SECURITY AND PRIVACY RISK ASSESSMENT

WebMintPro Platform

With an external third party posture review

Prepared by Oluwaseun J. Matthew
Governance, Risk, and Compliance
ILLRICH LLC | OJ@WebMintPro.com
June 2026 | Version 1.0

Table of Contents

1. Executive Summary

This report presents an independent security and privacy risk assessment of the WebMintPro platform, a business to business lead generation and website delivery service operated under ILLRICH LLC. The assessment evaluates how the platform identifies, protects, and governs the data it collects and processes, and maps current practice against the NIST Cybersecurity Framework version 2.0.

The report also includes a separate external posture review of OWASP Juice Shop, an intentionally vulnerable application that the Open Worldwide Application Security Project publishes for authorized testing and training. That section demonstrates a third party assessment approach without evaluating any system the assessor is not authorized to test.

Overall, the platform has a sound functional foundation but carries the risk profile common to early stage software built on low code tooling. The most significant exposures relate to access control on the multi tenant data store, management of application secrets, the absence of formal data governance documentation, outbound communications compliance, and limited monitoring and incident response capability. None of the findings indicate an active breach. They are gaps that should be closed before the platform scales its client base and the volume of stored personal data grows.

The assessment identified twelve risks: six rated High, five rated Moderate, and one rated Low. The headline items are summarized below.

- **Multi tenant access control.** Row level security on the shared backend must be verified to prevent one client from reading another client data.
- **Application secrets.** Service keys reachable from the low code front end could be extracted and must be moved server side and rotated.
- **Administrative authentication.** Multi factor authentication should be enforced on all operator and admin accounts.
- **Outbound communications.** Lead outreach and AI voice calling create CAN-SPAM and TCPA obligations that require consent and opt out handling.
- **Governance and response.** Data retention, subprocessor agreements, logging, and a basic incident response plan are not yet documented.

Section 9 sets out a prioritized roadmap that begins with a small set of high impact actions that can be completed quickly, followed by the governance work needed to support growth.

2. Scope and Methodology

2.1 Scope

This assessment covers the WebMintPro web application, its primary data store and authentication service, and the third party services that process platform data. The following are in scope and out of scope.

- **In scope.** The WebMintPro application, its Supabase backend (database, authentication, and storage), payment processing through Stripe, and the artificial intelligence services used by the platform.

- **Out of scope.** Client owned websites delivered to customers as separate engagements, end user devices, physical security, and the internal networks of any third party provider.

2.2 Framework

Findings are organized against the NIST Cybersecurity Framework version 2.0, which is structured around six functions: Govern, Identify, Protect, Detect, Respond, and Recover. Privacy and regulatory considerations are assessed against widely recognized principles, including those reflected in the NIST Privacy Framework, the California Consumer Privacy Act as amended, and the General Data Protection Regulation where applicable.

2.3 Methodology

The assessment followed a documentation and architecture review approach appropriate to a governance, risk, and compliance engagement. It included the steps below.

- Review of the platform architecture, data flows, and the services that store or process data.
- Classification of the data the platform collects and an inventory of where that data resides.
- Identification of risks, each rated by likelihood and impact using the scale in Appendix A.
- Mapping of current practice and gaps to the six NIST Cybersecurity Framework functions.
- A prioritized set of recommendations sequenced by effort and impact.

Because this review is based on the documented architecture rather than direct configuration access, several findings note that production validation is recommended to confirm the current state.

2.4 Authorization and ethics

The WebMintPro assessment was conducted by the system owner. The external review in Section 8 is limited to OWASP Juice Shop, an application that OWASP publishes specifically for authorized security assessment and education. No intrusive testing was performed against any system the assessor is not authorized to evaluate. This boundary reflects a core professional obligation: a security assessment of a system you do not own requires explicit permission and a defined scope.

3. System Overview

WebMintPro is a business to business platform that helps small businesses obtain and maintain a web presence. Operating under the motto Lead, Build, Pitch, it combines lead discovery with website delivery and ongoing maintenance. It is operated under ILLRICH LLC.

3.1 Architecture

The platform is built on a low code development environment with a Supabase backend that provides a managed PostgreSQL database, user authentication, and file storage. Payments are processed through Stripe. The platform uses a large language model service for content generation and offers an optional artificial intelligence receptionist feature delivered through a voice automation provider.

3.2 Roles and tenancy

The platform serves three broad roles: the agency operator who administers the platform, client businesses who subscribe to the service, and prospects whose business details are collected during

lead discovery. Because multiple clients are served from shared infrastructure, tenant isolation is a central control objective.

3.3 Data overview

The platform collects and stores business contact information for prospects and clients, account and billing details, generated website content, and, where the receptionist feature is enabled, call records. This personal and business data is the primary asset the assessment is concerned with protecting.

4. Data Classification and Inventory

The platform handles several categories of data that warrant different levels of protection. A simple four tier scheme is applied: Public, Internal, Confidential, and Restricted. Confidential and Restricted data includes personal information and must receive the strongest controls.

Data type	Classification	Primary storage or processor
Prospect and lead data (business name, contact name, email, phone, website)	Confidential, contains personal data	Supabase database
Client account data (profile, login identity)	Restricted	Supabase Auth
Payment information	Restricted	Stripe (tokenized, reduces card data scope)
Generated website content and assets	Internal	Supabase Storage
AI prompt and response data	Confidential	Language model provider
Call records and transcripts (receptionist feature)	Confidential, may contain personal data	Voice automation provider
Application logs	Internal	Platform and provider logs

Data flows from public facing forms and lead discovery into the Supabase backend, with payment data handled directly by Stripe and selected data passed to artificial intelligence providers for processing. Each external processor represents a point where data leaves direct platform control and where contractual and configuration controls become important.

5. Risk Register

The table below records the risks identified during the assessment. Each risk is rated by likelihood and impact, and the resulting inherent risk rating follows the matrix in Appendix A. Recommended treatments are summarized here and expanded in the roadmap in Section 9.

ID	Risk	Likelihood	Impact	Rating	Recommended treatment
R-01	Multi tenant access control. Incomplete or misconfigured row level security on the shared backend could allow one	High	High	**High**	Review and test all row level security policies, deny by default, and add automated tests for tenant isolation.

ID	Risk	Likelihood	Impact	Rating	Recommended treatment
	client to read another client lead or account data.				
R-02	Application secrets. Service keys reachable from the low code front end could be extracted by inspecting client side code or network traffic.	Medium	High	**High**	Move all secrets to server side functions and environment variables, rotate exposed keys, and never ship service role keys to the client.
R-03	Administrative authentication. Operator and admin accounts may lack enforced multi factor authentication, raising the impact of credential theft or reuse.	Medium	High	**High**	Enforce multi factor authentication on all admin and operator accounts, use a password manager, and review session timeouts.
R-04	Subprocessor agreements. Personal and business data is processed by third parties without documented data processing agreements or a maintained subprocessor list.	Medium	Medium	**Moderate**	Execute or confirm data processing agreements with each provider and maintain a current subprocessor register with data residency.
R-05	Data retention and deletion. Lead and prospect records appear to be retained without a documented retention schedule or deletion process.	Medium	Medium	**Moderate**	Define a retention schedule by data type and implement deletion on request and at end of retention.
R-06	Logging and monitoring. Limited centralized logging of access and administrative actions reduces the ability to detect misuse or investigate events.	Medium	Medium	**Moderate**	Enable database and authentication audit logging, centralize logs, and define basic alerting for anomalous access.
R-07	Incident response. No documented incident response plan or breach notification procedure exists, which would slow and weaken any response.	Medium	High	**High**	Create a lightweight incident response plan with roles, steps, and notification timelines aligned to applicable breach laws.

ID	Risk	Likelihood	Impact	Rating	Recommended treatment
R-08	Visitor privacy and consent. Public pages and forms may collect personal data without a published privacy notice or, where applicable, tracking consent.	Medium	Medium	**Moderate**	Publish a privacy notice, add consent management where tracking is used, and map collection points to a lawful basis.
R-09	AI data handling. Business and contact data sent to language model and voice providers may lack clear data use terms or disclosure to affected individuals.	Medium	Medium	**Moderate**	Confirm provider data use and training terms, disclose AI processing in the privacy notice, and minimize data sent.
R-10	Outbound communications. Lead outreach and AI voice calling create CAN-SPAM and TCPA obligations covering consent, identification, and opt out handling.	High	High	**High**	Maintain consent and suppression lists, honor opt outs promptly, include required identification, and confirm consent before AI calls.
R-11	Access provisioning. As a single operator business, there is no documented process to grant, review, or revoke access if staff or contractors are added.	Low	Medium	**Low**	Document an access provisioning and removal process, apply least privilege, and schedule periodic access reviews.
R-12	Backup and recovery. Backups of the primary data store may not be configured or tested, creating a risk of data loss and extended downtime.	Medium	High	**High**	Confirm automated backups, document recovery steps, and test restoration periodically.

6. NIST Cybersecurity Framework Mapping

The following table maps the current state of the platform to the six functions of the NIST Cybersecurity Framework version 2.0 and identifies the gap to close in each area.

Function	Current state	Gap and recommendation
Govern	Security and privacy decisions are made informally by the owner. There are no	Establish a short set of security and privacy policies, define data ownership, and

Function	Current state	Gap and recommendation
	documented policies or defined data ownership.	document how risk is accepted.
Identify	The architecture and data flows are understood informally. There is no maintained asset or data inventory.	Maintain an asset and data inventory, keep a subprocessor register, and document the system boundary.
Protect	The platform relies on provider defaults for authentication and access control. Secrets management and multi factor authentication are not confirmed.	Enforce multi factor authentication, secure secrets server side, review row level security, and apply least privilege.
Detect	Logging is limited and there is no centralized monitoring or alerting.	Enable audit logging, centralize logs, and define basic alerts for anomalous activity.
Respond	There is no documented incident response plan or breach notification process.	Create a lightweight incident response plan with roles, steps, and notification timelines.
Recover	Backup configuration and recovery testing are not confirmed.	Confirm automated backups, document recovery, and test restoration periodically.

7. Privacy and Regulatory Considerations

Because the platform collects personal data and conducts outbound outreach, several regulatory regimes may apply depending on where the affected individuals are located and how the platform contacts them. The most relevant are summarized below.

- **CCPA and CPRA.** If the platform handles the personal information of California residents at or above the statutory thresholds, obligations include a notice at collection and honoring requests to access, delete, and opt out. Adopting these practices is sound even below the thresholds.
- **GDPR.** If the platform processes the data of individuals in the European Union or the United Kingdom, it must establish a lawful basis, maintain data processing agreements with subprocessors, and support data subject rights.
- **CAN-SPAM.** Commercial outreach email must use accurate header and subject information, identify the message as an advertisement where required, include a valid physical postal address, and provide a working opt out that is honored promptly.
- **TCPA.** The artificial intelligence calling feature raises Telephone Consumer Protection Act obligations. Calls that use a prerecorded or artificial voice generally require prior express consent, and noncompliance can carry significant per call penalties.

The platform should publish a clear privacy notice, maintain consent and suppression records, disclose the use of artificial intelligence in processing and in calls, and confirm calling consent before any automated outreach.

8. External Third Party Posture Review

This section demonstrates an application security and third party risk approach using OWASP Juice Shop, an intentionally vulnerable application maintained by OWASP and provided for authorized

assessment and training. It was selected precisely because testing it is permitted, which allows the methodology to be shown without touching any unauthorized system.

A full authorized engagement would combine automated scanning with manual testing inside a dedicated environment. Because Juice Shop is designed to demonstrate the OWASP Top 10, the table below maps those categories to the control themes a reviewer would expect to address. These themes mirror several findings in the WebMintPro assessment, in particular access control, secrets and cryptography, and logging.

OWASP Top 10 (2021) category	Relevance in the target	Control recommendation
A01 Broken Access Control	The target intentionally exposes broken access control, such as reaching another user data or administrative functions.	Enforce server side authorization on every request and deny by default.
A02 Cryptographic Failures	Sensitive data may be weakly protected or unencrypted.	Use current strong algorithms, encrypt data in transit and at rest, and protect keys.
A03 Injection	Input handling allows injection, including database injection.	Use parameterized queries, validate input, and encode output.
A04 Insecure Design	Design level weaknesses are present by intent.	Apply threat modeling and secure design patterns early in development.
A05 Security Misconfiguration	Default and permissive configurations are present.	Harden configurations, remove defaults, and limit error detail returned to users.
A07 Authentication Failures	Authentication and session handling are weak.	Enforce strong authentication, multi factor authentication, and secure sessions.
A09 Logging and Monitoring Failures	Logging is insufficient to detect or investigate attacks.	Implement comprehensive protected logging with alerting.

The shared lesson across both the internal and external reviews is consistent: strong server side access control, careful secrets and key management, and reliable logging are the controls that most reduce risk for web applications of this kind.

9. Prioritized Remediation Roadmap

The recommendations are sequenced so that the highest impact and lowest effort actions come first, followed by the governance work that supports safe growth.

9.1 Quick wins (0 to 30 days)

- Enforce multi factor authentication on all operator and admin accounts.
- Move application secrets server side and rotate any keys that were reachable from the client.
- Review and test row level security to confirm tenant isolation.

- Publish a privacy notice and document how outreach opt outs are handled.

9.2 Short term (30 to 90 days)

- Execute or confirm data processing agreements and build a subprocessor register.
- Define a data retention and deletion policy by data type.
- Enable audit logging and basic alerting for access and administrative actions.
- Write a lightweight incident response plan with roles, steps, and notification timelines.

9.3 Longer term (90 days and beyond)

- Establish a recurring vendor and third party risk review.
- Confirm and periodically test backups and recovery.
- Build a simple, repeatable security awareness habit for anyone with access.
- Assess readiness for a SOC 2 or comparable attestation if the client base and data volume grow.

10. Conclusion

The WebMintPro platform is functional and serves a clear business purpose, and its risk profile is typical of an early stage application built on low code tooling. The findings in this report are not signs of an active compromise. They are addressable gaps, and the majority of the highest rated items can be closed with focused, low cost effort: enforcing multi factor authentication, securing secrets, verifying tenant isolation, and putting basic governance and response practices in place.

Closing these gaps before the platform scales will protect the personal data it holds, reduce regulatory exposure from its outreach activities, and position the business to meet the security expectations of larger clients.

Appendix A. Risk Rating Methodology

Each risk is rated on two dimensions, likelihood and impact, using the definitions below. The inherent risk rating is derived from the combination shown in the matrix.

- **Likelihood.** Low means the condition is unlikely under current conditions. Medium means it is plausible. High means it is likely or already present.
- **Impact.** Low means a minimal effect. Medium means a moderate operational, financial, or privacy effect. High means a significant data breach, regulatory, or business continuity effect.

Risk rating matrix:

Likelihood \ Impact	Low	Medium	High
Low	Low	Low	Moderate
Medium	Low	Moderate	High
High	Moderate	High	High

Appendix B. References

- NIST Cybersecurity Framework version 2.0, National Institute of Standards and Technology.
- NIST Privacy Framework, National Institute of Standards and Technology.
- OWASP Top 10 (2021), Open Worldwide Application Security Project.
- OWASP Juice Shop project, Open Worldwide Application Security Project.
- California Consumer Privacy Act, as amended by the California Privacy Rights Act.
- General Data Protection Regulation, European Union.
- CAN-SPAM Act, United States Federal Trade Commission.
- Telephone Consumer Protection Act, United States.

Appendix C. About the Assessor

Oluwaseun J. Matthew is an independent technologist focused on governance, risk, and compliance. He holds the CompTIA Security+ certification along with HIPAA and bloodborne pathogens training, and builds and operates production web applications, which informs a practical, system level view of security and privacy risk.

This document is a portfolio sample prepared to demonstrate risk assessment methodology, framework mapping, and clear reporting. Contact: OJ@WebMintPro.com.

Disclaimer: This assessment is based on the documented architecture of the platform and is intended for illustrative and portfolio purposes. A production engagement would include direct configuration review and validation of the findings noted throughout.