التزام مراقبة المورّد الخارجي

معيار أمن بيانات صناعة بطاقات السداد (PCI DSS)

الإصدار 10.0، أكتوبر 2020

التزام المعيار PCI DSS	الوصف	الأهمية
1. تحقيق الامتثال لبيانات البطاقة	يمتثل المورّد للإصدارات الحالية من معايير أمان بيانات صناعة بطاقات السداد كما صدرت من قِبل مجلس معايير أمان السداد، مثل: PCI DSS وPA-DSS (معيار أمان بيانات تطبيق السداد) وPCI-P2PE (تشفير صناعة بطاقات السداد من نقطة إلى نقطة) وPCI-PTS (أمان معاملات رقم التعريف الشخصي لصناعة بطاقات السداد) وإنتاج بطاقات PCI.	حماية بيانات حامل البطاقة: يُعد معيار PCI DSS هو المعيار المعترف به لتحقيق ذلك وهو مطلب تنظيمي للصناعة العالمية. وتُمثل معايير أمان PCI متطلبات تقنية وتشغيلية وضعها مجلس معايير أمان صناعة بطاقات السداد لحماية بيانات حامل البطاقة.
2. مصادقة المورد والتاجر	يتعين على المورد تقديم مصادقة امتثال للتقييمات الموقعية (AoC)، أو، عند الاقتضاء، لاستبيان التقييم الذاتي (SAQ)، تنطبق على نطاق الخدمات المقدمة إلى بنك باركليز، قبل التعاقد، وبعده بمعدل سنوي. ويلزم أن يتم ذلك بالتوافق مع متطلبات المعيار PCI DSS - انظر www.pcisecuritystandards.org/ في حال وجود استفسارات تنشأ عند مراجعة AoC مثل ما يتعلق بنطاق الخدمات أو وصف البيئة أو امتثال المورد لمعايير PCI، يمكن طلب تقرير الامتثال (RoC) الأساسي ومراجعته للحصول على مزيد من المعلومات. قد يكون RoC المنقَّح مقبولاً إذا أكد أن نطاق شهادة PCI ينطبق على نطاق الخدمات المقدمة، أو الأسئلة الأخرى التي طرحها بنك باركليز بعد مراجعة AoC. يتعين على المورد إخطار بنك باركليز بمجرد أن يصبح غير ممتثل، أي في أقرب وقت ممكن وفي موعد لا يتجاوز 30 يومًا من تاريخ انتهاء صلاحية مستندات المصادقة.	دليل على أن المورد أو التاجر قد حققا الامتثال لبيانات البطاقات ذات الصلة بنطاق الخدمات المقدمة إلى بنك باركليز والتزما بالمتطلبات. ودليل على أن مصادقة المورد لتقييمات RoC/AoC أو SAQ تتعلق بالخدمة المقدمة. إذا كان بنك باركليز يتعامل مع أي مورّد أو تاجر غير ممتثل للمعيار PCI DSS، فسيُطلب منه التواصل مع فريق أخطار الجهات الخارجية في Visa Europe عبر البريد الإلكتروني (agentcompliance@visa.com) للتأكيد على أن المورّد أو التاجر يطبقان المعيار PCI DSS وأنهما قد قدَّما خطة لحالة PCI DSS (باستخدام نموذج Visa Europe) إلى Visa Europe للمراجعة والاعتماد.

3. إقرار المورد	يلتزم المورد بالإقرار كتابيًا لبنك باركليز قبل التعاقد بأنه مسؤول عن أمان بيانات حامل البطاقة الخاصة بالخدمات الآتية والتي يمتلكها/يخزنها/يعالجها/ينقلها، أو التي قد تؤثر في أمان بيئة بيانات حامل البطاقة من عملاء بنك باركليز، مثل: خدمات الأمان (كخوادم المصادقة) واستضافة الويب وما إلى ذلك. كما يلزم الإقرار كتابيًا لبنك باركليز بأي تغييرات تطرأ على الخدمة المقدمة قبل تنفيذ أي تغيير.	**من المعيار PCI DSS، الإصدار 3.2.1** **إجراء الاختبار للمطلب 12.8.2:** راقب الاتفاقات الكتابية وتأكد من أنها تتضمن إقرارًا من موفري الخدمة بأنهم مسؤولون عن أمان بيانات حامل البطاقة التي يمتلكها موفرو الخدمة أو يقومون بتخزينها أو معالجتها أو نقلها نيابة عن العميل، أو إلى الحد الذي يمكن أن يؤثروا به في أمان بيئة بيانات حامل البطاقة لدى العميل. ملحوظة: بالاقتران مع المطلب 12.9، فإن هذا المطلب المتعلق بالاتفاقات الكتابية بين المؤسسات وموفري الخدمات يهدف إلى تعزيز مستوى ثابت من التفاهم بين الأطراف بشأن مسؤولياتهم المنطبقة الواردة في المعيار PCI DSS. على سبيل المثال، قد تتضمن الاتفاقية الحفاظ على متطلبات المعيار PCI DSS المنطبقة كجزء من الخدمة المقدمة. توجيه للمطلب 12.8.2: يدل إقرار موفري الخدمة على التزامهم بالحفاظ على الأمان المناسب لبيانات حامل البطاقة التي يحصلون عليها من عملائهم. ينبغي أن تتضمن السياسات والإجراءات الداخلية لموفر الخدمة ذات الصلة بعملية مشاركة العملاء وأي نماذج مستخدمة للاتفاقات الكتابية تقديم إقرار معمول به للمعيار PCI DSS إلى عملائهم. كما ينبغي الاتفاق بين موفر الخدمة وعملائه على أسلوب تقديم موفر الخدمة الإقرار الكتابي.

استخدام موفري الخدمات من جهات خارجية/الاستعانة بمصادر خارجية

قد يستعين موفر الخدمة أو التاجر بموفر خدمة من جهة خارجية لتخزين بيانات حامل البطاقة أو معالجتها أو نقلها بالنيابة عنه، أو لإدارة مكونات مثل أجهزة التوجيه و/أو جدران الحماية و/أو قواعد البيانات و/أو الأمان المادي و/أو الخوادم. في هذه الحالة، قد يتأثر أمان بيئة بيانات حامل البطاقة.

ينبغي للأطراف أن تحدد بوضوح الخدمات ومكونات النظام التي يشملها نطاق تقييم المعيار PCI DSS لموفر الخدمة، ومتطلبات المعيار PCI DSS المحددة التي يقوم بها موفر الخدمة، وأي متطلبات يتحملها عملاء موفر الخدمة لتضمينها في مراجعات PCI DSS الخاصة بهم. فينبغي مثلاً أن يحدد موفر خدمات الاستضافة المُدارة بوضوح أيًا من عناوين IP يتم فحصها كجزء من عملية فحص الثغرات الأمنية ربع السنوية التي يقوم بها، وأيًا من عناوين IP يتحمل عميله مسؤولية تضمينها في عمليات الفحص ربع السنوية الخاصة به.

يتحمل موفرو الخدمات مسؤولية إثبات امتثالهم للمعيار PCI DSS، وقد يُطلب منهم القيام بذلك باستخدام العلامات التجارية للسداد. وينبغي لموفري الخدمات التواصل مع البنك المشتري و/أو العلامات التجارية للسداد التي يتعاملون معها لتحديد المصادقة الملائمة للامتثال.

ثمة خياران أمام موفري الخدمات من الجهات الخارجية لمصادقة الامتثال:

1) **التقييم السنوي**: يمكن أن يخضع موفرو الخدمة لتقييم (تقييمات) سنوي للمعيار PCI DSS بأنفسهم، وتقديم أدلة إلى عملائهم لإثبات امتثالهم، أو

2) **التقييمات المتعددة عند الطلب**: إذا لم يخضع موفرو الخدمات لتقييمات المعيار PCI DSS السنوية الخاصة بهم، فسيتعين عليهم إجراء التقييمات عند الطلب من عملائهم و/أو المشاركة في كل مراجعة من مراجعات المعيار PCI DSS الخاصة بعملائهم، مع تقديم نتائج كل مراجعة إلى العميل (العملاء) المعني.

إذا خضعت الجهة الخارجية لتقييم المعيار PCI DSS الخاص بها، فينبغي لها تقديم الأدلة الكافية إلى عملائها للتحقق من أن نطاق تقييم المعيار PCI DSS الخاص بموفر الخدمة يشمل الخدمات المنطبقة على العميل وأنه تم فحص متطلبات المعيار PCI DSS ذات الصلة وتبيَّن أنها قيد التطبيق. وسيعتمد النوع المحدّد من الأدلة التي يقدمها موفر الخدمة إلى عملائه على الاتفاقات/العقود المبرمة بين هذه الأطراف. فقد يسهم تقديم التقييم AOC و/أو الأقسام ذات الصلة من التقييم ROC الخاص بموفر الخدمة (والذي تم تنقيحه لحماية أي معلومات سرية) -على سبيل المثال- في توفير كل المعلومات أو بعضها.

إضافة إلى ذلك، يتعين على التجار وموفري الخدمات إدارة ومراقبة الامتثال للمعيار PCI DSS من قِبل جميع موفري الخدمات من الجهات الخارجية ممن لديهم حق الوصول إلى بيانات حامل البطاقة. *راجع المطلب 12.8 في هذا المستند لمعرفة التفاصيل.*