EMBERION DIGITAL LLC

VENDOR RISK ASSESSMENT: MARBLISM

AI GOVERNANCE REVIEW

Gap to Decision: Scope-Based Adoption

Prepared for Emberion Digital, LLC

FINDINGS ◆ RISKS ◆ GUARDRAILS ◆ DECISION

Vendor Assessment | July 31, 2026

www.emberiondigital.com
djones@emberiondigital.com

Vendor Risk Assessment: Marblism

Prepared for	Emberion Digital, LLC
Subject	Risk-scoped adoption assessment: Marblism AI Employee Platform
Date	July 31, 2026
Purpose	Determine whether and how Marblism can be adopted to accelerate business development without creating governance, confidentiality, or credibility exposure for a firm that sells AI governance advisory services.

Bottom Line

Adoption is defensible for a narrowly scoped, documented use case. Adoption without that scoping is the actual risk, both operationally and reputationally. The tool is not the primary risk. Scope of use is.

1. Executive Summary

Marblism is a consumer and small-business SaaS platform offering six pre-built AI agents (email/EA, social media, SEO content, sales outreach, receptionist, legal-document support). Its published trust documentation shows reasonable baseline security practices for a tool in its class: encryption in transit and at rest, workspace-level data isolation, and a contractual prohibition on using customer data to train underlying models from OpenAI, Anthropic, and Google.

The core governance question is not whether Marblism is safe. It is what data will touch it. Used strictly for Emberion Digital's own marketing, outreach, and internal admin, the residual risk is low and manageable. Used for anything touching client deliverables, CUI, federal contract data, or third-party confidential information, the risk profile changes entirely, and becomes inconsistent with the standard you advise clients to hold themselves to.

2. Vendor Findings

Sources: Marblism's published Trust & Security Center, Privacy Policy, and Terms of Service [1] [2] [3]. Re-verified against the live pages on October 20, 2026.

AREA	FINDING
Security certification	CASA Tier 2 (Google Cloud Application Security Assessment), audited by TAC Security. Third-party tested, but a lighter-weight standard than SOC 2 Type II or FedRAMP. SOC 2 and ISO 27001 appear on the Trust Center only as Amazon Web Services attestations for its hosting regions, not as Marblism certifications. [1]
Encryption	TLS 1.2+ in transit; AES-256 at rest. [1]
Data isolation	Workspace-level isolation at the application, database, queue, and object-storage layers. [1]
Model training	Customer content is not used to train Marblism's models or third-party models. OpenAI, Anthropic, and Google act as inference providers under contracts that prohibit training on inference data. [1]
Sub-processors	Eight listed, including AWS, OpenAI, Anthropic, Google Cloud, Stripe, Loops, Sentry, and Mixpanel; all US-based as documented. Full register with DPA references available on request. [1]
Data residency	AWS us-east-1. [1]
Regulatory posture	GDPR listed as "Aligned" and a standard Data Processing Agreement available on request (Trust Center). The Privacy Policy itself does not cite GDPR or UK law by name. No FedRAMP, CMMC, or NIST 800-171 alignment found. [1] [2]

AREA	FINDING
Liability	Limitation of liability excludes indirect and consequential damages and caps total liability at the amount paid in the prior twelve months. Terms state AI outputs are not guaranteed accurate or reliable. Delaware governing law. [3]
Google Workspace access	Trust Center marks the Google API User Data Policy (Limited Use) as compliant. The Privacy Policy describes matching restrictions: no advertising use, no sharing beyond the requested service, and no use of Workspace data to train generalized models. These are stated commitments, not evidence of compliance. [1] [2]

Read as-is, this is a reasonably transparent vendor for its market segment. It is not written or certified for regulated, federal, or CUI-adjacent workloads, and does not claim to be.

3. Risk Assessment

RISK	SEVERITY IF UNSCOPED	SEVERITY IF SCOPED TO INTERNAL BIZ-DEV	NOTES
CUI / federal data exposure	**High**	**Low / None**	No FedRAMP authorization. Any contract data, agency correspondence, or client-shared federal information must never touch this platform.
Client confidentiality (NDA / consulting agreements)	**Medium to High**	**Low**	If future consulting agreements include data-handling clauses, routing client materials through an unauthorized third-party AI platform could itself be a breach.
Credibility / conflict-of-interest optics	**Medium**	**Low**	You are building a practice on AI governance rigor. If a prospect or client asks what AI tools you run your own business on, the answer needs to hold up. Outreach drafting and inbox triage are defensible; touching anything resembling regulated data is not.
Vendor / platform dependency	**Medium**	**Medium**	Subscription-based and lower-commitment than a $2K course, but plan for the platform changing terms, pricing, or disappearing. Do not build irreplaceable workflows on it.
Output reliability	**Low to Medium**	**Low to Medium**	The vendor disclaims AI output accuracy. Anything client-facing (proposals, outreach copy, deliverables) needs human review before it leaves the building.
Data training / IP leakage	**Low**	**Low**	The contractual non-training commitment is a genuine positive signal, assuming it holds.
Account / credential security	**Low**	**Low**	Standard SaaS account risk. Mitigate with a strong unique password and MFA if offered.

4. Recommended Guardrails (If Adopting)

1. **Draw a hard line at the data boundary.** The Marblism workspace connects only to accounts and inboxes used for Emberion Digital marketing, lead generation, and general business admin, never to anything containing client deliverables, contract-specific data, CUI, or federal correspondence.
2. **No client work product runs through it**, even in draft form, unless a future client's engagement terms explicitly permit named third-party AI tools.
3. **Human-in-the-loop on anything outbound.** Treat every Stan (outreach) or Penny (content) draft as a first draft requiring your review before it reaches a prospect, consistent with the disclaimer the vendor itself makes.
4. **Document the decision.** Keep this review on file as your own AI vendor risk-acceptance record. If you advise a client on vendor AI governance, you will have a working example of the process you are recommending they run.
5. **Revisit in 90 days.** Re-assess after initial use. Confirm the non-training commitment and security posture have not changed, and that the tool is saving time rather than adding oversight burden.

5. Bottom Line

Speed and governance are not in conflict here if the use case is scoped correctly. Marblism, used strictly as a business-development accelerant for Emberion Digital's own marketing and outreach, is a reasonable low-risk bet to buy back time. The moment it is used for anything touching a client's data, a federal contract, or CUI, the calculus changes completely. That is not a Marblism-specific problem. It is the same boundary you would tell any client to draw around any unvetted AI tool.

Terms of Use and Disclaimer

This assessment is provided for informational purposes only. It is based on the vendor's published documentation, is not a technical security audit, and does not constitute legal, regulatory, or compliance advice. Vendor terms and certifications change; re-verify before relying on them. Emberion Digital, LLC makes no representations or warranties, express or implied, about any third-party tool named here.

Citations & Sources

Vendor claims in this assessment were checked against the vendor's live pages on October 20, 2026. They reflect what Marblism publishes, not an independent audit.

[1] Marblism. Trust & Security Center.

CASA Tier 2, encryption, workspace isolation, non-training commitment, sub-processors, data residency, GDPR alignment and DPA, Google API Limited Use status.
https://www.marblism.com/trust-center

[2] Marblism. Privacy Policy.

User rights, Google user data commitments, and general security statements. No FedRAMP, CMMC, or NIST 800-171 language.
https://www.marblism.com/privacy-policy

[3] Marblism. Terms of Service.

Limitation of liability (Section 13), AI output disclaimers (Sections 5 and 12), Delaware governing law (Section 16).
https://www.marblism.com/terms-of-service