Vendor Risk Memo

bloomberg.com

Generated 2026-08-11 16:51 UTC | Decision support only - not a certification or audit.

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

Executive summary

Bloomberg maintains standard web security hygiene, including active vulnerability disclosure and robust transport encryption. However, the lack of publicly available enterprise-grade security documentation (SOC 2, ISO 27001) necessitates further due diligence before integrating with internal systems.

Key findings

[POSITIVE] Vulnerability Disclosure Program
Provides a clear channel for security researchers to report vulnerabilities, reducing the risk of unpatched exploits.

[MEDIUM] Lack of Enterprise Security Transparency
Absence of public SOC 2 or ISO 27001 documentation prevents verification of internal control effectiveness.

[MEDIUM] Data Sharing Practices
Privacy policy explicitly mentions sharing user information with third parties, which may introduce downstream vendor risk.

Risk by domain

Compliance	Data Security	Operational
0/100	22/100	12/100

Contract recommendations

- Include a Right to Audit clause to verify security controls in the absence of a public SOC 2 report.
- Require notification of any material data breach within 48 hours.
- Include a Data Processing Agreement (DPA) that restricts the use of customer data for AI model training.
- Specify data deletion timelines 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	Wt
SOC 2 Type II report	UNKNOWN	Request latest SOC 2 Type II report and bridge letter.	15
Data encrypted at rest	UNKNOWN	Request documentation on encryption standards for data at rest (e.g., AES-256).	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	Inquire about support for SSO/SAML and RBAC for administrative access.	10
Trains AI models on customer data	UNKNOWN	Confirm in contract that customer data is not used to train public or proprietary AI model	10
ISO 27001 certification	UNKNOWN	Request ISO 27001 certificate or statement of applicability.	10
MFA enforced internally	UNKNOWN	Verify if MFA is enforced for all administrative and user accounts.	5
Data retention/deletion policy	UNKNOWN	Request data retention and deletion policy documentation.	5
Subprocessors disclosed	UNKNOWN	Request a list of current subprocessors and their security compliance status.	5
Incident response / breach notification	UNKNOWN	Request summary of incident response plan and breach notification procedures.	5
Penetration testing performed	UNKNOWN	Request executive summary of the most recent third-party penetration test.	5
Data Processing Agreement available	UNKNOWN	Request standard Data Processing Agreement for review.	5
GDPR compliance stated	UNKNOWN	Verify GDPR compliance statement and data transfer mechanisms (e.g., SCCs).	5
Vulnerability disclosure / bug bounty	YES	bloomberg.com/.well-known/security.txt: Vulnerability Disclosure Contact Contact: mailto:r	3
Audit logging	UNKNOWN	Inquire about audit logging capabilities and log retention periods.	3
Uptime SLA published	UNKNOWN	Request published uptime SLA documentation.	3
Employee background checks	UNKNOWN	Confirm if vendor performs background checks on employees with access to production system	2
Backups / disaster recovery	UNKNOWN	Request summary of disaster recovery and backup testing frequency.	2
Vendor's own third-party risk program	UNKNOWN	Inquire about the vendor's internal third-party risk management program.	2
Data residency / region hosting	UNKNOWN	Confirm 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 latest SOC 2 Type II report and bridge letter.
[ ] Request documentation on encryption standards for data at rest (e.g., AES-256).
[ ] Inquire about support for SSO/SAML and RBAC for administrative access.
[ ] Confirm in contract that customer data is not used to train public or proprietary AI models.
[ ] Request ISO 27001 certificate or statement of applicability.
[ ] Verify if MFA is enforced for all administrative and user accounts.
[ ] Request data retention and deletion policy documentation.
[ ] Request a list of current subprocessors and their security compliance status.
[ ] Request summary of incident response plan and breach notification procedures.
[ ] Request executive summary of the most recent third-party penetration test.
[ ] Request standard Data Processing Agreement for review.
[ ] Verify GDPR compliance statement and data transfer mechanisms (e.g., SCCs).
[ ] Inquire about audit logging capabilities and log retention periods.
[ ] Request published uptime SLA documentation.
[ ] Confirm if vendor performs background checks on employees with access to production systems.
[ ] Request summary of disaster recovery and backup testing frequency.
[ ] Inquire about the vendor's internal third-party risk management program.
[ ] Confirm geographic regions where customer data is stored and processed.