GDPR Compliance – Take a lead from PCI DSS in your contact centre, says Encoded

Submitted by: PR Artistry Limited
Tuesday, 11 July 2017

Robert Crutchington and Matthew Tyler outline how applying the same principles as PCI DSS can help to meet the challenges of new data protection legislation

With the General Data Protection Regulation (GDPR) coming into force on 25th May 2018, many organisations are starting to consider what it will mean for them. Overriding national data protection laws and including new and more detailed protection legislation for personal data, GDPR will necessitate a review of data policies and practices that companies already have in place to ensure that they comply with how data is kept throughout the organisation.

GDPR is more than just payment card data

Many are seeing the introduction of the new legislation as a positive step. It encompasses how data is managed, processed and deleted by concentrating on ensuring that it is lawfully and fairly protected by documented and verifiable security measures. It includes all of a company's data dealing with EU citizens, such as that held in marketing, sales and finance, not just CRM systems in contact centres. It also contains a raft of new rights for individuals ie. data subject rights, these include the right to data portability, the right to be forgotten and a strengthening of access to their data or data access requests.

In essence this regulation aims to achieve two things:
•A single set of rules applying to all EU member states, creating a single digital marketplace
•Moving the rights of data to the data subject or individual

Organisations that fail to comply with the legislation face punitive fines of up to 4% of their annual global turnover or €20m, whichever is greater, not to mention reputational damage. So what does this mean for contact centres?

The good news - PCI DSS principles apply
Contact centres have always been focused on security of card payments, ensuring that customer card data is stored, transmitted or processed securely. Now the process needs to apply to all personal customer data – or Personally Identifiable Information (PII).

The good news is that if your contact centre is already Data Protection Act (DPA) compliant then you will be a long way to being GDPA compliant. In addition, the Payment Card Industry Data Security Standard (PCI DSS) is intended to protect cardholder data, which means that by complying with PCI DSS, you can be sure you meet legislation, security requirements and the burden of proof of compliance (which falls on the call centre), by demonstrating adherence to a recognised security standard.

Plus, if you are already working with a PC1 DSS Level 1 supplier, which is also DPA compliant, this further ensures you meet the regulations for your payment data.

De-scoping makes it easier to manage

To be PCI DSS compliant, organisations have to demonstrate that they have reached a level of security awareness and competence to a point where the risk of losing debit and credit card data is regarded as less than that of a non PCI DSS compliant organisation.

Therefore, PCI DSS principles are a good place to start when thinking about personal data. Companies can apply a process of ‘de-scoping’ to reduce the number of requirements (tick-boxes) for PCI compliance. This same method can be applied to personal information, where business processes can be ‘de-scoped’ from sensitive personal data, by the use of data anonymization, similar to the tokenisation solutions widely used to take repeat card payments without having access to sensitive card details.

Businesses attempt to reduce their PCI DSS scope by limiting the number of places where card data is present in a variety of ways including; removing redundant and obsolete storage facilities and applications, using technology solutions like tokenisation (unique identifiers that retain all the essential information about the data securely) and outsourcing elements of card handling, storage and processing to PCI DSS compliant third parties. As well as taking a risk based approach to justify proportionate controls and eliminate disproportionate costs.

Choose your partners carefully

If you do choose to work with partners it is a requirement of PCI DSS, to draw up a responsibility matrix, outlining compliance and competencies. This can help to set out what needs to be done and who is responsible to ensure data is secure. It’s also important to draw up a data breach plan, to identify what needs to happen in the event of a data breach – what actions need to be taken, regulatory disclosure, communications to stakeholders and customers, as well as forensic investigation.

Improve processes and agent training

Compliance with any legislation, whether PCI DSS or data protection, is not simply about implementing a piece of technology, it involves people and business processes as well as systems.

One of the biggest risks in any organisation relating to data is staff - not necessarily from fraudsters, but laxity of people in taking proper care of data. The relatively low cost of training and education of the risks involved can go a long way in making staff vigilant to perils such as phishing emails and fraudulent representation. Phishing emails can mean that innocently staff allow hackers to enter the system, and is a bigger risk than a rogue staff member writing the odd card number down.

A Trusted Partner takes away the headache

Taking areas of an organisation’s business out of the scope of PCI DSS compliance minimises the cost and complexity associated with many of the standards. Working with a Trusted Provider (one that is PCI-DSS Level 1) for your payment data ensures that you are compliant in the contact centre for payments data and is a good place to start on data protection. The Information Commissioner’s Office (ICO) has also published guidance [1] for companies preparing for GDPR to help plan an approach and identify what needs to be done.

Like PCI DSS compliance, the responsibility for GDPR cannot be entirely removed from the contact centre, however, the effort required can be dramatically reduced by following a similar approach to that of

de-scoping.

Remember that the buck stops with the merchant to ensure PCI DSS compliance and the same will be true for GDPR. Responsibility cannot simply be handed over to a third party – an organisation must also identify itself how data is to be managed. However, taking a lead from PCI DSS and working with the right people can go a long way to sleep filled nights and compliant days.

This article was co-authored by Rob Crutchington, managing director of PCI DSS Level 1 payment service provider Encoded and Matthew Tyler, director of information security specialists, Blackfoot.

[1]Information Commissioner's Office (ICO) published guidance (https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf)

ENDS

About Encoded

Encoded is a UK company founded in 2001 to offer affordable, pay-as-you-go IVR and payment solutions to small and large businesses. Hundreds of contact centres now rely on Encoded secure automated payments for their PCI DSS compliance requirements. Today the company's software supports many of the UK's leading brands including Virgin Holidays, Mercedes-Benz Finance, Green Star Energy and Anglian Water Business.
All the company's services are designed to fulfil three key objectives:
• Reduce costs by automating card payments
• Increase security around payments and reduce PCI DSS compliance scope
• Improve customer service by maximising resource efficiency.

Solutions include:

• Virtual Terminal Payments
• IVR Phone Payments
• Agent Assisted Card Payments
• Web Payments
• Tokenisation (Automated Recurring Payments)
For more information please visit: ENCODED (http://www.encoded.co.uk)

About Blackfoot

Blackfoot specialises in cyber security, data protection and compliance, helping clients make informed pragmatic decisions in an increasingly complex and regulated world. Blackfoot's risk based approach ensures focus is applied to what's most important to their clients.
For more information please visit: BLACKFOOT (http://www.blackfootuk.com)

Press contact:

Mary Phillips/Andreina West
PR Artistry Limited
T: +44 (0)1491 845553
E: mary@pra-ltd.co.uk