VGS Guide to De-identifying Service Usage Data

Data: The Double-edged Sword

Business today runs on data. Harnessed and used correctly, data sparks innovation, drives growth, helps organizations beat the competition, leads to higher customer retention and increased expansion.

Product-led organizations have a wealth of data waiting to be tapped in (as the name 'product-led' indicates) the product. They can do things like examine the data around the sign-up flow users take to convert from free to a paid subscription to determine broken steps, or A/B test different product variations to improve conversion rates or customer loyalty.

Inevitably, however, some sensitive personal information belonging to users is wrapped up in product data. This sensitive personal data is called personally identifiable information (PII). And this is where the challenge begins.

The Challenges of Securing PII

Protecting PII and meeting compliance for regulations such as GDPR, CCPA, LGDP, the upcoming CDPA and beyond is a challenging task. It often requires diverting critical resources away from revenue-generating projects. Misusing or losing PII can result in stiff fines, financial loss, and damage to your company's reputation (not to mention a violation of your existing privacy policy).

Even understanding exactly what data is considered PII can be confusing as most regulations are vague on this point. PII is any information that can be used to identify a specific individual (including consumers and employees). It can include an individual's name, work or personal email address, phone number, social security or driver's license number, birth date, login IDs, IP addresses, and many other pieces of information.

Another significant challenge is the lack of prescriptive guidelines explaining what safeguards or controls are needed to protect PII. This lack of specificity makes it difficult to securely collect, process, store, and disseminate PII.

For example, PII data can be emailed in cleartext. PII data can also be exposed when a customer provides their home address to a customer service representative. Even web forms have some risk of exposing PII (e.g., customers may unknowingly enter personal information into a web form infected by malicious JavaScript).

Storing PII in your environment also has its challenges requiring research and investment in encryption technology, deploying strong access controls and other data protection solutions, followed by continuous monitoring and management of your security infrastructure.

Who Needs Access to PII Data?

One way companies attempt to de-identify data is through access controls. Often, they will provide access to sensitive data only to a certain subset of users like site reliability or support engineers. The challenge here is that data is still identified somewhere on company systems.

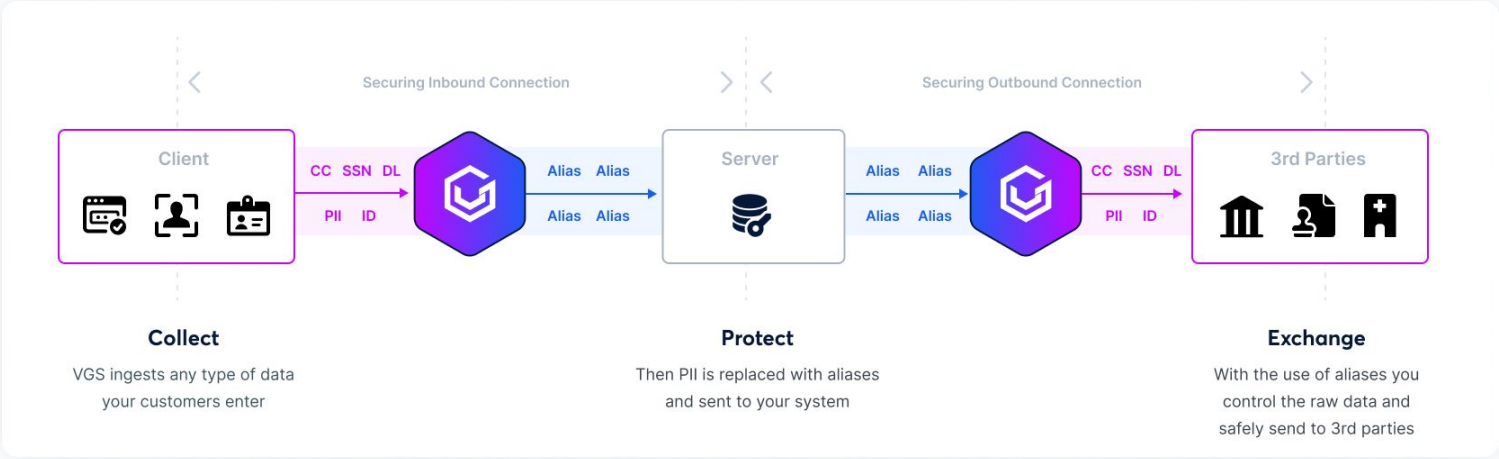
While this may meet an objective to de-identify users before information lands somewhere like an analytics environment, and before "non-secure" users (sales, marketing, UX, etc.) can see sensitive data, **it leaves sensitive data in the company's environment and exposed to the risk of data breach.**

There is a better way: offload your PII data so it never touches your servers, while maintaining full analytics utility.

De-identify with All of the Value, None of the Data

Very Good Security is on a mission to protect the world's sensitive data, enabling innovation while ensuring security and privacy. Data security and compliance are hard enough without the new economic headwinds businesses are facing today. **You should never have to choose between protecting your most precious data and growing your business. With VGS, you do not have to.**

Companies can collect and de-identify sensitive data for analytical purposes through VGS.



VGS allows companies to collect sensitive user, namespace, or account related information by:

1) Using VGS's aliasing technology to de-identify keys for data security during transit and rest in the VGS Vault.

2) Retrieving data from the VGS Vault by creating one source data model filtering for namespace records with more than 1 user to allow for further identification and analysis. Also, creating one source data model filtering for data from single user namespaces for aggregated analysis only. This will allow organizations to prevent identification of usage data related to one-person namespaces.

By adopting VGS, companies are able to store and retain their historical de-identified data for product analytics or advanced data analytics.

The following pages explore the VGS Vault technology in more detail.

VGS Vault

Technical Whitepaper

[VGS Vault](#)
[Vault Security](#)
[Inbound Connections](#)
[Outbound Connections](#)
[VGS Dashboard Security](#)
[Operational Security](#)
[VGS Code Security](#)
[Business Continuity Planning](#)

VGS Vault

The Very Good Security (VGS) Vault, a core component of the **VGS Zero Data™ Platform**, is a unique environment where you can securely store your sensitive data. VGS assumes the technical responsibility and legal liability of safeguarding your information, so that you can simply focus on growing your business and profits.

Examples of sensitive information that we secure in the VGS Vault are: payment data, personally identifiable information (PII), passwords, private keys, environment variables, and SIEM data. By working with VGS, you can reduce your compliance certification tasks by over 90% and quickly achieve certifications such as PCI and SOC2, as well as be compliant with regulations such as HIPAA and GDPR.

Now, your data becomes even more valuable to you. While your sensitive data is protected in the VGS vault, you immediately receive an “alias” of it that can be used to perform business transactions. This alias by itself means nothing, even if lost, hacked, or stolen, so no data thief or hacker can ruin your business or its reputation. Thus, you can store and process your data in many more ways than you could before, worry-free.

The VGS Vault lives in a highly available AWS virtual private cloud (VPC) where uptime is guaranteed and average latency is 100 milliseconds or less. At VGS, we process millions of requests every day, have robust system backups, business continuity planning, disaster recovery, and incident response.

Vault Security

Within the VGS Vault, your company's sensitive data is located in a logically segregated, exclusive "customer vault", that belongs only to you. Your data is always protected with multiple layers of security, but you may configure your own unique account-based access rules.

Inside the VGS Vault, data is encrypted at-rest with the Advanced Encryption Standard, adopted by the US Government in 2001 and now used worldwide. VGS uses AES-256-GCM, the longest and most robust AES key size. Your data is further protected with the latest Authenticated Encryption with Associated Data (AEAD) mode symmetric ciphers.

VGS key management is state-of-the-art. We use dedicated hardware security modules (HSM) for key storage. Encryption and decryption keys are kept in highly-secure, separate envelopes that are segmented from your vaulted data. Keys are rotated on a regular basis. Key access requires multiple layers of authentication. Role-based access controls ensure that only the VGS Vault application processes can touch the encrypt and decrypt operations. Data thieves and hackers cannot make use of any stolen information without the keys.

Clients have two choices for data aliasing: multiple token formats as defined by ANSI X9.119-2-2017 (Tokenization), in which your sensitive data is replaced with a data token; and NIST SP800-38G (Format Preserving Encryption), in which the output preserves the format of your original data.

The VGS Vault is continuously hardened against infrastructure, system level, and configuration vulnerabilities and exposures. It is shielded against viruses and other forms of malware.

We regularly test our systems, and always apply the latest applicable security patches and secure configurations to all operating systems, containers, applications, and infrastructure, to minimize exposure to vulnerabilities.

The VGS platform is continuously scanned using best-of-breed security experts and tools, including HackerOne. We undergo regular application and network vulnerability assessments, including architecture reviews, performed by independent Managed Security Services Providers (MSSP). VGS conducts annual internal/external penetration tests and bi-annual segmentation tests. All vulnerabilities discovered are documented and immediately remediated, including post-mortem analyses to identify root causes and implement future controls.

VGS employs 24/7 threat monitoring, intrusion detection, anomaly analysis, threat analytics, end-to-end event correlation, audit logging, change management controls, and traceability. VGS monitors, tests, and reviews all employees, customers, vendors, and operations, and we investigate all suspicious behavior and unauthorized activities.

The VGS incident response program includes clearly documented escalation and notification procedures. All incidents and vulnerabilities are immediately escalated to our security team, evaluated, risk ranked, and assigned for resolution by trained VGS personnel. Remediation takes place with minimal customer impact and interaction. We provide detailed customer post-mortems for all major incidents within 3 business days.

Inbound Connections

Our static, inbound/reverse proxy sits between your client and server. It directs traffic to the VGS Vault, where your sensitive data is stored. Key benefits of VGS architecture include the ability to: rewrite requests/responses before data enters or leaves your system, operate on data outside the scope of your backend systems, set/change/strip headers, and modify payloads beyond simple redaction/replacement.

In the VGS dashboard, simply point your client application to our reverse proxy and set the upstream to your server URL. You may also load your client website/app through the proxy. VGS protects your data in-motion via Transport Layer Security (TLS) 1.2 or 1.3, with Authenticated Encryption mode ciphers.

“VGS Collect” is the easiest way to securely collect sensitive data from any end-user interface. You quickly create forms that adhere to PCI, HIPAA, GDPR, or CCPA requirements, and have complete control over the look and feel of the input fields. VGS Collect isolates the sensitive data from your client side code, sending it directly to our proxy, which intercepts any sensitive data before it touches your servers, secures it in your tenant vault, and replaces it with aliased versions that you can use without worry.

Outbound Connections

The VGS outbound/forward proxy expands on the capabilities of the inbound/reverse proxy. It sits between your server and your third party integrations, and also directs traffic to the VGS vault. In your dashboard, simply set your server to send traffic through our outbound/forward proxy, and you have the option to create routes, filters, and operations for different API endpoints.

As with the inbound connection, you can rewrite requests/responses on the fly, operate on data outside the scope of your backend systems, set/change/strip headers, and modify the payload beyond simple redaction/replacement. Furthermore, you can perform edge computing, integrate third party services, set processor-specific configurations, and add a security layer requiring proxy-authorization credentials and a root certificate. VGS also offers IP anonymization as an upgrade.

HTTPS is required for all customer application communications. VGS encrypts data in-motion between VGS and your web applications with TLS 1.2 or 1.3. The outbound connection requires a unique TLS certificate for each environment. Your VGS tenant vault is password-protected to ensure that only your application can access or reveal sensitive data. You should protect these credentials as you would an API key.

Optional reverse proxy: If your server making outbound requests is already behind a proxy, it may be simpler to set up a VGS reverse proxy between your server and external services.

VGS Dashboard Security

The VGS Dashboard contains many configurable security and access controls. Strong authentication and session management is required for access, including TLS 1.2 or 1.3. Users must authenticate every time they log in with multi-factor authentication (MFA). One option is token-based one-time passwords (OTP). Passwords have minimum complexity requirements and are individually salted and hashed. Passwords are stored as hashed values, while one time passwords (OTP) are never stored.

Session cookies record encrypted authentication information for every session. They are stored locally in the browser, but do not contain user passwords. Sessions are capped at a maximum of eight hours, and may be set for shorter durations during times of higher risk levels. Role-based access control is available, and some authentication policies may be customer-defined.

Operational Security

VGS bakes security into our platform at every stage, level, and workflow, from architecture design to post-release. Strict IT security policies govern VGS response to a wide range of security and privacy incidents, from detection to response, forensics, and notification.

All employees receive regular information security and privacy training. Employees with access to production data or systems undergo mandatory background checks and receive additional training specific to their roles. VGS has a dedicated security staff including a Chief Information Security Officer and a cadre of Certified Information Systems Security Professionals.

VGS Code Security

VGS secure software development lifecycles begin at the design phase, from guiding principles to secure coding patterns, static code analysis, language/framework dependency checks, and vulnerability testing. Our coders undergo intensive security training and must write threat assessments on high-risk features.

We enforce rigorous release management. In pre-release, all proposed functionality must be validated with internal security requirements. In post-release, VGS employs independent security service providers to analyze our code and monitor potential security issues.

For change control, new functionality requires extensive testing and peer review. VGS works with our customers to minimize negative impact due to code changes and provides explicit notice for all changes that impact customer usage or experience.

Business Continuity Planning

The VGS platform and infrastructure operate on top of one of the world's most secure and reliable cloud service providers, and are monitored 24/7 against security threats. We maintain blue-green deployments, test our systems regularly, and have robust disaster recovery and incident response programs.

VGS risk management includes annual internal assessments to identify, prioritize, reduce, and mitigate known risks. High impact risks are remediated immediately upon discovery. The entire assessment process is thoroughly documented and audited annually by independent third parties. Findings are reviewed and remediation is approved by our internal security team and leadership.

VGS continuously monitors availability and uptime, evaluates processing capacity and usage, and is alerted when downtime thresholds are crossed. VGS maintains redundant systems, robust system backups, and publishes detailed recovery plans. We run daily backups of any changes, replicate backups across multiple availability zones, conduct full backups on a weekly basis, and conduct bi-annual disaster recovery drills.

Our Credentials

Founded in 2016 and named one of the fastest-growing startups in 2020 by CB Insights, Very Good Security is backed by Visa and leading venture firms, including Goldman Sachs and Andreessen Horowitz. VGS is also a Visa Level 1 Global Supplier.

contact@verygoodsecurity.com

verygoodsecurity.com