Teteza360 Discovery Questionnaire

Prepare for a tailored demonstration and implementation discussion

23 August 2026

Instructions

Answer at the level appropriate before a confidentiality/data-processing agreement. Do not include passwords, personal records, security keys or privileged legal advice. “Unknown” is useful: it identifies discovery work.

Organisation and objectives

1. Legal name, sector, primary country and operating regions?
2. Which entities, branches and departments are in scope?
3. What prompted the programme now (law, customer demand, audit, incident, board priority, registration)?
4. What outcomes must be visible in 30, 90 and 180 days?
5. Who are the executive sponsor, accountable owner, DPO/compliance lead and delivery lead?

Current operating model

6. Where are the current ROPA, assessments, DPIAs, incidents, rights requests, consent records, vendors, policies, training and evidence held?
7. Which processes rely on spreadsheets, shared drives, email or general task tools?
8. What is hardest to keep current or prove to management/reviewers?
9. Which reviews require independent approval today?
10. What reporting does the board, audit, customers or regulators expect?

People and access

11. Approximate active users by administrator, reviewer, contributor and read-only persona?
12. What branches/departments need scoped contribution?
13. What MFA, password, joiner/mover/leaver and periodic access-review policies apply?
14. Is enterprise SSO or automated user provisioning mandatory? (Not implemented in the current release.)
15. Who may authorise temporary ITES support access?

Data and workflow priority

16. Approximate processing activities, systems, vendors, transfers and evidence files?
17. Priority high-risk processing or vulnerable data subjects?
18. Current incident intake and response decision chain?
19. Current rights-request channels, identity verification and response process?
20. Current privacy notices, consent channels and guardian requirements?
21. Current vendor due diligence, contract review and transfer safeguards?
22. DPO appointment/programme, security assessment and training arrangements?
23. Registration and regulatory-change monitoring responsibilities?

Technology, security and operations

24. Preferred hosting model and required data location?
25. Availability, support hours, RPO and RTO expectations?
26. Security assurance, penetration test, logging, retention, encryption and backup requirements?
27. Required mail, object storage, malware scanning or document-processing services?
28. Required integrations/APIs and their authoritative data owners?
29. Restrictions on AI, external processing, recordings or document extraction?
30. Procurement, security review, legal review and go-live acceptance steps?

Migration and adoption

31. Which existing data must be migrated, archived or left in place?
32. File formats, quality issues, duplicates and accountable data validators?
33. Pilot group, training needs, internal communications and change champions?
34. Desired implementation date and known blackout periods?
35. Budget/approval range and preferred commercial model?

Demonstration selection

Rank up to five: organisation profile; assessment/scoring; actions/evidence; ROPA/DPIA; incident; rights request; notices/consent; vendors/transfers; DPO; security; training; registration; regulatory/policies; reporting/audit room; access assurance; governed AI/document/voice.

Return the completed questionnaire to **sales@itesmw.com** using the agreed secure channel.