Vendor Risk Memo: bloomberg.com

Generated 2026-08-11 16:40 UTC - Decision support only, not a certification.

INSUFFICIENT DATA | Score 22/100 (F) | Media/Publisher

Executive summary

Bloomberg maintains a mature public-facing security posture, evidenced by active vulnerability disclosure programs and robust email authentication. The primary gap is the lack of publicly available compliance documentation (SOC 2/ISO) for enterprise-grade verification.

Collection was partial - this vendor's site uses bot protection that limits public evidence. Obtain vendor documentation (SOC 2, security whitepaper) directly for a complete assessment.

Key findings

[POSITIVE] Active Vulnerability Disclosure Program

Demonstrates a commitment to external security research and proactive threat identification.

[POSITIVE] Strong Email Authentication

SPF and DMARC records are present, significantly reducing the risk of domain spoofing and phishing attacks.

[MEDIUM] Lack of Public Compliance Transparency

Absence of readily available SOC 2 or ISO 27001 documentation requires manual verification during procurement.

Risk by domain

Compliance	**0/100**	gaps: 6
Data Security	**22/100**	gaps: 4
Operational	**12/100**	gaps: 2

Contract recommendations

- Include a Right to Audit clause for security assessments.
- Require notification of any material data breach within 48 hours.
- Specify data deletion requirements upon contract termination.

Documents to request from bloomberg.com

Based on 18 unverified controls, prioritized by risk impact:

1. **SOC 2 Type II report**
   Please provide your most recent SOC 2 Type II report, including the bridge letter if the audit period ended more than 3 months ago.
2. **Encryption architecture summary**
   Please confirm encryption at rest (algorithm, key management, e.g. AES-256, KMS/HSM).
3. **Access control / SSO documentation**
   Please describe your RBAC model and confirm SSO/SAML support for enterprise accounts.
4. **AI/ML data use policy or DPA with AI clause**
   Please confirm in writing whether customer data is used to train AI/ML models, and if so, whether an opt-out mechanism exists.
5. **ISO 27001 certificate**
   Please provide your current ISO 27001 certificate and the Statement of Applicability.
6. **MFA policy**
   Please confirm MFA is enforced for all employee access to production systems.
7. **Data retention and deletion policy**
   Please provide your data retention schedule and confirm deletion timelines after contract termination.
8. **Subprocessor list**

Please provide your current list of subprocessors and commit to 30-day advance notice of changes.

9. Incident response plan summary

Please provide your incident response plan summary and confirm breach notification timelines (we require 72 hours or less).

10. Latest penetration test attestation

Please provide an attestation letter or executive summary from your most recent penetration test (full report not required).

Detailed control assessment

Control	Answer	Citation / verify note	Weight
SOC 2 Type II report	UNKNOWN	Request the most recent SOC 2 Type II report and bridge letter during the due diligence phase.	15
Data encrypted at rest	UNKNOWN	Request documentation confirming AES-256 encryption for data at rest in the vendor's environmen	10
Data encrypted in transit (TLS)	YES	TLS handshake succeeded, cert expires Jan 29 23:59:59 2027 GMT	10
Access controls / RBAC / SSO	UNKNOWN	Verify if the service supports SAML/SSO integration for enterprise accounts.	10
Trains AI models on customer data	UNKNOWN	Review the Privacy Policy and DPA for clauses regarding the use of customer data for model trai	10
ISO 27001 certification	UNKNOWN	Request a copy of the current ISO 27001 certificate.	10
MFA enforced internally	UNKNOWN	Confirm if MFA is available and mandatory for administrative and user access.	5
Data retention/deletion policy	UNKNOWN	Request the vendor's data retention and destruction policy.	5
Subprocessors disclosed	UNKNOWN	Request a list of material subprocessors used for service delivery.	5
Incident response / breach notification	UNKNOWN	Request a summary of the vendor's incident response plan and breach notification procedures.	5
Penetration testing performed	UNKNOWN	Request an executive summary of the most recent third-party penetration test.	5
Data Processing Agreement available	UNKNOWN	Request the standard Data Processing Agreement for review by Legal.	5
GDPR compliance stated	UNKNOWN	Verify GDPR compliance status via the DPA or privacy documentation.	5
Vulnerability disclosure / bug bounty	YES	security.txt: Vulnerability Disclosure Contact Contact: mailto:reportvuln@bloomberg.net	3
Audit logging	UNKNOWN	Verify availability of audit logs for customer-facing administrative actions.	3
Uptime SLA published	UNKNOWN	Request the published Service Level Agreement (SLA) for uptime guarantees.	3
Employee background checks	UNKNOWN	Confirm if the vendor performs background checks on employees with access to production systems	2
Backups / disaster recovery	UNKNOWN	Request an overview of the vendor's backup and disaster recovery strategy.	2
Vendor's own third-party risk program	UNKNOWN	Request documentation on the vendor's internal third-party risk management program.	2
Data residency / region hosting	UNKNOWN	Confirm the geographic regions where customer data is stored and processed.	2

Verification checklist for bloomberg.com

Items to verify directly with the vendor before signing:

[ ] Request the most recent SOC 2 Type II report and bridge letter during the due diligence phase.

[ ] Request documentation confirming AES-256 encryption for data at rest in the vendor's environment.

[ ] Verify if the service supports SAML/SSO integration for enterprise accounts.

[ ] Review the Privacy Policy and DPA for clauses regarding the use of customer data for model training.

[ ] Request a copy of the current ISO 27001 certificate.

[ ] Confirm if MFA is available and mandatory for administrative and user access.

[ ] Request the vendor's data retention and destruction policy.

[ ] Request a list of material subprocessors used for service delivery.

[ ] Request a summary of the vendor's incident response plan and breach notification procedures.

[ ] Request an executive summary of the most recent third-party penetration test.

[ ] Request the standard Data Processing Agreement for review by Legal.

[ ] Verify GDPR compliance status via the DPA or privacy documentation.

[ ] Verify availability of audit logs for customer-facing administrative actions.

[ ] Request the published Service Level Agreement (SLA) for uptime guarantees.

[ ] Confirm if the vendor performs background checks on employees with access to production systems.

[ ] Request an overview of the vendor's backup and disaster recovery strategy.

[ ] Request documentation on the vendor's internal third-party risk management program.

[ ] Confirm the geographic regions where customer data is stored and processed.