI systems. Instead, governance emerges from their interaction across different institutional levels. This report, therefore, has argued that AI sovereignty cannot be understood solely as a matter of national technological capacity. Rather, it is the outcome of interactions between actors and governance regimes operating at several levels simultaneously: workers, firms, markets, states, and international trade systems.

Three broad implications follow.

First, workplace data should be recognised as a strategic economic resource. As AI systems increasingly depend on post-deployment training data to improve performance in domain-specific tasks, control over such data will shape future patterns of market concentration and competitive advantage.

Second, achieving economic sovereignty requires a multi-level governance approach. Workers, enterprises, and the state each occupy distinct positions within the AI value chain and face different risks and opportunities. Effective governance therefore requires coordination across employment law, data protection, procurement practice, competition policy, and industrial strategy.

Third, there is a need for institutional experimentation and regulatory learning. The complexity of AI value chains makes it difficult to anticipate outcomes through legislation alone. Hybrid sandbox environments—combining operational experimentation with

regulatory oversight—may offer a practical mechanism for understanding how legal regimes interact in practice while supporting innovation.

Ultimately, the emergence of post-deployment training data represents a structural shift in how economic knowledge is generated, captured, and redistributed. The United Kingdom has a vibrant AI ecosystem and significant strengths in research and entrepreneurship. However, the long-term benefits of these capabilities will depend on whether the country can retain meaningful influence over the value derived from its workplaces.

The challenge of AI sovereignty is therefore not only technological but institutional: it concerns how societies organise the governance of knowledge in an economy increasingly shaped by machine learning systems. Decisions taken now - by workers, firms, regulators, and policymakers - will play a significant role in determining whether the benefits of this transformation are broadly shared or increasingly concentrated.

Sovereignty in practice involves a distributed set of capabilities within and beyond the state. Practical negotiations and coordination shape sovereignty at various scales, with even highly local or small-scale transactions between workers and firms, or between firms and SaaS companies, contributing to and shaping global processes.[111]

Each interest group also faces different potential benefits and risks emanating from these outcomes and shaped by wider conditions (see Table 5).

IFOW commits to continue working in this space to devise the best approaches to support benefits for UK PLC and its workers.

Table 5

	Risks	Potential Benefits	Conditions for Benefits (for further exploration)
Workers	Displacement of work Deskilling of work Downgrading of work	Improved work quality Dividend from training data contribution	Institutional, technical and legal architectures which promote contributor dividend.
Adopting Firms	Risks to sustainability where critical business information is held by other parties; opportunity cost of not capturing the value of workplace data for organisational development	Efficiency where cost of using inference is lower than human resourcing; potential to reallocate labour to new income-generating activity; potential to capitalise on inference where captured exclusively at the firm level	Social, technical and legal architectures which facilitate preserving inference at firm level; ongoing affordability of access to inferential power.
SaaS Firms	Out-competition by those further up the value chain who gain access to inference from workplace data	Access to new clients through GenAI Integration	Technical and legal confidence in ability to preserve access to work process inferences generated when incorporating GenAI, or sustainable business models which do not rely on this
Generative AI Providers	Liabilities where there is a lack of clarity around acceptability of post-deployment training data use; risks where business model is seen to hold risks for clients	Business model opportunity from holding inference about work processes from across whole economy.	Legal and economic impunity from risks presented to other entities by this business model and approach
Nation	Reduced economic sovereignty of UK PLC	Growth in GDP where conditions for workers, UK Adopting Firms and UK SaaS Firms are realised.	

References

1. Sowell, Thomas. Knowledge and decisions. Basic books, 2022 p.47
2. Susskind, R.E. & Susskind, D. (2015) The Future of the Professions: How Technology Will Transform the Work of Human Experts. Oxford University Press, Oxford, UK.
3. Microsoft Work Trend Index 2024. Available at: https://assets-c4akfrf5b4d3f4b7.z01.azurefd.net/assets/2024/05/2024_Work_Trend_Index_Annual_Report_6_7_24_666b2e2fafceb.pdf Accessed 15th April 2026.
4. McKinsey & Company, The future of work is Agentic, June 2025. Available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/people%20and%20organizational%20performance/our%20insights/the%20future%20of%20work%20is%20agentic/the-future-of-work-is-agentic_final.pdf Accessed 15th April 2026.
5. Salesforce Research, 'HR Leaders to Redeploy a Quarter of Their Workforce as Agentic AI Adoption Expected to Grow 327% by 2027', May 2025 Available at https://www.salesforce.com/uk/news/stories/agentic-ai-impact-on-workforce-research/ Accessed 15th April 2026.
6. Papiagianaki, Eleni (2026) 'Recent methodologies on AI and labour - a desk review' Institute for the Future of Work. Available at: https://www.ifow.org/publications/methodologies-on-ai-and-labour---a-desk-review.
7. Microsoft's Head of Cloud & AI on the AI Buildout's Risks and ROI — With Scott Guthrie. Available at: https://podcasts.apple.com/gb/podcast/microsofts-head-of-cloud-ai-on-the-ai-buildouts/id1522960417?i=1000729591629 Accessed 15th April 2026.
8. George Steer, Daniel Thomas and Philip Stafford Feb 3 2026 'US stocks drop on fears AI will hit software and analytics groups.' https://www.ft.com/content/48ec5657-c2e7-4111-a236-24a96a8d49e7.
9. Kalyeena Makortoff and Dan Milmo 'Goldman Sachs chief 'hyper-aware' of risks from Anthropic's Mythos AI' https://www.theguardian.com/business/2026/apr/13/goldman-sachs-chief-hyper-aware-risks-anthropics-mythos-ai-david-solomon Accessed 15th April 2026.
10. Schaffer, Aaron, Will Oremus and Nitasha Tike January 27, 2026 'Inside an AI start-up's plan to scan and dispose of millions of books' AI https://www.washingtonpost.com/technology/2026/01/27/anthropic-ai-scan-destroy-books/
11. Imran Rahman-Jones, 11th April 2025 BBC Website 'Microsoft rolls out AI screenshot tool dubbed 'privacy nightmare' Avialable at: https://www.bbc.co.uk/news/articles/cj3xjrj7v78o Accessed 15th April 2026.
12. Lee, Wendy, June 12th 2024 'Elon Musk blasts Apple's OpenAI deal over alleged privacy issues. Does he have a point?' LA Times. Available at: https://www.latimes.com/entertainment-arts/business/story/2024-06-12/elon-musk-blasts-apple-openai-deal-over-alleged-privacy-issues-does-he-have-a-point Accessed 15th April 2026.
13. Fred Cascarini and Toby Bond, Patentability of Artificial Neural Networks to be decided by UK Supreme Court on Wednesday 11 February' Two Birds Website. Available at: https://www.twobirds.com/en/insights/2026/uk/patentability-of-artificial-neural-networks-to-be-decided-by-uk-supreme-court-on-wednesday-11-februa? Accessed 15th April 2026
14. IFOW (2026). IFOW Sandbox: Year 1 Methodology Report. Available here: https://www.ifow.org/publications/ifow-sandbox---year-1-methodology-report
15. Gilbert, Abigail and Anna Thomas (2021) The Amazonian Era. Institute for the Future of Work. Available at: https://www.ifow.org/publications/the-amazonian-era-the-gigification-of-work
16. Michael Katell, Mhairi Aitken, Kester Brewin, Abigail Gilbert, Peaks Krafft, David Leslie, Mia Leslie, Alex Mehta Brown, Aoife Monks, Claddagh NicLochlainn, Antonella Perini, Vjosa Preniqi, Elona Shatri, Magdalena Soffia. Anna Thomas (2025) 'Creative Industries and GenAI Good Work impacts on a sector in rapid transition' Institute for the Future of Work Available at: https://cdn.prod.website-files.com/64d5f73a7fc5e8a240310c4d/683ec3772a7d7d5015c3edde_CREAATIF%20Good%20Work%20Report%20-%20FINAL%202.pdf Accessed 15th April 2026.
17. Richard Speed 'Microsoft CEO: AI sovereignty isn't where it runs, it's who controls it: Ownership of models, embedded corporate knowledge matters more than server location', Nadella says. Wed 21 Jan 2026 Available at: https://www.theregister.com/2026/01/21/nadella_ai_sovereignty_wef/ Accessed 15th April 2026.
18. UNCTAD (2019). Digital Economy Report—Value Creation and Capture: Implications for Developing Countries. United Nations Conference on Trade and Development. Geneva, Switzerland.
19. McKinsey & Company, The future of work is agentic, June 2025. Available at: https://www.mckinsey.com/~/media/mckinsey/business%20functions/people%20and%20organizational%20performance/our%20insights/the%20future%20of%20work%20is%20agentic/the-future-of-work-is-agentic_final.pdf Accessed 15th April 2026
20. Nonaka, I. (1994) A Dynamic Theory of Organizational Knowledge Creation. Organization Science, 5(1), pp. 14–37; Brown, J.S., Collins, A. & Duguid, P. (1989) Situated Cognition and the Culture of Learning. Educational Researcher, 18(1), p. 32.
21. This table was iterated through interaction and several stages of content entry and prompting with ChatGPT before being reviewed by domain experts.
22. This table was iterated through interaction and several stages of content entry and prompting with ChatGPT before being reviewed by domain experts.
23. Rikap, Cecilia. "Capitalism as usual? Implications of digital intellectual monopolies." New Left Review 139 (2023): 145-160.
24. Department for Science, Innovation and Technology 'Artificial Intelligence Sector Study' 3rd September 2025 Available at: https://www.gov.uk/government/publications/artificial-intelligence-sector-study-2024/artificial-intelligence-sector-study-2024 Accessed 15th April 2026.
25. Attard-Frost, B. & Widder, D.G. (2025) The Ethics of AI Value Chains. Big Data & Society, 12(2); Heeks, R. & Spiesberger, P. (2024) Constructing an AI Value Chain and Ecosystem Model, Digital Development Working Paper Series, 109, Centre for Digital Development, University of Manchester, Manchester, UK.
26. Rosa de Acosta, John Liu 'How Nvidia became the first $5 trillion company, in 4 charts' Available at: https://edition.cnn.com/2026/02/07/business/nvidia-trillion-valuation-ai-chips-vis Accessed 15th April 2026.
27. Nigel Toon, 'Graphcore Joins Softbank Group To Build Next Generation Of Ai Compute' Jul 11, 2024 Available at: https://www.graphcore.ai/posts/graphcore-joins-softbank-group-to-build-next-generation-of-ai-compute Accessed 15th April 2026.
28. Secretary of State for Science, Innovation, and Technology, Liz Kendall, delivered a speech at Bloomberg on Wednesday 28 January 2026. Available at: https://www.gov.uk/government/speeches/liz-kendalls-speech-at-bloomberg Accessed 15th April 2026.
29. Dara Kerr 'Trump plans 100% tariffs on chips but spares companies 'building in US' Available at: https://www.theguardian.com/us-news/2025/aug/06/trump-tariffs-chips-semiconductors#:~:text=6%20months%20old-,Trump%20plans%20

100%25%20tariffs%20on%20chips%20but%20spares%20companies%20'building,bn%20domestically%20earlier%20this%20year. Accessed 15th April 2026.
30. Competition and Markets Authority Press Release, 28 January 2025 'CMA independent inquiry group publishes provisional findings in cloud services market investigation' Available at: https://www.gov.uk/government/news/cma-independent-inquiry-group-publishes-provisional-findings-in-cloud-services-market-investigation Accessed 15th April 2026.
31. Ofcom (2023) Cloud services market study: Final report. Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-3-4-weeks/244808-cloud-services-market-study/associated-documents/cloud-services-market-study-final-report.pdf?v=330228 Accessed 15th April 2026.
32. The Parliamentary Office of Science and Technology, 29 June 2020 'Cloud Computing' Available at: https://researchbriefings.files.parliament.uk/documents/POST-PN-0629/POST-PN-0629.pdf Accessed 15th April 2026.
33. Tambiama Madiega (2020) Towards a more resilient EU: Digital sovereignty for Europe. EPRS | European Parliamentary Research Service. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf Accessed 15th April 2026.
34. International Trade Association 'United Kingdom Cloud Services Market' Available at: https://www.trade.gov/market-intelligence/united-kingdom-cloud-services-market Accessed 15th April 2026.
35. Department for Science, Innovation and Technology 'Independent Review of The Future of Compute: Final report and recommendations' Updated 6 March (2023) https://www.gov.uk/government/publications/future-of-compute-review/the-future-of-compute-report-of-the-review-of-independent-panel-of-experts#:~:text=Yet%2C%20despite%20compute's%20value%20to,the%20Top%20500%20global%20systems Accessed 15th April 2026.
36. Ofcom, Cloud Services Market Study (2023) Available at: https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-3-4-weeks/244808-cloud-services-market-study/associated-documents/cloud-services-market-study-final-report.pdf?v=330228 Accessed 15th April 2026.
37. Department for Science Innovation and Technology 'Delivering AI Growth Zones' Published 31st November 2025. Available at: https://www.gov.uk/government/publications/delivering-ai-growth-zones/delivering-ai-growth-zones Accessed 15th April 2025.
38. Solaiman, I. (2023) The Gradient of Generative AI Release: Methods and Considerations. Paper presented at: New York, NY, USA, 12th June. Available from: https://dl.acm.org/doi/10.1145/3593013.3593981.
39. van der Vlist, F., Helmond, A. & Ferrari, F. (2024) Big AI: Cloud Infrastructure Dependence and the Industrialisation of Artificial Intelligence. Big Data & Society, 11(1), p. 20539517241232630.
40. Department for Science, Innovation and Technology. Available at: https://www.gov.uk/government/publications/artificial-intelligence-sector-study-2024/artificial-intelligence-sector-study-2024 Accessed 15th April 2026.
41. Our data on investment in UK AI firms is gathered from S&P Capital IQ Pro. We gathered data on all equity deals involving self-declared AI firms headquartered in the UK, a total of 2704 transactions. Percentages represent relative share of overall deal value by nationality of buyer.
42. Tyagi, Kalpana. "Mapping competition concerns along the generative AI value chain." Available at SSRN 5282596 (2025).
43. Hayton, James, Bertha Rohenkohl, Pissarides Christopher, and Hong Yu Liu (2023) "What drives UK firms to adopt AI and robotics, and what are the consequences for jobs?." Institute for the Future of Work.
44. Renieris, E. M. et al. (2023). Building Robust RAI Programs as Third-Party AI Tools Proliferate Published by Boston Consulting Group (BCG) and MIT Sloan Management Review. Available at: https://web-assets.bcg.com/1b/18/c684f0174e088e068efc4c62c942/building-robust-rai-programs-as-third-party-ai-tools-proliferate.pdf?utm_source=chatgpt.com Accessed 15th April 2026.
45. Ibid.
46. Department for Business and Skills Research and analysis 'AI Skills for Life and Work: summary report'. Published 28 January 2026 Available at: https://www.gov.uk/government/publications/ai-skills-for-life-and-work-summary-report/ai-skills-for-life-and-work-summary-report--2 Accessed 15th April 2026.
47. The Fintech Times 'UK Retailers Race to Adopt 'Agentic AI' for Payments Despite Infrastructure and Liability Gaps' December 19, 2025 Available at: https://thefintechtimes.com/uk-retailers-race-to-adopt-agentic-ai-for-payments-despite-infrastructure-and-liability-gaps/#:~:text=Almost%20half%20of%20the%20UK's,this%20innovation%20is%20outpacing%20governance Accessed 15th April 2026.
48. Microsoft Reporter (2025) Rise in 'Shadow AI' tools raising security concerns for UK organisations' Available at: https://ukstories.microsoft.com/features/rise-in-shadow-ai-tools-raising-security-concerns-for-uk/ Accessed 15th April 2026.
49. Department for Business and Trade, Trade union statistics 2024, table 1.3a, 22 May 2025.
50. Coase, Ronald H. "The nature of the firm (1937)." The nature of the firm: origins, evolution, and development (1993): 18-33.
51. Fang, Jinyuan, Yanwen Peng, Xi Zhang, Yingxu Wang, Xinhao Yi, Guibin Zhang, Yi Xu et al. "A comprehensive survey of self-evolving ai agents: A new paradigm bridging foundation models and lifelong agentic systems." arXiv preprint arXiv:2508.07407 (2025).
52. Advert, Forward Deployed Engineer (FDE) - SF. Available at: https://openai.com/careers/forward-deployed-engineer-(fde)-sf-san-francisco/ Accessed 15th April 2026.
53. Blancato, F.G. & Carr, M. (2024) The Trust Deficit. EU Bargaining for Access and Control over Cloud Infrastructures. Journal of European Public Policy, pp. 1–32.
54. Cao, Keyan, Yefan Liu, Gongjie Meng, and Qimeng Sun. "An overview on edge computing research." IEEE access 8 (2020): 85714-85728.
55. PWC 2024 Cloud and AI Business Survey. Available at: https://www.pwc.com/us/en/tech-effect/cloud/cloud-ai-business-survey.html Accessed 15th April 2026.
56. Bishop, Laura M., Phoebe M. Asquith, and Phillip L. Morgan. "The employee cybersecurity awareness framework." Human Behavior and Emerging Technologies 2025, no. 1 (2025): 1025045.
57. Blancato, F.G. & Carr, M. (2024) The Trust Deficit. EU Bargaining for Access and Control over Cloud Infrastructures. Journal of European Public Policy, pp. 1–32.
58. Grohmann, Rafael, and Alexandre Costa Barbosa. "Sovereignty-as-a-service: How big tech companies co-opt and redefine digital sovereignty." Media, Culture & Society 48, no. 2 (2026): 416-424.
59. Updated: January 8, 2026 Enterprise privacy at OpenAI. Available at: https://openai.com/enterprise-privacy Accessed 15th April 2026.
60. Anthropic Commercial Terms of Service. 17th June 2025. Available at: https://www.anthropic.com/legal/commercial-terms Accessed 15th April 2026.
61. Data, privacy, and security for Azure Direct Models in Microsoft Foundry' June 2-3, 2026. Available at: https://learn.microsoft.com/en-us/azure/foundry/responsible-ai/openai/data-privacy?tabs=azure-portal Accessed 15th April 2026.
62. Wendy Lee, June 12th 2024 'Elon Musk blasts Apple's OpenAI deal over alleged privacy issues. Does he have a point?' Available at: https://www.latimes.com/entertainment-arts/business/story/2024-06-12/elon-musk-blasts-apple-openai-deal-over-alleged-privacy-issues-does-he-have-a-point Accessed 15th April 2026.
63. Imran Rahman-Jones, 11th April 2025 'Microsoft rolls out AI screenshot tool dubbed 'privacy nightmare'' BBC. Available at:

https://www.bbc.co.uk/news/articles/cj3xjrj7v78o Accessed 15th April 2026.
64. Fred Cascarini and Toby Bond FEB 10 2026 'Patentability of Artificial Neural Networks to be decided by UK Supreme Court on Wednesday 11 February' Available at: https://www.twobirds.com/en/insights/2026/uk/patentability-of-artificial-neural-networks-to-be-decided-by-uk-supreme-court-on-wednesday-11-februa? Accessed 15th April 2026.
65. Silbey, Susan S. "After legal consciousness." Annu. Rev. Law Soc. Sci. 1, no. 1 (2005): 323-368.
66. Luhmann, Niklas. Law as a social system. Oxford socio-legal studies, 2004.
67. Brown, I. (2023) Allocating Accountability in AI Supply Chains, Ada Lovelace Institute, London, UK.
68. The party seeking to rely on the common law protection would need to go to court in order to enforce it, subject to the decision of that court of law.
69. Kateryna Nekit, The (im)possibility of personal and industrial (machine-generated) data to be subject to property rights, International Journal of Law and Information Technology, Volume 32, 2024.
70. Ibid. [1974] A.C. 391 at 401.
71. In Terrapin Ltd v Builders' Supply Co (Hayes) Ltd [1967] RPC 375, 391 Roxburgh J.
72. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR, European Data Protection Board, October 2019.
73. G Resta, 'The New Frontiers of Personality Rights and the Problem of Commodification: European and Comparative Perspectives' 2011 26 Tul Europ and Civ L Forum 33–65.
74. Kateryna Nekit, The (im)possibility of personal and industrial (machine-generated) data to be subject to property rights, International Journal of Law and Information Technology, Volume 32, 2024, https://doi.org/10.1093/ijlit/eaae008.
75. Marcello Ienca, Gianclaudio Malgieri, Mental data protection and the GDPR, Journal of Law and the Biosciences, Volume 9, Issue 1, January-June 2022.
76. Ibid.
77. Campbell v Mirror Group Newspapers Ltd [2004] UKHL 22, [2004] 2 AC 457, [2004] 2 All ER 995, [2004] 2 WLR 1232, [2005] 1 LRC 397, [2004] IP & T 764, [2004] 21 LS Gaz R 36, [2004] NLJR 733, (2004) Times, 7 May, 148 Sol Jo LB 572, 16 BHRC 500, [2004] All ER (D) 67 (May).
78. Alexander, Laura M. "Competition and Countervailing Power." Ohio State Legal Studies Research Paper 935 (2025).
79. Thomas, Anna (2023) Good Work Algorithmic Impact Assessment: A Partnership Approach. IFOW. Available at: https://www.ifow.org/publications/gwaia---a-partnership-approach Accessed 15th April 2026.
80. Stenhouse Australia Ltd. Ibid. [1974] A.C. 391 at 401.
81. Group Lotus plc and another v 1Malaysia Racing Team SDN BHD and others [2011] EWHC 1366(CH).
82. Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR, European Data Protection Board, October 2019.
83. This section on Data Ownership and its sub-sections has been taken, and adapted with permission, from its original and first publication by Lexology Pro in the item: 'The Guide to Data as a Critical Asset' specifically the chapter by Toby Bond, 'How Best to Protect Proprietary Data in Data Sharing Deals' Available at: Avail https://www.twobirds.com/-/media/new-website-content/pdfs/2022/articles/2022_gdr-data_how-best-to-protect-proprietary-data.pdf Accessed 15th April 2026.
84. For example, both interim and final injunctions prohibiting the use or disclosure of confidential information are commonly awarded by English courts and relief may be granted in relation to goods that significantly benefit from the unlawful acquisition, use or disclosure of confidential information. See The Trade Secrets (Enforcement, etc.) Regulations 2018, Regulations 11 and 14.
85. The Racing Partnership Limited v. Sports Information Services Limited [2020] EWCA Civ 1300 at [70].
86. In other words, information that has a sufficient degree of accessibility such that it would be unjust to require the party against whom a duty of confidence is alleged to treat it as confidential.
87. See, for example, The Racing Partnership Limited v. Sports Information Services Limited [2020] EWCA Civ 1300, in which the majority of the Court of Appeal held that there was no breach of confidence by a recipient of horse racing data because they had been entitled to rely on an express contractual warranty that the supplier had all necessary rights from third parties to provide the information and that the recipient's use of the data would not breach any third-party rights.
88. The Agreement on Trade-Related Aspects of Intellectual Property Rights.
89. Copyright, Designs and Patents Act 1988, Section 1(1).
90. Ibid., Section 1(2).
91. Infopaq International A/S (Case C-5/08), at [37]).
92. Painer (Case C-145/10), at [88]–[89].
93. Bezpečnostní softwarová asociace (Case C-393/09).
94. SAS Institute Inc v. World Programme Ltd [2013] EWCA Civ 1482, at [31].
95. Copyright, Designs and Patents Act 1988, Section 3A.
96. Including The Berne Convention for the Protection of Literary and Artistic Works and the World Intellectual Property Organization Copyright Treaty.
97. Directive 2001/29/EC (on the harmonisation of certain aspects of copyright and related rights in the information society), Directive 2006/116/EC (on the term of protection of copyright and certain related rights) and Directive 2009/24/EC (on the legal protection of computer programs).
98. Except for Directive (EU) 2019/790 (on copyright and related rights in the Digital Single Market), which the United Kingdom chose not to implement as the transposition date fell after the end of the transition period under the EU–UK Withdrawal Agreement. This Directive provided exceptions to copyright for the purposes of text and data mining, that have not been replicated in UK law to date.
99. The Copyright and Rights in Databases Regulations 1997.
100. The contract defines the scope of the permission granted to the data recipient to undertake acts in relation to data or a database that would otherwise infringe that copyright or database right
101. For example, acting outside the scope of a contractual licence to a database protected by a database right would give rise to a claim for both IP infringement and breach of contract.
102. See Atheraces & Anor v. British Horse Racing Board [2007] EWCA Civ 38, at [153], in which the Court of Appeal agreed with the High Court's conclusion that the British Horse Racing Board was entitled to charge for use of its data irrespective of whether it had any IP rights in that data.
103. Attorney General v. Barker [1990] 3 All E.R. 257, at 259.
104. Once the data 'escapes' beyond the control of the contracting parties, the data supplier may have a breach of contract claim against the data recipient if it is responsible for the 'escape', but will not have a breach of contract claim against third parties who receive the data. Tortious claims for procuring breach of contract or unlawful means conspiracy, however, may be available if the third party has played an unlawful part in securing access to the data.
105. For example, damages for breach of contract are generally limited to placing the claimant in the same position had the contract been performed and equitable remedies such as injunctions are less commonly awarded in breach of contract claims than in IP infringement and breach of confidence cases.

106. Department for Science, Innovation and Technology. 'Data Use and Access Act 2025: plans for commencement A summary of the government's plans for bringing into force provisions in the Data (Use and Access) Act 2025' Available at: https://www.gov.uk/guidance/data-use-and-access-act-2025-plans-for-commencement Accessed 15th April 2026.
107. UN Trade and Development Data Hub. Available at: https://unctadstat.unctad.org/datacentre/ Accessed 15th April 2026.
108. These are classified under supply mode 1, of the General Agreement on Trade in Services (GATS).
109. Including: the Trade and Cooperation Agreement (TCA) between the European Union and the European Atomic Energy Community, of the One Part, and the United Kingdom of Great Britain and Northern Ireland, of the Other Part (Art. 201); the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), which include nine countries; the Agreement between the United Kingdom of Great Britain and Northern Ireland and Japan for a Comprehensive Economic Partnership (Art. 8.84); the Australia-United Kingdom Free Trade Agreement (Art. 14.10); the Free Trade Agreement between the United Kingdom of Great Britain and Northern Ireland and New Zealand (Art. 15.14); the Digital Economy Agreement between the United Kingdom of Great Britain and Northern Ireland and the Republic of Singapore (Art. 8.61-F); and the Free Trade Agreement between Iceland, the Principality of Liechtenstein and the Kingdom of Norway and the United Kingdom of Great Britain and Northern Ireland (Art. 4.11).
110. Digital Trade Tracker. Available at: https://digitaltradetracker.org/ Accessed 15th April 2026.
111. Written Evidence to the call for evidence by House of Lords International Agreements Committee on the UK-India Free Trade Agreement (FTA). Dr Karishma Banga & Dr Christopher Foster (UIA0005) Available at: https://committees.parliament.uk/writtenevidence/149919/default/ Accessed 15th April 2026.
112. Edwards PN (2013) A Vast Machine: Computer Models, Climate Data, and the Politics of Global Warming (First Paperback Edition). Cambridge, MA: MIT Press. Also, Lowenhaupt Tsing (2004) Friction: An Ethnography of Global Connection. Princeton, NJ: Princeton University Press.

IFOW is an independent research and development institute dedicated to transforming working lives for the better, co-founded by former employment barrister Anna Thomas MBE, Nobel prize-winning economist Sir Christopher Pissarides, and technologist Naomi Climer CBE.

Our vision is a future in which everyone flourishes in work they shape.

Our mission is to understand together how to transform working lives for good.

Our belief is that creating and sustaining good work is the best way to achieve this mission and ensure that innovation and social good advance together.

About our Reports

Our expert Reports present new work from across IFOW's research team, research fellows, practioners and partners, offering policymakers, firms and academics access to the latest research in the Future of Work space.

If you would like to further information, please contact team@ifow.org

Funded by:

Friends Provident Foundation

Fair economy. Better world.

The Friends Provident Foundation is an independent charity that makes grants and uses its endowment towards a fair and sustainable economic system that serves people and planet. It connects, funds, supports and invests in new thinking to shape a future economy that works for all.

We are grateful for support from:

ESRC Centre for Digital Futures at Work

This work was supported by the UKRI Economic and Social Research Council [grant number ES/Z504713/1] as part of the ESRC Centre for Digital Futures at Work.

Institute for the Future of Work
Somerset House
Strand
London
WC2R 1LA
ifow.org / @ifow.org

Citation

Gilbert, A., Shemtov, Treleaven, P., N., Shaw, T., Rolf, S., Foster, C., Challis, E., Balcazar, C., Harris, S., Baines, J., Germann, J., Peters, T., *Economic Sovereignty and the Question of Post-Deployment Training.* London: Institute for the Future of Work.
DOI: 10.5281/zenodo.19388140

Permission to share