# European Chemicals M&A: Privacy-Preserving Data Rooms for Process and Customer Diligence

*A transaction framework for testing margins, formulations, customer overlap and regulatory continuity without uncontrolled disclosure*

**Authored by Chennakeshav Adya**

Independent Researcher

September 2026

## Abstract

*European chemicals transactions require buyers to test earnings quality, customer concentration, formulation economics, regulatory continuity and manufacturing capability. Much of the evidence needed for those tests is also commercially sensitive, protected as a trade secret, personal data, subject to regulatory data-sharing restrictions or capable of changing competitive conduct before closing. Conventional virtual data rooms provide access controls and audit logs, but they can still disclose customer identities, prices, formulations, production yields and forward-looking plans to people who should not receive them. Excessive redaction creates the opposite problem: the buyer cannot reproduce the analysis, lenders cannot understand the earnings base and the parties discover material issues after signing.*

*This paper develops a Privacy-Preserving Chemical M&A Diligence Framework. It separates transaction questions from raw records, classifies information by legal and competitive sensitivity, assigns each question to the least-disclosive analytical method and connects clean-team governance with technical controls. The framework combines conventional restricted data rooms with aggregation, pseudonymisation, private set intersection, secure multiparty computation, differential privacy and trusted analytical environments. It also addresses REACH and CLP legal-entity changes, data-sharing rights, trade secrets, customer evidence, merger-control submissions, model validation, financing diligence and post-close integration.*

*The method is demonstrated through a hypothetical European specialty-chemicals acquisition. Management assumptions include enterprise value of EUR 420 million, reported last-twelve-month revenue of EUR 310 million, reported EBITDA of EUR 46 million, 620 active customers, 1,850 formulations and 340 substances or mixtures requiring regulatory mapping. The clean-room analysis identifies EUR 8.4 million of revenue overlap, EUR 3.6 million of price-normalisation exposure, EUR 2.1 million of unsupported formulation margin and EUR 1.4 million of annual remediation and operating cost. After management-assumed adjustments, illustrative maintainable EBITDA is EUR 40.9 million. These figures demonstrate the framework only. They are not observed company data, a valuation opinion, legal advice, regulatory advice, accounting advice or investment advice.*

**JEL Classification:** G34, K21, K22, L22, L65, M15, O32

**Keywords:** European chemicals M&A, privacy-preserving data rooms, clean teams, customer overlap, process diligence, REACH, chemical formulations, data minimisation, secure multiparty computation, merger control

## 1. Define the transaction decision

The transaction decision is how a buyer should obtain decision-useful evidence about a European chemicals business without disclosing information beyond what diligence, financing and regulatory review require. The parties must decide which questions can be answered through ordinary documents, which require a clean team, which require privacy-preserving computation and which should remain unavailable until clearance or closing. The design affects price, representations, financing certainty, regulatory risk, employee and customer protection, and the ability to integrate the business after completion.

The decision is narrower than selecting a data-room vendor. A conventional platform can restrict users and record downloads while still exposing clear-text customer identities, prices, recipes, process settings or employee records. A technical clean room can also fail if its permitted queries are poorly designed, its outputs reveal small groups, its administrators have uncontrolled access or its results cannot be reconciled to source systems. Governance and technology must therefore operate as one control system.

The framework tests six conditions. Every requested dataset must link to a defined transaction question. The method must use the minimum information required. Access must reflect role, competitive sensitivity and legal basis. Analytical outputs must be reproducible and resistant to reconstruction. Regulatory and commercial rights must permit the use. The resulting evidence must be strong enough to support valuation, financing, merger-control and integration decisions.

**Table 1. Chemical M&A diligence questions and minimum-disclosure methods**

| Transaction question | Sensitive evidence | Minimum-disclosure method | Decision output |
|---|---|---|---|
| Customer concentration and churn | Names, prices, volumes and contracts | Pseudonymised cohorts with controlled drill-down | Revenue-at-risk range and concentration bridge |
| Customer overlap | Customer identities held by both parties | Private set intersection or independent clean team | Count, revenue and segment overlap without unmatched identities |
| Formulation profitability | Recipe, input cost, yield and selling price | Trusted analytical environment with masked ingredients | Margin bridge and unsupported-margin exceptions |
| Regulatory continuity | Registration ownership, tonnage, uses and data rights | Restricted regulatory clean team | Transfer actions, data-access gaps and closing conditions |
| Capacity and process capability | Line rates, yields, downtime and control limits | Aggregated time series with plant-specific identifiers masked | Sustainable capacity and capital requirement |
| Synergy validation | Procurement, production and customer combinations | Staged clean-team model with competition review | Executable synergy range and protected integration plan |

*The method should answer the transaction question while limiting disclosure of identities, formulations and competitively sensitive records.*

## 2. Start with questions, not datasets

Data requests often expand because the diligence team begins with available systems rather than investment decisions. The buyer asks for complete customer, product and production extracts; the seller responds with partial files and redactions; advisers spend time reconciling versions; and sensitive information reaches users who cannot explain why they need it. A question-led design reverses that sequence.

Each workstream should state the decision, metric, population, period, granularity and tolerance. A customer-concentration test may require monthly revenue by stable pseudonymous customer, product family, country and channel for thirty-six months. It may not require customer names, individual contacts or clear-text contract files at the first stage. A formulation-margin test may require standard and actual material cost, yield, energy use and realised price by masked formulation family. It may not require the full recipe until an exception passes a defined threshold.

The output specification should be agreed before source data enter the environment. This allows counsel, competition specialists, data-protection officers, regulatory experts and financial advisers to determine whether the proposed analysis is necessary and proportionate. It also creates a measurable completion test. Diligence is complete when the agreed decision questions have evidence, explanations and unresolved exceptions, rather than when a large volume of files has been uploaded.

## 3. Map the chemical information perimeter

European chemical businesses hold information across enterprise resource planning, laboratory, manufacturing, regulatory, customer, supplier and product-stewardship systems. A single product can connect a confidential formulation, raw-material suppliers, hazardous classifications, safety data, customer-specific specifications, production routing, batch yields, complaints, prices and regulatory registrations. These relationships make the diligence perimeter wider than the finance ledger.

The map should identify systems of record, owners, retention, jurisdictions, identifiers and dependencies. Relevant sources commonly include ERP sales and purchase ledgers, customer relationship management, manufacturing execution systems, laboratory information management systems, quality records, process historians, environmental systems, IUCLID datasets, REACH-IT records, classification and labelling files, safety data sheets, substance-information exchange records and contract repositories. ECHA uses IUCLID and REACH-IT for structured regulatory information and submission workflows [1-2].

The map should also identify rights. A seller may possess a study summary without the right to transfer or permit reference to the underlying study. A formulation may incorporate licensed know-how. Customer specifications can contain third-party confidential information. A process historian may be hosted by a vendor whose terms limit extraction. Data possession does not prove transaction use, transferability or post-close continuity.

## 4. Classify information by harm and purpose

Classification should consider competitive, privacy, trade-secret, regulatory, contractual, cybersecurity and operational harm. Customer-level prices, bid intentions, future capacity and product strategy can influence market conduct if disclosed before closing. Formulations, catalysts, process windows and yield data can reveal trade secrets. Employee, contact and complaint records can contain personal data. Regulatory studies and registration records can carry data-sharing conditions and cost rights.

The EU Merger Regulation protects information covered by professional secrecy in Commission proceedings [3]. The Commission's data-room practice limits the people who can access information and the use they may make of it when confidentiality must be balanced with procedural rights [4]. These procedural protections do not automatically govern private diligence, but they illustrate a useful principle: access should be limited to the extent necessary for the defined purpose.

A practical classification uses both sensitivity and permitted purpose. The same customer record might be available as an aggregated segment view for the commercial team, a pseudonymous longitudinal record for the financial clean team and a clear-text contract for external counsel. Classification should travel with extracts and outputs. A file should not lose its restrictions when copied into a model, slide deck or lender report.

## 5. Establish the legal and governance basis

The parties should identify the lawful and contractual basis for each processing activity before data are transferred. Under the GDPR, personal data must be processed lawfully, fairly and transparently, collected for specified purposes and limited to what is necessary [5]. Pseudonymised information remains personal data when it can be reconnected to an individual [6]. Data protection by design and by default requires controls to be embedded in the processing method and reviewed throughout its life [7-8].

The governance pack should identify controllers and processors, purposes, categories, retention, recipients, transfers, security measures and data-subject implications. A data protection impact assessment may be required when proposed processing is likely to create high risk [9]. Transaction counsel should confirm the actual roles and legal bases. A confidentiality agreement does not replace data-protection duties, competition controls or third-party contractual restrictions.

The governance body should include transaction leadership, legal, competition, privacy, cybersecurity, finance, regulatory affairs and the relevant technical owners. It approves questions, methods, users and outputs. It should maintain a decision log showing why information was required, why the selected method was proportionate and who accepted residual risk. This evidence becomes important when a regulator, customer, lender or board later asks how sensitive information was handled.

## 6. Design the clean-team perimeter

A clean team is a restricted group that receives information unavailable to the commercial decision makers. The European Commission's 2023 Horizontal Guidelines describe clean teams as people outside commercial operations who are bound by strict confidentiality protocols; trustees can perform a similar role, and outputs can be limited to need-to-know aggregated information [10]. The concept is useful for transaction diligence when the parties compete or when disclosure could change market conduct.

Membership should follow function and independence rather than job title. External advisers, specialist accountants, economists, regulatory consultants and designated internal personnel may participate if they are separated from pricing, sales, procurement and other competitive decisions. The protocol should define appointment, conflicts, training, permitted devices, communication channels, escalation, output approval, recusal, retention and post-project restrictions.

The clean team should not become an unrestricted parallel transaction team. It receives only the source information required for approved analyses. Clear-text identities and recipes remain hidden unless the question cannot be answered another way and the governance body approves escalation. Every release to the wider team should use an output template that records population, method, assumptions, thresholds, limitations and reviewer approval.

## 7. Build the layered analytical architecture

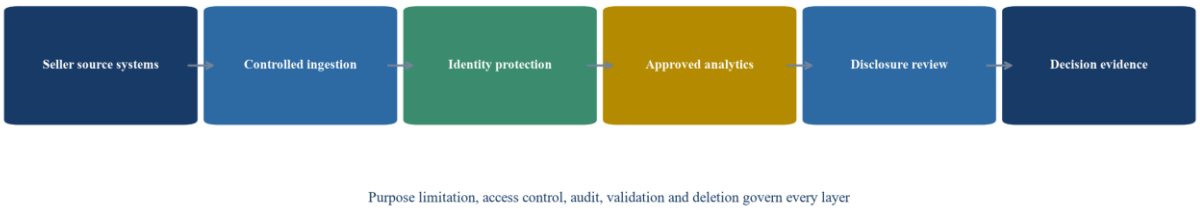
The architecture should have separate ingestion, identity, computation, review and output layers. Source files enter through controlled transfer, malware scanning and schema validation. Identity keys are tokenised or held by an independent custodian. Computation occurs in a restricted environment with approved code and query controls. Reviewers test outputs for accuracy and disclosure risk. Approved results move to the transaction record through a one-way release process.

Different techniques solve different problems. Aggregation reduces granularity. Pseudonymisation supports longitudinal analysis without routine identity disclosure. Private set intersection can identify records shared by two datasets while protecting unmatched records. Secure multiparty computation can calculate a joint function without combining clear-text inputs. Differential privacy can reduce the risk that an output reveals a particular record. Trusted execution environments can isolate approved code and data.

NIST, ENISA and the UK Information Commissioner's Office describe these techniques and their limits [11-14].

The architecture should remain understandable to transaction users. Advanced cryptography does not correct poor identifiers, inconsistent units or invalid commercial assumptions. The parties should select the simplest technique that satisfies the question and risk. High-complexity methods need independent technical validation, key management, performance testing and a fallback when the computation fails or produces results that cannot be reconciled.

**Figure 1. Privacy-preserving chemical M&A diligence architecture**




*Source systems remain separated from transaction users; approved computations produce controlled evidence rather than unrestricted data copies.*

## 8. Create a permission architecture

Permissions should combine user role, dataset, purpose, field, action, time and environment. A financial clean-team member may analyse pseudonymous customer revenue but cannot export row-level results. External competition counsel may view clear-text overlap records for a filing but cannot share them with the buyer's sales team. A regulatory specialist may inspect registration rights and tonnage bands without seeing customer prices.

Administrative privilege requires separate control. Platform administrators can sometimes access data despite front-end restrictions. The parties should define whether administrators are independent, how privileged sessions are approved and recorded, and whether encryption keys are separated from infrastructure operators. Dual control should apply to identity re-linking, bulk export, rule changes and deletion.

Access should expire automatically. Closing, termination, clearance and role changes alter the legitimate purpose. The environment should revoke credentials, rotate keys and preserve required evidence without leaving dormant accounts. Periodic access reviews should compare actual use with approved questions. Unused access is a signal that the dataset may not have been necessary.

**Table 2. Illustrative permission architecture**

| Role | Permitted information | Prohibited access | Output authority |
|---|---|---|---|
| External financial clean team | Pseudonymous customer, product and margin records | Clear-text identities and buyer commercial systems | Aggregated earnings and concentration outputs |
| Competition counsel | Identity-matched overlap and filing evidence | Buyer pricing and integration planning outside approved scope | Legally reviewed overlap and market evidence |

| Role | Permitted information | Prohibited access | Output authority |
|---|---|---|---|
| Regulatory clean team | Registration, study rights, uses, tonnage and legal-entity records | Customer pricing and unrelated employee data | Regulatory continuity schedule |
| Technical diligence team | Masked formulations, yields, process capability and asset data | Full recipe keys and unrestricted source export | Capability, capital and exception report |
| Buyer deal team | Approved outputs and disclosed exceptions | Raw clean-room datasets | Valuation, protection and financing decisions |
| Integration team before clearance | Sanitised workplans and dependency maps | Competitively sensitive current and future conduct | Day-one readiness subject to legal approval |

*Access is granted to answer defined questions and expires when the purpose ends.*

## 9. Test customer concentration without exposing identities

Customer analysis should begin with stable pseudonyms, revenue, volume, contribution, product family, geography, channel, contract type and monthly history. Stable pseudonyms allow churn, cohort and concentration analysis without routine disclosure of names. The tokenisation key should remain with the seller, an independent custodian or a tightly controlled service. The buyer receives identities only for approved exceptions, such as a material change-of-control clause or a customer-specific regulatory dependency.

The analysis should reconcile to audited or management accounts. It should explain gross-to-net adjustments, rebates, freight, returns, intercompany sales and currency. Customer groups and legal entities require a controlled hierarchy; otherwise, concentration can be understated by splitting one economic group across accounts. Small-cell suppression should prevent an output from revealing an identity through a narrow product-geography combination.

Contracts can be reviewed through staged disclosure. The first stage provides extracted fields and clause flags. External counsel can inspect clear-text documents and issue a privilege-aware exception report. The buyer receives the identity only when the commercial decision requires it and the clean-team protocol permits release. This structure supports decision quality while limiting unnecessary copying of customer information.

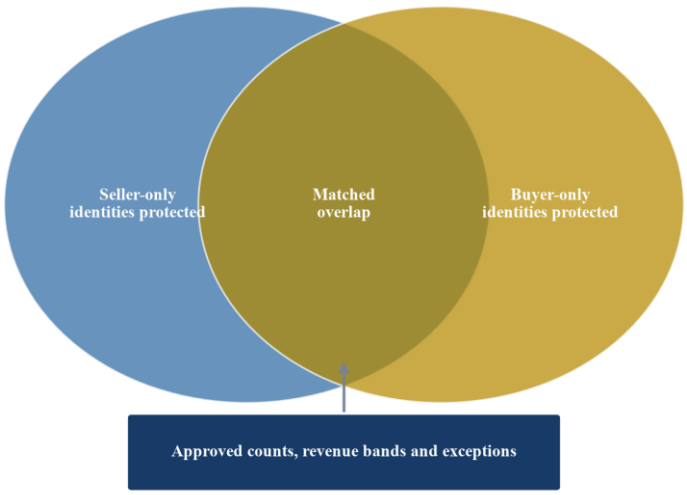
## 10. Measure customer overlap with private set intersection

Customer overlap matters for competition assessment, cross-selling, retention and revenue dis-synergy. Direct exchange of complete customer lists can reveal each party's unmatched relationships. Private set intersection allows the parties to identify common elements without disclosing elements outside the intersection [11-12]. An independent clean team can achieve a similar result through tokenisation and controlled matching.

Identifier quality determines the result. Legal name, trading name, tax identifier, address, parent group and ship-to location can differ. The parties should agree normalisation rules and measure false matches and missed matches. A two-stage process can use deterministic identifiers first and restricted review of uncertain pairs second. The output should distinguish legal-entity overlap, economic-group overlap and site-level overlap.

Overlap revenue should be analysed by product substitutability, geography, customer segment and purchasing behaviour. The Commission's 2024 Market Definition Notice identifies customer preferences, purchasing behaviour, prices, suppliers and trade flows among relevant evidence [15]. A numerical overlap does not by itself define a market or establish competitive harm. Competition counsel should control interpretation and filing use.

**Figure 2. Customer-overlap analysis with protected unmatched identities**




*Each party contributes normalised identifiers; only approved overlap statistics and reviewed exceptions leave the controlled environment.*

## 11. Reconstruct margin without revealing full formulations

Chemical-product margin depends on composition, purchasing terms, yield, batch size, energy, labour, waste, co-products, packaging, freight and quality losses. A buyer needs to distinguish sustainable economics from standard-cost artefacts. Full recipe disclosure may be disproportionate at the first stage. The seller can provide masked ingredient families, quantities as indexed proportions, standard and actual costs, process route, yield and realised price within a trusted environment.

The clean-team model should reconcile product-level gross margin to the general ledger. It should test standard-cost updates, raw-material pass-through, inventory revaluation, purchase-price variance, off-spec disposal and intercompany allocation. Exceptions can be ranked by value and uncertainty. A formulation crosses the disclosure threshold when the unresolved value is material and cannot be tested through masked data or independent review.

The output should separate price, mix, input cost, yield and accounting effects. It should also state whether the buyer can reproduce the economics after closing. A high-margin formulation may depend on a seller group purchasing contract, a non-transferable licence, a single technical employee or a study right that does not transfer. Margin quality therefore includes operational and legal continuity, not only arithmetic.

## 12. Protect recipes and trade secrets

Trade-secret protection depends on the information being secret, having commercial value because it is secret and being subject to reasonable steps to preserve secrecy under the applicable law. Transaction disclosure should follow a documented need-to-know process, with contractual and technical measures aligned to the risk. The EU Data Act recognises strict access protocols, technical standards and confidentiality arrangements as measures that can protect trade secrets in data-sharing contexts [16].

Recipe keys should remain separate from analytical extracts. Ingredient names can be replaced with functional classes or tokens where the transaction question concerns cost, volatility or supplier dependence. Exact ratios can be transformed into indexed quantities for early-stage analysis. Clear-text access should require a recorded exception, named reviewers and a defined expiry. Screenshots, printing, copy-paste and local downloads should be restricted where proportionate.

The parties should also control inference. A masked formulation may still be reconstructed from supplier, quantity, process and product data. Output review should consider linkage across files and repeated queries. A sequence of permitted analyses can reveal more than any single result. Query budgets, minimum cohorts, suppression and reviewer judgement reduce that risk.

## 13. Verify REACH registration continuity

REACH continuity can affect the legal ability to manufacture or import a substance. The diligence team should map the target's role, legal entity, substances, tonnage bands, uses, registrations, joint submissions, only-representative arrangements and dossier-update obligations. ECHA states that mergers, splits and changes of only representative can require a legal-entity change process and verification of related dossier updates [17].

The clean team should distinguish registration ownership from access to study data and practical control of IUCLID records. It should test whether the target holds the latest substance dataset, can access its REACH-IT account and has evidence for rights relied upon. ECHA notes that registrants and potential registrants must make every effort to agree data sharing and that costs should be fair, transparent and non-discriminatory [18]. A payment history or letter of access may be essential to continuity.

The output should identify actions required before signing, before closing and after closing. These may include legal-entity change preparations, only-representative consents, account administration, evidence of asset transfer, dossier updates and data-access confirmation. Regulatory specialists should verify the transaction-specific sequence. The framework does not determine the legal effect of a particular corporate reorganisation.

## 14. Review CLP, safety data and product stewardship

Classification, labelling and packaging records should connect each substance or mixture to current classifications, notifications, safety data sheets, language versions and customer uses. The buyer should identify whether the transaction changes the responsible legal entity, importer, downstream user or only representative. It should also test whether product labels, poison-centre notifications or other market-specific records require updates.

The analytical environment can compare regulatory identifiers, classifications and commercial product masters without releasing full recipes. Exceptions should include inconsistent identifiers, missing composition ranges, outdated safety data, unsupported uses and products sold under a registration held elsewhere in the seller group. Each exception needs an owner, legal analysis, remediation cost and business consequence.

Product-stewardship data often reveal customers, applications and technical performance. Access should therefore follow the same clean-team boundaries as commercial data. Regulatory necessity does not automatically justify sharing the record with the buyer's sales or product teams before closing.

## 15. Test study and data-sharing rights

Chemical registrations can rely on jointly owned studies, letters of access, consortium arrangements and cost-sharing agreements. ECHA's data-sharing guidance addresses confidential business information, intellectual property and competition-law issues alongside the obligation to share certain data [19]. The buyer should establish what the target owns, what it may refer to, what transfers automatically and what requires consent or additional payment.

A rights matrix should link each material substance to the study owner, agreement, scope, territory, legal entity, payment status, transfer clause and evidence. The clean team can review full agreements and provide the buyer with a structured exception schedule. Missing rights should be valued through

remediation cost, delay, supply interruption and negotiation risk rather than treated as a binary compliance flag.

Disputes can arise from cost itemisation, substance sameness, delay and whether the parties made every effort. ECHA publishes decisions on data-sharing disputes that illustrate these recurring issues [20]. Transaction documents can allocate known gaps through conditions, covenants, price adjustments, escrow or specific indemnities. The selected remedy should reflect the likelihood, timing and consequence of failure.

## 16. Analyse process capability and capacity

Manufacturing diligence should test demonstrated output, yield, quality, downtime, changeover and bottlenecks under the relevant product mix. Raw historian data can reveal process know-how and operating weaknesses. The seller can create approved aggregates by line, product family, batch type and period while preserving the underlying records for clean-team validation.

The model should distinguish nameplate, demonstrated, sustainable and saleable capacity. It should account for maintenance, campaign length, cleaning, hazardous-material constraints, environmental permits, labour, utilities, storage and quality release. A buyer synergy case that moves production between sites needs evidence that receiving assets can process the formulation safely, legally and economically.

Outliers deserve controlled drill-down. A small number of high-value products may depend on narrow process windows or manual operator knowledge. The technical clean team can inspect detailed batch records and issue a conclusion without disclosing the full process to integration teams before clearance. Capital requirements should include instrumentation, containment, quality, utilities and regulatory validation where applicable.

## 17. Govern analytics and model validation

Every analytical output should have a documented population, transformation, code version, assumptions, exclusions, thresholds and reconciliation. The seller or custodian should confirm completeness of the source extract. The clean team should test duplicate records, missing periods, unit conversions, currency, hierarchy and changes in system configuration. Material outputs should be independently reviewed.

Privacy-preserving computation introduces additional failure modes. Entity matching can produce false positives. Differential privacy can add noise that obscures a small but material exposure. Secure multiparty computation can calculate the wrong function perfectly if business definitions differ. A trusted environment can still be compromised by an administrator or a permitted export. Technical validation should therefore cover confidentiality, correctness and decision usefulness.

The model register should identify owner, reviewer, approved purpose, inputs, performance tests, limitations and expiry. Transaction users should receive explanations that allow challenge. A result should not be treated as reliable merely because it came from a sophisticated technique. Human accountability remains with the people approving valuation, financing, filing and integration decisions.

## 18. Build a disclosure-control matrix

Output review should assess direct identifiers, small cells, rare combinations, differencing, linkage and commercial sensitivity. A table with no names can still identify a customer when one account dominates a narrow country-product segment. Repeated queries can isolate a record by subtracting one result from another. Reviewers need authority to aggregate, suppress, delay or reject an output.

The matrix should specify minimum cohort sizes, rounding, value bands, permitted dimensions, query frequency and escalation. Thresholds should reflect the dataset and decision. A minimum of five records may be inadequate when one record represents most of the value. A minimum revenue share can

complement record count. Competition counsel should approve outputs concerning prices, customers, capacity and future conduct.

**Table 3. Illustrative disclosure-control matrix**

| Output type | Default control | Escalation trigger | Approved recipient |
|---|---|---|---|
| Customer concentration | Stable pseudonyms; groups of at least ten where identities are unnecessary | One customer exceeds ten percent of revenue or a consent clause is material | Financial clean team and approved deal leadership |
| Customer overlap | Counts and revenue bands by broad segment | Filing question requires identity or contract evidence | Competition counsel and regulator-facing team |
| Formulation margin | Masked ingredient classes and indexed ratios | Unresolved EBITDA effect exceeds EUR 0.5 million | Technical clean team and designated counsel |
| Process capacity | Monthly line and family aggregates | Safety, permit or capital exception needs batch evidence | Technical diligence specialists |
| Employee analysis | Aggregated role and location cohorts | Named retention or change-of-control obligation | Employment counsel and authorised HR clean team |
| Synergy output | Range with assumptions and prohibited implementation actions | Proposed action could influence pre-close competition | Competition counsel and board transaction committee |

*Thresholds are management assumptions for the hypothetical case and require transaction-specific legal and technical approval.*

## 19. Connect diligence to valuation

The clean-room output should translate into a maintainable earnings bridge. Customer churn, rebates, one-off price effects, raw-material normalisation, unsupported formulation margins, capacity constraints and regulatory remediation can affect sustainable cash generation. Each adjustment should have an evidence trail, owner and uncertainty range. The buyer should avoid combining conservative assumptions that arise from the same cause.

The hypothetical case starts with reported EBITDA of EUR 46.0 million. Management assumptions identify EUR 3.6 million of price-normalisation exposure, EUR 2.1 million of unsupported formulation margin, EUR 0.8 million of customer and product attrition not already captured, and EUR 1.4 million of annual remediation and clean-room operating cost. A positive EUR 2.8 million adjustment reflects removal of identified non-recurring costs supported by clean-team evidence. Illustrative maintainable EBITDA is therefore EUR 40.9 million.

The analysis does not predict actual earnings. It excludes tax, financing, working capital, capital expenditure, environmental liabilities, pension, litigation, purchase-price allocation and negotiated protections. It also excludes unapproved synergies. The purpose is to show how protected evidence can support a valuation bridge without disclosing every source record to the full buyer team.

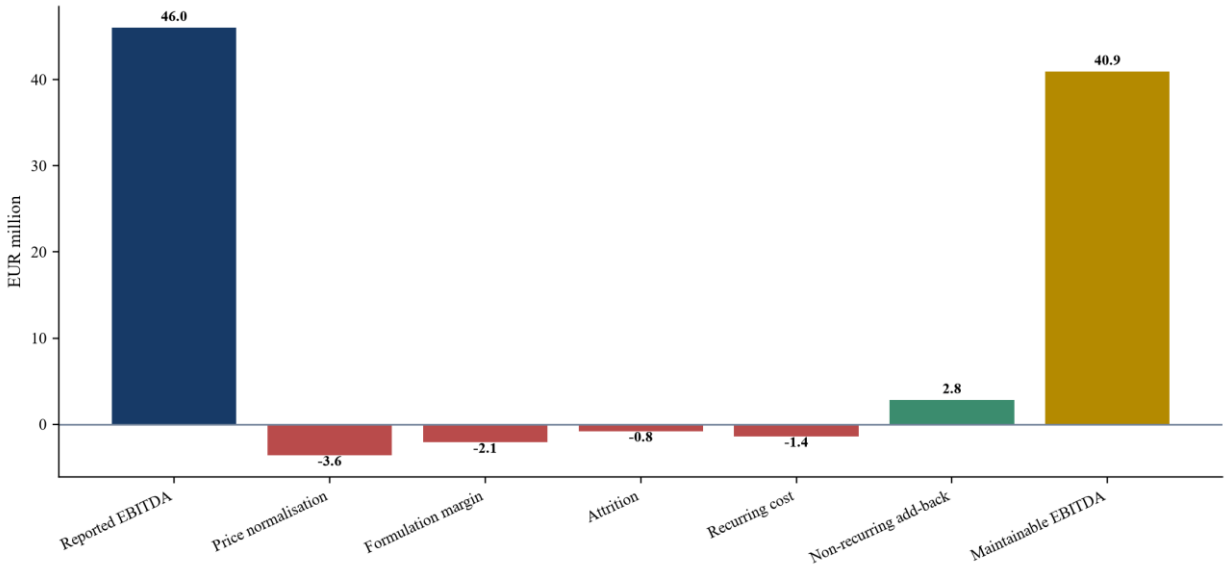
**Table 4. Hypothetical maintainable EBITDA bridge**

| Item | Management assumption | EBITDA treatment | Evidence route |
|---|---|---|---|
| Reported last-twelve-month EBITDA | 46.0 | Starting point | Reconciled management accounts |
| Price-normalisation exposure | (3.6) | Reduce | Pseudonymous customer and product analysis |
| Unsupported formulation margin | (2.1) | Reduce | Masked formulation clean-room review |

| Item | Management assumption | EBITDA treatment | Evidence route |
|---|---|---|---|
| Customer and product attrition | (0.8) | Reduce | Cohort and contract exception analysis |
| Recurring remediation and operating cost | (1.4) | Reduce | Regulatory, security and governance plan |
| Supported non-recurring costs | 2.8 | Add back | Invoice and ledger review by financial clean team |
| Illustrative maintainable EBITDA | 40.9 | Decision output | Approved bridge after independent review |

*All figures are management assumptions in EUR millions and demonstrate the framework only.*

**Figure 3. Hypothetical maintainable EBITDA bridge**




*Management assumptions show the movement from reported to maintainable EBITDA after evidence-based adjustments.*

## 20. Support financing diligence

Lenders need evidence of earnings, customer concentration, working capital, regulatory continuity and downside resilience. They rarely need unrestricted access to formulations or customer identities. The borrower and seller can agree a lender-output pack derived from approved clean-room analyses. It should identify the method, reconciliations, limitations and material exceptions.

The pack should distinguish verified data from management assumptions. Customer concentration can be presented through pseudonymous rankings and revenue bands. Regulatory continuity can be presented as a status and action schedule reviewed by specialists. Formulation dependence can be expressed as revenue and EBITDA at risk, with identities held back unless a lender's credit decision genuinely requires them and disclosure is permitted.

Financing conditions should align with the diligence design. If a lender requires a clear-text dataset late in the process, the parties may face delay or breach existing controls. Early agreement on outputs reduces that risk. The facility documents can address material regulatory actions, loss of key registrations, data-security incidents and delivery of post-close remediation evidence where commercially appropriate.

## 21. Prepare the merger-control evidence set

The European Commission's merger process can require complete, correct and timely information, internal documents and customer or competitor contact details [21-23]. The privacy-preserving transaction

environment should preserve the source-to-output lineage needed for a filing. It should not irreversibly aggregate evidence that may later be required in native or clear-text form by a regulator.

Competition counsel should maintain a separate filing evidence branch. Customer overlap, product substitution, switching, capacity and trade-flow analyses should use definitions consistent with the legal assessment. The 2024 Market Definition Notice explains the Commission's use of evidence concerning demand and supply substitution, purchasing behaviour, differentiation, R&D and geographic conditions [15]. Transaction models should record how their categories map to those concepts.

Regulatory disclosure follows legal process and authority. A private clean-room protocol cannot prevent a regulator from requesting information within its powers. It can improve readiness by preserving accurate records, limiting uncontrolled circulation and documenting methodology. The parties should avoid designing privacy controls that obstruct lawful investigation or create misleading filing evidence.

## 22. Separate integration planning from implementation

Pre-close integration planning should identify dependencies, resources and decisions required for day one without coordinating competitive conduct. Competition counsel should define permitted activities. Clean-team outputs can support planning through ranges, dependency maps and sanitised work packages. Customer-specific pricing, current bids, future commercial strategy and other competitively sensitive information should remain restricted until legally permitted.

The plan should translate diligence exceptions into owners and milestones. REACH-IT access, legal-entity changes, safety-data updates, supplier consents, identity management, data migration, formulation access, laboratory systems and cybersecurity can all affect continuity. The clean team can prepare detailed execution material for release at closing or clearance.

The release process should be deliberate. Information does not become unrestricted merely because signing occurred. The relevant trigger may be regulatory clearance, closing or another legal condition. At the trigger, the environment should change permissions, preserve the audit record and release only the materials approved for the integration team.

## 23. Design transaction protections

Representations and warranties should address ownership and permitted use of data, material registrations, accuracy of regulatory records, study rights, trade secrets, cybersecurity incidents, customer data, third-party restrictions and completeness of disclosed systems. The drafting should follow identified risks and applicable law. A broad warranty cannot replace a missing registration right or an inaccessible dataset.

Conditions precedent can require regulatory transfers, consents, account control, delivery of approved datasets or remediation of a critical access gap. Covenants can preserve data, maintain registrations, restrict unusual disclosures and support filing responses. Specific indemnities, escrow, retention or price mechanisms can address known exposures. Counsel should determine the enforceability and proportionality of each protection.

The clean-room record supports negotiation. It shows the population tested, exceptions found, evidence reviewed and uncertainty that remains. The buyer should avoid presenting a model output as a factual warranty. The seller should avoid using privacy as a reason to withhold decision-critical evidence when a controlled method can answer the question.

## 24. Plan the first hundred days

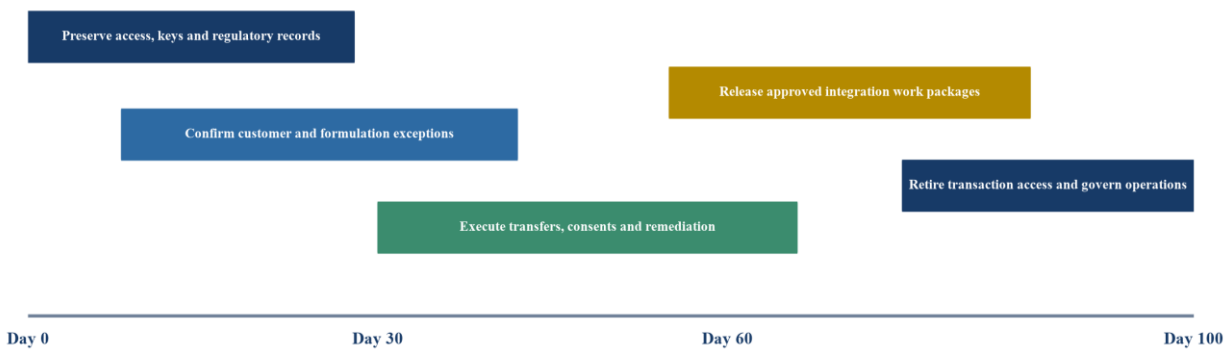
The first thirty days should preserve access, identifiers and regulatory continuity. The buyer confirms system owners, tokens, identity keys, administrator privileges, IUCLID datasets, REACH-IT access,

study-right evidence and critical customer or supplier consents. It maintains the clean-room restrictions required for residual legal, contractual or competition purposes.

Days thirty-one to sixty should resolve high-value exceptions. Finance closes the EBITDA bridge. Regulatory teams execute legal-entity and dossier actions. Technical teams validate formulation and process access. Cybersecurity tests identity, export, backup and deletion controls. Customer and supplier engagement follows approved communications and consent plans.

Days sixty-one to one hundred should transition from transaction analytics to governed operations. The business establishes permanent data ownership, retention, access reviews, product-stewardship workflows and management reporting. It measures realised benefits against the acquisition case. Unused transaction copies are deleted or archived according to the approved retention schedule.

**Figure 4. First hundred day transition from clean-room diligence to governed operations**




*The roadmap preserves evidence and continuity, resolves exceptions and then retires transaction-only access.*

## 25. Manage retention, deletion and evidence

Retention should follow purpose, law, contractual duty, litigation need and transaction record requirements. Raw seller data should not remain indefinitely in adviser accounts, local downloads or temporary processing stores. The parties should identify the authoritative archive, required evidence and deletion trigger for every environment.

Deletion needs verification. Platform deletion may leave backups, exports, logs or derived files. The custodian should issue a record describing systems covered, method, date, exceptions and residual retention. Encryption-key destruction can support effective deletion when designed correctly. Legal holds should be specific and reviewed rather than used as a general reason to retain everything.

The transaction record should preserve decisions and reproducibility without preserving unnecessary personal or commercially sensitive data. Approved outputs, code hashes, source manifests, reconciliations, review logs and exception schedules may be sufficient. The parties should confirm evidential requirements with counsel and auditors.

## 26. Recognise failure modes

A clean room can create false confidence. Access controls may be bypassed by administrators. Pseudonyms may be reversible through auxiliary information. Aggregated outputs may expose small groups. Private set intersection may misstate overlap because identifiers are inconsistent. Differential privacy may reduce accuracy. Sophisticated computation may be impossible to explain to a credit committee or board.

Commercial teams may also misuse approved outputs. A range intended for valuation can influence pre-close pricing conduct. An integration plan can become premature coordination. A reviewer can reveal an identity during an informal conversation. Training, monitoring and escalation remain essential. Technology supports governance but does not replace judgement.

The framework cannot determine the legality of a specific processing activity, merger filing, REACH transfer, formulation disclosure or competition arrangement. Requirements depend on the parties, jurisdictions, markets, data, systems and current law. European and national legal, competition, privacy, chemical-regulatory, cybersecurity, tax and accounting specialists should review the actual transaction.

## 27. Apply the hypothetical case

The hypothetical target has EUR 310 million of revenue, EUR 46 million of reported EBITDA, 620 active customers, 1,850 formulations and 340 substances or mixtures in the regulatory map. The buyer and seller compete in selected product families. The governance body approves four analytical lanes: customer overlap, maintainable margin, regulatory continuity and process capability.

Private set intersection and clean-team review identify EUR 8.4 million of revenue associated with shared customer groups. That figure is a management assumption and does not establish a relevant market or competitive concern. Pseudonymous customer analysis identifies EUR 3.6 million of price-normalisation exposure. Masked formulation analysis identifies EUR 2.1 million of margin that lacks sufficient support. Regulatory and governance work adds EUR 1.4 million of recurring cost. Supported non-recurring costs of EUR 2.8 million are added back.

The board receives the maintainable EBITDA bridge, an overlap analysis reviewed by competition counsel, a regulatory action schedule, a formulation exception register and a process-capability report. Clear-text identities, recipes and unrestricted source files remain within approved clean teams. The transaction decision can therefore address price, protections, financing and integration while limiting disclosure.

## 28. Draw the transaction conclusion

Privacy-preserving diligence is an evidence architecture for chemical M&A. It begins with transaction questions, maps the information perimeter, classifies harm, applies legal and competition governance, and selects the least-disclosive method that can produce decision-useful evidence. Conventional data rooms remain useful, but sensitive analyses often require additional clean-team and technical controls.

The strongest design connects customer, formulation, process and regulatory evidence. It allows the buyer to test maintainable earnings, concentration, overlap, study rights, registration continuity and capacity. It gives the seller a defensible method for protecting customers, recipes, trade secrets and people. It preserves a regulator-ready lineage from source to output.

The economic result depends on disciplined execution. The parties should agree questions and outputs early, validate identity and model logic, restrict administrators, review disclosure risk and design closing transitions. A controlled environment that produces reproducible evidence can improve transaction certainty while preserving the information boundaries required before closing.

## Frequently asked questions

### What is a privacy-preserving data room in chemicals M&A?

It is a governed diligence environment that combines restricted access with techniques such as aggregation, pseudonymisation, private set intersection or secure computation. It produces approved transaction evidence while limiting disclosure of customer identities, recipes and other sensitive records.

## Can a conventional virtual data room provide the same protection?

A virtual data room provides useful permissions, audit and document controls. Sensitive customer, formulation and overlap analyses may require additional identity separation, clean-team restrictions, approved computation and output review.

## How can a buyer test customer overlap without receiving both customer lists?

The parties can use private set intersection, tokenised matching or an independent clean team. The output can show counts, revenue bands and approved exceptions while protecting unmatched identities.

## Can formulation profitability be tested without disclosing the recipe?

Often, yes. Masked ingredient classes, indexed ratios, costs, yields and prices can support an initial margin test. Material unresolved exceptions may require controlled clear-text review by designated specialists.

## What should be checked for REACH continuity?

Check legal entities, roles, substances, tonnage bands, uses, registrations, IUCLID datasets, REACH-IT access, joint submissions, study rights, only-representative arrangements and required post-transaction updates.

## Does pseudonymisation remove GDPR obligations?

No. Pseudonymised data remain personal data when they can be linked back to an identifiable person. The parties still need an appropriate purpose, legal basis, minimisation, security and governance.

## Who should approve clean-room outputs?

Approval should reflect the subject. Competition counsel should review competitively sensitive customer and pricing outputs. Privacy, regulatory, finance and technical specialists should review outputs within their disciplines before release to decision makers.

## What happens to the clean room after closing?

Permissions should change only on the applicable legal trigger. Required evidence and approved integration materials are preserved, transaction-only access is retired, and unnecessary data are deleted or archived under a verified retention plan.

# References


**[1]** European Chemicals Agency, IUCLID https://iuclid6.echa.europa.eu/

**[2]** European Chemicals Agency, Registration process and REACH-IT https://echa.europa.eu/en/support/dossier-submission-tools/reach-it/registration

**[3]** EUR-Lex, Council Regulation (EC) No 139/2004 on the control of concentrations between undertakings, Article 17 https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32004R0139

**[4]** European Commission, Data rooms and confidentiality rings https://competition-policy.ec.europa.eu/index/data-rooms-and-confidentiality-rings_en

**[5]** EUR-Lex, Regulation (EU) 2016/679, General Data Protection Regulation https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

**[6]** European Commission, Application of the GDPR https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/application-gdpr_en

**[7]** European Data Protection Board, Guidelines 4/2019 on data protection by design and by default https://www.edpb.europa.eu/documents/guideline/guidelines-42019-on-article-25-data-protection-by-design-and-by-default_en

**[8]** European Data Protection Board, Data protection by design and by default summary, February 2026 https://www.edpb.europa.eu/system/files/2026-02/edpb-summary-gdpr-data-protection-design-default_en.pdf

**[9]** European Commission, Data-protection obligations and impact assessments https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/obligations_en

**[10]** European Commission, Guidelines on horizontal cooperation agreements, paragraphs 407-408 https://competition-policy.ec.europa.eu/document/download/fd641c1e-7415-4e60-ac21-7ab3e72045d2_en?filename=2023_revised_horizontal_guidelines_en.pdf

**[11]** National Institute of Standards and Technology, Privacy-Enhancing Cryptography tools https://csrc.nist.gov/projects/pec/pec-tools

**[12]** National Institute of Standards and Technology, Privacy-enhancing cryptography to complement differential privacy https://www.nist.gov/publications/privacy-enhancing-cryptography-complement-differential-privacy

**[13]** European Union Agency for Cybersecurity, Data Pseudonymisation: Advanced Techniques and Use Cases https://www.enisa.europa.eu/publications/data-pseudonymisation-advanced-techniques-and-use-cases

**[14]** UK Information Commissioner's Office, Privacy-enhancing technologies https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/privacy-enhancing-technologies/

**[15]** EUR-Lex, Commission Notice on the definition of the relevant market for the purposes of Union competition law, C/2024/1645 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52024XC01645

**[16]** EUR-Lex, Regulation (EU) 2023/2854 on harmonised rules on fair access to and use of data https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2854

**[17]** European Chemicals Agency, Prepare for updating your registration https://echa.europa.eu/support/registration/prepare-for-updating-your-registration

**[18]** European Chemicals Agency, Working together with co-registrants https://echa.europa.eu/support/registration/working-together

**[19]** European Chemicals Agency, Guidance on data sharing, December 2023 https://echa.europa.eu/view-article/-/journal_content/title/guidance-on-data-sharing

**[20]** European Chemicals Agency, Decisions on data-sharing disputes under REACH https://echa.europa.eu/regulations/reach/registration/data-sharing/data-sharing-disputes/echa-decisions-on-data-sharing-disputes-under-reach

**[21]** European Commission, Practical information for EU merger notifications https://competition-policy.ec.europa.eu/mergers/practical-information_en

**[22]** European Commission, Electronic requests for information in merger investigations https://competition-policy.ec.europa.eu/mergers/procedures/erfi_en

**[23]** European Commission, Communication on transmission of documents and Form CO internal documents https://competition-policy.ec.europa.eu/system/files/2023-04/Merger_Control_in_the_EU_Further_simplification_of_procedures_OJ_Communication.pdf

**[24]** European Commission, Mergers legislation, notices and guidelines https://competition-policy.ec.europa.eu/mergers/legislation_en

## About the Author

Chennakeshav (CK) is a corporate finance and investment banking executive with 25+ years of global experience in deal origination, structuring and execution across M&A, growth capital and corporate strategy. He has led value-creation mandates for founders, corporates and funds — bridging the boardroom view to hands-on execution and closure.

His career spans Morgan Stanley, HSBC, Lloyds Banking Group, EWEC, ADQ portfolio companies and Emirates Growth Fund, across TMT, real estate, fintech, deeptech, cleantech, infrastructure and energy. He has partnered with C-suite leaders, private equity and venture funds, sovereign wealth funds and family offices to finance complex fund raises and scale-up ventures, and has led M&A due diligence, post-merger integration and business-transformation initiatives to create value.

At Matchpoint Partners, he is Managing Partner and leads the firm's corporate finance, M&A and capital-raising practice. He holds an MBA from London Business School, an engineering degree from VTU and a Master of Laws (LLM, in progress) from UCL London.

An active start-up mentor, CK mentors at Techstars, DIFC FinTech Hive, Startup Grind, Founder Institute and IN5, serves as Entrepreneur Mentor in Residence (EMiR) at London Business School, and judges the Entrepreneurship World Cup.

https://www.linkedin.com/in/ckadya/

https://www.matchpoint-partners.com/team/ck-adya.html

This paper is part of a continuing series on the structure of private and alternative markets. The views expressed are the author's own. The paper is for information only, describes market structure in general terms, and does not constitute investment, legal, tax or regulatory advice or a recommendation in respect of any security, vehicle or counterparty.