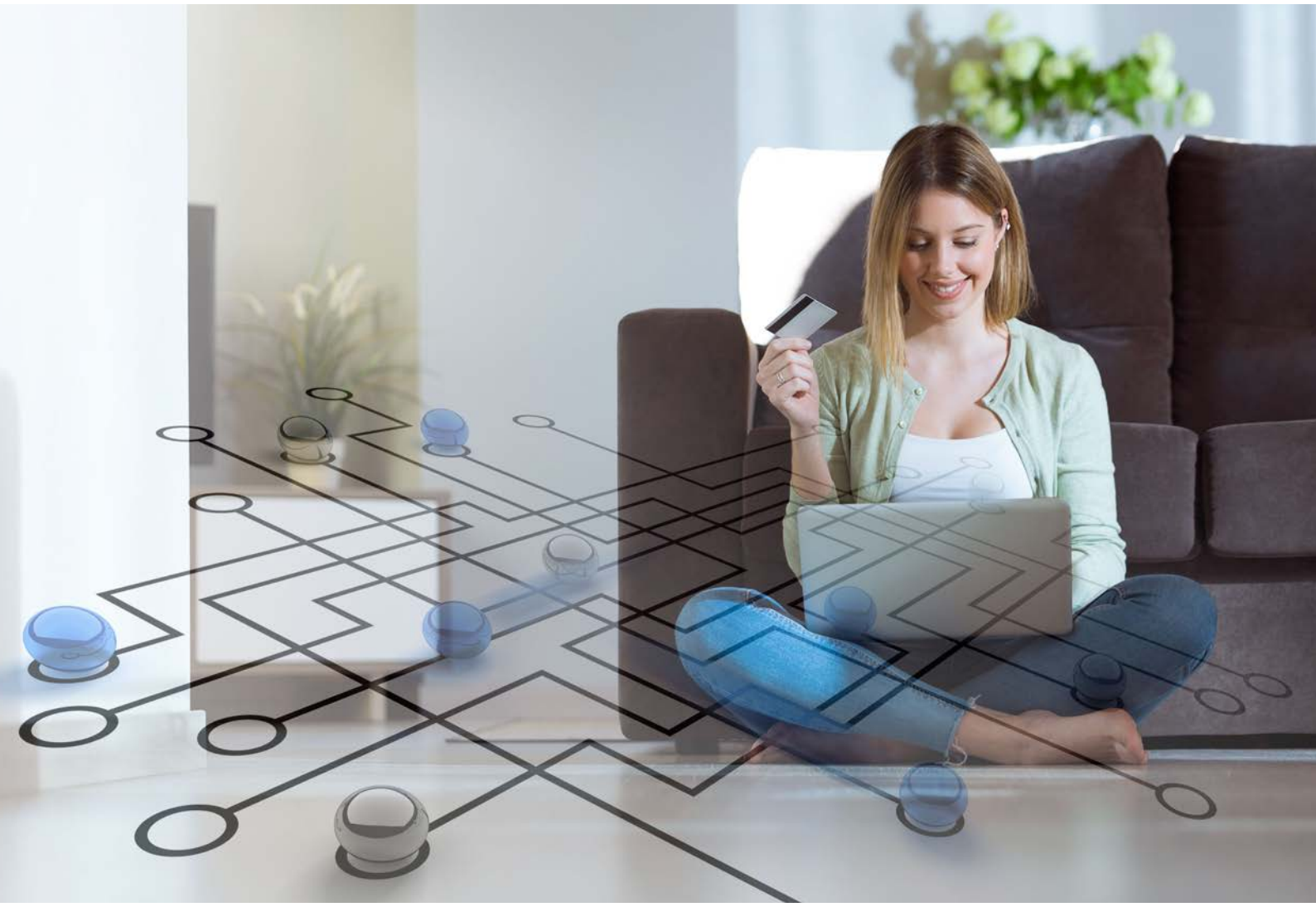
Cross-regulatory Compliance for Payment Service Providers: How to Find the Right Strategy



Cross-regulatory Compliance for Payment Service Providers: How to Find the Right Strategy

Introduction

Payment service providers, especially those that operate internationally, have to comply with a slew of data protection regulations from various geographies. While these regulations may differ 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 white paper explores the overlapping requirements of PCI DSS and GDPR as an example for developing a cross-regulatory compliance strategy. Many other regulations, such as Brazil's LGPD or the State of California's CCPA, have similar core requirements.

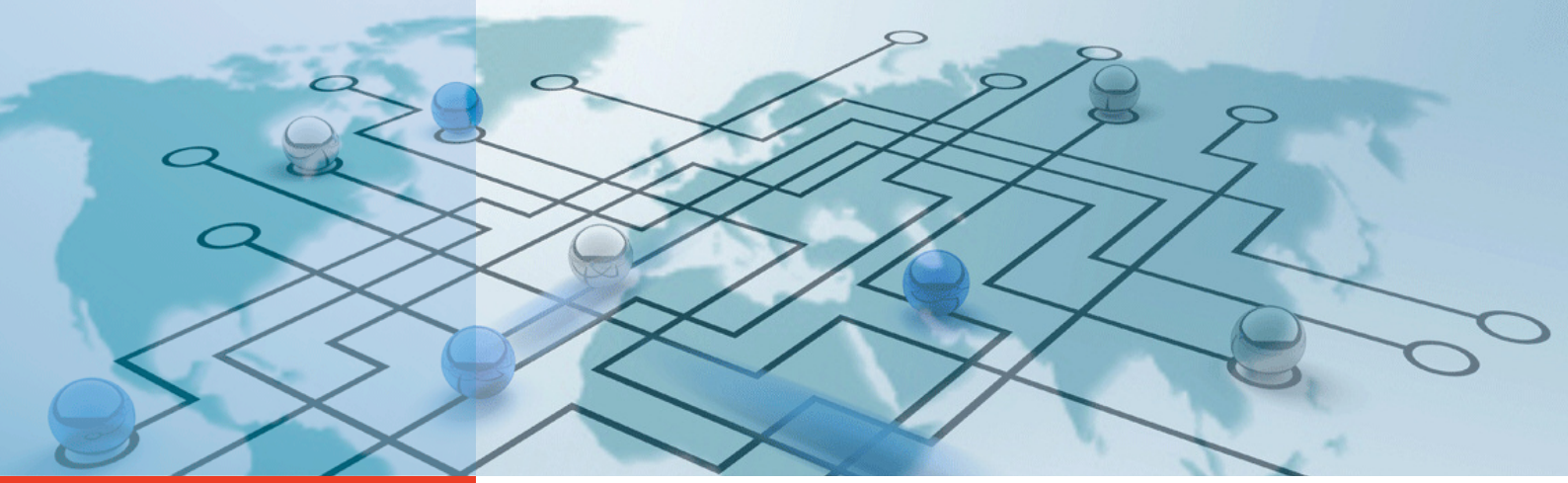
Step 1

Define What Kind of Data Needs to be Protected

According to PCI DSS, cardholder data is a Primary Account Number (PAN) either by itself or a combination of other data elements attached to it, such as the cardholder name, expiration data and service code. If those elements cannot be traced back to a specific PAN, then they are not considered cardholder data as far as PCI DSS is concerned. A PAN must be present for any given data to be considered cardholder data.

Personal data according to Article 4(1) of GDPR is significantly broader in scope and includes all of the above data elements and many more, either as individual elements or a combination of multiple data types. Put simply, GDPR defines personal data as any information that could possibly reveal the identity of a human being. This includes concrete information such as names, ID numbers and location data, but it also encompasses more abstract elements such as physical description and biometric data, physiology, genealogy, social identity, mental status and economic status.

When developing a GDPR compliant data security strategy, many of the technology, processes and policies for protecting cardholder data can also be applied to personal data. The following sections explore the many scenarios in which this is possible.



Step 2

Decide How to Protect the Data

Both GDPR and PCI DSS require some form of cryptography to protect data at rest and data in motion. That includes stored data as well as data being transmitted or processed. Cryptography ensures that even if an unauthorised entity gains access to sensitive data, that data will be in a state that has no exploitable value. There are a number of options for securing data with methods that satisfy both regulations.

Encryption can pseudonymise data by replacing every element with an algorithmically determined cipher resulting in a completely unrecognisable series of numbers, letters and characters. While this can be an effective method of protecting data, encryption changes the length and type of the data into formats that are not always compatible with intermediate systems. Encrypting and decrypting also require a significant amount of computational resources which can affect throughput.

Tokenisation is an equally effective, yet more versatile method that replaces sensitive data with non-sensitive substitutes without changing the type or length of the data. This can be a critical difference because certain intermediate systems such as databases are only capable of reading specific data types and lengths. Furthermore, tokens require significantly less computational resources to process. Specific data is kept full or partially visible for business functions such as processing and analytics while sensitive information is kept hidden. Tokenised data can therefore be processed much more efficiently, which reduces the strain on system resources. This is a key advantage in systems that rely on high performance.

PCI DSS Requirement 3.4 stipulates that PANs must be unreadable anywhere they are stored. It specifies that data at rest can be protected with tokenisation, truncation, one-way hashes of the entire PAN or encryption with proper key-management. Requirement 4 calls for similar measures to protect data being transmitted over public networks.

These requirements are nearly identical to Article 32 of GDPR, which calls for "pseudonymisation and encryption of personal data… whether in storage, transmitted or otherwise processed." Given the definition of pseudonymisation as described in Article 4(5), personal data must be stored and processed in such a way that it cannot be traced back to a specific data subject without the use of tightly secured additional information. This can be achieved with any of the methods mentioned in PCI DSS Requirement 3.4.

Step 3

Map out Where the Data is and Where it Goes

In order to effectively secure personal data or cardholder data, companies must identify all places where that data is stored. This is a necessary first step in complying with many PCI and GDPR requirements such as carrying out regular risk assessments, logging access and data disposal. In the event of a breach, knowing where data is stored will also facilitate investigations into what data stores were compromised and how.

Additionally, GDPR Article 17 guarantees the right to erasure or the "right to be forgotten", which means that data subjects can request that all of their personal data be deleted. This can only be done properly if a company knows exactly how many copies of the data in question exist and where they are stored.

Step 4

Regularly Assess Data Breach Readiness

The threats to personal data and cardholder data are changing constantly. In order to keep up, organisations must conduct regular reviews to gauge how well personal data is protected. In addition, whenever an organisation undergoes major changes that might affect data security policy and processes, such as mergers and acquisitions, relocation or the adoption of new data processing systems, risk assessments must be carried out. These common sense policies are required by both PCI DSS and GDPR.

GDPR identifies a broad range of processing operations that are subject to review while PCI DSS defines a timeframe and suggests specific risk assessment methodologies. The risk assessment framework defined by PCI DSS provides clearer and more specific answers to the questions of how to conduct reviews and how often. Organisations that are already equipped for PCI mandated risk assessments could apply the same methodologies to the additional processing operations specified by GDPR.

GDPR Article 35 requires organisations carry out a data protection impact assessment (DPIA) for processing operations that are "likely to result in a high risk to the rights and freedoms of natural persons." In October 2017, the EU Article 29 Working Party (WP29) published their revised guidelines defining what processing activities may pose such a risk and therefore necessitate a DPIA. That would include any processing activities that fulfil at least two and in some cases just one of the following criteria:

- Evaluation or scoring
- Automated decision making with legal or similar significant effect
- Systematic monitoring
- Sensitive data or data of a highly personal nature
- Data processed on a large scale
- Matching or combining datasets
- Data concerning vulnerable data subjects
- Innovative use or applying new technological or organisational solutions
- When the processing prevents data subjects from exercising a right or using a service or a contract

For instances where it is not clear whether a DPIA is necessary, it is advisable to err on the side of caution. Also note that the European Data Protection Board (EDPB), referred to throughout GDPR as "the Board", replaces the WP29.
In order to minimise redundancy, Paragraph 1 states that "a single assessment may address a set of similar processing operations that present similar high risks". That means that if the nature, scope, context and purpose of multiple processing operations are similar, then the results of only one DPIA are necessary.

Step 4

Regularly Assess Data Breach Readiness

GDPR also specifies the context in which a DPIA should be carried out. Paragraph 1 of Article 35 suggests that an assessment be conducted "in particular [when] using new technologies." Paragraph 11 indicates that they should be performed "at least when there is a change of the risk represented by the processing operations." This is very similar to the risk assessment framework laid out by the PCI.

PCI DSS 12.2 requires that a risk assessment be performed whenever there are significant changes that might affect data processing procedures and cites examples that include but are not limited to mergers and acquisitions, relocation and the introduction of new processing technology. The PCI additionally requires a risk assessment be carried out at least annually, even if there are no major changes to the data processing environment.

These assessments must identify critical assets, threats and vulnerabilities and result in a formally documented analysis of risk. PCI DSS also provides examples of some of the methodologies that may be used to fulfil this requirement, such as OCTAVE, ISO 27005 and NIST SP 800-30. These methodologies as well as the schedule for PCI mandated risk assessments can be applied to processing activities subject to a DPIA as required by GDPR Article 35.

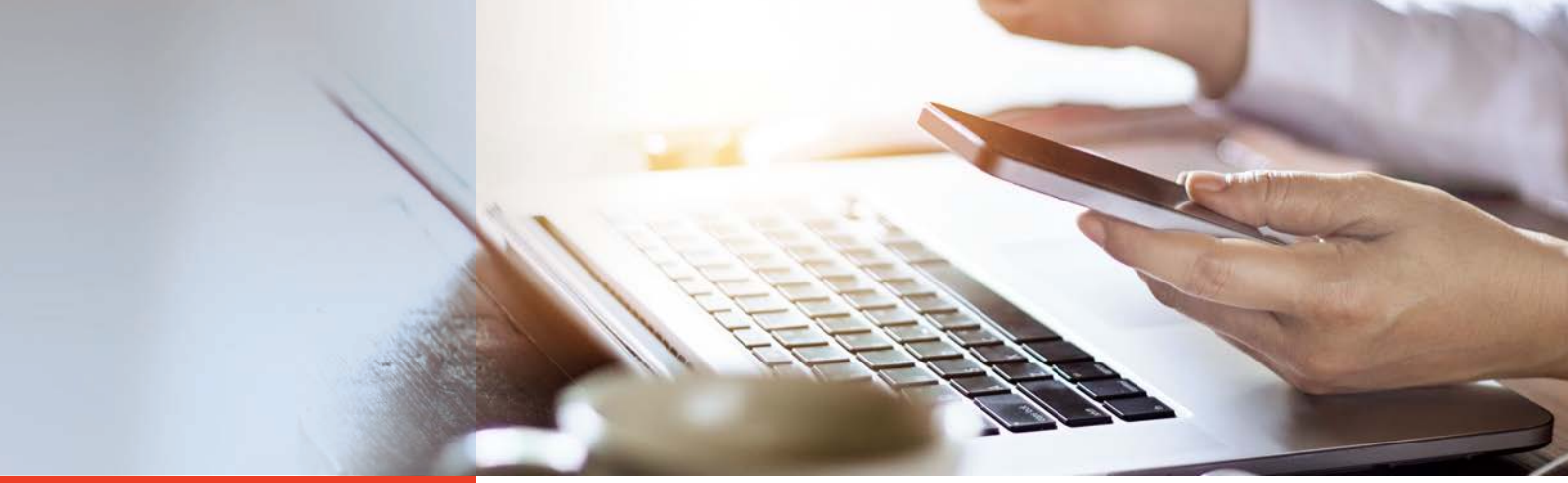
Step 5

Only Store Sensitive Data When Necessary

Both the PCI and GDPR provide guidelines for reducing the amount of data being processed. This has the advantage of minimising risk and reducing the time, effort and costs associated with securing excess data. PCI DSS Requirement 3.1 stipulates that cardholder data storage should be kept to a minimum and recommends a number of methods for minimising data storage.
These include setting retention times based on legal, regulatory or business requirements; defining specific requirements for retaining cardholder data; defining processes for secure deletion of data and scheduling a quarterly review to identify and securely delete cardholder data that is no longer needed.

GDPR mandates a very similar policy with regard to personal data in Article 25. The controller is obligated to "implement data-protection principles such as data minimisation" and "only personal data which are necessary for each specific purpose of the processing [may be] processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility." As a result, the methods and standards for limiting cardholder data storage as suggested by PCI can be applied to personal data in order to achieve compliance with GDPR Article 25.

In addition to minimising the amount of sensitive data being processed and stored, Article 25 also mentions limiting accessibility, which is covered in the following section.



Step 6

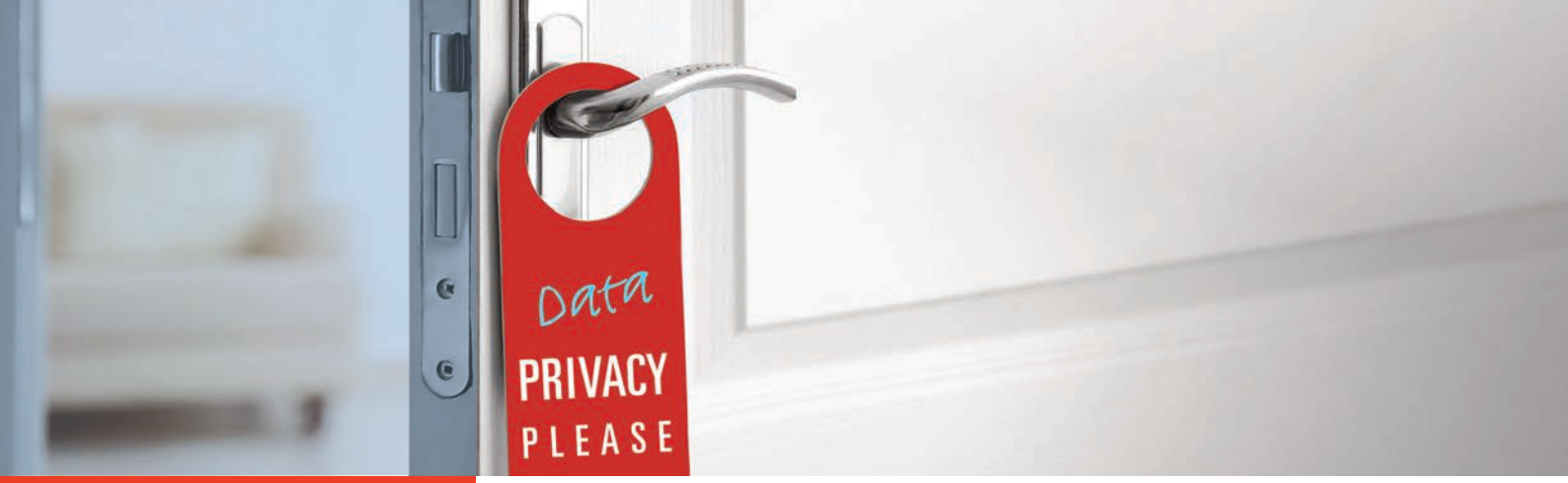
Limit Internal Access to Sensitive Data

Limiting access to sensitive data is a key component of GDPR and PCI DSS. The advantage of this kind of policy is twofold. First, every account with access to sensitive data is a possible attack vector and therefore limiting access is analogous to limiting vulnerability. Even if users are properly trained in handling sensitive data, their credentials have the potential to be compromised by malicious actors so it is advisable to only grant access to those who absolutely need it. Second, limiting access narrows down the list of possible sources during an investigation should a breach ever occur. As such, it can be seen as both a proactive and retroactive security measure.

PCI DSS Requirements 7 through 9 describe how to limit access to cardholder data. This includes restricting access to only those with a specific business need, authenticating access to system components and controlling physical access to cardholder data touchpoints. Each requirement delineates a number of concrete measures to take in order to fulfil them effectively.

According to Requirement 7, access needs and levels of privilege such as user or admin should be determined for each unique user ID and, by default, only the least amount of privilege required to fulfil a given role should be granted to a given user. Requirement 8 describes how to maintain the integrity of log-in credentials, such as user account management, standards for passwords and multi-factor authentication. While 7 and 8 deal with digital access, Requirement 9 concerns physical access management. This includes measures such as door locks, ID badges, video surveillance in accordance with local law, etc.

PCI Requirements 7 through 9 can be interpreted as a set of best practices to follow when determining how to limit access as required by GDPR Article 25(2). These checks are prerequisites to the obligation to log access to sensitive data.



Step 7

Log Access to Sensitive Data

In addition to the accessibility limitations referenced above, logging access to sensitive data is another indispensable part of any data security strategy. Access logs are useful for proactively detecting potentially malicious activity and, if a breach does occur, they are essential to investigations to determine the source of the breach.

GDPR Article 30 requires that both processors and controllers keep records of all processing activities and specifies what information those records must contain. This includes the name of the processor or controller, the name of the DPO, the categories of the data subjects and personal data, the names of any recipients, a timeline for erasure and a description of the data safety measures taken.

These requirements overlap to a large extent with PCI Requirement 10: "track and monitor all access to network resources and cardholder data." This requirement calls for audit trails that can answer who, what, when, where and how at a moment's notice regarding any access to cardholder data over the past three months. Furthermore, the PCI recommends retaining logs for at least a year because in some cases a breach might not detected until months after the fact. Requirement 10 also lays out a framework for securing the integrity of access logs, such as time-synchronisation of network systems, strictly controlling any alterations to records, a yearlong retention period and a schedule for regular reviews of logs and incidents.

Step 8

Develop a Data Breach Response Plan

In the event of a breach, organisations will not necessarily be penalised, but they will have to demonstrate that their security apparatus was up to par and that they responded accordingly upon discovering the breach. Additionally, organisations are obligated to report any breaches of sensitive data to the appropriate parties in a timely manner. Failing to do so is what can result in considerable penalties. If the sensitive data involved in the breach was protected with the appropriate measures, such as tokenisation or encryption, then it is not necessary to report it.

PCI DSS requires organisations to come up with an incident response plan ahead of time. If a breach occurs, the effected organisation should notify affected payment card brands, banks and any other third parties with whom the organisation has a contractual requirement to notify. Contact information for all of these parties should be updated on a regular basis.

For such scenarios, the definition of "appropriate authorities" varies between GDPR and PCI DSS. According to Article 33, in the event of a breach of personal data, the Supervisory Authority of the respective Member State must be notified within 72 hours. In addition, Article 34 requires that the affected data subjects be informed as well. This can be done individually or, if individual communication is not feasible, the breach must be announced publicly.

The obligation to report breaches is much stricter under GDPR in terms of who to contact and when. For example, some organisations may find it wiser to report suspected breaches to the Supervisory Authority before they have been verified so as to avoid violating the 72 hour disclosure rule. Whether a breach has been confirmed or not, if the decision is made to report, an incident response plan as described in PCI DSS Requirement 12.10 can be used to prepare an organisation to act quickly and accordingly.

Conclusion

The risks to personal and cardholder data are many. Together, GDPR and PCI DSS provide a clear roadmap on how organisations can most effectively protect that data. In order to develop and maintain an effective data security strategy, these regulations should not be seen as just a burden, but rather as a standard to strive for.

Since these regulations overlap in many ways, PCI compliant organisations have a head start in becoming GDPR compliant and any organisation, including those who are not PCI compliant, can use PCI DSS for inspiration on how to interpret some of the more vague aspects of GDPR.

This document is not intended as legal advice or to recommend any specific course of action. Always consult with your legal counsel when determining the legally binding obligations of any regulation or contract.