How Data Security Enables Cross-Regulatory Compliance for Payment Service Providers

INTRODUCTION

Payment service providers (PSPs) in all geographies, especially those that operate internationally, have to comply with a slew of data protection laws & regulations. While these different regulations may differ from each other in some aspects, most have the same core requirements in common, such as protection of sensitive data and timely notifications in the event of a breach. In order to minimize redundant work and get the most of compliance efforts and investments, PSPs should map out in what ways applicable regulations overlap and develop an overall cross-regulatory compliance strategy.

This document looks at the overlapping requirements of PCI DSS and GDPR as an example for developing a cross-regulatory compliance strategy.

GDPR put privacy controls in the hands of the consumer, rather than in the hands of a business or government. As a result, GDPR has become the blueprint for many other privacy laws coming out in the US, which took those principals and built laws around protecting consumer privacy in their state. The California Consumer Privacy Act (CCPA) is a prime example. There is even talk now of the possibility of a Federal Data Privacy Law in the works.

The General Data Protection Regulation (GDPR) is the most sweeping set of privacy regulations enacted by any governing body to date, in this case, the European Commission. The GDPR centers on the personal data of Data Subjects in the EU (and in the UK, which is honoring the GDPR even in the wake of Brexit) residing in the systems of any organization on the planet. Enacted by the EC in 2016 with a two-year assimilation and preparation period, and now in effect as of 25 May 2018, the GDPR is a reaction (some might argue, an overreaction) by the public sector to the general failure by the private sector to sufficiently address how organizations make use of the data they collect on each citizen/consumer. Much has been written about the GDPR, and this report will offer some enhanced perspective on the subject, but in short, every organization on the planet needs to care about the GDPR because failure to comply with its provisions ignores risk, disrespects the privacy and privacy concerns of citizen/consumers, and can hit an organization hard financially. The EC will assess penalties for non-compliance of either €10 million (in excess of USD 11 million at time of publication) or 2% of "annual turnover" (an organization's annual revenue) for what one might term standard violations and, for the most serious violations, penalties of either €20 million (more than USD 23 million) or 4% of annual turnover/revenue.

The Payment Card Industry Data Security Standard (PCI DSS, on all subsequent mentions "PCI") is a widely accepted set of policies and procedures designed to optimize the security of credit, debit, and cash card transactions and protect cardholders against misuse of their personal information. Jointly created in 2004 by credit card issuers Visa, MasterCard, Discover, and American Express, the PCI establishes fines of up to $500,000 per incident for security breaches when merchants are not PCI-compliant.

The good news is that by adopting a truly effective data security strategy, organizations can avoid financially crippling, reputation-shredding battles and their increasingly global customer bases over privacy—while establishing a rock-solid foundation for cybersecurity best practices that supports the organization's business objectives in all areas. This report explores these issues and discusses the foundation for such a strategy.

Poor Security Opens the Door to Privacy Violations

Up to now, most organizations have taken a limited view of which personal data residing in their systems deserves to be classified (and treated) as sensitive or at risk, and therefore worthy of special attention and protection. This has commonly included name, address, date of birth, Social Security number (in the US, with other national identification numbers in other nations), and driver's license information.

The GDPR Expands the Scope of Personal Data

The GDPR takes a far more expansive view of sensitive personal data:

- Any data elements that can be traced to a specific person
- Location data
- Genetic and biometric data
- Browser cookies
- Mobile identifiers (UDID and IMEI) and MAC addresses
- IP addresses and application user IDs
- Many others

The issue is not, however, merely the GDPR's broader definition of what constitutes sensitive data. It is that missing the mark on security can result in costly violations even for those organizations that are otherwise doing everything right with regard to respecting privacy.

Two factors contribute to either GDPR compliance or violations:

- An organization's approach to privacy
- An organization's approach to security

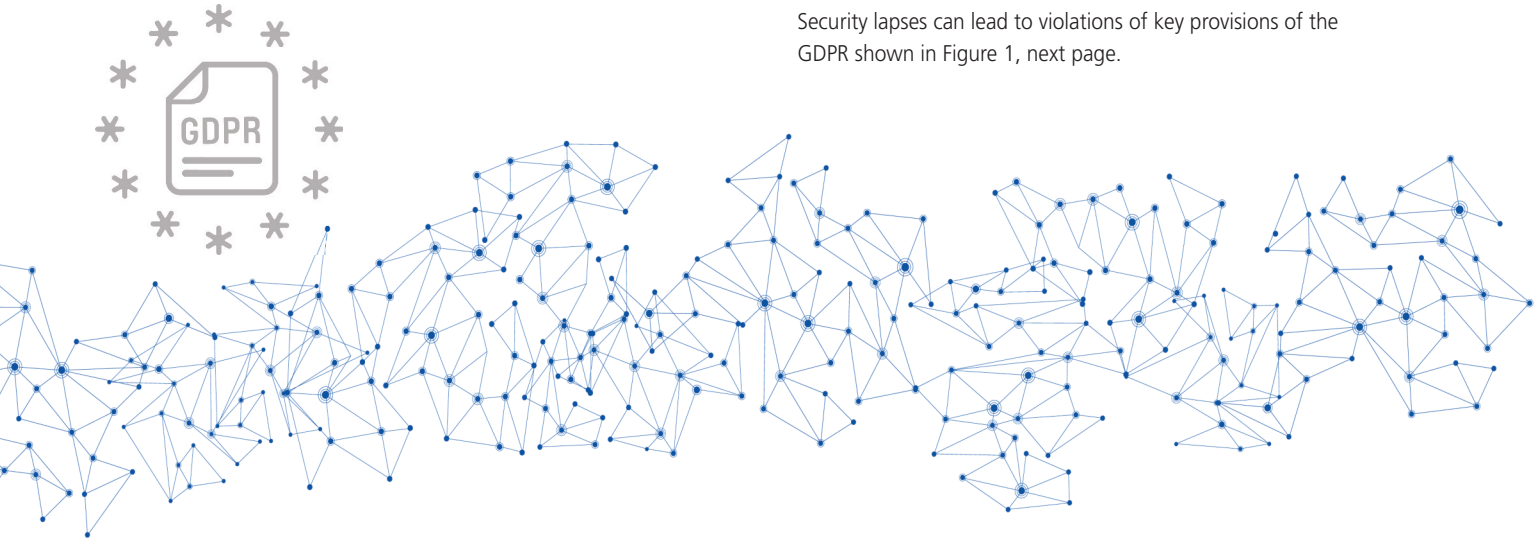
If a company itself misuses or mishandles the data of Data Subjects in the EU or UK, and the company is found to be in violation of the GDPR, the EC will assess penalties as described at the outset. That is a privacy issue and may ultimately reveal either intent on the part of the organization to violate privacy or simply a lack of training, awareness, or competence with regard to avoiding violations.

The more chilling aspect of GDPR violations is that a lack of security preparedness opens the door to privacy violations not by the organization itself but by potentially anyone with nefarious or outright criminal intent:

- If weak security leads to privacy violations, organizational intent does not matter, the results are the same.

- The organization has exposed sensitive personal data that resides in its databases to compromise; it can be found to be in violation of the GDPR and it will pay (monetarily and in terms of market/public opinion) just as surely as if it had committed the violations itself.

Security lapses can lead to violations of key provisions of the GDPR shown in Figure 1, next page.



PROVISION	OVERVIEW AND REQUIREMENTS
PRIVACY BY DESIGN	Calls for the inclusion of data protection from the onset of system design, rather than as an addition or afterthought. The Data Controller shall implement appropriate technical and organizational measures in an effective way to meet the requirements of this regulation and protect the rights of Data Subjects. Controllers must hold and process only the data absolutely necessary for the completion of their duties and limit access to personal data only to those who actually need to perform the processing of the data.
CONSENT	The request for consent must be given in an intelligible and easily accessible form, with the purpose for data processing attached to that consent.
BREACH	Breach notification will become mandatory in all member states where a data breach is likely to result in a risk for the rights and freedoms of individuals. This must be done within 72 hours of an organization first having become aware of the breach.
RIGHT TO BE FORGOTTEN (DATA ERASURE)	Entitles the Data Subject to have the Data Controller (any company) erase his/her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data. The conditions for erasure include the data no longer being relevant to original purposes for processing or simply a data subject withdrawing consent.
INCREASED TERRITORIAL SCOPE	Extends jurisdiction of the GDPR to all companies that process the personal data of Data Subjects residing in the EU, regardless of where the companies are located or where the data processing occurs. In other words, any organization on the planet, processing personal data of EU Data Subjects anywhere on the planet, must comply with the GDPR. Businesses located outside the EU that are processing the data of EU Data Subjects must appoint a representative in the EU (and EU Data Controller).

Figure 1 / Source: CyberEdge Group

PCI Requires Security of Consumer Data and Transactions

Key requirements of PCI are as follows:

1. Cardholder data must be protected physically and electronically, wherever it is stored. Systems must be protected against hackers.
2. PCI Requirement 3.4 requires that sensitive data must be rendered unreadable anywhere it is stored.
3. Access to system information and operations should be restricted and controlled. Cardholders must not be forced to provide information to businesses unless those businesses must know that information to protect themselves and effectively carry out a transaction.
4. All individuals whose information is believed to have been compromised must be notified in writing to be on alert for fraudulent charges.

The Costs of Leaving Data at Risk

Data is at risk across every information ecosystem, as shown in Figure 2.

Where Data Is at Greatest Risk

Data	Company Types Impacted	Points of Access/Vulnerability
PAYMENT CARD DATA: • Primary account numbers (PANs) • Cardholder data (CHD)	**Primarily these company types:** • Payment processors • Merchants/retailers • Financial services companies	**Primarily in these locations or states:** • At the POS device • Stored in databases or files • On-premises • In motion between processors
OTHER SENSITIVE DATA: • Protected health information (PHI) • Tax IDs or SSNs • Intellectual property or industry secrets	**Primarily these verticals/sectors:** • Healthcare • Insurance • Accounting and tax • Financial services	**Stored in databases or files:** • On-premises • Off-premises • In the cloud
PERSONALLY IDENTIFIABLE INFORMATION (PII)	**All verticals and sectors**	**Stored in databases or files:** • On-premises • Off-premises • Cloud

Figure 2 / Source: CyberEdge Group

As stated at the outset, the costs imposed by regulators for privacy violations are serious in their own right. The most serious GDPR violations carry penalties of either €20 million (more than USD 23 million) or 4% of annual turnover/revenue, and PCI establishes fines of up to $500,000 per incident. These can represent serious financial setbacks or even company-killing events. However, a wide range of other immediate and long-term costs can accrue to privacy violators, including:

- Increased audit requirements
- Potential for shutdowns of credit card activity by financial institutions and others
- Costs associated with customer notifications
- Cost of employee and other resources responding to and recovering from privacy-related events

Companies whose systems are compromised have found themselves in the position of buying millions of customers credit monitoring services. They may kill customer loyalty and generate churn, sending their best customers to competitors. C-level executives must justify to the board of directors whether the data breach could have been prevented, and, in the case of violations by publicly traded companies, their stock prices may drop.

If it takes or allows a lax approach to security, leadership is in effect placing the success or even survival of the organization at risk – and in the hands of cybercriminals.

GDPR "Solutions" That Aren't

Some in the industry have put forth simple-sounding solutions that do not square with reality or best practices:

Give Up on Doing Business in the EU

For any company doing business across more than a single world region, at minimum this severely limits its business prospects, and in truth, for many organizations this borders on the absurd.

Place All Data on EU Data Subjects in a Separate Database

This is at best a partial approach to the problem, because by definition it means being unable to effectively commingle data across world regions, thus rendering an organization operating globally or across regions unable to make organization-wide or global decisions. It also implies reliance on the weakest level of data protection, which we will discuss in the following section of the report.

These measures also fly in the face of the reality that the need for effective cybersecurity transcends the GDPR.

Other attempts at technology solutions to securing data include:

- Simple endpoint and mobile protection
- Security monitoring and operations
- Cloud security
- Application security
- Threat and vulnerability management
- Network and gateway defense

These, however, only protect against known attack methods and are useless in attempting to guard against the very data breaches that open the door to GDPR and PCI violations.

Paradigm Shift: An Organization Can No Longer Be Defined by One Location; Nor Can Data Security

Perhaps the most profound example of a failed data protection strategy is encryption. Some organizations favor this, specifically database- and storage-level encryption, because in most cases it is the data security method that shipped by default with their database. Others like it because they view it as a "set it and forget it" method: just turn on encryption and all is well.

Nothing could be further from the truth:

- If hackers obtain the encryption key, the algorithms are public, and all they have to do to compromise the data is match up the right algorithm with the encryption key
- If hackers can decrypt data, they in effect have the key to unlock all of the personal data being stored; with elevated credentials they can see the data in the clear
- DB-level encryption only protects (in a limited fashion, as described above) data at rest; it does nothing to protect data in use or in motion

Those points address the core security weaknesses of encryption. Other issues center on the issues it also creates in terms of business continuity:

- Data reduction processes like compression and deduplication fail with encrypted data, which limits the options available to companies with regard to how they handle their data
- Encryption does not preserve the format of the data, so it increases complexity and requires more computer processing resources to implement
- Applications connected to the DB often cannot be encrypted, leaving the entire system vulnerable to attack

Encryption proponents point to format-preserving encryption, whereby data values are unchanged and data is more workable for day-to-day usage, but even then, system admin must pass out encryption keys to code and decode data – and it does not change the fact that once hackers gain access, they can see (and leverage) data in the clear.

Data is on the Move. Data-centric Security moves with it.

If data merely sat still in DBs, DB-level encryption could provide some level of protection – until the moment hackers gain access to the encryption key. The reality is that data is a pervasive, critical asset that crosses traditional silo boundaries on-premises and in the cloud. Data is always on the move, and data security must move with it. This requires a data-centric security strategy that prioritizes datasets and mitigates evolving business risks such as regulatory compliance and threats from hacking, fraud, and ransomware.
An effective data security strategy must protect the data itself, not just the perimeter.

Data-centric Security Offers Granular Protection that Moves with the Data

Protecting data at rest, as in database- and storage-level security approaches, is not enough. What organizations need is data-centric security, which is about protecting the data itself, not networks and endpoints, throughout the data lifecycle: data in use, such as when data is being accessed by users to carry out work, and data in motion, such as when data is uploaded from an organization's on-premises data stores to the cloud.
A data-centric security model protects the individual data elements wherever possible. That means if a dataset contains a mix of sensitive data such as PII along with other data that is not sensitive or regulated, the system protects the data at the individual element level.

(Keyless) Tokenization Holds the Key

Tokenization addresses the shortcomings of encryption. Tokenization replaces the original data with a unique placeholder the system randomly generates. There is no algorithm to re-create the original data, so hackers cannot reverse-engineer credit card and other per-sonal data. It is a proven fact that hackers are going to succeed in gaining access to systems through various attack vectors – but when they do, the protected data has no exploitable value.
Thus, tokenization:

- Supports GDPR compliance, because even if hackers gain access to a DB, they cannot obtain actual personal data of EU or UK Data Subjects
- Supports PCI compliance because it renders consumers' PANs unreadable

Format-preserving tokens maintain referential integrity, resulting in a dataset that is the same size as the original, but that is now full of tokens to protect sensitive data, and has the identical statistical distribution as the original data to ensure the original characteristics and properties of the dataset are preserved.
In addition to providing compliance and easing day-to-day data operations, tokenization aids in scope reduction. Common tokenization applications replace sensitive cardholder data in business systems with tokens and store PANs securely (separately) in a data vault. This eliminates the possibility of a hacker gaining access to database tables containing both customer information and corresponding PANs. The only way for an attack to succeed would be to breach the tokenizing system and look up the corresponding PAN for each token, or to induce the system into responding to a query for PAN, both of which are extremely difficult if not impossible. If the tokenization system is properly segmented, then the tokenization system and the systems that connect to it are the only systems that are within scope, which greatly simplifies compliance.

comforte Offers Tokenization-powered, Data-centric Security that Protects Data – and Protects the Organization Against GDPR and PCI Violations

The SecurDPS data protection suite by comforte is a scalable, fault-tolerant enterprise data-centric security solution that protects sensitive data with minimal effort and little to no impact on existing applications. It helps organizations achieve end-to-end data protection, compliance with security regulations and standards such as PCI DSS and GDPR, and a significant reduction in the impact and liability impact of data breaches. comforte's patented tokenization algorithm provides linearly scalable, high performance tokenization. The algorithm is stateless, vaultless, and collision-free. The tokenization table holds a large set of random numbers gathered during initialization of the system. Once started, the static tokenization table then loads fully into memory, so all tokenization operations occur purely in memory and on CPU, thus in real time, without any disk IO.

Stateless tokenization randomly generates multiple token tables one time for all possible PANs, using random numbers and a provably secure method. Each PAN in the numeric range has a token assigned to it for the life of the table(s), and since every token PAN is pre-associated with a token, the tables are stateless; they do not change. This eliminates the need to synchronize a database across data centers or constantly back it up, all of which slashes the cost of administration and complying with audits.

A tokenization strategy controls how a sensitive data element is protected, and SecurDPS allows for a number of strategies including:

- Tokenization table
- Algorithm attributes
- Token format - how many leading and trailing characters are left in the clear
- Distinguish method - how plain values can be distinguished from tokens

The system can generate format-preserving tokens for credit card and Social Security numbers, and other PII elements such as names and email addresses.
SecurDPS integrates with existing perimeter, network, and storage security solutions. Wherever it goes or whoever sees it, the data is protected.

Beyond its commercial attributes, comforte's solutions have been independently verified by, and are providing reference architecture and methodologies, for the industry. comforte's tokenization approach and algorithm have been vetted by independent cryptologists, and the combined solution is one of the reference schemes for static table-driven tokenization in the ANSI X9.119-2 tokenization standard (C.3.3.2).

Data-centric Security in Action: Thailand Implements PCI-Compliant Data Protection Nationwide

Government Savings Bank (GSB) has the largest network of ATMs and branches in Thailand, with more than 6,000 ATMS and 1,000 branches across the nation handling travel, capital accumulation, and home deposit savings for millions of citizens.

The Challenge

All of these operations and services represent an enormous volume of sensitive data, and threats to that data are constantly evolving, so financial institutions must continually adapt their data security strategy to stay ahead of the curve.
GSB needed an easy-to-implement solution that would map out sensitive data across a large and highly complex network and render that data unreadable, without affecting service levels, and on a short timeline: to fully comply with the mandate from Thailand's Central Bank, GSB had to achieve PCI compliance in months, not years.

The Solution

Working with comforte AG and its partner DataOne, GSB deployed comforte's SecurDPS solution. SecurDPS offers transparent integration, which means that it can be implemented on a complex IT infrastructure without any changes to existing applications. This made it possible to effectively secure data in a fraction of the time and at a fraction of the cost of competitive solutions. The solution included a tool from a comforte AG partner designed for mission-critical HPE systems that scans the network and detects any unprotected PANs. Once it has discovered and pseudonymized any sensitive data, the system validates and verifies that all PANs across a system are protected in accordance with PCI.

Results

GSB is now PCI compliant and has passed audits by Thailand's Central Bank. GSB's millions of customers across the country can rest assured that their payment card information is safe.

CORE CONCLUSIONS and CALL TO ACTION

The GDPR was enacted in 2016, and the EC began enforcing it in 1H2018. PCI was established more than a decade earlier, in 2004. Yet, well into 2H2018, organizations are still grappling with the security lapses and privacy violations these two measures were designed to combat.

The GDPR is designed to enforce a new standard of privacy by persuading companies (through the force of law) to avoid violating privacy. Even companies that scrupulously follow the provisions of the GDPR can, however, be betrayed by their own security shortcomings. If a company allows hackers to get their hands on the personal data of citizen/consumers, and when those hackers inevitably commit privacy violations, it is no different than if the organization had violated the GDPR of its own accord – and it can be just as costly. By contrast, PCI is focused on technology-based security measures companies must to use to protect the sensitive data of citizen/consumers wherever it resides. The GDPR's Privacy by Design provision complements this with its requirement that Data Controllers must implement technical methods as part of protecting privacy.

Clearly, the prerequisite to protecting data privacy is effective data security. Yet, many organizations are challenged in this regard. We assert that in most cases this is a result of organizations entrusting their data to database- and storage-level encryption. Encryption leaves the organization vulnerable to attack and, to add insult to injury, complicates day-to-day data processes.

A better approach is tokenization-based, data-centric security. Data-centric security focuses on the security of the data itself, in all forms. Encryption fails because it is only useful, and then only marginally so, in protecting data at rest, in the database. Data-centric security succeeds because it protects data everywhere it goes, in use and in motion, with a granular level of protection that safeguards individual data elements. It also substantially reduces the footprint of systems that are in scope with regard to PCI audits, which simplifies compliance.

Any organization that continues to rely solely on classic encryption for "security" – quotation marks purposefully inserted – is betting the company on an antiquated technology (and mindset) that cannot effectively address the multitude of threats that are aimed in its direction every second of every day. Data-centric security based on tokenization technology equips the organization to take on the hackers and secure not only its data but its future. And if an enterprise has doubts about the necessity of acting on this now, the GDPR (through its governing body, the EC) and PCI stand ready to issue persuasive and costly reminders.