Obrigações de controlo de fornecedores externos

Padrão de segurança dos dados no setor dos cartões de pagamento (PCI DSS)

Versão 13.0 Datada de setembro de 2023

Obrigação do PCI DSS	Descrição	Por que é importante
1. Conseguir a conformidade no âmbito dos dados de cartões	O fornecedor estará em conformidade com as atuais versões dos Padrões de segurança de dados no setor dos cartões de pagamento emitidos pelo Payment Security Standards Council, como o PCI DSS, PA-DSS, PCI-P2PE, PCI-PTS, PCI Card Production.	Proteger os dados do titular do cartão: o padrão reconhecido para alcançar este objetivo é o PCI DSS, sendo um requisito regulamentar global do setor. As normas de segurança do PCI constituem requisitos técnicos e operacionais definidos pelo Payment Card Industry Security Standards Council com vista à proteção dos dados do titular do cartão.
2. Certificado de fornecedor e comerciante	O fornecedor tem de fornecer um Certificado de conformidade (AoC) para avaliações no local ou, sempre que aplicável, um Questionário de autoavaliação (SAQ), aplicável ao âmbito dos serviços prestados ao Barclays, previamente ao contrato e uma vez por ano daí em diante. Tal requisito deverá estar em conformidade com as exigências do PCI DSS - ver www.pcisecuritystandards.org/ Se forem levantadas questões após a análise do AoC, por exemplo, relacionadas com o âmbito dos serviços, com a descrição do ambiente ou com a conformidade do fornecedor em termos de PCI, o Relatório sobre conformidade (RoC) subjacente poderá ser solicitado e analisado para obtenção de mais informações. Poderá ser aceitável um RoC censurado se este confirmar que o âmbito da certificação no PCI também se aplica ao âmbito dos serviços prestados ou a outras questões levantadas pelo Barclays após a análise do AoC. O fornecedor notificará o Barclays caso entre em situação de não conformidade, ou seja, o mais rapidamente possível e nunca após 30 dias a	Evidências de que um fornecedor ou comerciante obteve a conformidade relevante na área dos dados de cartões para o âmbito dos serviços prestados ao Barclays e respeitou os requisitos. Evidência de que os certificados AoC/RoC ou SAQ do fornecedor dizem respeito ao serviço prestado. Se o Barclays estiver a utilizar um fornecedor ou comerciante que não esteja em conformidade com o PCI DSS, este terá de contactar a equipa de Risco de Terceiros da Visa Europa (agentcompliance@visa.com) via e-mail a fim de confirmar que o fornecedor ou comerciante está a implementar o PCI DSS e que forneceu à Visa Europa um plano de estado relativo ao PCI DSS (utilizando o modelo da Visa Europa) para análise e aprovação da Visa Europa.

	contar da data de expiração dos documentos de validação.	
3. Confirmação por parte do fornecedor	O fornecedor terá de confirmar, por escrito, perante o Barclays e antes de celebrar o contrato com este, que é responsável pela segurança dos dados dos titulares de cartões para os seguintes serviços e que este possui/armazena/processa/transmite, ou que poderiam afetar a segurança do ambiente de dados dos titulares de cartões clientes do Barclays, por ex., serviços de segurança (tais como servidores de autenticação), alojamento na Web, etc. Quaisquer alterações ao serviço prestado devem ser confirmadas por escrito ao Barclays antes da implementação da alteração.	**Do PCI DSS v3.2.1** **Procedimento de teste para 12.8.2:** respeitar os acordos escritos e confirmar que incluem uma confirmação, por parte dos prestadores do serviço, de que são responsáveis pela segurança dos dados dos titulares de cartões que estes possuem ou, de outra forma, armazenam, processam ou transmitem em nome do cliente, ou na medida em que poderiam afetar a segurança do ambiente de dados dos titulares de cartões clientes do cliente. Nota: juntamente com o Requisito 12.9, este requisito relativo a acordos escritos entre as organizações e os prestadores de serviços destina-se a promover um nível de entendimento consistente entre as partes relativamente às suas responsabilidades aplicáveis na área do PCI DSS. Por exemplo, o acordo pode incluir os requisitos de PCI DSS aplicáveis a manter como parte do serviço prestado. **Orientação para 12.8.2:** a confirmação por parte dos prestadores de serviços evidencia o seu compromisso em manter um nível adequado de segurança no que concerne os dados dos titulares de cartões que estes obtêm por parte dos seus clientes. As políticas internas e procedimentos dos prestadores de serviços relativos ao processo de envolvimento dos clientes e quaisquer modelos usados para os acordos escritos devem incluir a disposição de uma confirmação na área do PCI DSS destinada aos seus clientes. O método através do qual o prestador de serviço apresenta a confirmação por escrito deve ser acordado entre o prestador e os seus clientes.

Utilização de prestadores de serviços externos/"outsourcing"

Um prestador de serviços ou comerciante poderá utilizar um prestador de serviços externo para armazenar, processar ou transmitir os dados dos titulares de cartões em seu nome, ou para gerir componentes como routers, firewalls, bases de dados, segurança física e/ou servidores. Se assim for, poderá ocorrer um impacto na segurança do ambiente dos dados de titulares de cartões.

As partes devem identificar claramente os serviços e componentes do sistema que são incluídos no âmbito da avaliação do PCI DSS do prestador de serviços, os requisitos do PCI DSS específicos abrangidos pelo prestador de serviços e quaisquer requisitos que sejam da responsabilidade dos clientes do prestador de serviços incluir nas suas próprias análises do PCI DSS. Por exemplo, um fornecedor de alojamento gerido deve definir claramente quais os seus endereços IP analisados como parte do seu processo de análise de vulnerabilidades trimestral e quais os endereços IP cujos clientes devem incluir nas suas próprias análises trimestrais.

Os prestadores de serviços são responsáveis por demonstrar a sua conformidade em termos do PCI DSS, sendo que tal poderá ser solicitado pelas marcas de pagamentos. Os prestadores de serviços devem contactar o seu adquirente e/ou marca de pagamentos para determinar a respetiva validação de conformidade.

Existem duas opções para os prestadores de serviços externos validarem a sua conformidade:

1) **Avaliação anual**: os prestadores de serviços podem submeter-se a avaliações de PCI DSS anuais, de forma autónoma e providenciar evidências aos seus clientes que demonstrem a sua conformidade; ou

2) **Múltiplas avaliações mediante solicitação**: se não realizarem as suas próprias avaliações de PCI DSS anuais, os prestadores de serviços terão de se submeter a avaliações mediante solicitação dos seus clientes e/ou participar em cada análise de PCI DSS dos seus clientes, fornecendo os resultados de cada análise ao(s) respetivo(s) cliente(s).

Se o prestador de serviços externo se submeter à sua própria avaliação de PCI DSS, deverá fornecer evidências suficientes aos seus clientes a fim de confirmar que o âmbito da avaliação de PCI DSS do prestador de serviços abrangeu os serviços aplicáveis ao cliente e que os requisitos de PCI DSS relevantes foram analisados e considerados em vigor. O tipo de evidências específico fornecidas pelo prestador de serviços aos seus clientes dependerá dos acordos/contratos em vigor entre as partes em questão. Por exemplo, fornecer o AoC e/ou secções relevantes do RoC do prestador de serviços (censurado de forma a proteger todas as informações confidenciais) poderá ajudar a prestar todas ou algumas informações.

Adicionalmente, os comerciantes e prestadores de serviços terão de gerir e monitorizar a conformidade de PCI DSS de todos os prestadores de serviços externos associados e com acesso a dados de titulares de cartões. *Consultar o Requisito 12.8 neste documento para obter mais detalhes.*