ShieldQ

ISO 27001 CERTIFICATION EUROPE

PCI Security Standards Council

Getting ready for GDPR:

If you're PCI DSS compliant, you may be halfway there

GDPR READY

www.shieldq.com

Getting ready for GDPR:

If you're PCI DSS compliant, you may be halfway there

You are not alone in thinking, "where do I begin," when it comes to the General Data Protection Regulation *(GDPR)*, replacing the Data Protection Directive in 2018.

New, tougher rules will require a steep learning and implementation curve, because, while the GDPR is specific about what the requirements are, it is somewhat vague about how organizations can get ready.

Before we delve into the how, however, let's review the main points of the GDPR.

GDPR rules: a whole new way of compliance

The European Commission, the European Parliament and the Council have adopted the GDPR to consolidate digital data protection rules across the EU. It has been designed to enhance personal data protection, while minimizing current red tape, providing one set of rules for all.

Among the new imperatives:

One-stop shop

With one set of rules, the GDPR streamlines bureaucracy – and its significant resource cost. Organizations large and small will only have to deal with one independent supervisory authority *(SA, but also known as data protection authorities or DPAs)* in each EU member state, coordinated by the European Data Protection Board *(EDPB). [1]*

The EDPB will comprise one representative of each EU member state's supervisory authorities and a representative of the European Commission. If a business owns multiple companies in other member states, it must decide which SA in which country will be responsible for all. This decision could be determined by where data processing management is handled, which could very well be in the group's headquarters.

"Some research institutions estimate that unstructured content [email messages, word processing documents, social media posts, videos and photos] accounts for a whopping 80-90% of digital data – a lot of it in different types of data storage, different locations, varying formats"

Worldwide reach

The GDPR states that all organizations worldwide handling European citizens' data must comply with its rules. Thus, for example, financial organizations in North American processing EU-residents' data must be GDRP compliant; hotels in Japan must safeguard EU-citizens' payment card data according to the same rules.

And, while the Federal Trade Commission-enforced US Privacy Shield has been passed, replacing Safe Harbor, it remains to be seen how it will be implemented, together with the GDPR. The two regulations do share some similar obligations, including contractually obligating third parties to delete personal data that is no longer required for processing, as well as accountability.

Data breach notifications

GDPR representatives must be notified within 72 hours of data breach discovery, defined as those that are likely to place individuals' rights and freedoms at "high risk": e.g., identity theft or fraud, and financial loss. Interestingly, the only type of breach that doesn't require notification is a new GDPR concept, "pseudonymous data": information that has been scrambled or encrypted, making it impossible to identify the data without additional information. There is very little chance of deciphering, such data.

Sanctions

Often mentioned, in addition to "the right to forget," are the dreaded sanctions for breaching GDPR: this is where the pocket feels the pain: fines can reach €20 million, or up to 4% of annual worldwide turnover. The maximum fine applies to discrepancies in international data transfers or breaching processing principles, such as conditions for consent.

Other violations can carry fines up to 2% of annual worldwide turnover.

Data protection officer (DPO)

This requirement primarily pertains to companies that handle big data, regularly monitor data subjects on a large scale, or handle large-scale processing of special data categories *(e.g., data on health, racial, ethnic origin, political opinions, religious or philosophical beliefs).*

The DPO is responsible for informing your organization of its obligation to abide by GDPR and other data protection laws:

- Monitoring compliance *(via such actions as internal data protection activities, internal audits, training data center staff)*
- Responding to individuals' requests: such as requesting the right to be forgotten, or requesting access to data that the company is holding on
  that person.
- Serving as contact point with the SA, notifying it of any data breaches, much like PCI card payment breaches are handled.

Regulations that are all about the data

The following GDPR regulations require a prerequisite of knowing where the data is:

Personal data consent

Individuals must agree to provide data, which must be "freely given, specific, informed and unambiguous," and can include such activities as ticking a box on a website, or another action or statement that clearly indicates consent to processing information.

But the personal data definition can be very broad. For the purposes of GDPR compliance, it includes any information relating to a person in their private, professional or public life, e.g., name, photo, email address, bank details, payment card details, mobile device IDs *(IMEI codes),* IP addresses, social networking posts, genetic and biometric data and pseudonymous data.

For organizations, this means seriously reassessing the way you collect data. But even before you start your evaluation, you first need to know – that's right – where your data is.

Accountability

You will need to demonstrate that you've implemented a technical and organizational infrastructure that ensures GDPR compliance. What it means in practical terms? That once again, you need to know where the data is, and how to protect it, continually.

Right to be forgotten

A very well-publicized GDPR rule is individuals' right to have personal data deleted, after it is no longer needed. Individuals may also ask to access any information you have on them *(free)*, and may ask to transfer this data from one processing system to another.

Here, too, the issue revolves around where the information is. And if your data is stored in unstructured documents, such as email messages, word processing documents, social media posts, videos and photos, then you'll face a huge project: percentages vary, but some research institutions estimate that unstructured content accounts for a whopping 80-90% of digital data – a lot of it in different types of data storage, different locations, varying formats.

So where's the data?

Data discovery may seem obvious, but it isn't. Qualified security assessors *(QSAs)* report situations where stored personal data is still available, somewhere in physical or digital files or servers, long after it's no longer needed. For example, when uncovering data sources, companies could find expired payment card numbers, or an investment transaction for an extinct startup's shares.

That's why you need to establish mechanisms that can answer the following:

- Where is the data stored?
- Where does it move?
- Who accesses it?

If you don't already know where PII and payment card data is located, you can use a data discovery tool *(e.g., Spirion, Ground Labs)*, to locate it in your organization.

Then, once you know what type of sensitive data you have, what format it's in and where it's located, you can decide how you want to handle it. Using accredited, cloud-based solutions like ShieldQ, which enables you to receive and store data in a compliant control panel, you could choose to delete, encrypt or redact the data; or place it in quarantine.

Such solutions will let you keep track of every single bit of GDPR-relevant data. Using strict access policies, you can decide who shares the data.

You could also accurately classify, index and store data.

How do you protect the data?

Once you know where the data is, you need to conduct a privacy risk assessment exercise, to determine how well protected information is.

This type of protection includes:

- Implementing internal processing, providing very detailed information on why you need to process personal data, and how long you plan to keep it. This requires organized retention policies.
- Keeping technical and organizational records to prove you are protecting data

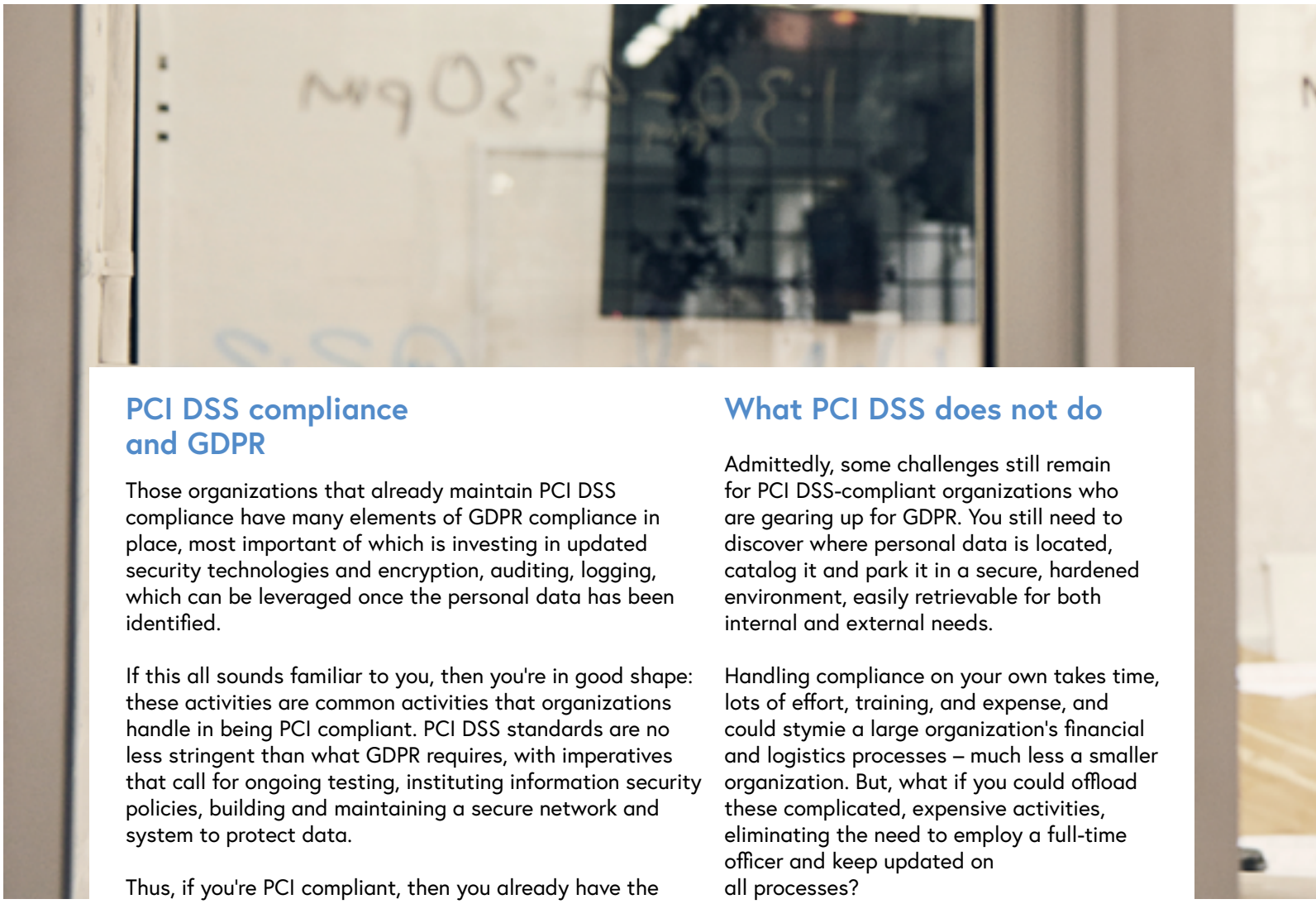
"Those organizations that already maintain PCI DSS compliance have many elements of GDPR compliance in place, most important of which is investing in updated security technologies and encryption, auditing, logging, which can be leveraged once the personal data has been identified"

You'll need to prove you have these mechanisms in place, so that when the SA comes to call, you'll be covered. That's why it's so key to ensure your IT systems are set up and updated for maximum data protection, even though it may require your IT team to learn new technologies, and to always be on guard, day in and day out. Unfortunately, many companies still use outdated security systems and data protection software; it's only to be expected, considering that new threats appear daily, requiring ever new solutions.

But that means that your IT team must be on guard all the time, to protect your systems from any breaches, or else face GDPR's stiff non-compliance fines. It means hiring a full-time security officer to make sure you're compliant. It also means ongoing investment in security software that has built-in obsolescence.

You'll find yourself shelling out and shelling out, with no end in sight.

These requirements can paralyze organizations into inaction, with great consequences. But if you're already PCI DSS compliant, you're already halfway there.



PCI DSS compliance and GDPR

Those organizations that already maintain PCI DSS compliance have many elements of GDPR compliance in place, most important of which is investing in updated security technologies and encryption, auditing, logging, which can be leveraged once the personal data has been identified.

If this all sounds familiar to you, then you're in good shape: these activities are common activities that organizations handle in being PCI compliant. PCI DSS standards are no less stringent than what GDPR requires, with imperatives that call for ongoing testing, instituting information security policies, building and maintaining a secure network and system to protect data.

Thus, if you're PCI compliant, then you already have the infrastructure in place.

You'll have already taken steps to protect stored data by

1. **Maintaining an information security policy.** Similar to GDPR, where you need to establish accountability for protecting data.

2. **Developing secure systems and applications.** Like GDPR, putting in place the mechanisms you need to ensure compliance, including a firewall, continually updated antivirus software, access control and any other systems required to prevent data breaches.

3. **Encrypting cardholder data and sensitive information.** You need to ensure it's protected when in motion across public networks. Encryption is similar to pseudonymous data, which is actually considered part of personal information, excluded from data breach notifications because it has little chance of being unencrypted successfully.

What PCI DSS does not do

Admittedly, some challenges still remain for PCI DSS-compliant organizations who are gearing up for GDPR. You still need to discover where personal data is located, catalog it and park it in a secure, hardened environment, easily retrievable for both internal and external needs.

Handling compliance on your own takes time, lots of effort, training, and expense, and could stymie a large organization's financial and logistics processes – much less a smaller organization. But, what if you could offload these complicated, expensive activities, eliminating the need to employ a full-time officer and keep updated on all processes?

You could rely on secure, cloud-based services that ensure compliance. With such a solution, you can eliminate situations that may come back to bite you: An accredited, document acceptance and storage solution like ShieldQ provides the best of all worlds – keeping all data safe in a unified environment that meets the most stringent compliance standards.

Although there are those who may still be reluctant to use a solution that is out in the cloud, such products for years have shown to be as secure as solutions implemented within an organization – with the added assurance that no one can access the cloud unless they have permission. They are also accessible anywhere, at any time.

How it works

You can accept data via uploads, emails or faxes, forwarded into ShieldQ's central control panel. All information is accessible from anywhere, but by permission only, using two-factor authentication. ShieldQ also lets you share individually or by group, automatically or manually.

What about all the sensitive data you've uncovered in physical folders? Scan them into ShieldQ, and have it all readily available, whenever you need it.

Retrieval becomes easy too: no more looking for a needle in a haystack: define customized search terms based on your own, common business lingo.

It's simple to comply with GDPR's data deletion requirements: just set up retention policies based on your chosen parameters. For example, you can assign a blanket rule; e.g., "delete after 90 days," or an individual rule per document, assigning a date, and you're done.

No matter which storage policies you choose, you can retain documents free for the first 12 months.

"Although there are those who may still be reluctant to use a solution that is out in the cloud, such products for years have been shown to be as secure as solutions implemented within an organization – with the added assurance that no one can access the cloud unless they have permission. They are also accessible anywhere, at any time"

Need more info?

GDPR changes the rules of the game for organizations worldwide. And it can be confusing. Contact us with any questions you may have on whether your organization is ready for GDPR.

ShieldQ

Global offices:

Interfax Communications Limited,
Unit 7, Coolport Coolmine Business Park,
Blanchardstown, Dublin 15, Ireland, D15 HC91

Phone: +353 1 905 8968
Email: sales@shieldq.com

US offices:

Interfax Communications US
7915 Westglen, Houston,
TX 77063, USA

Phone: 1 (713) 429 1217
Email: salesus@shieldq.com

www.shieldq.com