

BEYOND COMPLIANCE THEATRE

GDPR Is a Governance Reset, Not a Compliance Deadline

Why accountable data ownership must replace the scramble for documentary compliance

Giovanni Leonardi

May 2018



Contents

1. Executive Summary

2. The Green Report and the Unanswered Question

3. Why the Compliance–Led Approach Is Attractive

4. The Evidence Is in the Friction

5. What the Regulation Changes

6. Options for the Board and Executive Team

7. The Recommended Governance Reset

7.1 Establish an authoritative processing record

7.2 Assign decision rights, not honorary ownership

7.3 Govern the lifecycle, including copies

7.4 Move privacy decisions to the point of change

7.5 Make control operation produce evidence

8. A Worked Illustration: From Forty–Seven Emails to Eight Decisions

9. Implementation Without Creating Another Programme That Never Ends

9.1 The first ninety days: stabilise accountability

9.2 The following six months: embed the lifecycle

9.3 The continuing cycle: assure and improve

10. Measures That Reveal Control Rather Than Activity

11. Data Ethics Begins Where Legal Sufficiency Ends

12. The Recommendation

13. Conclusion

3

4

4

5

6

7

8

8

8

9

10

10

10

10

10

11

11

12

12

13

13

14

15

GDPR Is a Governance Reset, Not a Compliance Deadline

Transformation · No. 215

Originally written May 2018 | Re-edited and re-rendered for the WhereBeyond Edition, 2025

“A privacy notice cannot repair a data estate that nobody can explain.”

1. Executive Summary

At 8:30 this morning, a transformation director can receive two apparently reassuring messages. Legal confirms that the revised privacy notices are live. The programme office reports that the General Data Protection Regulation workstream is green. Yet, in the same organisation, an analyst is still tracing a customer identifier through a billing platform, a marketing database, three overnight file transfers and a spreadsheet maintained by a former project team. The documents may be ready; the data estate is not.

That distinction matters as the Regulation begins to apply. GDPR is commonly framed as a legal deadline with a large potential penalty attached. The legal obligations are real, and disciplined compliance work is indispensable. But the deeper value of the Regulation is diagnostic: it forces organisations to answer questions that many transformation programmes have repeatedly deferred. What personal data do we hold? For what purpose? On whose authority? Where does it travel? Who decides how long it remains? Who can correct or erase it? Which third parties receive it? What evidence proves the answer?

These are governance questions before they are compliance questions. Where the answers are weak, the underlying causes are familiar: fragmented ownership, inherited duplication, project-by-project interfaces, retention without decision, and accountability that stops at the boundary between business and technology. Treating GDPR only as a documentary exercise can produce a defensible file while leaving those causes untouched.

This paper recommends a federated data-governance reset. It retains central legal interpretation and minimum controls, but places accountable decisions with the business owners of data and processes. The reset has five connected elements:

- an authoritative record of processing tied to real systems and transfers;
- named decision rights for purpose, access, quality, retention and remediation;
- lifecycle controls that follow data from collection to disposal;
- evidence-producing routines built into change, operations and supplier management;

- measures that expose uncertainty and reduce it over time.

The recommendation is not to rebuild the entire data estate before claiming compliance. Nor is it to place a new bureaucracy above already stretched teams. It is to use GDPR obligations as a forcing mechanism: convert temporary discovery into durable ownership, convert policy into operational decisions, and convert scattered evidence into a governance system that survives the deadline.

The test of GDPR readiness is not whether the organisation can describe its policy. It is whether it can explain, operate and evidence the life of the data to which that policy applies.

2. The Green Report and the Unanswered Question

Consider a composite organisation with seven million customer records accumulated through acquisitions and product launches. Its GDPR programme has completed 93 per cent of the actions in the central plan. Contracts have been reviewed, employee briefings issued and website wording changed. The remaining action is described as “confirm deletion capability”.

When the team examines that line, it discovers that it is not one action. The primary customer platform can mark an account inactive but does not physically remove the record. A billing archive retains monthly extracts for seven years without distinguishing disputed invoices from ordinary accounts. Marketing receives a weekly file through a managed transfer service, then loads it into a separate database. Local sales teams keep their own prospect spreadsheets. A service supplier holds call recordings under a contract that predates the current retention policy. Nobody owns the end-to-end decision because each component has a plausible local owner.

The status report is green because the plan measures completion of activities. The unresolved question concerns the operation of the enterprise: who has the authority and information to decide what should happen to this person's data across the chain?

This pattern recurs because regulatory programmes naturally organise around obligations and deliverables. They create policy documents, contract clauses, training packs, privacy notices and risk logs. Those artefacts are necessary. They are also easier to count than the quality of ownership beneath them. A completed privacy notice can be reviewed centrally; a reliable account of how data moves through twenty years of systems requires cooperation among operations, technology, records management, procurement, security and business leadership.

A privacy notice cannot repair a data estate that nobody can explain.

3. Why the Compliance-Led Approach Is Attractive

The strongest case for a narrow compliance programme deserves serious treatment. The Regulation is detailed, the deadline is fixed and interpretation requires specialist judgement. Distributed business teams should not invent their own reading of lawful basis, data-subject rights or processor obligations. Central coordination reduces inconsistency, protects legal privilege where appropriate, and focuses scarce effort on demonstrable requirements. At a moment when many organisations are still completing inventories and contract changes, expanding the programme into broad transformation can look irresponsible.

That objection is correct in three respects.

- Legal interpretation must be coherent. The organisation needs a common position on controller and processor responsibilities, lawful bases, consent, legitimate interests, special categories of data and international transfers.
- Evidence matters. Policies, records of processing, data protection impact assessments, processor terms, breach procedures and training records are not “paperwork” in a dismissive sense. They demonstrate decisions and enable repeatable action.
- Scope must be controlled. A promise to cleanse every database, replace every legacy platform and redesign every process would turn an urgent regulatory obligation into an unfinishable technology programme.

The mistake lies not in doing these things, but in assuming they are sufficient. The obligations themselves depend on operational facts. A lawful-basis assessment is only as good as the stated purpose and actual use. A retention schedule is only as good as the systems that can apply it. A processor clause is only as useful as the knowledge of which data the supplier receives. A subject-access procedure is only as reliable as the organisation's ability to find, review and assemble the relevant records. A breach-notification process cannot start promptly if nobody recognises which owner must assess the affected data.

The narrow approach therefore contains its own contradiction: it seeks defensible compliance while treating the information needed for that defence as somebody else's problem.

4. The Evidence Is in the Friction

An organisation does not need a perfect enterprise model to diagnose weak governance. The evidence is already present in the effort required to answer ordinary questions.

A subject-access request provides one revealing test. In a well-governed environment, the request is authenticated, routed to known data owners, searched across an agreed system scope, reviewed for the rights of others, assembled and approved against a recorded timetable. In a weak environment, a central privacy team sends emails to a changing list of system contacts and waits. Each recipient interprets “all data” differently. Search methods vary. Duplicate extracts arrive without provenance. The final response depends on personal persistence.

The mechanism is straightforward: unclear ownership increases search paths; more search paths increase delay and inconsistency; delay forces manual escalation; manual escalation conceals the absence of a stable control.

The same mechanism appears elsewhere:

- A retention schedule states “six years”, but the archival platform stores complete monthly snapshots. The policy records an intention; the architecture preserves duplication.
- A consent withdrawal reaches the marketing platform, but a campaign list created the previous evening has already been sent to an agency. The front door works; the downstream propagation does not.
- A data protection impact assessment is completed shortly before launch, when the design can no longer change cheaply. The control exists; its timing makes it ceremonial.
- Procurement records a processor, but the operating team later adds a new file exchange under a change request. The contract is governed; the data flow evolves outside it.

These are not isolated privacy defects. They expose the joins between policy and process, process and system, system and supplier, and central authority and local decision.

Question	What a compliance file may show	What governance must prove
Why is the data held?	A stated lawful basis	A specific purpose understood by the process owner
Where does it travel?	A high-level inventory	Traceable systems, extracts, interfaces and recipients
Who is accountable?	A policy owner	Named decision rights at each material stage
How long is it kept?	A retention schedule	Executable rules, exceptions and disposal evidence
Can a right be fulfilled?	A documented procedure	Reliable search, review, correction, export and erasure capability
Can a breach be assessed?	An incident plan	Data context, ownership and escalation available at operational speed

5. What the Regulation Changes

GDPR sharpens the consequences of ambiguity. The principle of accountability requires more than passive adherence; it requires the organisation to be able to demonstrate its approach. Records of processing bring purpose, categories, recipients, transfers, retention and security into one accountable view. Data protection by design and by default moves privacy questions closer to investment and design decisions. The expanded

rights of individuals test whether processes and systems can act on data, not merely store it. The 72-hour breach-notification timetable makes slow ownership visible. Obligations on processors require a clearer grasp of the extended delivery chain.

These requirements change the economics of deferred decisions. Before the Regulation, a duplicate customer extract could remain a local inconvenience. Now it may enlarge search effort, complicate erasure, extend breach exposure and weaken evidence of purpose limitation. A vague owner could once be tolerated until a system change demanded attention. Now that ambiguity can delay a rights request or an incident assessment.

The change is not simply that privacy becomes more important. It is that the organisation must govern data as a lifecycle rather than as a collection of applications.

Applications have managers. Processes have owners. Contracts have sponsors. Data frequently falls between them because it persists and travels across all three. GDPR makes that gap difficult to ignore.

6. Options for the Board and Executive Team

Four broad responses are available. They differ less in stated ambition than in where they place accountability.

Option	Strength	Limitation	Judgement
Legal-led compliance	Fast interpretation and consistent policy	Operational facts arrive late and ownership remains indirect	Necessary foundation, insufficient operating model
Technology-led discovery	Reveals databases, files and interfaces at scale	Tools find instances, not purpose, authority or acceptable use	Valuable evidence, not governance by itself
Central data office control	Creates visible standards and specialist capability	Can become a queue for decisions the business should own	Useful for assurance, risky as a substitute for ownership
Federated governance reset	Connects central rules to local accountable decisions	Requires sustained executive sponsorship and role clarity	Best balance of control, practicality and durability

A legal-led response is the quickest way to establish a coherent minimum position. It should continue, but it cannot own every purpose decision or verify every operational flow.

Technology-led discovery is increasingly attractive as organisations confront large file estates and poorly catalogued platforms. Search and classification can narrow the field. Yet a tool cannot determine whether an old extract remains necessary, whether two uses are compatible, or which executive accepts the residual risk. Discovery without decision rights produces a longer list.

A central data office can set standards, maintain common artefacts and challenge weak evidence. The danger is the creation of an expert bottleneck. If every retention exception, purpose change or remediation priority waits for central approval, business accountability has been displaced rather than strengthened.

The recommended model is federated: central functions define the rules, common method and assurance; business and process owners make and evidence decisions within those rules; technology and operations implement controls; internal assurance tests whether the whole chain works.

7. The Recommended Governance Reset

The reset should not begin with a new committee. It should begin with the decisions the organisation repeatedly fails to make. Five elements turn those decisions into an operating system.

7.1 Establish an authoritative processing record

Many inventories assembled for the deadline are spreadsheets collected by questionnaire. They are useful first approximations, but they become stale as soon as a process, supplier or interface changes.

The organisation should establish one authoritative record of processing, connected to the systems and suppliers through which each activity operates. The record need not contain every technical field. It must be sufficient to answer:

- purpose and lawful basis;
- categories of individuals and personal data;
- source, destination and material transfers;
- accountable business owner and operational custodian;
- recipients and processors;
- retention rule and disposal mechanism;
- security classification and key safeguards;
- applicable rights-handling route;
- date and authority of the last material decision.

The record should be updated through normal change control, procurement, project governance and service management. If it relies on an annual campaign of emails from the privacy team, it is an archive of last year's beliefs.

7.2 Assign decision rights, not honorary ownership

“Data owner” is often added to a job description without stating what the owner can decide. Ownership then becomes ceremonial and difficult to enforce.

Each material processing activity needs explicit rights and duties.

Role	Decisions owned	Evidence produced
Executive data owner	Purpose, risk acceptance, remediation priority, material retention exceptions	Signed decisions and funded action
Process owner	Operational use, procedure, rights fulfilment, local control performance	Process map, control results, issue log
Technology custodian	System implementation, access, extraction, correction, deletion and recovery behaviour	Configuration evidence, test results, change records
Privacy and legal	Interpretation, minimum standard, high-risk challenge, regulatory interface	Opinions, policies, assessment criteria
Information security	Threat assessment, protective controls, incident response	Risk assessment, monitoring and incident evidence
Records management	Retention authority, disposal rules, preservation exceptions	Schedule, disposal approval and exception record
Procurement and supplier owner	Processor terms, due diligence, service change and exit	Contract evidence, review record, exit assurance
Internal assurance	Independent testing of design and operation	Findings, ratings and follow-up

The crucial distinction is between accountability and custody. A system manager may operate deletion; the business owner decides whether the processing purpose and retention remain justified. A privacy specialist may challenge that decision; the specialist should not silently inherit it.

7.3 Govern the lifecycle, including copies

The lifecycle should cover collection, use, sharing, change, archiving and disposal. In practice, the most neglected stages are sharing and disposal because both occur outside the primary application.

Controls should follow the data into:

- batch interfaces and report extracts;
- user-maintained spreadsheets and shared folders;
- test environments and copied production data;
- archives, back-ups and recovery arrangements;
- call recordings, correspondence and scanned documents;
- processors, sub-processors and temporary project suppliers.

This does not require immediate physical deletion from every back-up. It requires a reasoned, documented approach that prevents ordinary use, applies the retention decision through the recovery cycle, and explains exceptions. Governance is credible when the practical constraint is visible and controlled, not when it is omitted from the inventory.

7.4 Move privacy decisions to the point of change

A late data protection impact assessment is an expensive discovery mechanism. By the time a project seeks approval to launch, contracts may be signed, interfaces built and customer communications prepared.

Privacy-by-design should therefore be connected to the earliest investment and design gates. A proposed change should answer, before detailed build:

1. What new purpose or material change in purpose is proposed?
2. Which categories of personal data and individuals are affected?
3. Can the outcome be achieved with less data, shorter retention or fewer recipients?
4. What rights, fairness or transparency concerns arise?
5. Which existing processing record, supplier assessment and security classification must change?
6. Who accepts the decision, and what evidence will be retained?

Not every change requires a full impact assessment. A proportionate screening step should identify the changes that do. The trade-off is deliberate: a small amount of early friction prevents larger redesign and weaker evidence later.

7.5 Make control operation produce evidence

Governance fails when evidence is assembled only for review. The better design is for ordinary operation to leave a usable trail.

Access reviews should record who approved exceptions. Deletion routines should produce counts and failures. Subject-rights cases should record systems searched and owners responding. Supplier reviews should identify changed data flows. Project gates should link the approved purpose to the live processing record. Incidents should capture affected categories and the time ownership was established.

A control that operates without evidence cannot be defended; evidence assembled without a control cannot be trusted.

8. A Worked Illustration: From Forty-Seven Emails to Eight Decisions

A composite retail and service business tested its subject-access process using a former customer with a five-year relationship. The first exercise took 26 calendar days and generated 47 internal emails. Fourteen systems were searched. Three further repositories were discovered during the search. Two teams supplied the same billing extract in different formats. One supplier response arrived without confirmation of the search criteria. The privacy team spent most of its time coordinating rather than reviewing.

The organisation resisted the temptation to call this merely a case-management problem. It reconstructed the mechanism.

First, the processing record named applications but not report extracts or correspondence stores. Second, system contacts were custodians but had no duty to certify search coverage. Third, customer identifiers differed across sales, billing and service systems. Fourth, no owner had decided whether local spreadsheets were authorised records. Fifth, the supplier contract described assistance with requests but the operating procedure did not name a responsible role or timetable.

The remediation programme made eight governance decisions:

1. The customer-service process owner became accountable for search completeness across the service chain.
2. Each custodian received a defined search instruction and a standard evidence return.
3. The three identifier patterns were documented in the processing record.
4. Approved repositories were listed; unapproved local copies were removed or brought under control.
5. The supplier owner established a five-working-day response and quarterly test.
6. Duplicate billing extracts were replaced by one controlled report.
7. The case record captured scope, exceptions, review and approval.
8. A sample request was rehearsed every quarter, with failures entering the transformation backlog.

In the second exercise, eleven systems and two controlled repositories were searched. The evidence was complete in nine calendar days, with twelve coordination emails. The important improvement was not simply seventeen days saved. The search universe had become explainable. Three systems disappeared from the count because duplicate holdings were removed; two repositories were added because their purpose was recognised and governed. A lower number alone could have meant an incomplete search. The combination of documented scope, accountable certification and measured time showed a real control improvement.

This illustration also reveals why technology alone is insufficient. Better search could have accelerated discovery, but only a decision could eliminate duplicate extracts, authorise repositories, align identifiers and hold the supplier to an operating timetable.

9. Implementation Without Creating Another Programme That Never Ends

The reset should be staged according to risk and learning, not postponed until an ideal enterprise catalogue exists.

9.1 The first ninety days: stabilise accountability

The immediate aim is to make the current position governable.

- Confirm central interpretations, minimum standards and escalation routes.

- Identify the highest-risk processing activities using volume, sensitivity, vulnerability of individuals, external sharing, automated decision impact and current uncertainty.
- Name executive owners, process owners and custodians for those activities.
- Test three end-to-end obligations: one subject-access request, one deletion or retention scenario, and one breach-assessment scenario.
- Record gaps as owned decisions with dates and funding routes, not as general observations.

The output is a prioritised processing record, a decision-rights map, tested procedures and a remediation portfolio.

9.2 The following six months: embed the lifecycle

The next stage connects governance to the machinery of change and operations.

- Integrate processing-record updates into project gates, service changes and procurement.
- Translate retention schedules into executable rules for priority systems and repositories.
- Establish supplier-flow reviews and exit requirements.
- Introduce standard evidence for access, correction, export, restriction and erasure actions.
- Reconcile customer, employee and supplier identifiers where fragmentation obstructs rights fulfilment or incident assessment.

The output is not “GDPR complete”. It is a controlled reduction in uncertainty, with evidence that priority risks are moving.

9.3 The continuing cycle: assure and improve

Thereafter, assurance should test a sample of processing activities from purpose to disposal. Reviews should combine document inspection with operational rehearsal. The questions are simple:

- Does the recorded purpose match actual use?
- Can the owner explain material flows and recipients?
- Do systems apply access and retention decisions as intended?
- Can a right be fulfilled within the required timetable?
- Can an incident team identify the affected data and owner promptly?
- Have changes since the last review entered the record?

A governance forum should resolve cross-cutting decisions and allocate investment. It should not receive routine status presentations that operating owners could settle themselves.

10. Measures That Reveal Control Rather Than Activity

Programme measures tend to count policies issued, staff trained and assessments completed. Those measures show mobilisation. They do not show whether governance works.

A balanced set should include:

Measure	What it reveals	Warning sign
Processing coverage	Share of priority activities with verified purpose, owner, flow, recipient and retention	Rapid coverage growth without independent sampling
Ownership latency	Time to identify an accountable owner during a request, change or incident	Reliance on personal networks
Rights fulfilment	Time, completeness, rework and exceptions by request type	Falling time accompanied by unexplained scope reduction
Retention execution	Records due, disposed, failed and excepted	Policy dates with no system evidence
Change integration	Material changes updating the processing record before approval	Assessments completed after design commitment
Supplier assurance	Priority processors tested against actual operating obligations	Contract review without service evidence
Issue closure	Age, risk and recurrence of governance defects	Large closure counts with repeated root causes

Targets should encourage truthful discovery. If teams are punished for finding previously unknown repositories, inventories will become optimistically complete. Early in the reset, an increase in known flows or issues may indicate better governance, not deterioration. Executive judgement is needed to distinguish improved visibility from uncontrolled growth.

11. Data Ethics Begins Where Legal Sufficiency Ends

The Regulation also creates an opportunity to improve the quality of decisions beyond minimum legality. An organisation may establish a lawful basis and still need to ask whether a use is proportionate, intelligible and consistent with the expectations it has created.

In 2018, organisations are expanding behavioural analysis, automated scoring, data matching and the use of large external datasets. The practical debate should not be

reduced to whether a consent box has been written correctly. Governance should examine the purpose, the consequences of error, the ability to challenge an outcome, and the groups who may bear disproportionate harm.

This does not require an abstract ethics council for every analytical model. It requires existing owners to answer harder questions and record their reasoning:

- Would the individual reasonably understand this use from the relationship and explanation provided?
- Is the same outcome possible with fewer variables or a shorter history?
- What happens when the data is wrong, incomplete or associated with the wrong person?
- Which decisions are automated, which are reviewed, and by whom?
- Can an affected person obtain a meaningful explanation and correction?

The governance reset makes these questions possible because it establishes purpose, ownership and traceability. Without those foundations, “ethics” becomes another policy detached from the data.

12. The Recommendation

Executive teams should resist both extremes: declaring victory because the compliance file is complete, and launching an indiscriminate replacement of the data estate. The defensible course is a federated governance reset built from the obligations now testing the organisation.

The recommendation is to mandate that every priority processing activity has:

1. a specific, approved purpose and lawful basis;
2. an accountable executive owner with explicit decision rights;
3. a verified map of systems, material copies, recipients and processors;
4. an executable retention and disposal approach, including controlled exceptions;
5. tested procedures for applicable individual rights and incidents;
6. privacy screening at the point of material change;
7. operational evidence and independent sampling.

Central privacy, legal, security, records and data specialists should set the method and challenge the evidence. Business owners should own purpose, priority and risk. Technology and operations should implement and demonstrate the controls. Investment governance should fund remediation according to the combined effect on individual rights, regulatory exposure and operational fragility.

The first benefit will be a more credible GDPR position. The larger benefit is an organisation that can finally make deliberate decisions about its data rather than inheriting them from old projects, interfaces and storage habits.

13. Conclusion

Today's deadline will pass. The questions it exposes will not.

Organisations that treat GDPR as a campaign will spend the coming years rediscovering the same data, reconstructing the same ownership and reopening the same retention debates whenever a request, incident, audit or transformation programme demands an answer. Organisations that treat it as a governance reset can preserve the value of the work already done and turn regulatory pressure into operating discipline.

The decisive move is modest in wording but substantial in effect: connect every policy to a real processing activity, every activity to an accountable decision-maker, every decision to an operational control, and every control to evidence.

That is not regulation imposed on transformation. It is transformation made governable.