



Kime: Tüm IATA Seyahat Acenteleri

Tarih: 28 Haziran 2018

Konu: **Ödeme Kartı Sektörü Veri Güvenliği Standardı (PCI DSS)**

Sayın Seyahat Acentesi,

Ödeme Kartı Sektörü Veri Güvenliği Standardı (PCI DSS) uygunluğu ve IATA Yolcu Acentesi Konferansınca onaylanan gereklilikler hakkında çeşitli iletişimler gerçekleştirilmiş bulunmaktadır.

Dağıtım Danışma Konseyi (Yolcu Ajansı Konferansı ve Yolcu Hizmetleri Konferansı'ndan hava yolları, GDS'ler (Global Dağıtım Sistemleri) ve IATA'dan oluşmuştur) adına bu mektubun amacı IATA akredite acenteler için gereklilikleri açıklığa kavuşturmak ve IATA ile GDS'lere gelen ana sorulara yanıt vermektir. PCI DSS Uygunluğu Kanıtının Sağlanması.

Önceki iletişimlerde belirtildiği gibi, eğer acenteniz kredi veya hesap kartı (debit kartı) verilerini işliyor, iletiyor veya depoluyorsa PCI Uyumlu olmanız gereklidir. Bu, ödeme sektörü, özellikle de PCI Konseyi ve Ödeme Programı'nın bir gerekliliğidir. Kendi tüccar KİMLİĞİNİZ (merchant ID) altında veya hava yolu şirketi adına kartla ödeme kabul ediyorsanız PCI Uyumlu olmanız gerekir. Bazı tüccar alıcı bankaları, tüccarlara PCI DSS Uygunluk kanıtı sağlamazlarsa aylık uyumsuzluk ücreti veya güvenlik ihlalleri için her olay başına \$500.000'a kadar cezalar uygulamaktadır.

İlaveten, bir IATA Acentesi olarak Uygunluk Onayınızın (AoC - Attestation of Compliance) bir kopyasını, IATA'nın PCI DSS uygunluk talep tarihini takip eden 30 gün içerisinde IATA'ya ibraz ederek PCI DSS uygunluğunuzun kanıtını sağlamanız gerekmektedir.

PCI SSC web sitesi tarafından sağlanan formata sahip AoC, uygun Öz Değerlendirme Anketinin (SAQ - Self-Assessment Questionnaire) yapıldığını ve PCI DSS ile uygunluk durumunun onaylandığını göstermek için kullanılan tek belgedir. PCI DSS doğrulamasında uygunluk sertifikaları kabul edilmez.

Şu anda BSP üzerinden Kredi Kartıyla ödeme şeklini kullanan herhangi işlem yürütmüyorsanız ve yürütmeyi düşünmüyorsanız, Kredi Kartı Geçmeme Beyanını gönderebilirsiniz.

PCI DSS yönergelerine göre, tüm Seyahat Acenteleri 12 aylık süre içerisindeki kredi işlemi miktarlarına dayalı olarak dört tüccar seviyesinden birisinde olacaktır, seviye 1 en yüksek (yılda 6 milyondan fazla işlem) ve seviye 4 en düşük (yılda 20.000'den az işlem) olanıdır.

Kredi kartı kabul ediyorsanız ve henüz hazır değilseniz, uyumluluk sağladığınızdan emin olmak için izlemeniz gereken temel seçenekler şunlardır:

**a)** Yetkili Güvenlik Denetçisi (Qualified Security Assessor - QSA) olarak bilinen bir sertifikalı PCI Güvenlik Standartları Konseyi ortağından sertifika alın. IATA sadece bir sertifikalı PCI Güvenlik Standartları Konseyi ortağından alınmış olan uygunluk kanıtını kabul edecektir. Uygunluğu sertifikalayan belgeye PCI Konseyinin antetli kâğıdının dâhil olduğundan lütfen emin olun, belgenin başlığında "Uygunluk Onayı" (Attestation of Compliance) yazıyor olması zorunludur, bu genellikle pdf formatında mevcuttur. Kabul edilecek tek resmi belge budur.

**b)** Eğer seviye 2, 3 veya 4 iseniz, PCI DSS ayrıca öz değerlendirme anketini doldurmak için QSA kullanmak yerine, kendi kendinize, kendi seyahat acentenizden genel veri güvenliği sorumluluğu/gözetim görevi olan bir görevli tarafından imzalanan bir dahili değerlendirme yapma seçeneği sağlamaktadır.

Her iki seçenek için de, IATA talebinden sonra, AoC veya Kredi Kartı Geçmeme Beyanı IATA Müşteri Portalına yüklenmelidir.

Acentelerin ilk grubu başlatılmış olup çok yakında tüm ülkelerin PCI DSS uygunluk kanıtını ibraz etmeleri gerekecektir.

PCI DSS hakkında daha fazla bilgi, tahsis edilen web sayfasından bulunabilir <http://www.iata.org/services/finance/pages/pci-dss.aspx>. Ayrıca, Herhangi bir yorumunuz ve sorunuz olursa lütfen Müşteri Portalımız ([www.iata.org/cs](http://www.iata.org/cs)) üzerinden bizimle iletişime geçmekten çekinmeyin

Saygılarımızla,  
**IATA Global Sevkiyat Merkezi**