# What happens next? 3 Steps to contact centre compliance

Submitted by: PR Artistry Limited
Wednesday, 31 July 2019

Rob Crutchington at Encoded looks at the impact of GDPR on contact centres and discusses three ways to help them remain compliant using technology

Contact centres are challenging places. There is certainly plenty to think about with the rising cost of salaries, managing schedules to meet customer demand, looking after staff wellbeing, PCI DDSS compliance and now the added requirements of GDPR (General Data Protection Regulation).

Initial concerns about how the new GDPR regulations would affect contact centres, in terms of increasing costs and complexity of managing enquires, have to some extent dissipated. For those contact centres taking payments and already PCI DSS compliant, it was a relatively straightforward process to embrace GDPR regulations. They had typically invested in secure technologies, encryption and working with third party compliant companies in terms of PCI DSS. On the whole they were able to extend their technology and processes to protect personal data and meet GDPR requirements.

However, other organisations are still evaluating how new ways of streamlining processes can help meet GDPR data governance and management regulation, but are uncertain how to choose the best solution. At Encoded we have identified three ways that contact centres can apply technology to help them remain GDPR compliant:

1. Mobile Automated Identification & Verification (ID &V) - often a significant amount of time can be spent on identifying and verifying the caller. Having a person perform this task is expensive and means that customer data is at risk. A customer engagement platform is an alternative way to offer a cost-effective, secure solution to automate the screening and identification process. It can take the customer through set identification questions using Artificial Intelligence (AI) to simulate agent conversations, or it can use SMS text messages to authenticate the device being used. On initial registration and once the two-factor authentication process has been successful, the platform will accept and authorise payment requests that are automatically debited from the card holder's account.

The advantage of this approach is that all information is encrypted and the agent is not exposed to any personal data, thereby complying with GDPR and PCI DSS. The data is processed and stored securely elsewhere. In addition, having signed up to the service, the customer has agreed to a data handling agreement that sets out how their information can be shared with a third party, ensuring confidentiality.

2. Customer self-service screening using IVR - accepting credit and debit cards via IVR has long proved to be an effective and secure way of taking payments. It allows customers to pay quickly, via their own unique identifiers – a PIN, date of birth, even voice recognition. Again, reducing or removing agent contact time is a more secure way for contact centres and their customers to comply with PCI DSS. Since everything is fully automated and confidential, the client information is stored centrally and securely within the system hosting the data, taking it out of scope for both PCI DSS and GDPR.

Capturing customer data via IVR also enables calls to be routed to the right agent with the correct

skills, in the event of a request to speak to an advisor. The agent then has all of the relevant information available to manage the call successfully, but with key identification data screened, thereby ensuring GDPR compliance.

3. Cloud-based third party payment solutions – the third option to consider, and one that has gained significant traction over recent years, is to choose a cloud-based payment service provider. A trusted third party that complies with PCI DSS demonstrates proven adherence to a recognised security standard, which can also help contact centres to meet the GDPR legislation. Companies can apply a process of 'de-scoping' to reduce the number of requirements (tick-boxes) for GDPR, in the same way that they might do for PCI DSS compliance.

Of course, 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 working in partnership with a payment solution provider.

Aligning GDPR and PCI DSS – the route to successful compliance

There is no doubt that GDPR has improved standards around privacy and data protection but at what cost? Contact centres that have worked hard to blend people and technology to enhance data and payment processes in the last year, have typically done everything they can to comply with both GDPR and PCI DSS.

For the rest, the good news is that it's not too late to review what's in place and make the switch, to new technology and/or a third party solution provider, to enable a secure, multi-channel seamless route for customer payments. The choice is there for the taking.

Rob Crutchington is Managing Director of Encoded – www.encoded.co.uk

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.  Many 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 FS, BMW FS, Green Star Energy and Anglian Water Services.

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:
• Agent Assisted Card Payments
• IVR Phone Payments
• Mobile App
• Instant Messaging, SMS Customer Engagement
• Virtual Terminal Payments

• Web Payments

For further information visit Encoded (http://www.encoded.co.uk)

Press Contacts
Mary Phillips/Andreina West
PR Artistry Limited
01491 845553
mary@pra-ltd.co.uk