ObituaryMonitor

Security Whitepaper

How ObituaryMonitor protects customer data

Version 1.1 | November 2026

Northgate Leland LLC | 214-206-4534 | obituarymonitor.com

Document Information

Company:	Northgate Leland LLC
Brand:	ObituaryMonitor
Document:	Security Whitepaper (Public)
Version:	1.1, November 2026
Owner:	Keith Thomas, Owner
Contact:	security@obituarymonitor.com | 214-206-4534
Website:	obituarymonitor.com
Next Review:	November 2027

Summary

ObituaryMonitor is a brand of Northgate Leland LLC, a Texas company based in Dallas. We provide obituary monitoring and death verification services to law firms, insurers, financial services companies and other businesses through a web portal and the Verify API.

This document describes how we host, protect and handle customer data today. It is written to support vendor security reviews.

ObituaryMonitor has not completed a SOC 2 audit or any other third party security certification. Where this document names a certification, it is held by the named provider, not by ObituaryMonitor.

Contents

1. Company and Security Ownership 3
2. Architecture and Hosting 4
3. Encryption 5
4. Access Control and Authentication 6
5. Logging, Monitoring and Backups 7
6. Data Privacy 8
7. Sub-processors 9
8. Data Retention and Deletion 10
9. Incident Response 11
10. Certifications and Contact 12

1. Company and Security Ownership

Northgate Leland LLC is a small company. Keith Thomas, the owner, is responsible for information security. He approves production changes, access to production systems, data changes and the providers we use. There is no separate security team or Chief Information Security Officer.

Data we process:

• Customer account data: names, business email addresses, company names, billing contacts and sign-in records (time, IP address and browser).
• Customer submitted data: details of people a customer asks us to monitor or verify, such as name, date of birth, city and state.
• Public obituary data: information from published obituaries and funeral home notices, such as name, date of death, location and funeral home, with a link to the source.
• Payment data: handled by Stripe. We do not receive or store full card numbers.

Our obituary data does not include Social Security numbers or financial account numbers.

2. Architecture and Hosting

Our systems and our stored data are in the United States. Some outside services we call are described in section 7.

• Website and customer portal: hosted on Netlify. Pages and server functions run on Netlify's platform.
• Verify API: runs on our own virtual server at IONOS (api.obituarymonitor.com) behind the Caddy web server.
• Primary database: Supabase managed PostgreSQL, hosted on AWS in the US West (Oregon) region.
• Background processing: our own virtual servers at IONOS run scheduled jobs that collect public obituary records, run verification searches and build structured summaries. One of these servers holds a synced copy of the database for those jobs.
• Job queue and cache: Upstash.

How a request flows:
A browser or API client connects over HTTPS to Netlify (portal) or to our API server (Verify API). Both connect to the database over TLS. Background servers load public web pages and call the search and AI providers listed in section 7.

3. Encryption

In transit:

• The website, customer portal and Verify API accept TLS 1.2 and TLS 1.3 only. TLS 1.0 and 1.1 connections are refused.
• The website sends an HSTS header so browsers always use HTTPS.
• Certificates are issued by Let's Encrypt and renew automatically.
• Our application requires TLS when it connects to the Supabase database. Connections to the database copy on our own server use TLS over the IONOS private network.
• Calls to payment, email, search and AI providers use HTTPS.

At rest:

• Supabase encrypts stored database data with AES-256, as stated in Supabase's published security documentation.
• Netlify encrypts data at rest with AES-256, as stated by Netlify.
• Data on our own IONOS servers is protected by the access controls in section 4. We do not claim disk level encryption on those servers.

Credentials:

• Passwords are hashed with bcrypt (cost factor 10) and a unique salt. Plain text passwords are never stored.
• API keys are stored as a SHA-256 hash for lookup, plus a copy encrypted with AES-256-GCM so the account owner can view the key again in the portal. The encryption key is kept in server configuration, not in the database.
• Provider credentials are kept in server and hosting configuration, not in source code.

4. Access Control and Authentication

Customer accounts:
• Customers sign in with email and password. A session is a signed token in a Secure, HTTP-only cookie that expires after 7 days.
• We can end all of a user's sessions at once, for example after a suspected compromise.
• Account owners can invite team members with full or read-only access.

Staff roles:
• The platform has three roles: user (customers), sales (limited staff access for demos and account setup) and admin (full staff access). Only the owner holds the admin role.
• When staff open a customer's account view, the start and end are recorded in the activity log.

API keys:
• Each key belongs to one customer account and is either a live key or a test key.
• Customers can revoke or rotate keys at any time in the portal. A revoked key stops working immediately.
• Keys can have an expiry date and an IP allowlist.
• The Verify API enforces per-account quotas and rate limits.

Webhooks:
• Webhooks we send to customers are signed with HMAC-SHA256 so the receiver can confirm they came from us.
• Webhooks we receive from Stripe and from our job queue are checked against their signatures before we act on them.

Production access:
• Only the owner, and automated tools he runs and approves, can access production servers and databases. Access is over SSH or encrypted database connections.
• Routine database checks are run read-only. Before any data change we take a backup and prepare a way to undo it.
• Source code is in a private GitHub repository. Changes are made through pull requests with automated tests, and the owner approves each merge and production deploy.

5. Logging, Monitoring and Backups

Logging:
• The portal keeps an activity log of sign-ins, sign-outs, sign-ups, subscription changes, staff access to customer accounts and admin changes, with time, IP address and browser.
• Each Verify API request is recorded with the API key, time and result. We use these records for billing, support and security review.
• Our servers keep system and application logs. Netlify keeps logs for portal functions.

Monitoring:
• Automated checks watch the Verify API, background jobs and data pipelines, and alert the owner by email when something fails.

Server upkeep:
• Automatic security updates are turned on for our servers.
• The API server runs a host firewall that allows only the ports it needs.

Backups:
• Supabase backs up the primary database.
• A synced copy of the database is kept on our own database server.
• The API server is backed up with Acronis Cyber Protect.

6. Data Privacy

• We do not sell personal information.
• We use customer submitted data to provide the service the customer asked for, and for billing, support and security.
• We store and process customer data in the United States, apart from the outside services listed in section 7.
• AI providers receive public obituary text to produce structured fields and summaries in our own words. When needed for matching, they may also receive the name and details being checked.
• Customers can ask to access, correct or delete their personal information by email. We confirm the request comes from the account holder and respond within the time required by applicable law, such as the CCPA.
• We have not appointed a Data Protection Officer. The owner handles privacy requests.
• We can sign a data processing agreement with business customers on request. A customer agreement can set stricter terms, such as a shorter retention period for API request data.

Healthcare:
We do not process protected health information and do not offer Business Associate Agreements.

7. Sub-processors

These providers process customer data or run systems that hold it. Certifications are listed only where the provider publishes them. They belong to the provider, not to ObituaryMonitor.

• Netlify, Inc.: website and customer portal hosting. United States. SOC 2 Type II, ISO/IEC 27001.
• Supabase, Inc.: primary PostgreSQL database (AWS US West, Oregon). United States. SOC 2 Type II.
• IONOS Inc.: virtual servers for the Verify API, background processing and the database copy. United States. ISO/IEC 27001 certified data centers.
• Stripe, Inc.: payments and billing. United States. PCI DSS Level 1.
• Upstash, Inc.: job queue and cache. SOC 2 Type II.
• Microsoft Corporation (Microsoft 365): business email. SOC 2 Type II, ISO/IEC 27001.
• Hostinger: email hosting and outgoing service email (account, alert and billing notices).
• OpenRouter, Inc.: AI model access for structured fields and generated summaries. United States. SOC 2 Type II.
• Serper: web search service used during verification. Search terms can include the name being checked.
• Google (Google Maps Platform): address geocoding.
• RapidAPI: API marketplace, used only for customers who buy API access through RapidAPI.

We review a provider's published security information before we start using it. A current list is available from security@obituarymonitor.com.

8. Data Retention and Deletion

Retention:

• Customer account data: kept while the account is open. Deleted within 30 days after the customer asks us to close and delete the account, except records we must keep by law.
• Watches, matches and reports: kept while the account is open and deleted with the account.
• Verify API request records: kept for billing, support and security review. Where a customer agreement sets a shorter period, we follow the agreement.
• Activity and sign-in logs: kept while the account is open. They are not deleted on a fixed schedule today.
• Payment and invoice records: kept by Stripe and in our accounting records for as long as tax and accounting rules require.
• Public obituary data: kept as part of our ongoing records database.
• Backups: deleted data can remain in provider backups until those backups expire on the provider's schedule.

Deletion:

Customers can ask for deletion by emailing support@obituarymonitor.com or privacy@obituarymonitor.com. We delete the account and the watches, matches and API keys linked to it. Self-service account deletion is not available in the portal today.

Export:

Customers can export their watches and matches as CSV from the portal, and matches as JSON. Verify batch results can be downloaded as CSV.

9. Incident Response

Keith Thomas leads our response to any security incident.

1. Detect: automated alerts, log review, and reports from customers, providers or security researchers.
2. Contain: revoke affected API keys or sessions, rotate credentials, block traffic, or take an affected service offline.
3. Assess: use activity logs, API request records and server logs to find what happened and which data and customers were affected.
4. Fix and recover: fix the cause, restore from backups where needed, and confirm systems are working normally.
5. Notify: tell affected customers without undue delay, and within 72 hours after we confirm an incident that affected their data, or sooner if their agreement requires it. We also make any notices the law requires.
6. Review: record what happened and what we changed to prevent it happening again.

Report a security concern to security@obituarymonitor.com or call 214-206-4534.

10. Certifications and Contact

Certifications:
ObituaryMonitor has not completed a SOC 2 audit and has not had an independent penetration test. We can complete customer security questionnaires on request.

Security:
Keith Thomas, Owner
Email: security@obituarymonitor.com
Phone: 214-206-4534
We reply to security reports within one business day.

Privacy requests: privacy@obituarymonitor.com
Support: support@obituarymonitor.com

Northgate Leland LLC (ObituaryMonitor)
633 W. Davis St. Suite A PMB 1269
Dallas, Texas 75208

This document describes our practices as of November 2026. We review it at least once a year and when our systems or providers change. For questions, contact security@obituarymonitor.com.