Bigeye

Bigeye GPAI Vendor Compliance Questionnaire

By: Joan Pepin | CISO, Bigeye

Assessing your vendors' readiness for the EU AI Act

Purpose

Most organizations are scrambling to understand GPAI compliance requirements for their own AI systems. But there's a critical blind spot: the vendors powering your AI stack may not be ready either.

This questionnaire cuts through vendor marketing claims and compliance theater to reveal whether your AI partnerships can actually support regulatory requirements. It's designed for procurement teams, legal departments, and technical leaders who need concrete answers about vendor GPAI readiness, not vague assurances.

The 12 sections address everything from basic regulatory awareness to technical capabilities and contractual commitments. Each question is crafted to expose gaps that create compliance risk, with clear scoring guidance to help you make informed vendor decisions.

Use this when: evaluating new AI vendors, auditing existing partnerships, or preparing for contract renewals in this new GPAI compliance world.

How to Use

Send this questionnaire to every vendor providing AI models, data processing services, or pipeline components. Score responses using the guide at the end. The 12 sections cover critical GPAI compliance areas, any "No" in Critical sections signals significant compliance risk.

Timelines matter: The **August 2027 compliance deadline** means vendor assessment and remediation must begin now. Vendors need development time, contracts need renegotiation, and alternative evaluation takes time.

Bottom line: No vendor relationship is irreplaceable, but GPAI compliance requirements are definitive. Better to identify gaps during procurement than during regulatory review.

SECTION 1

Basic GPAI Awareness (Critical)

Purpose: Confirm that the vendor understands GPAI requirements, has a defined compliance plan, and is willing to contractually support it.

1. Are you aware of the EU AI Act's requirements for General-Purpose AI models?

- ☐ Yes, and we have a compliance program
- ☐ Yes, but still assessing requirements
- ☐ No / Not sure

Warning: If the vendor isn't aware of GPAI obligations, stop here, they're not compliance-ready.

2. Do you have documented policies for GPAI compliance?

- ☐ Yes (please attach)
- ☐ In development (ETA: _____)
- ☐ No

Note: "In development" policies without clear timelines show poor readiness.

3. Will you provide contractual guarantees for GPAI compliance support?

- ☐ Yes
- ☐ Negotiable
- ☐ No

Note: If a vendor refuses, escalate to legal immediately before proceeding.

4. For models already deployed before August 2, 2025: What's your compliance timeline?

Target date: _____

Tip: Vendors must achieve full compliance before August 2, 2027 to meet EU requirements.

Data Lineage & Documentation (Critical)

Purpose: Ensure the vendor can demonstrate complete, accessible data lineage (down to the column level) across all systems and transformations.

5. Can you provide complete data lineage for your services?

- ☐ Column-level lineage
- ☐ Table-level lineage
- ☐ High-level documentation only
- ☐ No lineage available

Note: GPAI compliance requires column-level lineage visibility

6. How do you document data transformations?

- ☐ Automated documentation with version control
- ☐ Manual documentation, regularly updated
- ☐ Ad-hoc documentation
- ☐ No documentation

Tip: Automated or regularly updated manual documentation both meet compliance expectations.

7. Can you provide real-time or API access to lineage information?

- ☐ Real-time API available
- ☐ Batch exports available (frequency: _____)
- ☐ Manual requests only
- ☐ Not available

Note: Manual-only access introduces operational bottlenecks and increases compliance risk.

8. Do you track data lineage across these specific areas?

- ☐ Source to transformation mapping
- ☐ Transformation to output mapping
- ☐ Cross-system dependencies
- ☐ Version history of changes
- ☐ None of the above

Tip: Vendors should check off the first three items at minimum. Make sure they map data from source → through transformation → to output (and ideally maintain version history of all changes.)

SECTION 3

Training Data (For Model Providers - Critical)

Purpose: Verify that all training data is legally sourced, transparently documented, and retained for regulatory audit.

9. Can you provide complete documentation of training data sources?

- ☐ Yes, with licenses and rights documentation
- ☐ Yes, high-level sources only
- ☐ Partially
- ☐ No - proprietary
- ☐ Proprietary doesn't exempt you from compliance

Warning: "Proprietary" is not a defense for missing documentation, regulators expect verifiable evidence of lawful data sourcing.

10. How do you document training, validation, and test data splits?

- ☐ Complete documentation with data samples
- ☐ Statistical descriptions only
- ☐ High-level percentages
- ☐ Not documented

Tip: At minimum, provide statistical descriptions and sampling methods for each dataset split.

11. Can you prove absence of copyrighted material in training data?

- ☐ Yes, with audit trail
- ☐ We filter known copyrighted sources
- ☐ Best effort basis
- ☐ Cannot guarantee

Note: "Best effort" answers aren't enough, vendors must show evidence of exclusion and audit trails.

12. Do you maintain training data artifacts?

- ☐ Yes, indefinitely
- ☐ Yes, for _____ years
- ☐ No, deleted after training
- ☐ Varies by model

Note: GPAI requires at least 10 years of training data retention for compliance validation.

Preprocessing & Feature Engineering (Important)

Purpose: Confirm that preprocessing steps are documented and traceable, especially where they affect privacy or fairness outcomes.

13. How do you document tokenization and encoding processes?

- ☐ Complete technical documentation
- ☐ High-level description
- ☐ Available on request
- ☐ Proprietary/not shared

Tip: Detailed documentation helps confirm consistent handling of PII and reproducibility of preprocessing steps.

14. Can you trace how PII is handled through preprocessing?

- ☐ Yes, with field-level tracking
- ☐ Yes, at dataset level
- ☐ Partially
- ☐ No

Note: Vendors must track PII at the field level when dealing with sensitive data.

15. Do you document feature engineering that could affect protected attributes?

- ☐ Yes, with bias impact analysis
- ☐ Yes, basic documentation
- ☐ No
- ☐ Not applicable

Note: Lack of bias impact analysis or documentation can create fairness compliance gaps.

Bias Testing & Fairness (Critical for High-Risk)

Purpose: Verify that the vendor regularly tests for and documents bias, and provides transparent results.

16. Do you conduct bias testing on your models/services?

- ☐ Yes, comprehensive testing with documentation
- ☐ Yes, basic testing
- ☐ No, customer responsibility
- ☐ No testing performed

Warning: Vendors cannot defer bias testing to customers, GPAI requires shared responsibility.

17. Which bias metrics do you track?

- ☐ Demographic parity
- ☐ Equal opportunity
- ☐ Disparate impact
- ☐ Custom metrics (specify: _____)
- ☐ None

Tip: Vendors should be tracking at least one of these.

18. Can you provide bias testing results?

- ☐ Yes, detailed reports
- ☐ Yes, summary statistics
- ☐ No - confidential
- ☐ No testing conducted
- ☐ Must have some visibility

Warning: A refusal to share testing results is a major transparency risk.

Monitoring & Observability (Critical)

Purpose: Ensure the vendor provides timely, auditable visibility into model and data performance through accessible monitoring and logging.

19. What operational metrics do you expose?

- ☐ Performance metrics
- ☐ Data quality metrics
- ☐ Drift detection
- ☐ Audit logs
- ☐ None

Tip: Vendors must at least provide access to audit logs to prove compliance readiness.

20. How quickly can you provide audit logs for compliance reviews?

- ☐ Real-time access
- ☐ Within 24 hours
- ☐ Within 72 hours
- ☐ Within 1 week
- ☐ Longer/not available

Note: GPAI requires incident logs to be retrievable within 72 hours.

21. Do you support integration with our observability platforms?

- ☐ Yes, standard integrations (list: _____)
- ☐ Yes, via API
- ☐ Custom integration possible
- ☐ No

Tip: API-based integrations best enable automation and ongoing visibility into your data.

Incident Management (Critical)

Purpose: Confirm that the vendor has a defined process to detect, document, and report incidents within required timelines and with full transparency.

22. What's your incident notification timeline?

- ☐ Within 24 hours
- ☐ Within 72 hours
- ☐ Within 1 week
- ☐ No formal SLA

Note: GPAI regulations mandate notification within 72 hours of a compliance incident.

23. What information is included in incident reports?

- ☐ Root cause analysis
- ☐ Affected data/systems
- ☐ Timeline of events
- ☐ Remediation steps
- ☐ None/ad-hoc

Tip: Complete and compliant reports need to include root cause, affected systems, timeline, and remediation steps.

24. Do you maintain incident history and provide access?

- ☐ Yes, full history with API access
- ☐ Yes, available on request
- ☐ Limited retention (period: _____)
- ☐ No

Note: Long-term, accessible incident history is essential for regulatory audits.

Data Rights & Privacy (Critical)

Purpose: Ensure the vendor protects data subject rights, uses AI-specific contractual safeguards, and discloses all data processing locations.

25. How do you handle data deletion requests?

- ☐ Automated with confirmation
- ☐ Manual process (SLA: _____)
- ☐ Not supported
- ☑ Varies by service

Note: Vendors must support automated or confirmed deletion workflows to meet GDPR requirements.

26. Can you provide data processing agreements (DPAs) that cover AI-specific requirements?

- ☐ Yes, AI-specific DPAs available
- ☐ Standard DPAs only
- ☐ No DPAs
- ☐ Negotiable

Tip: Ensure DPAs explicitly cover AI use cases, model training, and data retention.

27. Do you process data outside the EU?

- ☐ No, EU only
- ☐ Yes, with adequate safeguards
- ☐ Yes, various locations
- ☐ Cannot disclose

Warning: Vendors that cannot disclose processing locations or safeguards should be disqualified.

SECTION 9

Technical Integration (Important)

Purpose: Verify that the vendor's systems integrate seamlessly with your workflows and that version changes are transparent and controlled.

28. What integration methods do you support?

- ☐ REST API
- ☐ GraphQL
- ☐ Webhooks
- ☐ Batch files
- ☐ Manual only

Tip: API-based integrations are essential for real-time automation and monitoring.

29. Do you provide sandboxes for testing?

- ☐ Yes, with production parity
- ☐ Yes, limited functionality
- ☐ No
- ☐ On request

Note: Lack of a sandbox limits your ability to validate integrations safely.

30. How do you handle version updates?

- ☐ Versioned APIs with deprecation notices
- ☐ Blue-green deployments
- ☐ Rolling updates with notice
- ☐ Unannounced updates

Warning: Unannounced updates are unacceptable, they introduce compliance risk.

Human Oversight Support (Critical for High-Risk)

Purpose: Confirm that humans can review, override, and audit AI-driven decisions to maintain control and accountability in high-risk use cases.

31. Do you support human review workflows?

- ☐ Built-in review queues
- ☐ API for custom workflows
- ☐ Manual process
- ☐ Not supported

Tip: Built-in or API-based review queues are required for high-risk models.

32. Can humans override AI decisions in your system?

- ☐ Yes, with full audit trail
- ☐ Yes, limited audit
- ☐ No
- ☐ Not applicable

Note: Override capability must include a full, auditable trail to meet compliance expectations.

Contractual & Legal (Critical)

Purpose: Verify that the vendor accepts liability for GPAI compliance, allows audits, and maintains recognized certifications for security and governance.

33. Will you accept liability for GPAI non-compliance caused by your service?

- ☐ Yes, full liability
- ☐ Shared liability model
- ☐ No liability accepted
- ☐ Negotiable

Warning: Vendors refusing liability transfer unacceptable risk to your organization.

34. Will you support customer audits?

- ☐ Yes, unlimited
- ☐ Yes, annually
- ☐ Yes, for cause
- ☐ No, certifications only
- ☐ No

Note: Vendors should allow at least annual audits as part of the agreement.

35. What certifications do you maintain?

- ☐ SOC 2 Type II
- ☐ ISO 27001
- ☐ ISO 42001 (AI Management)
- ☐ Industry-specific (list: _____)
- ☐ None

Tip: ISO 42001 certification is the gold standard for AI governance and risk management.

Future Readiness

Purpose: Confirm that the vendor has a clear GPAI compliance roadmap and commits to evolving with regulatory standards over time.

36. What's your roadmap for GPAI compliance features?

- ☐ Next 3 months: _____
- ☐ Next 6 months: _____
- ☐ Next 12 months: _____

Note: Note: A vendor leaving this blank signals a lack of planning or investment in compliance readiness.

37. Will you commit to maintaining compliance as regulations evolve?

- ☐ Yes, contractually
- ☐ Yes, best effort
- ☐ Cannot commit

Tip: Contractual commitments provide stronger assurance than "best effort" promises. Look for a vendor willing to provide you with one.

Scoring Guide

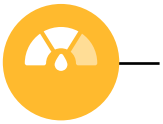
This checklist isn't meant to be graded, it's meant to surface risk fast.

Use your best judgment, but here's a simple way to interpret what you find:

Low Risk:

You're in good shape

If all responses in Critical sections are "Yes" or otherwise acceptable, this vendor understands GPAI compliance and is operating responsibly.

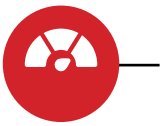


Medium Risk:

Needs follow-up

If there are one or two gaps in Critical sections (for example, policies "in progress" or missing audit details), that's manageable, but only if there's a remediation plan.

Next steps: Ask for timelines and add accountability clauses before you sign anything.



High Risk:

Pause and re-evaluate

If there are three or more "No" responses in Critical sections, or if the vendor refuses to share compliance information, they're not ready.

Next steps: Escalate to Legal or Risk. In most cases, you'll want to look for another option.

Red Flags (Immediate Disqualifiers)

These indicate fundamental non-compliance or refusal to share critical documentation.
If a vendor triggers any of these, stop due diligence and escalate to Legal or Risk immediately.

- No GPAI awareness
- No audit log capabilities
- No liability acceptance
- Proprietary as excuse for no documentation
- Cannot provide training data information (for models)
- No incident reporting SLA

Action:
Disqualify or replace the vendor unless they can remediate and prove compliance within 30 days.

Yellow Flags (Proceed with Caution)

Yellow flags represent gaps that can be fixed, but they require follow-up and contractual safeguards.
These vendors may be viable with a remediation plan and tighter monitoring.

- Manual-only processes
- In development without dates
- Limited retention periods
- No API access
- Shared liability only

Action:
Document gaps, request a remediation timeline, and include compliance checkpoints in the contract.
Proceed only with management approval.

Green Flags (Move Ahead)

These vendors are demonstrating proactive GPAI readiness and strong internal controls.
They understand compliance expectations and can serve as model partners or benchmarks.

- ISO 42001 certification
- Real-time lineage API
- Automated bias testing
- 10+ year retention
- Contractual compliance guarantee
- Human oversight built-in

Action:
Prioritize these vendors for long-term partnerships.

Follow-Up Questions

If vendors push back or claim exemptions, these are your go-to follow-ups to clarify accountability and documentation boundaries.

If they claim “proprietary information”

We get it, vendors want to protect IP. But GPAI doesn’t exempt them from documentation.
Ask them to show enough structure to prove they’re compliant, even if details are redacted.

- **Ask:** We understand IP concerns. Can you share redacted documentation that outlines your process and controls without revealing proprietary elements?
- **Why it matters:** Even redacted proof shows whether a vendor actually has internal governance in place or if they’re winging it.

If they say “that’s customer responsibility”

Shared accountability doesn’t mean you’re off the hook.
Push for clarity on who owns what under GPAI obligations.

- **Ask:** We need to understand where your responsibility ends and ours begins. Can you provide a RACI matrix that defines roles for each GPAI compliance area?

If they have no documentation

No documentation means no audit trail.
You can’t prove compliance with verbal assurances, so use this as a turning point—either they fix it, or you reconsider the partnership.

- **Ask:** What would it take to create the required documentation? Would you be open to building it as part of our contract or onboarding plan?
- **Why it matters:** If they’re willing to create documentation, great. If not, that’s your signal they’re not prepared for regulated markets.

If they refuse audits

Refusing audits is a major red flag. There are plenty of compliant ways to allow oversight without sharing sensitive data.

- **Ask:** Would you consider a third-party audit with shared results? If not, can you provide equivalent certifications such as SOC 2 Type II or ISO 42001 coverage for AI operations?
- **Pro Tip:** Pushback is information. The vendors who resist questions the hardest usually reveal the most about their actual readiness.

Use this template to capture vendor responses, assess initial risk, and document any needed remediation.

Vendor Response Template

Vendor Name: _____

Date Sent: _____ Response Due: _____ (recommend 2 weeks)

Respondent Name/Title: _____

Initial Risk Assessment:

- ☐ Low Risk - Proceed
- ☐ Medium Risk - Negotiate
- ☐ High Risk - Seek alternatives
- ☐ Disqualified - Critical gaps

Required Remediation (if medium risk):

1. _____
2. _____
3. _____

Timeline for Remediation: _____

Legal Review Required: ☐ Yes ☐ No

Business Justification if High Risk: _____