



MICRO-PLAYBOOK

The Confidential Sale Playbook

Disclose enough to progress, never more than necessary.

LANGUAGE

EN

STATUS

RELEASE CANDIDATE

EVIDENCE CUTOFF

24 September 2026

REFERENCE

S02

The Confidential Sale Playbook

The legitimate fear

Poorly sequenced disclosure can trigger rumours, employee anxiety, supplier pressure, lender questions and competitor opportunism. The answer is not to hide everything until the last day. It is to **give the right information to the right person at the right time for a documented reason.**

Core principle

Confidentiality is not a document. It is an architecture: audience, information tier, NDA, permissions, access, duration, download, revocation, Q&A and external communication.

What changes by stage

T0 — minimum permitted existence/presentation. In governed share deals, identity, price and sensitive terms are not public.

T1 — a controlled teaser that lets a buyer decide whether to qualify further without opening the full file.

Admission + NDA — verify the counterparty, obtain the required undertaking and record the access decision.

T2 / VDR — detailed information by permission, purpose and diligence stage.

Four decisions before any teaser

Which information would be harmful if circulated? Who internally needs to know? What can a qualified buyer see before NDA? Which data requires even tighter access?

Confidentiality Map

Audience	T0	T1	Post-NDA	Restricted VDR
public / unqualified	minimum permitted	no	no	no
qualified buyer	yes	yes	gated	permissioned
external adviser	by mandate	by mandate	scoped	scoped + expiry
employee	operational need	communication plan	rarely	no by default
support admin	operational metadata	no by default	break-glass	audited break-glass

Data requiring particular care

Customer names and concentration, customer-level margins, HR personal data, trade secrets/code/recipes, disputes, banking terms, change-of-control contracts, live bids and competitively sensitive strategy.

Depending on the deal, information may be summarised, aggregated, redacted or restricted to a Clean Team.

When should employees be told?

There is no universal date. Decide with counsel by considering legal obligations, process staffing, leak risk, reliance on key managers and the point at which uncertainty becomes more dangerous than communication.

Prepare message, spokesperson, FAQ, known/unknown impacts, question channel and confidentiality expectations before communication.

Customers, suppliers and banks

Banks may need earlier engagement where consent, waiver, debt or change-of-control issues exist. Customers/suppliers depend on contract and dependency. Regulated partners may have approval requirements. Confidentiality never means ignoring consent obligations.

Buyer-access checklist

Before T2/VDR: verified identity, authority, thesis, NDA, RPS admission where applicable, scope, expiry, download policy, purpose and owner approval.

Revocation

Design the exit before granting access: expiry, manual revocation, expert assignment end, exclusivity end or buyer withdrawal. Revocation should also remove affected sources from AI/retrieval access.

If a leak occurs

Preserve logs, determine the exposure, restrict access, notify security/compliance, assess contractual/regulatory obligations, and document remediation and restart decisions.

DealPME role

RPS, T0/T1/T2, Permission Lens, VDR and logs provide structure. They do not replace seller judgement, law or professional advice.

Aggregate, redact or restrict: three different tools

Aggregation shares useful information without named detail, for example customer concentration bands. **Redaction** removes a specific sensitive field from an otherwise necessary document.

Restriction/Clean Team gives detailed access to a limited group when evidence is material but too sensitive for the wider team.

The choice follows the diligence question. Hiding too much can prevent a buyer from reaching a conclusion; showing too much too early creates unnecessary risk.

Rehearse communication before using it

For employees, strategic customers or suppliers, prepare the core message, difficult questions, approved answers, known unknowns and contact person. A spokesperson should be able to say “we cannot answer that yet” without improvising.

What should not be sent by reflex

Named customer lists, personal HR data, technical secrets, bank credentials, passwords, API keys, unnecessary full contracts or third-party data unrelated to the diligence question. Disclosure should remain proportionate.

Mini-FAQ

Does an NDA mean everything can be shared? No. It creates a contractual obligation but does not replace permissions, data minimisation or regulatory restrictions.

Can access be restored after revocation? Only through a new authorised gate; old links or cached retrieval should not bypass revocation.

Working tool — Buyer Access Checklist

Print or complete this table during the process. Blank fields are intentional and should be completed using deal-specific evidence or decisions.

Control	Status	Evidence	Owner
Identity verified			
Authority verified			
NDA executed			
Purpose/scope defined			
Expiry set			
Download policy set			

Working tool — Confidentiality Map

Print or complete this table during the process. Blank fields are intentional and should be completed using deal-specific evidence or decisions.

Audience	T0	T1	Post-NDA	Restricted VDR	Owner
Public/unqualified					
Qualified buyer					
External adviser					
Employees					

Sources, methodology and limitations

The sources below support the rules, methods or context used in this playbook. They do not turn the document into transaction-specific legal, tax, financing, valuation or investment advice.

DealPME governed product baseline - Core Build Pack and P04-P25 process reference

Publisher: DealPME · Tier: Governed internal source

Use: Product rules for disclosure, qualification, VDR, diligence, closing, Deal-Ready, partner boundaries and human decision ownership.

Source interne gouvernée / Governed internal source