PCI DSS as a Foundation for GDPR Compliance

Introduction

The online business world is dynamic and expanding rapidly, and businesses as well as legislators have been struggling to keep up. As more and more consumers become accustomed to online services, a greater amount of their data is being stored, transmitted and processed digitally. Concerns over data security prompted the Payment Card Industry (PCI) to publish a consolidated Data Security Standard (DSS) to protect cardholder data in 2004. This replaced the standards that were previously set on an individual basis by each payment card provider. Since then, the PCI DSS has been revised and updated continually to reflect the changing online business environment and the threats to cardholder data.

Within the European Union, not only cardholder data but the protection of personal data in general has been a priority for many years. The latest iteration of EU legislation regarding personal data is the General Data Protection Regulation (GDPR), which supersedes the Data Protection Directive (DPD) of 1995. The GDPR applies to many more organisations than the DPD and the repercussions for non-compliance are significantly more severe.

The GDPR requires all organisations handling any personal data of individuals residing in the EU to bolster their data management and security strategy. This includes organisations based outside of the EU that handle data of EU residents. Penalties for non-compliance can be as high as 4% of global annual revenue or 20€ million, whichever is higher. Many of the organisations affected by this new regulation have still not achieved GDPR compliance. According to the Cloud Security Alliance's GDPR Preparation and Challenges Survey Report, just a few weeks before the deadline on 25 May 2018, 83% of companies did not feel very prepared for GDPR .

The GDPR requires all organisation handling any personal data of individuals residing in the EU to bolster their data management and security strategy. This includes organisations based outside of the EU that handle data of EU residents.

According to Gartner, "on 25 May 2018, less than 50% of all organisations impacted will fully comply with the GDPR." Furthermore, "before 2020, we will have already seen a multimillion Euro regulatory sanction for GDPR noncompliance." Gartner, Inc., research note GDPR Clarity: 19 Frequently Asked Questions Answered, Bart Willemsen, 29 August 2017*

**NOTE: This document, while intended to inform our clients about the current data privacy and security challenges experienced by IT companies in the global marketplace, is in no way intended to provide legal advice or to endorse a specific course of action.*

For companies striving to become GDPR compliant, the PCI DSS can used as a useful point of reference for a number of GDPR requirements. While far from identical, there are certain areas where the PCI DSS and GDPR overlap. Whether your organisation is already PCI compliant or moving in that direction, the technologies and processes required for PCI compliance can be used as a framework for GDPR compliance. Depending upon your company's status of PCI compliance, this overlap makes it possible to either fulfil certain requirements of each regulation simultaneously or to leverage existing PCI compliant technology and processes and apply them to the GDPR's definition of personal data. This document provides insight on how to take advantage of this overlap as a part of your overall data security strategy.

Definitions of Cardholder Data and Personal Data

According to the 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 the 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 the 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, the 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.

The technologies and processes required for PCI compliance can be used as a framework for GDPR compliance.

Securing Data at Rest and Data in Motion

Both the 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.

The 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 the 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..

Mapping out Data Stores

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.

Data Protection Risk and Impact Assessments

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 the PCI DSS and the GDPR.

The GDPR identifies a broad range of processing operations that are subject to review while the PCI DSS defines a timeframe and suggests specific risk assessment methodologies. The risk assessment framework defined by the 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 the 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 the GDPR as "the Board", replaces the WP29.

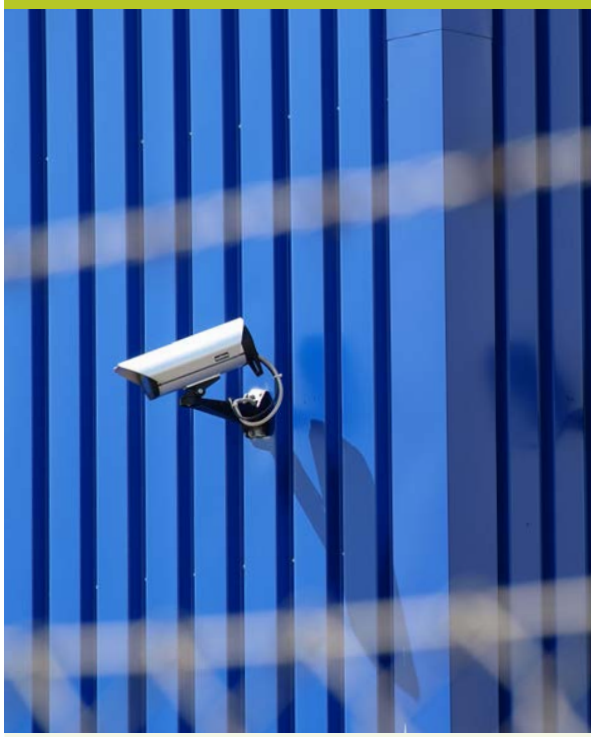
Organisations that are already equipped for PCI mandated risk assessments could apply the same methodologies to the additional processing operations specified by the GDPR.

Data Minimisation and Reduction of Scope

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.

The 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.



Limiting Access

Limiting access to sensitive data is a key component of the 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.

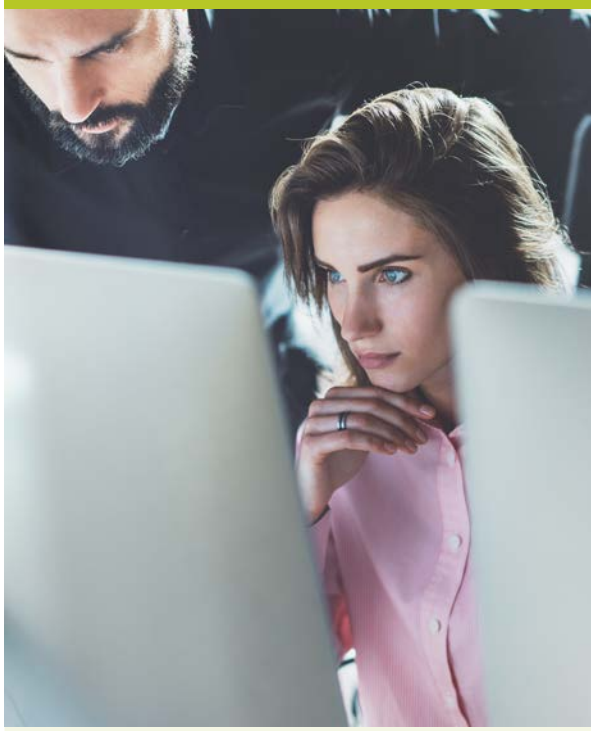
According to Requirement 7, access needs and levels of privilege such as user or admin should be determined for each unique user ID and, by default, only the least amount of privilege required to fulfil a given role should be granted to a given user. Requirement 8 describes how to maintain the integrity 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.

Logging Access

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 DSS 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.



Liability and Obligations in Case of a Data Breach

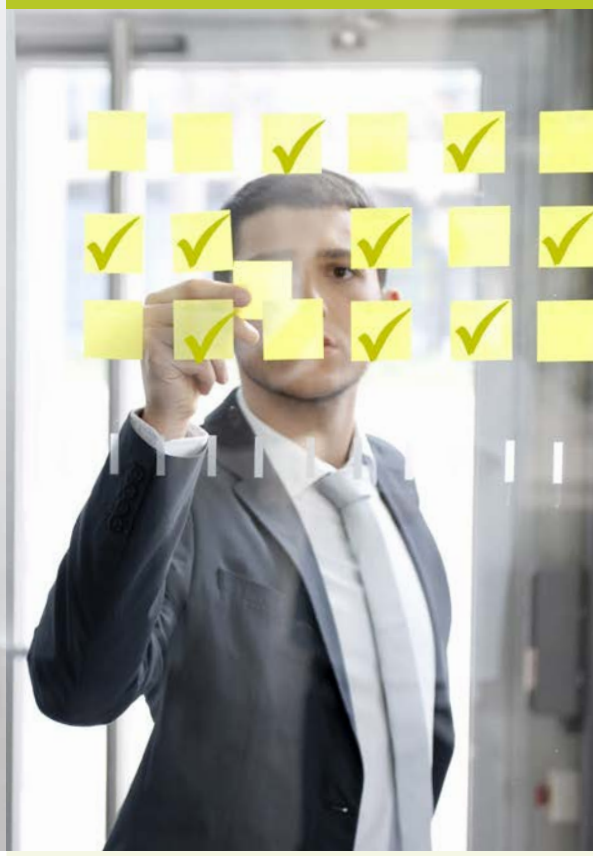
In the event of a breach, organisations will not necessarily be penalised, but they will have to demonstrate that their security apparatus was up to par and that they responded accordingly upon discovering the breach. Additionally, organisations are obligated to report any breaches of sensitive data 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.

The 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 the GDPR and the 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 the 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.

PCI DSS as a Foundation for GDPR Compliance



Conclusion

The risks to personal and cardholder data are many. Together, the 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 the GDPR.

References:

Cloud Security Alliance. (2018, April 17). CSA Research News. Retrieved from https://cloudsecurityalliance.org/media/press-releases//gdpr-preparation-and-challenges-survey-report/

European Commission. (2017, October). EU Newsroom. Retrieved from http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

Gartner, Inc. (2017, August 29). GDPR Clarity: 19 Frequently Asked Questions Answered.

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.