CrossPeak

# Beyond the SSL Illusion:

## *Why Your Gravity Forms Data is Sitting in Plain Text (and How to Fix It)*

05212026

## Executive Summary

In today's hyper-regulated digital landscape, data privacy is no longer a luxury—it is a baseline operational requirement. Organizations worldwide rely on WordPress and Gravity Forms to capture everything from standard lead generation details to highly confidential information, including medical histories, financial accounts, legal intake data, and personally identifiable information (PII).

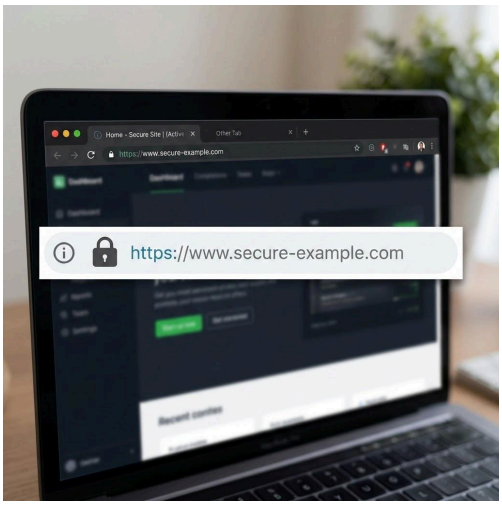
However, a dangerous security blind spot exists within the WordPress ecosystem. While millions of site owners believe their forms are secure because their website uses an SSL certificate (HTTPS), this only protects data in transit. Once a user clicks "Submit," Gravity Forms stores that information in the WordPress database as plain, unencrypted text.

If a malicious actor bypasses your perimeter defenses, compromises your hosting environment, or steals a database backup, your customers' private data becomes instantly readable. This whitepaper explores the mechanics of this vulnerability, the regulatory and financial risks of leaving data exposed, and how the CrossPeak Gravity Forms Encryption Plugin provides enterprise-grade, AES-256 encryption at rest—seamlessly, effortlessly, and without breaking your workflow.

# The Plain-Text Trap (The Illusion of Total Security)

## The SSL Misconception

Ask the average WordPress administrator if their forms are secure, and they will likely point to the padlock icon in the browser address bar. They have installed an SSL/TLS certificate, meaning data traveling from the user's browser to the web server is encrypted.




**But what happens when that data arrives?**
Once the data is processed, WordPress writes it to the database **(wp_gf_entry_meta)**. By default, it is written exactly as it was typed. Names, phone numbers, addresses, social security numbers, and corporate secrets sit in plain text.

## Why Your Database is a Target

Perimeter security (firewalls, security plugins, strong passwords) is essential, but it is not infallible. Database exposure happens through multiple vectors:

- **SQL Injection (SQLi) Vulnerabilities:** Found in third-party plugins or themes, allowing hackers to query and download database tables directly.
- **Unsecured Backups:** Automated database backups stored in public directories, unencrypted cloud storage buckets, or downloaded onto local developer machines.
- **Server Misconfigurations:** Exposed database ports or compromised hosting control panels (cPanel, SSH keys).
- **Insider Threats:** Disgruntled employees or contractors with low-level database access who can view records they shouldn't see.

If your data is sitting in plain text, a single breach in any of these areas results in total data exposure.

CrossPeak

# The Cost of Exposure: Compliance and Trust

Leaving user data unencrypted at rest isn't just a technical oversight; it's a massive legal and financial liability.

## Regulatory Penalties

Data protection authorities worldwide have shifted from passive guidelines to aggressive enforcement:

- **GDPR (General Data Protection Regulation):** Explicitly mandates "pseudonymization and encryption of personal data" (Article 32). Non-compliance can lead to fines of up to €20 million or 4% of global annual turnover.
- **CCPA/CPRA (California Consumer Privacy Act):** Gives consumers the right to sue businesses if their unencrypted personal information is stolen in a data breach.
- **HIPAA & PCI-DSS:** Storing protected health information (PHI) or financial workflows in plain text violates core data-at-rest protection standards, leading to immediate audits, loss of processing privileges, and heavy penalties.

## The Erosion of Brand Trust

Beyond fines, a data breach destroys a company's reputation. When customers find out their private data was stored without basic encryption safeguards, trust vanishes overnight. Rebuilding a brand after a public plain-text data leak costs exponentially more than implementing proactive security measures.

CrossPeak

# The Solution: CrossPeak Gravity Forms Encryption

The solution is not to stop using Gravity Forms—the most robust form builder on WordPress—but to complement it with enterprise-grade data security.

The **CrossPeak Gravity Forms Encryption Plugin** closes the plain-text loophole by automatically encrypting sensitive form data *before* it is committed to the WordPress database.

**[ User Submits Form ] ---> [ SSL Transit ] ---> [ CrossPeak Encryption (AES-256) ] ---> [ Encrypted Database Storage ]**

## Key Pillars of the CrossPeak Solution:

1. **True Encryption at Rest:** Sensitive fields are scrambled into unreadable cryptographic strings using military-grade AES-256 encryption via PHP's native OpenSSL extension. Even if a hacker dumps your database, they see nothing but randomized characters.

2. **Seamless Administrator User Experience:** Security shouldn't ruin your workflow. When an authorized administrator logs into the WordPress backend to review Gravity Forms entries, the plugin decrypts the data *on the fly*. Authorized users see the data normally; unauthorized database viewers see absolute gibberish. There is zero change to your daily routine—decryption happens instantly and invisibly in the background for logged-in admins.

3. **No External Dependencies:** Your data stays on *your* server. The plugin doesn't rely on third-party cloud APIs to process or store keys, keeping you in complete control of your data lifecycle.

CrossPeak

# Comprehensive Protection Across the Data Lifecycle

Data security isn't limited to standard text boxes. The CrossPeak plugin provides a holistic shield across three vital data vectors: Fields, Files, and Email Notifications.

## 1. Granular Field-Level Encryption

Not all data requires encryption. You don't need to encrypt a generic "How did you hear about us?" dropdown, but you absolutely must encrypt a "Tax ID Number" or "Medical History" paragraph field. CrossPeak allows you to toggle encryption on a field-by-field basis for standard and advanced field types, including:

- Single Line & Paragraph Text
- Dropdowns, Checkboxes, and Radio Buttons
- Names, Dates, Times, and Phone Numbers
- Multi-selects, Lists, and Addresses

## 2. Secure File Upload Encryption

One of the biggest security gaps in WordPress forms is the handling of uploaded files (e.g., driver's licenses, bank statements, medical records). Normally, these are saved to a predictable directory on your server (/wp-content/uploads/gravity_forms/), where anyone can download them via the direct URL.

- **The CrossPeak Advantage:** Our plugin encrypts uploaded files directly on disk at the moment of submission. The file name is randomized into a secure string, and the contents are locked. When an authorized admin downloads the file via the WordPress dashboard, the plugin seamlessly decrypts it and restores the original filename.

CrossPeak

### 3. Plugging the Email Leak

Email is inherently insecure. If Gravity Forms sends standard email notifications containing sensitive data, that data travels across the internet in plain text and sits indefinitely in local mailboxes.

- **Default Security Shield:** CrossPeak automatically intercepts outbound email notifications. Any field marked for encryption is replaced with a secure placeholder, ensuring sensitive data never leaks into email loops.

- **Granular Control:** If your workflow requires it, you can explicitly override this feature for verified secure email setups using strict TLS configurations via our "Show Decrypted Values in Email" setting.

## Under the Hood: Technical Architecture

For developers, security architects, and IT managers, the technical implementation matters. CrossPeak is built following modern, rock-solid cryptographic standards.

- **Cryptographic Standard:** Utilizes industry-standard **AES-256 encryption** via the PHP OpenSSL extension with a 32-byte (256-bit) key.

- **Isolated Key Management:** The generated encryption key is stored outside of the standard database tables in a dedicated configuration file (**wp-content/gf_encryption_configuration.php**).

- **Environment Variable Compatibility:** For high-security or enterprise-hosting setups (such as AWS, Kinsta, WP Engine), developers can move the encryption key entirely out of the file system and load it via a server environment variable using the **CROSSPEAK_GRAVITYFORMS_ENCRYPTION_KEY con**stant in **wp-config.php**.

CrossPeak

# Conclusion & Action Plan

If your organization collects user data through WordPress, you must ask yourself the question driving today's security-conscious brands: **Is your customer data sitting in plain text?**

Relying solely on SSL is an outdated and incomplete security posture. Protecting your users, complying with global privacy mandates, and defending your brand reputation require encryption at rest.

## Step-by-Step Implementation Plan:

1. **Audit Your Forms:** Identify every Gravity Form on your site collecting PII, financial info, or confidential attachments.
2. **Deploy CrossPeak Gravity Forms Encryption:** Install the plugin to instantly unlock enterprise-grade AES-256 field and file locking capabilities.
3. **Configure Your Keys:** Back up your encryption key locally or isolate it via server environment variables.
4. **Gain Peace of Mind:** Rest easy knowing that even in a worst-case database breach scenario, your customer data remains entirely secure and unreadable.
5. **Download the plugin:** Visit CrossPeak Software to secure your forms today.

Don't wait for a database breach to reveal your security blind spots. Lock down your forms, protect your users, and build unshakeable digital trust today.