Leveraging your investment in PCI DSS for GDPR

We can benefit from many of the gains we have achieved within PCI DSS for GDPR.

PCI DSS in the UK is beginning to win the battle in reducing credit card fraud as demonstrated by the annual reduction in 2017 of debit and credit card fraud from £618m to £566m. Other than frauds including internal actors, nearly all frauds were perpetrated against businesses that were not PCI DSS compliant. According to Verizon's 2018 Data Breach Investigations Report, 73% of 2017 breaches were perpetrated from outsiders. This leads to the conclusion that PCI DSS as a set of security controls has been very successful in stopping external actors from gaining access to sensitive cardholder data. This short paper proposes that organisations adopt the lessons learned through PCI DSS in addressing the security requirements of privacy data under GDPR.

Unlike PCI DSS, GDPR is not a prescriptive regulation. It is clear that privacy data should be made secure and it documents the potential fines should such privacy data be compromised. However, it does not state how such data should be made secure. As the 300 plus PCI DSS prescriptive security controls have been successful in protecting card privacy data from outsiders, it is proposed that these same controls be applied to securing GDPR privacy data. Furthermore, as the PCI DSS controls have been less successful in protecting sensitive cardholder data from internal actors, it is proposed that this is addressed additionally in securing GDPR privacy data.

There have been a number of key lessons learned in cost effectively achieving PCI DSS. The first of these has been how to de-value data. The primary techniques utilised within PCI DSS to achieve this has been through encryption and tokenisation. It has been discovered how critical it is to de-value the data at the end point at which the data is captured.

Unlike PCI DSS, GDPR is not a prescriptive regulation. It is clear that privacy data should be made secure and it documents the potential fines should such privacy data be compromised. However, it does not state how such data should be made secure.

Many frauds are perpetrated where data is being transmitted rather than at rest. If privacy data is de-valued prior to transmission this eliminates this risk.

As tokenised data is deemed out of scope from PCI DSS controls, there are considerable advantages of de-valuing data through tokenisation. This eliminates the necessity of the 300 plus PCI DSS controls for the infrastructure as the environment is now handling tokens as opposed to cardholder data. The same principals will hold true for GDPR in that devalued privacy data through tokenisation is not at risk and therefore could be deemed out of scope for GDPR. By reducing the scope, this can vastly reduce risk and the cost of securing privacy data as less infrastructure requires the necessary security controls.

Where PCI DSS and GDPR diverge is that PCI DSS is predominantly concerned with numeric data and GDPR privacy data is alphanumeric. So where end points have been secured with P2PE devices for PCI DSS, this will not be possible for GDPR. However, this does not eliminate the need to secure the privacy data at the end point on which it is captured. By isolating the privacy data from the end point device and performing tokenisation within this isolated environment, it is possible for the end device to only be exposed to de-valued data. This isolation is achieved by creating a secure environment on the device with remote security controls that shield it from the device itself. These protections afford the ability to still secure the privacy data even if the device itself has been compromised.

Having established this secure isolated environment on the device, then the device can be securely connected with an audit certified cloud where tokenisation and communications to third parties can be managed. This secure cloud environment provides remote desktop sessions on which the privacy data is captured and visualised to the end point device. As the isolated environment on the device prevents any keyboard logging, screen printing and frame images, the privacy data remains secure.

Such an architecture removes all privacy data from organisations and has their privacy data managed in a third-party token vault. Alternatively, organisations can implement their own token vault and have this

DataDivider reports

By adopting tokenisation for all GDPR privacy data and implementing the tokenisation and de-tokenisation within isolated secure devices, we can vastly reduce the cost of GDPR and the risk of GDPR breaches.

as the sole environment where they have to secure privacy data. It would be recommended that the PCI DSS controls be applied across the token vault infrastructure.

This still leaves the management of privacy data within the business where privacy data is required for more than viewing on a device. Where the privacy data is required to communicate with bonefide third parties then this can be managed through the secure cloud environment, again not increasing GDPR scope or exposing the organisation to privacy data. Where privacy data must be printed for external distribution then it would be recommended to utilise a specialist secure partner. If printing is required internally then an isolated network would need to be established with all PCI DSS security controls applied within this environment.

Finally, we need to address how to protect GDPR privacy data from internal actors. By de-valuing the data through tokenisation, we have made the first step in protecting this privacy data. The next required step is in controlling bulk detokenisation. Only a few bonefide processes will require this function. By restricting bulk de-tokenisation to these bonefide processes and alerting upon bulk de-tokenisation it is possible to safe guard against fraudulent internal actors.

In conclusion, we can benefit from many of the gains we have achieved within PCI DSS for GDPR. By adopting tokenisation for all GDPR privacy data and implementing the tokenisation and de-tokenisation within isolated secure devices, we can vastly reduce the cost of GDPR and the risk of GDPR breaches. □

DataDivider provides the ability to de-scope desktops, data networks and backend systems for telephone, mail, fax, email and chat payments. Entering its eighth year as a PCI certified Level 1 Service Provider, DataDivider provides its solution to over 80 Level 1 to Level 4 merchants.

For more information, please visit
datadivider.com

δ/δ datadivider