

Response to the UK Government Smart Data: multi-sector call for evidence

Agrifood (Q28–Q34) | Governance (Q48–Q53) | Trade (Q16–Q20) | Wider considerations (Q54–Q55)

Consent makes data shareable.
Provenance makes it usable as evidence.

Submitted by	BioChain Limited (company number 16211490)
Contact	Ashley Morgan, CEO – ashley.morgan@thebiochain.com
Respondent type	UK SME – provenance and verification infrastructure for biological and agri-food data
Questions answered	Q16–Q20, Q28–Q34, Q48–Q55
Date	30 September 2026
Website	thebiochain.com

 This response concentrates on agrifood, where BioChain Limited is running UK livestock and veterinary trial and development work, and on the cross-sector governance that agrifood Smart Data will depend on.

Summary

Inside one organisation's system, the history of a fact is usually intact. The moment it crosses into another organisation, the receiving party gets the value and loses the history — who asserted it, under what authority, from which record, by which method, and whether it has.

The problem

If Smart Data is extended to agrifood, it will make data move. On its own, it will not make that data trustworthy once it arrives.

When a value crosses from one organisation's system into another's, the receiving party usually gets the value and loses its history: who asserted it, under what authority, from which source record, by which method, and whether it has since been corrected. Inside one system that history exists. At the boundary it disappears. Smart Data is, by design, a programme of boundaries.

UK agri-food is about to meet this problem in three places at once:



Farm-level carbon data. Defra's Food Data Transparency Partnership aims, over the long term, to encourage business-specific primary data alongside better average data^[3]. Once a farm- or product-level footprint affects a supplier contract, a green loan or a retail claim, a buyer or lender will need to know which data and which methodology version produced it – and methodologies will change.



Livestock traceability. Defra's new cattle service replaces the Cattle Tracing System in England in 2027, with bovine electronic identification expected for all newborn calves during 2027^[4]. The veterinary, diagnostic, post-mortem and processing evidence around each animal will still sit in other systems – as it does for pigs, sheep and poultry.



Agri-food data-sharing infrastructure. The Food Data Transparency Partnership, the Food Data Infrastructure and Governance project and AHDB's Farm Data Exchange are building the routes by which farm data can be reused^{[5][6][7][8]}. The first question every reuse raises is the same: where did this figure come from, and can we rely on it?

Our answer

Provenance must travel with the data, as data. Every high-value assertion shared under a Smart Data scheme should carry a minimum, machine-readable record of its source, authority, method, version, relationships and integrity – proportionate to the decision it supports.

BioChain Limited, a UK company, has built this capability. The BioChain connects existing systems without replacing them, structures and links the evidence they hold, authenticates who asserted each important fact, and makes that history independently verifiable. The core architecture is demonstrated in the Ancient BioChain www.theancientbiochain.com, and we are now applying it in UK livestock and veterinary settings:

PigWare – a 12-month trial, launched in September 2026 on two commercial pig farms under ADOPT (part of Defra's Farming Innovation Programme, delivered in partnership with Innovate UK), capturing electronic identification, sensor, environmental and health-event data automatically at source; its findings feed our HerdWare livestock platform, and we will share results as they emerge^{[9][10]}.

PathPal – an early-stage discussion with the University of Surrey, whose Veterinary Pathology Centre provides farm-animal post-mortem and surveillance services, about a veterinary post-mortem reporting system in which post-mortem records and supporting evidence would be maintained within The BioChain provenance framework. Nothing has been commissioned or agreed^[11].

The Ancient BioChain – our working reference implementation of the provenance architecture for scientific data^[10].

What we recommend

1. **Define a minimum provenance profile once, centrally**, alongside accreditation and authentication, for schemes to adopt wherever shared data is relied on as evidence – disease control, certification, lending, regulatory reporting – rather than each sector inventing its own.
2. **Keep “verified” and “true” separate**. Trust frameworks should say exactly what has been checked – identity, authority, provenance, integrity – and never imply that a signed record is factually correct.
3. **Connect, do not replace**. Build agrifood Smart Data around the systems and programmes that already work – the new cattle service, FDTP, FIG, Farm Data Exchange, farm software, laboratory systems – rather than a new central platform.
4. **Add animal health to the agrifood agenda**. The call develops environmental data in detail but does not yet cover the animal-health, diagnostic and biosecurity evidence chain, which is at least as fragmented and carries higher-consequence decisions.
5. **Start voluntary and bounded**; mandate only where evidence shows a blocked market. Agrifood is too uneven in digital maturity for broad mandation now.
6. **Design for farmers and SMEs** – multiple compliant ways to connect, reusable accreditation, and explicit incentives for data holders.

What we offer

A small, measurable feasibility pilot, built from a live UK setting rather than a hypothetical architecture: the PigWare farms, with our trial partners’ agreement, as the farm-data context, connected to veterinary, diagnostic, post-mortem and processing evidence. Success is simple to state: **one animal or batch, one navigable evidence chain, several existing systems, provenance intact** – and measurably less time spent reconstructing it by hand.

The same architecture extends to a cattle cohort alongside the 2027 cattle service and to a grain-to-bread carbon chain. We propose nine months on one evidence chain across three to five existing systems; the scale, the inputs we would need and the outputs are set out at Q55.

PART A.

The gap Smart Data has not yet closed

This part sets out, once, the argument and the model used throughout the numbered answers that follow. Readers going straight to specific questions can start at Part B.

A1. Consent is necessary. It is not sufficient.

Part 1 of the Data (Use and Access) Act 2025 allows regulations to require a data holder – a trader, or a person processing data on its behalf – to provide customer data to the customer or to a person the customer authorises, and to publish or provide business data to specified recipients^[2]. DBT policy describes the accredited recipients in this model as authorised third-party providers (ATPs)^[1]. In agrifood the customer is often a business – a farm – and the data holders are the traders that supply it directly: its vet practice, feed and input suppliers, processors and farm-software providers. Other evidence, such as laboratory results commissioned by a vet or surveillance records held by APHA, sits in different relationships.

That model answers the question may this data be shared? It does not answer the question every recipient asks next: can I rely on it? A laboratory result that reaches an ATP without its sample reference, method, issuing laboratory and version is a number, not evidence. The call asks how Smart Data governance should align with developments in artificial intelligence and digital verification services^[1] – both of which make this more urgent, because automated services consume and combine data faster than anyone can reconstruct its origin by hand.

Not every record in an agrifood evidence chain will fall within the Act. Public, regulatory and research data will often participate through separate statutory, contractual or voluntary routes. Feasibility work should map the legal route data element by data element rather than assume one mechanism covers the chain.

A2. What must travel with the data

We recommend a minimum provenance envelope for any high-value assertion shared under a scheme. It builds on established models such as W3C PROV^[12] and GSI EPCIS^[13] rather than inventing a new one:

Element	What it records
Origin	The organisation and system that created the record, and its original identifier
Authority	Who made the assertion, the credential used, and the role that entitled them to make it
Relationships	The animal, sample, batch, holding, consignment or document the record relates to
Method	The method, standard or methodology – and its version – used to produce the value
Time and version	When it was created, and whether it corrects or supersedes an earlier record (which is retained, not overwritten)
Integrity	A cryptographic fingerprint allowing any later alteration to be detected
Permission	The purpose and duration for which it was shared, under whose authorisation

Requirements should be proportionate. A low-risk comparison service may need little more than a trusted source and a timestamp. A disease-control, certification, lending or regulatory decision needs the full envelope.

A3. Verified is not the same as true

This is the single most important design point in our response, and the one most often blurred. A digitally signed laboratory result proves that a named laboratory issued it and that it has not changed since. It does not prove that the test was performed correctly or on the right sample. If a Smart Data service labels such a record “verified”, users will assume more than has been checked – and as data moves faster, that false confidence becomes a risk in its own right.

Question	What answers it
Identity – who made the assertion?	Authentication of the organisation or system
Authority – were they entitled to make it?	Role, accreditation or credential checks
Provenance – where did it come from and what does it relate to?	Provenance records and links
Integrity – has it changed since it was recorded?	Cryptographic fingerprints and signatures
Accuracy – is the underlying claim correct?	Validation, accreditation, quality assurance, inspection or expert review – not cryptography

A4. Connect, do not replace

Farm software, the national traceability services, laboratory information management systems, processor ERP, assurance platforms and regulatory databases each do their job and hold their own audit history. A scheme that requires participants to move onto a new platform would add cost and resistance and duplicate what already works. The call notes that schemes may be mandated or delivered through voluntary or contractual arrangements [1]; either way, the right model is a thin trust layer across existing systems. Source systems remain the system of record. Only the data and provenance needed for the agreed purpose move.

A5. How The BioChain does it

Step	What it does	The question it answers
01 CONNECT	Attaches to existing systems through APIs, feeds, files or controlled imports	Which sources participate, without replacing them?
02 STRUCTURE	Represents identifiers, provenance and selected evidence consistently	What does this record represent?
03 LINK	Relates records across systems – animal to sample to result to batch – retaining each original source	How does this evidence relate to what came before and after?
04 AUTHENTICATE	Attributes important assertions to an identified, authorised organisation or system; key claims can be digitally signed	Who asserted this, and were they entitled to?
05 VERIFY	Fingerprints key evidence so any authorised party can check source, version and integrity independently	Is this still what was recorded?

Separating the steps makes failures diagnosable. A system can be connected but badly structured; a record can be structured but linked to the wrong animal; a signature can be intact from a party that lacked authority; a record can be authentic and unchanged and still wrong. Each failure needs a different control, and each is auditable.

A6. What a BioChain evidence record looks like

To make this concrete, below is the kind of record The BioChain holds for a single diagnostic result reused beyond the laboratory.

Question	What answers it
Assertion	Diagnostic PCR result for sample S-4471: target detected
Relates to	Pig group G-17, holding 12/345/6789; sample S-4471 taken 14 March 2027 by the attending vet
Asserted by	Accredited veterinary diagnostic laboratory (organisational credential; role: authorised to issue diagnostic results)
Source record	Laboratory information management system, record 88213
Method and version	PCR assay, laboratory standard operating procedure v3.2
Created	Reported 16 March 2027, 10:42
Status	Supersedes record EV-000171 (sample reference corrected); earlier record retained and visible
Integrity	SHA-256 fingerprint of the signed result; verifies unchanged
Shared with	Farm and attending vet; processor for 90 days under the farmer's authorisation
Does not prove	That the test was performed correctly – that rests on the laboratory's accreditation and quality assurance

 Illustrative: identifiers and values are fictional

Every field answers a question a regulator, buyer, investigator or ombudsman would otherwise have to chase by phone and email. None of it requires the laboratory to expose its whole LIMS record or give up its system.

A7. Where BioChain sits

BioChain Limited is a technology supplier: we provide provenance infrastructure and evidence-chain design that data holders, ATPs and sector bodies can use. We are not proposing in this response to act as an ATP or data intermediary in our own right. Our recommendations are technology-neutral: a ledger is one possible component of a provenance layer, not a requirement, and the envelope in A2 can be implemented by more than one provider.

PART B.

Agrifood supply chains (Q28–Q34)

Agrifood is the strongest candidate sector for trusted Smart Data evidence chains.

The information needed to understand an animal, a batch or an environmental claim is already spread across many independent organisations; the decisions that depend on it – disease control, food safety, market access, green finance – are high-consequence; and government has live programmes to build on rather than compete with.

Q28. What data sets do you use as part of your role (e.g. production, pricing, logistics, compliance)? What barriers, if any, do you face when accessing, using or sharing this data?

IN BRIEF

We design and build evidence chains across livestock identity and movement, veterinary and laboratory records, post-mortem findings, automated on-farm sensor data, processing and batch events, and assurance records. The recurring barrier is not a lack of data. It is that data loses its source, method and authority the moment it leaves the system that created it.



DATA WE WORK WITH

Data class	Examples	Typical barrier
Identity	Animal, holding, sample, batch and organisation identifiers	Different numbering schemes; weak cross-system mapping
On-farm operational	Electronic ID, sensor and environmental monitoring, health events	Held in proprietary farm systems; varying granularity
Movement	Animal movements, dispatch and receipt	Different event models; manual hand-offs
Veterinary and laboratory	Treatments, samples, diagnostic results, post-mortem findings	Result detached from sample, method and issuer outside the source system
Processing and batch	Slaughter, processing, mixing, splitting	Many-to-many transformations; identifiers change between systems
Assurance and compliance	Certificates, inspections, audit evidence	Digitised as documents without the evidence behind the claim
Environmental	Farm activity data, emissions and product-level calculations	Inconsistent methods and disjointed sharing, as FDTP itself identifies ^[3]

BARRIERS WE SEE REPEATEDLY

- **Discoverability** – participants know evidence exists but not which system is authoritative for it.
- **Identifier and semantic mismatch** – the same animal, sample or field means different things in different systems.
- **Provenance loss** – a copied value is separated from its source, method, version and issuer.
- **Correction ambiguity** – downstream users cannot tell whether a value has been corrected or superseded.
- **Commercial sensitivity** – a participant is willing to prove a fact but not to expose the whole commercial record.
- **Uneven capability** – farms and small businesses cannot run an enterprise integration stack.

OUR EVIDENCE: PIGWARE

PigWare began in September 2026 as a 12-month trial on two commercial pig farms under Defra's Farming Innovation Programme (ADOPT), using electronic identification, sensors, continuous environmental monitoring and hands-free health-event recording^{[9][10]}.

It shows where agrifood data is heading: once evidence is captured automatically at source, the hard problem stops being how do we collect it? and becomes how do we preserve its identity, context and authority when it is reused elsewhere? That is the problem Smart Data will inherit, and the one The BioChain addresses.

RECOMMENDATION

Before defining any sector-wide data model, government should require each candidate agrifood use case to produce a data inventory: the minimum data needed, the authoritative source for each element, the identifier that links it, its legal or contractual access route, the provenance that must travel with it, and who is responsible for corrections.



Q29. Which parts of the agrifood sector should be prioritised for Smart Data intervention, and why? For example, primary production, processing, logistics, waste management or areas such as green finance.

IN BRIEF

Prioritise evidence chains that several independent organisations already hold in pieces, where missing or inconsistent data has real consequences, and where success can be measured in a bounded pilot. On that test: livestock and animal health first, environmental and carbon data second, then food provenance and laboratory evidence, and once-used-many-times reporting.



Priority	Why	Foundation to build on
1. Livestock, animal health and biosecurity	Identity, movement, veterinary, laboratory and post-mortem evidence cross several institutions; disease-control decisions are high-consequence; not yet covered in the call	New cattle service in England from 2027, and the devolved systems – ScotMoves+ in Scotland, EIDCymru in Wales and NIFAIS in Northern Ireland ^{[4][32][33][34]} ; pig movement reporting (eAML2); APHA surveillance and its partner post-mortem providers; Animal Health and Welfare Pathway vet visits
2. Environmental and carbon data, including green finance	Repeated reporting and inconsistent methods; farm-level figures are acquiring commercial and financial value	FDTP, FIG and AHDB Farm Data Exchange ^{[3][6][8]}
3. Food provenance, laboratory evidence and recalls	Products must be traced through transformations and linked to test and supplier evidence	GSI EPCIS event semantics ^[13]
4. Once-used-many-times reporting	The call itself notes duplicated regulatory reporting and a lack of standard formats ^[1]	Existing compliance and assurance processes

Q30. What specific data access challenges exist in the agrifood sector and what action could be taken to address this? How might these challenges impact the development of a Smart Data scheme? For example, there are difficulties accessing particular types of data such as pricing, traceability, sustainability or compliance data.

IN BRIEF

Access in agrifood is not one problem but several: finding the authoritative source, getting a technical route in, matching identifiers, protecting commercial detail, establishing the right to reuse, and accommodating very different digital capability. An API entitlement alone solves none of them.



Challenge	Design response
Several parties hold copies or derived versions of the same fact	Define the authoritative source and correction route for every data element
Systems lack APIs or offer only exports	A minimum interoperability profile with several compliant connection methods – API, file, managed intermediary
Animals, batches and organisations are identified differently	Use authoritative identifiers where they exist; explicit mapping rules where they do not
Pricing, volumes, routes and formulations are competitively sensitive	Purpose limitation, data minimisation and selective disclosure – share the proof, not the ledger
Contracts and platform terms restrict export or onward use	Make portability and permitted onward use explicit in scheme rules
Evidence spans private systems and public traceability or regulatory systems	Let public data join as an authoritative source through its own legal route rather than forcing it into trader–customer powers
Users do not know what exists or on what terms	Discoverable metadata: holder, scope, identifiers, access conditions and provenance expectations

LEGAL SCOPE MUST BE TESTED EARLY

The DUAA powers apply where data arises from a trader–customer relationship [1]. Some animal–health and laboratory data, and most regulatory, research and public data, will need other routes depending on how it is held. Define the evidence chain first, then the legal mechanism for each element.

A PRECEDENT THAT WORKS: AHDB FARM DATA EXCHANGE

AHDB's proof of concept drew existing cattle movement, processor and feed data together with farmer permission, to avoid farmers re–entering the same information for environmental reporting. In a survey of 450 farmers, more than half said they would use the system if AHDB developed it, and respondents particularly valued the prospect of less administrative duplication [8]. It shows the demand. It also shows the next problem: once the same data feeds carbon, assurance and finance decisions, the recipient needs to know which source supplied it, which method used it, and whether it has changed.

RECOMMENDATION

Require each candidate use case to produce a data–access map before any build: for every data element, the holder, authoritative source, interface, identifier, legal or contractual basis, sensitivity, permitted purpose, correction route and required provenance. This turns “data access” from a generic barrier into a set of testable design decisions.



Q31. What specific data quality, accuracy or completeness issues exist in the agrifood sector today? How might these impact the development of a Smart Data scheme? For example, the data is held or shared in an unstandardised or non-digital format.

IN BRIEF

A Smart Data scheme will amplify whatever quality it is given. The common agrifood failures are manual transcription, inconsistent identifiers and units, results detached from their method, stale copies, silent overwriting and broken transformation links. Quality and provenance should be specified together, because a value you cannot trace is a value you cannot assess.



Failure	Consequence	Control
Manual transcription	Mistyped animal, batch or sample identifiers	Electronic capture where proportionate; validation at source. Defra notes electronic ID reduces transcription errors ^[4]
Inconsistent identifiers and units	Records cannot be joined, or are joined wrongly	Standard vocabularies, units and explicit mapping
Missing method context	A result or footprint cannot be interpreted or compared	Method and version as mandatory fields
Stale or duplicated copies	Decisions taken on superseded data	Version and supersession handling with one authoritative source
Silent overwriting	The basis of an earlier decision disappears	Retain prior states; record who changed what, when and why
Broken transformation chain	A batch cannot be traced to its inputs	Capture links at every mixing, splitting or processing event

FDTP identifies consistency, accuracy, accessibility, infrastructure and governance as linked challenges, and notes that interoperability reduces the burden of translating and re-reporting the same data [3]. We agree, and add one point: a perfectly formatted number with no trustworthy source is worth less than an awkward record whose origin is clear.

RECOMMENDATION

Evaluate pilots not only on whether data was exchanged but on whether the receiving party could determine its quality, origin and current status. Each use case should publish a minimum data-quality profile – mandatory identifiers, units and methods, freshness, provenance fields, correction rules, which assertions must be authenticated, and how conflicts are resolved.



Q32. What use cases could a Smart Data scheme enable in the agrifood sector, and what outcomes could these deliver? Please detail the barriers that would need to be addressed, and necessary governance structures required for these to be successful.

IN BRIEF

The highest-value use cases need evidence from several systems to answer one operational question. We propose three, each mapped to an existing government priority and each testable with the same architecture: livestock health evidence, farm-level carbon evidence, and food provenance through processing.



Use case	Outcome	Main barrier	Governance needed
Animal health and biosecurity	Faster reconstruction of evidence in an investigation; gaps and conflicts made visible	Evidence spread across traceability, veterinary, laboratory and post-mortem systems	Authoritative roles, access controls, auditable corrections
Farm-level carbon and environmental evidence	Figures reused across buyers, lenders and assurance without re-entry; lower-emission producers recognised	Method inconsistency, farmer burden, blending of commodities	Farmer control, permitted purposes, method versioning
Food provenance, laboratory and certification	Faster trace-back and trace-forward; claims tied to the right evidence and version	Many-to-many transformations; inconsistent batch identifiers	Authenticated issuers, selective disclosure
Once-used-many-times compliance	Less duplicate entry and reconciliation	Different forms and semantics; unclear onward-use rights	Purpose limitation, source responsibility

CARBON: THE NUMBER IS NOT ENOUGH

As farm- and product-level carbon figures start to carry commercial and financial weight, the evidence behind a figure matters as much as the figure [3]. A reusable footprint should show which source data contributed, which methodology and version produced it, who produced or approved the calculation, and when. Methodologies will be revised; a buyer or lender must be able to tell a figure calculated under one version from one calculated under the next.

Blended commodities make this harder. A loaf of bread can contain wheat from many farms, pooled at the grain store and again at the mill. Unless the link from each farm's grain lot survives each blend – with its proportion and method – farm-level performance collapses back into an average, which is precisely the outcome farm-specific footprinting is meant to end. Individual millers and bakers have run their own grower programmes, but each sits in its own system; a Smart Data provenance layer lets that evidence be reused across buyers.

ANIMAL HEALTH: THE MISSING USE CASE

A farmer is the customer of their vet practice; the practice is often the laboratory's customer. Where records the vet holds about the farmer's animals fall within the DUAA customer-data model, the farmer could authorise specified records to reach an ATP [2]. Laboratory results, APHA surveillance and post-mortem records will usually need their own contractual or statutory routes – and mapping those routes is itself a valuable feasibility output. The evidence chain is naturally distributed – identity, observations, samples, results, movements, post-mortem findings, processing – and today it is reconstructed by hand when something goes wrong. PigWare gives us a live on-farm context for this chain, and early discussions on veterinary post-mortem reporting point to a complementary one [9].

PROPOSED FEASIBILITY PILOTS

Pilot	Setting	What it tests
A. Pig health evidence chain (first)	The two PigWare farms, with our trial partners' agreement, connected to pig movement records (eAML2), veterinary, diagnostic, post-mortem and abattoir or processor records	Customer-authorised flow; linkage across 3–5 existing systems; authenticated laboratory assertion; a correction propagated without erasing history
B. Cattle cohort alongside the 2027 service	Electronically identified calves born in England in 2027 on a handful of farms, from registration to slaughter	The new cattle identity as anchor; links across electronic and conventional tags; disease testing and surveillance evidence
C. Grain-to-bread carbon chain	A handful of farms supplying one store, mill and bakery	Method and version on every figure; farm-level evidence surviving blending; reuse across buyers

Each pilot should connect three to five existing systems, replace none of them, and measure: time to reconstruct the evidence chain against today's manual process; duplicate entry removed; the share of evidence whose origin, version and issuer are visible; unresolved linkage exceptions; whether a correction is visible downstream; and integration cost for each type of participant, including farms and SMEs.

GOVERNANCE BEFORE INGESTION

Before any data moves, each pilot must settle who is authoritative for each data class; who may create, authenticate, correct, view and export it; how credentials are issued and revoked; how conflicting records are resolved; what is retained; which purposes are permitted; and how participants leave or change provider. These are not legal afterthoughts. They are the architecture.

RECOMMENDATION

Take at least one animal-health evidence chain into targeted feasibility work alongside environmental data. It tests the same Smart Data principles in a higher-consequence setting, complements FIG rather than competing with it, and can start from a live UK context.



Q33. To what extent do existing commercial arrangements, including contractual obligations, constrain your ability to share data with supply chain partners or third parties? What considerations should a Smart Data scheme include to address these constraints?

IN BRIEF

We do not hold sector-wide evidence on the prevalence of restrictive contracts and will not overstate it. In practice, sharing is constrained by confidentiality duties, platform and API terms, charges for export, rights in derived data, unclear liability and restrictions on onward use. A scheme should make each of these explicit – and must also answer why a data holder would take part at all.



CONSTRAINTS A SCHEME SHOULD EXPECT

- **Confidentiality** – pricing, formulation, volumes, routes and customer relationships.
- **Ownership language** – contracts that assign data to one party although another created or needs the underlying facts.
- **Platform terms** – limits on automated access, export frequency and third-party use.
- **Derived data** – footprints, scores and models carrying intellectual property beyond the raw inputs.
- **Liability** – reluctance to allow reliance when responsibility for an inaccurate or outdated record is unclear.
- **Power imbalance** – small suppliers pressed to share broad datasets with large buyers.

DATA HOLDERS NEED A REASON TO PARTICIPATE

Veterinary practices, laboratories, software vendors and processors bear the integration, security and support costs of exposing data, and may see little direct benefit. The value exchange should be designed, not assumed: who benefits, who pays, what service levels apply, and whether cost recovery is appropriate. Part 1 of the DUAA allows regulations to provide for fees and levies in defined circumstances^[2], so the funding model can be deliberate. Pilots should test the data-holder incentive as rigorously as the farmer's.

WHAT THE SCHEME SHOULD SPECIFY

- The minimum data for each use case – a narrow verifiable assertion rather than broad disclosure wherever that suffices.
- A clear distinction between custody, intellectual property and permission to access for a stated purpose.
- Permitted purposes, onward-use rules and retention, and when reuse needs fresh permission.
- Liability boundaries between the source of an assertion, any intermediary and the relying party.
- Portability, so a participant can change provider without losing its provenance history.

FDTP already sets out the principles: respect commercial sensitivity, give data owners control over who data is shared with, avoid lock-in to any one data-service provider and minimise reporting burden^[3]. They should carry directly into any agrifood scheme.

RECOMMENDATION

Treat commercial permissions as part of the interoperability profile. Every pilot should record which evidence can be reused, by whom, for what purpose, for how long and under whose liability. Technical success without a clear right to reuse is not interoperability.



Q34. How could a Smart Data scheme complement existing data-sharing and digitalisation initiatives in the agrifood sector? What additional value could it provide, and are there any risks that it could duplicate or hinder existing initiatives?

IN BRIEF

Smart Data should be the connective tissue between existing agrifood programmes, not a parallel estate. Its distinct value lies at the boundaries between them – where a movement record, a laboratory result and a processing event, each authoritative in its own system, have to be relied on together.



Use case	Outcome	Main barrier
New cattle service and the devolved traceability systems	Identity and movement; together, a UK-wide movement picture ^{[4][32][33][34]}	Use identity as the anchor for external evidence; do not turn traceability into a repository for every adjacent domain
FDTP and FIG	Consistent environmental data; data-sharing infrastructure and governance design and pilots ^{[3][6][7]}	Enable authorised reuse beyond the original purpose and link to non-environmental evidence; do not build a competing architecture
AHDB Farm Data Exchange	Farmer-controlled reuse of existing data ^[8]	Carry provenance with reused data; do not recreate its permission centre
APHA surveillance, Animal Health and Welfare Pathway, assurance schemes	Disease surveillance and post-mortem networks; funded vet visits; farm assurance such as Red Tractor	Link their evidence to the animal and batch with its issuer intact; do not duplicate their data collection
GS1 EPCIS systems	Supply-chain visibility events ^[13]	Add authentication and links to evidence outside the event stream; do not replace mature semantics
Farm, laboratory, processor and assurance systems	Operational records and workflows	Standard interfaces and a portable provenance layer; no rip-and-replace

DUPLICATION RISKS TO AVOID

- Another central database copying records already well managed elsewhere.
- New identifiers where authoritative ones exist.
- A proprietary data model instead of mappings between established standards.
- A second reporting workflow or governance structure alongside existing ones.
- New provider lock-in, created while claiming to remove old silos.
- Scaling before a pilot has shown measurable operational value.

RECOMMENDATION

Require every proposed agrifood use case to pass a complementarity assessment before funding or regulation: which existing system or programme owns each function, what is reused, what genuinely new capability Smart Data adds, and what duplication or lock-in risk it creates.



PART C.

Governance and cross-sector coordination (Q48–Q53)

Our governance position in one line: centralise the trust rules that must travel across schemes; leave sector decisions with the bodies that understand the sector.

Q48. What aspects of governance are most important for Smart Data schemes in practice, and why?

IN BRIEF

Clear accountability, trustworthy identity and authority, customer control, proportionate accreditation, explicit rules for provenance and corrections, open interoperability, incident handling, redress and long-term stewardship. Governance is not an organisation chart: who may assert what, which source is authoritative and how a correction propagates all change the technical design.



DBT-commissioned research recommends a federated model in the medium term – sector implementation entities, a central coordination entity that sets common standards, accredits third parties and manages cross-sector services such as authentication, and existing regulators enforcing in their sectors – with a possible move towards central leadership later [15][1]. We support the federated model. It combines common trust infrastructure with sector knowledge.

Common across schemes	Sector-specific	Use-case-specific
Accreditation	Authoritative datasets and identifiers	The exact fields shared
Organisational identity and authentication	Vocabularies and data models	Who may rely on them
Minimum consent semantics	Assurance levels and timing	The assurance level required
Minimum provenance envelope	Laboratory, veterinary and certification rules	The customer benefit that justifies the exchange
Portability	Correction and dispute processes	
Conformance testing	The enforcing regulator	
Incident escalation and redress routing		

MATURITY MATTERS: DO NOT START WITH MANDATION IN AGRIFOOD

Agrifood is uneven in digital maturity, and DUAA applicability will differ by data element and relationship. We would begin with voluntary or contractual pilots, use targeted Smart Data powers where feasibility work shows a clear customer benefit or a portability barrier, and reserve mandation for bounded use cases with evidence of persistent market failure, blocked access or a strong public-interest case^{[1][2]}. Banking, where the model is mature, is a poor template for timing.

RECOMMENDATION

RDefine a cross-economy governance baseline – accreditation, identity and authentication, customer control, minimum provenance, portability, incident handling and redress routing – that sector implementation entities extend rather than redefine.



Q49. How should Smart Data schemes be governed and coordinated in practice where services or data flows span more than one sector?

IN BRIEF

Through the federated model, with provenance added to the common functions. Authentication tells a receiving service who an organisation is. Provenance tells it what that organisation asserted, from which record and method, and whether it has changed. Without a shared provenance expectation, cross-sector services will combine technically compatible data whose evidential status cannot be compared.



Issue	If schemes diverge	Common approach
Organisational identity	The same organisation needs different credentials in each sector	One reusable identity with scheme-specific roles layered on top
Accreditation	Duplicated audits for providers serving several sectors	A reusable core with sector modules
Consent	The same customer journey expressed differently	Common minimum semantics for scope, purpose, duration and withdrawal
Provenance	Source and version become inconsistent when data is combined	A common minimum provenance envelope
Redress	Customers cannot tell which scheme failed	Common routing and a no-wrong-door principle
Portability	Switching in one scheme breaks a cross-sector service	Portable permissions and exportable provenance history

Agrifood shows why this matters. A farm carbon service uses agrifood data to inform a lending or insurance decision. An animal-health evidence chain starts on the farm, passes through a laboratory, supports a trade certificate and relies on verifying who is entitled to act for the organisations making key assertions – where the UK digital verification services trust framework and its delegated-authority guidance are directly relevant [16]. The customer should not need to know which scheme supplied which piece of trust.

RECOMMENDATION

The central coordination body should maintain a common trust-and-provenance profile that sector schemes adopt rather than re-create. Cross-sector pilots should test whether one organisation can reuse its accreditation, identity and provenance controls across at least two schemes.



Q50. How should customers be protected and able to seek redress where Smart Data services span more than one scheme or sector?

IN BRIEF

One understandable journey and one door to knock on, however many schemes sit behind the service. Redress is an evidence-chain problem: when something goes wrong, provenance is what allows anyone to establish which control failed and who is responsible.



Take a “verified” laboratory result later found to be wrong. The laboratory may have produced an inaccurate result; a data holder may have shared an out-of-date version; an ATP may have linked it to the wrong animal; a credential may have been compromised; or a downstream service may have used it outside the permitted purpose. To the customer, each looks the same: the service was wrong. The responsible party is different in every case, and only a retained provenance record can tell them apart.

Party	Accountable for	Evidence needed
Source of the assertion	Accuracy and correction of what it asserted	Original record, method and version, correction history
Data holder	Correct sharing and maintenance of the correction route	Sharing log, permission basis, version supplied
ATP or service provider	Use within scope, correct linkage, security, customer service	Processing history, linkage evidence, permission scope
Identity service	Issuance and revocation of credentials	Credential status and revocation log
Relying party	Use within the permitted purpose	Decision record and evidence relied on

The call asks how this should interact with the ICO and the Financial Ombudsman Service [1]. Both should keep their statutory roles. The gap lies in problems that span schemes or involve non-personal business data, linkage errors or provenance disputes that fit no existing ombudsman. We would not create a new ombudsman before feasibility work has mapped that gap; we would require a common complaints taxonomy, a lead-handler obligation on the customer-facing service and mandatory hand-off between schemes

RECOMMENDATION

Adopt a no-wrong-door redress model, common incident categories, and mandatory provenance and audit evidence sufficient to establish which control and which organisation failed



Q51. What factors would encourage and deter your organisation from participating in a Smart Data scheme?

IN BRIEF

As a UK SME building provenance infrastructure, we would be encouraged by clear use cases, open standards, reusable accreditation, proportionate assurance, transparent liability, testing environments and a credible route from pilot to sustained service. We would be deterred by duplicated accreditation, high fixed compliance costs, proprietary standards, unclear liability and slow, uncertain procurement.



Encourages	Deters
A defined service with a visible customer benefit	An obligation to share with no visible outcome
One accreditation core with sector modules	A separate accreditation, identity framework and test suite per sector
Published schemas, mappings and conformance tests	Mandatory proprietary schemas or closed technology stacks
APIs for mature participants and file, batch or intermediary routes for others	API-only participation
Published allocation of liability	Expectation that providers insure against failures outside
Sandbox with test data and credentials	Fees and audits sized for banks rather than specialist
A funded route from pilot to operation	Pilots with no operator or funding once they succeed

Farmers need the same proportionality. DBT’s inclusive-design research identifies trust, consent, control, support and redress as central^[17], and Open Banking guidance stresses clear consent and a seamless hand-off between providers^[18]. Both lessons transfer directly to business customers with little time to manage data-sharing arrangements. Data holders need explicit incentives too (see Q33).

BioChain Limited is not proposing in this response to act as an ATP. Our role is provenance infrastructure and evidence-chain design that data holders, ATPs and sector bodies can use; any future accredited role would be judged against final scheme rules.

RECOMMENDATION

Use tiered, risk-based and reusable assurance: a common accreditation core, sector modules, transparent costs, open standards and several compliant connection methods. Proportionality should change how compliance is achieved, not the security outcome required.



Q52. What lessons from existing UK data-sharing initiatives should shape Smart Data governance?

IN BRIEF

Interfaces are necessary and never sufficient. Durable data-sharing needs common standards, trusted governance, a usable consent journey, operational stewardship, and a way to fund the service after the build.



OPEN BANKING: THE RAILS ARE NOT THE JOURNEY

Open Banking shows the value of standard interfaces and accredited third parties, and its customer-experience work shows that adoption depends on people feeling informed and in control, with clear consent and a smooth hand-off between providers^[18]. API conformance is not scheme usability.

AHDB FARM DATA EXCHANGE: TRUSTED INTERMEDIATION REDUCES BURDEN

Farmers responded to a farmer-first exchange that reused existing records rather than adding a reporting task, and saw AHDB as trusted and potentially well placed to act as a neutral intermediary^[8]. Adoption follows a trusted sector body that can explain purpose, permission and benefit.

PATHPAL: A USEFUL TOOL NEEDS AN OPERATING MODEL

Our discussions about PathPal, a veterinary post-mortem reporting concept, illustrate a general lesson: useful digital tools need a funded model for maintenance, standards stewardship, support, security and long-term evidence retention after the initial project ends.

DIGITAL MARKETS: START NARROW AND PROTECT CHOICE

The government's 2026 response on Smart Data in digital markets records support for phased, use-case-driven delivery, clear allocation of responsibilities, proportionality and customer choice of provider – and warns that solving too many problems at once creates complexity and weak accountability^[19].

RECOMMENDATION

Before any scheme moves from pilot to scale, require four artefacts: a customer-journey model, an accountability model, a technical conformance profile and a sustainable operating and funding model. A technically successful pilot without all four is not ready to scale.



Q53. Are there international examples of data-sharing or Smart Data-style approaches, in the sectors covered by this Call for Evidence or in other sectors, where lessons may be transferable?

IN BRIEF

Three: Estonia’s X-tee for distributed exchange with strong trust controls; the EU Data Act for user rights over connected-product data, including farm machinery; and Biocheck.UGent for sector-specific livestock data governance. None is a template; each carries a transferable principle.



Example	Transferable principle	Limitation
Estonia – X-tee	Secure exchange between organisations' own systems using authentication, multi-level authorisation, logs, encryption and signed traffic, without centralising the data ^[20]	Organisation-to-organisation exchange, not a customer-consent scheme
EU Data Act	Users' right to access data from connected products in structured, machine-readable form; applies from 12 September 2025, with access-by-design for products placed on the market after 12 September 2026;	Different legal framework; would need UK design choices
Biocheck.UGent	Standardised livestock biosecurity assessment used in over 100 countries, with confidentiality controls, benchmarking and integration into national programmes ^[22]	A sector service model, not a statutory governance framework

X-tee is the closest match to the architecture we recommend: interoperability without a central database, with trust made explicit in every exchange. The Data Act is a live signal that farm machinery and sensor data – the data PigWare-type monitoring generates – will increasingly come with user access rights in the UK’s largest trading partner.

RECOMMENDATION

Align internationally on principles and standards – distributed exchange, customer control, portable trust, machine-readable metadata and sector semantics – rather than importing another jurisdiction’s governance wholesale.



PART D.

Governance and cross-sector coordination (Q48–Q53)

Our trade answers are deliberately short and focus on where trade meets agrifood: sanitary and phytosanitary (SPS) evidence, provenance and certification.

We note the call's point that Smart Data is primarily about unlocking private sector data rather than government bodies reusing their own, and have framed these answers accordingly: the evidence we describe – veterinary, laboratory, processing and certification records – is created and held by private actors, and our recommendations concern how it reaches the party that must rely on it.

Q16. Are existing frameworks sufficient to support the sharing of trade-related data held by private sector actors, particularly where such data relates to the trader itself or its customers? Please provide details and evidence of areas where this is not working so well.

IN BRIEF

Necessary, not sufficient. The UK has strong legal and policy foundations for digital trade; the gap is interoperability, provenance and trust between the systems and standards that already exist.



The Electronic Trade Documents Act 2023 gives qualifying electronic documents the legal effect of paper without prescribing a technology [23] – so interoperability has to be achieved elsewhere. DBT's research with SME exporters finds low awareness, limited capability, fragmented systems and inconsistent international acceptance [24]. Customs Modernisation is examining how the customs model can align with digitalised business operations [25]. In practice the same fact is re-entered across documents, identifiers differ between systems, and values arrive without the record of who asserted them or which version was used.

RECOMMENDATION

Define a minimum provenance envelope for trade-related Smart Data exchanges that travels alongside existing trade data models rather than becoming another competing one.



Q17. How might Smart Data approaches build on current digitalisation initiatives (for example where there are current gaps), rather than duplicating systems or platforms already in use and support existing trade digitalisation activity?

IN BRIEF

Sit between existing initiatives, not beside them. Capture or validate a fact once, keep its provenance, and let authorised parties reuse it across documents and regulatory interactions.



The Trade Strategy commits to piloting Digital Trade Corridors and helping smaller businesses escape the “physical paper-chase” [26]; the corridors programme is testing digital processes on real routes [27]. Smart Data adds value where these meet: between a commercial platform and a regulator, a logistics record and an SPS certificate, an electronic document and the source evidence behind it. Digitising documents alone can preserve paper’s duplication in electronic form; the mature model distinguishes the underlying evidence from the documents that present it.

RECOMMENDATION

Test a “connect, map and reuse” approach on an existing Digital Trade Corridor using an agrifood consignment, rather than commissioning a new end-to-end platform.



Q18. What trade requirements that rely on tracking throughout the supply chain to ensure smooth movement across borders could benefit from a Smart Data framework to ensure smooth data capture and sharing?

IN BRIEF

Those where the border decision depends on evidence created earlier by several independent actors: SPS, animal-health and food-safety evidence; origin and chain of custody; regulated product conformity; and customs-supporting documentation.



A border authority rarely creates the evidence it relies on. It originates with producers, vets, laboratories, processors and certifiers. The call itself identifies supply-chain traceability and provenance at the border, and the role of accurate information in SPS enforcement, fraud detection and risk-based inspection [1]. An animal-derived consignment is the ideal test: identity, veterinary and laboratory evidence, processing and certification each sit in a different system, and the border needs to know that each claim is attributable and current – without receiving every upstream record.

RECOMMENDATION

Prioritise at least one cross-border agrifood/SPS evidence chain in feasibility work, sharing only the data and proofs the border decision requires.



Q19. What risks or challenges could arise from using Smart Data in trade, and how might these be mitigated in practice? (For example, risks relating to data accuracy, unequal access for different types of businesses, cybersecurity, unintended impacts on competition, or the readiness of existing trade systems and processes).

IN BRIEF

The biggest risks are not only cyber. They are poor source data presented as “verified”, wrong entity matching, over-exposure of commercial data, SME exclusion, unclear accountability for corrections, cross-border non-recognition and new lock-in. Each is manageable if designed for from the start.



Risk	Mitigation
False confidence: signed data assumed true	State exactly what was verified; keep accuracy controls separate (see Part A3)
Identity and authority failures	Trusted organisational credentials, role-based authority, revocation and auditable delegation
Wrong entity matching	Authoritative identifiers, explicit mapping rules, human review of ambiguous matches
Commercial over-exposure	Data minimisation, purpose limitation, selective disclosure
SME exclusion	Several compliant connection methods and assisted onboarding; measure burden in pilots [24]
Corrections and liability	Retain prior versions; record who corrected what and why; allocate accountability in governance
Cyber security	Least privilege, key protection, monitoring, incident response, independent assurance
Lock-in	Open standards, documented interfaces and portable provenance

RECOMMENDATION

Evaluate any trade pilot against a published risk model covering these risks. Success is safe, usable interoperability – not the volume of data exchanged.



Q20. What international data standards, data models or frameworks do you currently use in relation to trade data? In your view, to what extent do these enable or constrain interoperability, data sharing and the effective use of Smart Data? Please provide evidence or examples where possible.

IN BRIEF

No single standard covers the trade evidence chain, and none should be invented to do so. Our architecture is designed to map to established standards and add the provenance and authentication layer between them; we do not claim to be a production implementation of each.



Layer	Standard	Role in Smart Data
Border and regulatory data	WCO Data Model ^[28]	Use or map to established border semantics
Trade and supply-chain semantics	UN/CEFACT Buy-Ship-Pay Reference Data Model, UN/EDIFACT, UN/LOCODE ^[29]	Preserve internationally recognised models and codes
Supply-chain events	GSI EPCIS / CBV 2.0 ^[13]	Event-level visibility, complemented by provenance and authentication
Trade documents	ICC Digital Standards Initiative Key Trade Documents and Data Elements ^[30]	Align document data elements to support reuse
Provenance	W3C PROV ^[12]	Origin, derivation and responsibility
Digital trust	UK digital verification services trust framework ^[16]	Trusted verification, including delegated authority to act for an organisation

Standards can become silos in their own right. UNECE and the WCO are mapping the WCO Data Model to the UN/CEFACT Core Components Library^[31] – a useful precedent: mapping mature standards is worth more than forcing one to absorb every use case.

RECOMMENDATION

Publish a standards-mapping and conformance approach for any trade pilot, judged on semantic compatibility, provenance, authentication, access and verification – not on adoption of any single vendor or database.



PART E.

Wider considerations (Q54–Q55)

Q54. Are there any other risks, opportunities or benefits (such as environmental or societal) you would like to raise that relate to Smart Data?

IN BRIEF

The opportunity is reusable, trusted evidence across sectors without centralising source records. The risk is that data becomes easier to move, combine and automate faster than its origin, authority, method and permitted purpose can be understood.



OPPORTUNITIES

- **Provenance-ready automation.** As AI and automated services consume shared data, machine-readable provenance lets decisions be explained and challenged later. Automation should never strip out the evidence a human reviewer would need.
- **Carbon figures that stay interpretable.** Recording source data, method and methodology version with every figure lets buyers, lenders and assurers compare like with like as methods evolve.
- **Lower-burden capture.** Farm Data Exchange and PigWare point to a model where data is captured once, often automatically, and reused for permitted purposes [8][9]. The saving should be measured, not assumed.
- **Better evidence for high-consequence decisions.** Faster, reconstructable evidence for disease, food-safety and assurance investigations.

RISKS TO DESIGN OUT

- **False certainty** – authenticated data presented as correct.
- **Over-collection** – access for one service becoming a general right to reuse.
- **Exclusion** – farms, SMEs and small providers priced out by enterprise-scale requirements.
- **Lock-in** – permissions and provenance history that cannot move with the customer.
- **Automated errors** – corrections that fail to reach downstream copies.
- **Unsustainable pilots** – services with no operator once grant funding ends.

RECOMMENDATION

Require each use case to define a proportionate evidence profile alongside its technical standard: what provenance accompanies the data, how identity and authority are established, how corrections propagate, which purposes are permitted, how permissions are withdrawn, and what is retained for redress. For derived figures such as carbon footprints, method and version are part of the evidence.



Q55. Is there anything you haven't said already that you would like to add in response to the Call for Evidence?

IN BRIEF

One principle summarises our response: consent makes data shareable; provenance makes shared data usable as evidence.



SIX PRINCIPLES TO CARRY FORWARD

1. Start with a defined use case – the decision, the customer benefit, the data holder and the party that must rely on the evidence.
2. Connect rather than replace existing systems and programmes.
3. Treat provenance as first-class data for high-value evidence.
4. Keep authority, integrity and accuracy separate, and say which has been checked.
5. Design for portability and proportionate participation, so farmers, SMEs and small providers can take part.
6. Measure operational value in bounded pilots before scaling.

OUR OFFER

The capability this response describes already exists in the UK and is being applied to UK livestock and veterinary data. BioChain Limited would welcome the opportunity to contribute to targeted agrifood feasibility work – starting with a pig health evidence chain on the PigWare trial farms, which our trial partners have agreed to, and extending to a cattle cohort alongside the 2027 cattle service and a grain-to-bread carbon chain. We will share PigWare results as they emerge.

THE SHAPE OF THE PILOT WE PROPOSE

7. Duration. Nine months: two months on design and governance, four on connection and reconstruction, three on evaluation and reporting.
8. Scope. One evidence chain, three to five existing systems, one farm cohort. No system replaced and no new central database.
9. Participants. The PigWare trial farms, their veterinary practice, a diagnostic laboratory, a post-mortem provider, and an abattoir or processor.
10. What we bring. The provenance layer and its connectors, the evidence model, the measurement framework, and the automated on-farm data capture already funded through ADOPT.
11. What we would need. Data-sharing agreements with the participating organisations; access to movement records by the appropriate route; a named counterpart in government or the sponsoring programme; and agreed funding for the connection and evaluation work.
12. Outputs. A working evidence chain across the participating systems; a published report against the measures set out at Q32; a data-access map for every element; and a proposed minimum provenance profile for agrifood.
13. Cost. To be scoped with the sponsoring programme. The design is deliberately small: the purpose is to establish cheaply whether cross-system provenance does what we describe, at a scale where being wrong is inexpensive.

WHAT WE ARE, AND WHAT WE ARE NOT

BioChain Limited is a young company building infrastructure for a problem the sector is only beginning to name. We have a working implementation, a live on-farm trial and a defined model. We do not have years of operational data across multiple agrifood deployments, and we will not imply otherwise.

That is the argument for a bounded pilot rather than a programme. A nine-month test on one evidence chain is the least expensive way for government to establish whether provenance travelling with the data changes anything measurable. If the measures at Q32 hold, the case for a wider provenance profile is evidenced rather than asserted. If they do not, the finding is still useful to the sector, and it will have cost very little to learn.

RESPONDING TO THE STRATEGY'S OWN INVITATION

Smart Data 2035 sets a horizon of 20 or more interoperable schemes by 2035, names agrifood among the sectors in scope, and records that government is commissioning research in 2026 into how smart data regulations could support environmental data sharing, beginning with greenhouse gas emissions [35]. It also issues an invitation: "Where industry and innovators see potential for smart data schemes to benefit customers and the economy, we call on them to convene and collaborate to move towards pilots in their sectors, building on best practice that already exists."

This response is that. BioChain Limited is a British company, and the provenance capability the strategy's agrifood work will need is built and running today on public research data. We would rather test it against a real UK evidence chain in 2027 than describe it again in 2030.

The test for each is the same: one animal or batch, one navigable evidence chain, several existing systems, provenance intact – and less time spent reconstructing it by hand. If those properties hold in practice, scale becomes a design choice rather than an assumption.

WE WOULD WELCOME CONTACT

We would welcome direct contact about any part of this response: from the Smart Data team at the Department for Business and Trade; from Defra colleagues working on the Food Data Transparency Partnership and the Food Data Infrastructure and Governance project; and from anyone convening agrifood feasibility work, an animal-health evidence chain or a farm-level carbon chain. We can demonstrate a working provenance chain rather than a slide deck, and we can join a workshop, a technical session or a scoping conversation at short notice.

Ashley Morgan, Chief Executive

BioChain Limited (company number 16211490)

Email: ashley.morgan@thebiochain.com

Web: thebiochain.com.

REFERENCES

- [1] Department for Business and Trade (2026). Smart Data: multi-sector call for evidence. CP 1608. Published on GOV.UK 8 July 2026. GOV.UK. <https://www.gov.uk/government/calls-for-evidence/smart-data-multi-sector-call-for-evidence> (accessed 25 September 2026).
- [2] Data (Use and Access) Act 2025, c. 18, Part 1 and Explanatory Notes: access to customer data and business data. <https://www.legislation.gov.uk/ukpga/2025/18> (accessed 25 September 2026).
- [3] Department for Environment, Food & Rural Affairs (Defra) (2024). FDTP: towards consistent, accurate and accessible environmental impact quantification for the agri-food industry. Published 23 April 2024; updated 10 May 2024. GOV.UK. <https://www.gov.uk/government/publications/food-data-transparency-partnership-agri-food-environmental-data/fdtp-towards-consistent-accurate-and-accessible-environmental-impact-quantification-for-the-agri-food-industry> (accessed 25 September 2026).
- [4] Department for Environment, Food & Rural Affairs (Defra) (2026). Livestock Information Transformation Programme (LITP). Published 20 January 2026; updated 23 July 2026. GOV.UK. <https://www.gov.uk/government/publications/livestock-information-transformation-programme-litp/livestock-information-transformation-programme-litp> (accessed 25 September 2026).
- [5] Food Data Transparency Partnership (FDTP), a shared programme involving Defra, DHSC and the Food Standards Agency. GOV.UK. <https://www.gov.uk/government/groups/food-data-transparency-partnership> (accessed 25 September 2026).
- [6] Open Data Institute (ODI) (2026). Arup, ODI, WRAP, AHDB and HESTIA partner to design and test Data Sharing Infrastructure (DSI) and governance for the UK agri-food sector. Published 3 February 2026. <https://theodi.org/news-and-events/news/arup-odi-wrap-ahdb-and-hestia-partner-to-design-and-test-data-sharing-infrastructure-dsi-and-governance-for-the-uk-agri-food-sector/> (accessed 25 September 2026).
- [7] Department for Environment, Food & Rural Affairs (Defra) (2025). Food Data Infrastructure and Governance. Tender notice 2025/S 000-061730, published 2 October 2025. Find a Tender. <https://www.find-tender.service.gov.uk/Notice/061730-2025> (accessed 25 September 2026).
- [8] Agriculture and Horticulture Development Board (AHDB) (2026). Farm Data Exchange; and 'Proof of concept pilot demonstrates AHDB's Farm Data Exchange is viable and supported by industry', 15 April 2026. <https://ahdb.org.uk/fde> and <https://ahdb.org.uk/news/proof-of-concept-pilot-demonstrates-ahdb-s-farm-data-exchange-is-viable-and-supported-by-industry> (accessed 25 September 2026).
- [9] FarmPEP / ADOPT (2026). PigWare: A Pilot Study of Smart Behaviour and Environmental Monitoring for Sustainable Production. ADOPT is part of Defra's Farming Innovation Programme, delivered in partnership with Innovate UK. <https://farmpep.net/index.php/adopt/case-study/pigware-pilot-study-smart-behaviour-and-environmental-monitoring-sustainable>; see also BioChain Limited, PigWare trial launch note, 1 September 2026: <https://thebiochain.com/pigware-trial-launch/> (accessed 25 September 2026).
- [10] BioChain Limited (2026). The BioChain: provenance and verification infrastructure for biological and agri-food data – company website, including the Ancient BioChain reference implementation and the PigWare and HerdWare livestock data work. <https://www.thebiochain.com> (accessed 29 September 2026).
- [11] University of Surrey. Veterinary Pathology Centre: surveillance services and post-mortem examinations. <https://www.surrey.ac.uk/veterinary-pathology-centre/surveillance-services> and <https://www.surrey.ac.uk/veterinary-pathology-centre/post-mortem-examinations> (accessed 25 September 2026).
- [12] World Wide Web Consortium (W3C) (2013). PROV-O: The PROV Ontology. W3C Recommendation, 30 April 2013. <https://www.w3.org/TR/prov-o/> (accessed 25 September 2026).
- [13] GSI (2022). EPCIS and Core Business Vocabulary (CBV) 2.0. Supply-chain visibility event data standards. <https://www.gsi.org/standards/epcis> (accessed 25 September 2026).
- [14] National Institute of Standards and Technology (NIST) (2025). NIST SP 800-63-4: Digital Identity Guidelines. July 2025. <https://csrc.nist.gov/pubs/sp/800/63/4/final> (accessed 25 September 2026).
- [15] Department for Business and Trade (2026). Research into governance models for Smart Data: The future of Smart Data – developing governance models. Published 26 January 2026; updated 30 January 2026. GOV.UK. <https://www.gov.uk/government/publications/research-into-governance-models-for-smart-data> (accessed 25 September 2026).
- [16] Department for Science, Innovation and Technology / Office for Digital Identities and Attributes (2026). UK digital verification services trust framework (1.0). First published 3 March 2026; final release updated 9 June 2026; and supporting guidance 'How to check whether someone has delegated authority 1.0'. GOV.UK. <https://www.gov.uk/government/publications/uk-digital-verification-services-trust-framework-1-0> and <https://www.gov.uk/government/publications/how-to-check-whether-someone-has-delegated-authority-1-0> (accessed 25 September 2026).
- [17] Department for Business and Trade (2023). Design principles for inclusive Smart Data schemes research (Savanta). Published 10 July 2023. GOV.UK. <https://www.gov.uk/government/publications/design-principles-for-inclusive-smart-data-schemes> (accessed 25 September 2026).
- [18] Open Banking Limited (2026). Customer Experience Guidelines v4.0.1. Published 18 March 2026. <https://standards.openbanking.org.uk/customer-experience-guidelines/latest/> (accessed 25 September 2026).
- [19] Department for Science, Innovation and Technology (2026). Smart Data opportunities in digital markets: government response. Published 12 May 2026. GOV.UK. <https://www.gov.uk/government/calls-for-evidence/smart-data-opportunities-in-digital-markets/outcome/smart-data-opportunities-in-digital-markets-government-response> (accessed 25 September 2026).
- [20] Estonian Information System Authority (RIA). Data exchange layer X-tee. <https://www.ria.ee/en/state-information-system/data-exchange-platforms/data-exchange-layer-x-tee> (accessed 25 September 2026).

- [21] European Union (2023). Regulation (EU) 2023/2854 (Data Act). Applies from 12 September 2025; the Article 3(1) access-by-design obligation applies to connected products and related services placed on the market after 12 September 2026; Recital 14 cites agricultural machinery as an example. EUR-Lex. <https://eur-lex.europa.eu/eli/reg/2023/2854/oj> (accessed 25 September 2026).
- [22] Biocheck.UGent. Why Biocheck.UGent?; Checklists and data-sharing information. <https://biocheckgent.com/en/about-us/why-biocheckugent> and <https://biocheckgent.com/en/checklists> (accessed 25 September 2026).
- [23] Electronic Trade Documents Act 2023, c. 38, and Explanatory Notes. <https://www.legislation.gov.uk/ukpga/2023/38> (accessed 25 September 2026).
- [24] Department for Business and Trade (2026). Electronic trade documents: SME exporter research. Published 6 July 2026. GOV.UK. <https://www.gov.uk/government/publications/electronic-trade-documents-small-and-medium-sized-enterprises-smes-exporter-research> (accessed 25 September 2026).
- [25] HM Revenue & Customs and HM Treasury (2026). Customs Modernisation (call for evidence); supporting document: Modernising the UK Customs Regime. Published 23 June 2026; closed 15 September 2026. GOV.UK. <https://www.gov.uk/government/calls-for-evidence/customs-modernisation> (accessed 25 September 2026).
- [26] Department for Business and Trade (2025). UK Trade Strategy. Published 26 June 2025; updated 25 July 2025. GOV.UK. <https://www.gov.uk/government/publications/uk-trade-strategy> (accessed 25 September 2026).
- [27] Department for Business and Trade (2026). Digital Trade Corridors programme. Published 6 July 2026. GOV.UK. <https://www.gov.uk/guidance/digital-trade-corridors-programme> (accessed 25 September 2026).
- [28] World Customs Organization (WCO). WCO Data Model. <https://www.wcoomd.org/en/topics/facilitation/instrument-and-tools/tools/data-model.aspx> (accessed 25 September 2026).
- [29] UNECE / UN/CEFACT. Supply Chain Management standards, including the Buy-Ship-Pay Reference Data Model, UN/EDIFACT and UN/LOCODE. <https://unece.org/trade/standards/trade-and-uncedfact/uncedfact/supply-chain-management> (accessed 25 September 2026).
- [30] International Chamber of Commerce Digital Standards Initiative (2024). ICC Digital Standards Initiative launches complete framework for supply chain digitalisation. Published 24 April 2024. <https://iccwbo.org/news-publications/news/icc-digital-standards-initiative-launches-complete-framework-for-supply-chain-digitalisation/> (accessed 25 September 2026).
- [31] UNECE / UN/CEFACT (2025). Briefing Note: updates on mapping between the World Customs Organization Data Model and the UN/CEFACT Core Components Library and next steps. ECE/TRADE/C/CEFACT/2025/INF.2, June 2025. <https://unece.org/trade/documents/2025/06/informal-documents/briefing-note-updates-mapping-between-world-customs> (accessed 25 September 2026).
- [32] Scottish Government (2026). Livestock identification and traceability: guidance – cattle. ScotMoves+ records all cattle births, deaths and movements, and is operated by ScotEID on behalf of the Scottish Government, which has issued cattle passports through it since 4 October 2021. Last updated 1 July 2026. <https://www.gov.scot/publications/livestock-identification-and-traceability-guidance/pages/cattle/> (accessed 29 September 2026).
- [33] Welsh Government (2026). Planned move from the British Cattle Movement Service (BCMS) to EIDCymru. Cattle registration and movement reporting in Wales is planned to move from BCMS and the Cattle Tracing System to EIDCymru in winter 2026, creating a single Welsh system for livestock registration and movement reporting. Last updated 20 March 2026. <https://www.gov.wales/planned-move-british-cattle-movement-service-bcms-eidcymru> (accessed 29 September 2026).
- [34] Department of Agriculture, Environment and Rural Affairs (DAERA). Northern Ireland Food Animal Information System (NIFAIS), replacing the legacy Animal and Public Health Information System (APHIS); the bovine stage was deployed in September 2023, with further species following. <https://www.daera-ni.gov.uk/topics/northern-ireland-food-animal-information-system-nifais> (accessed 29 September 2026).
- [35] Department for Business and Trade (2026). Smart Data 2035: The UK's Smart Data Strategy. CP 1551, presented to Parliament by the Secretary of State for Business and Trade, March 2026. ISBN 978-1-5286-6348-9. <https://assets.publishing.service.gov.uk/media/69c11f9ed588c92c483e4b66/smart-data-strategy.pdf> (accessed 29 September 2026).