AMERICAN EXPRESS

Adatvédelmi működési szabályzat (DSOP)

Fogyasztóvédelemben élenjáró cégként az American Express sok éve elkötelezett a kártyatulajdonosi adatok és az érzékeny hitelesítési adatok védelme mellett, garantálva ezen adatok biztonságát.

Az adatok veszélybe kerülése kedvezőtlen hatással van a fogyasztókra, a kereskedőkre, a szolgáltatókra és a kártyakibocsátókra. Akár egyetlen incidens is súlyosan csorbíthatja a vállalat hírnevét, és csökkentheti képességét a hatékony üzletmenetre. Ha ezt a kockázatot biztonsági működési szabályzatok bevezetésével kezelik, az segíthet növelni a fogyasztói bizalmat, fokozni a nyereségességet, valamint javítani a vállalat hírnevét.

Az American Express tisztában van azzal, hogy kereskedőink és szolgáltatóink (együttesen: **Ön vagy Önök**) osztoznak az aggályainkban, és elvárja, hogy ezért kötelezettségeik részeként Önök betartsák az American Express® kártya elfogadásával (kereskedők esetében) vagy feldolgozásával (szolgáltatók esetében) kapcsolatos szerződés (külön-külön mindegyik: **szerződés**) adatvédelmi rendelkezéseit, valamint a jelen *adatvédelmi működési szabályzat* mindenkor hatályos verzióját. Ezek a követelmények vonatkoznak az Ön minden olyan berendezésére, rendszerére és hálózatára (és ezek összetevőire), amelyeken titkosítási kulcsokat, kártyatulajdonosi adatokat vagy érzékeny hitelesítési adatokat (vagy ezekből álló kombinációt) tárolnak, dolgoznak fel vagy továbbítanak.

Az itt használt, de a szövegben nem definiált, nagy kezdőbetűvel írt kifejezések jelentésének magyarázata a jelen szabályzat végén lévő szószedetben található.

1. rész Titkosítási kulcsok, kártyatulajdonosi adatok és érzékeny hitelesítési adatok védelmére vonatkozó előírások

Ön köteles az alábbiakat betartani és a szerződött feleivel betartatni:

- kizárólag abból a célból tároljon kártyatulajdonosi adatokat, hogy a szerződésnek megfelelően és annak előírásai szerint elősegítse az American Express kártyát érintő tranzakciókat.
- feleljen meg a kártyatulajdonosi adatok és érzékeny hitelesítési adatok Ön által végzett feldolgozására, tárolására vagy továbbítására érvényes PCI DSS- és PCI SSC-követelmények hatályos verziójának legkésőbb a vonatkozó követelmény adott verziója hatálybalépésének napjától.
- kizárólag a PCI által jóváhagyott PIN-beviteli eszközöket vagy fizetési alkalmazásokat (vagy mindkettőt) használjon, amikor új vagy a régit felváltó eszközt vezet be a felügyelt helyszíneken.

Ön köteles a jelen adatvédelmi rendelkezéseknek megfelelően védeni a szerződés szerint megőrzött terhelési és jóváírási American Express-nyilvántartásokat; ezeket a nyilvántartásokat kizárólag a szerződés szerinti célokra használhatja fel, és annak megfelelően köteles védeni azokat. Ön anyagi és egyéb felelősséggel tartozik az American Express felé annak biztosításában, hogy a szerződött felei betartják a jelen adatvédelmi rendelkezéseket (azon túl, hogy bizonyítja, hogy a szerződött felei is betartják a jelen szabályzatot a lenti 4. rész, „Az Ön rendszereinek fontos periodikus érvényesítése” – szerint, kivéve, ha ez a rész másként nem rendelkezik).

2. rész Adatvédelmiincidens-kezelési kötelezettségek

Ön köteles értesíteni az American Expresst haladéktalanul, de legfeljebb huszonnégy (24) órával azt követően, hogy adatvédelmi incidensről szerez tudomást.

Kérjük, az American Express értesítése érdekében forduljon az American Express Enterprise Incident Response Programhoz (*EIRP*) a +1 (602) 537-3021-es telefonszámon (a + jelzi a nemzetközi közvetlen hívás [„IDD"] előtagot, nemzetközi hívásdíj vonatkozik rá), vagy e-mailben az EIRP@aexp.com címen. Az adatvédelmi incidens vonatkozásában Önnek kötelessége kijelölni egy személyt kapcsolattartóként. Ezenfelül:

- Minden adatvédelmi incidensről alapos igazságügyi vizsgálatot kell lefolytatnia.
- A 10 000 vagy annál több egyedi kártyaszámot érintő adatvédelmi incidens esetében egy Ön által alkalmazott PCI-igazságügyi nyomozónak (PCI Forensic Investigator, PFI) kell lefolytatnia ezt a vizsgálatot öt (5) napon belül azt követően, hogy az adatvédelmi incidensről tudomást szereztek.
- Az igazságügyi nyomozói jelentést szerkesztés nélkül át kell adni az American Express részére az elkészüléstől számított tíz (10) munkanapon belül.
- Ön köteles haladéktalanul megadni az American Expressnek minden feltört kártyaszámot. Az American Express fenntartja a jogot, hogy saját belső elemzést végezzen az adatvédelmi incidens által érintett kártyaszámok azonosítása érdekében.

Az igazságügyi vizsgálati jelentést a PCI-nál elérhető végleges incidensvizsgálati jelentés sablon használatával kell elkészíteni. A jelentésnek tartalmaznia kell az igazságügyi felülvizsgálatokat, a megfelelőségi jelentéseket és minden más információt az adatvédelmi incidenssel kapcsolatban; azonosítania kell az adatvédelmi incidens okát; igazolnia kell, hogy Ön betartotta-e a PCI DSS-t az adatvédelmi incidens időpontjában; továbbá alá kell támasztania azt is, hogy Ön minden későbbi adatvédelmi incidenst meg tud akadályozni azzal, hogy (i) tervet biztosít az összes PCI DSS-hiányosság orvoslására, és (ii) részt vesz az American Express (alábbiakban ismertetett) megfelelési programjában. Az American Express kérésére Ön köteles a hiányosságok orvoslásáról szóló, minősített biztonsági felmérő (Qualified Security Assessor, QSA) által készített igazolást rendelkezésre bocsátani.

A jelen 2. rész, „Adatvédelmiincidens-kezelési kötelezettségek" fenti bekezdéseitől függetlenül:

- Az American Express saját mérlegelési jogkörében felkérheti Önt, hogy bízzon meg egy PFI-t azzal, hogy folytasson vizsgálatot a 10 000-nél kevesebb egyedi kártyaszámot érintő adatvédelmi incidensek esetén is. Minden ilyen vizsgálatnak meg kell felelnie a jelen 2. rész, „Adatvédelmiincidens-kezelési kötelezettségek" fentebb meghatározott követelményeknek, és az American Express által előírt határidőn belül kell befejeződniük.
- Az American Express saját mérlegelési jogkörében külön is megbízhat egy PFI-t, hogy folytasson vizsgálatot valamely adatvédelmi incidens kapcsán, és a vizsgálat költségeit Önre terhelheti.

Ön vállalja, hogy az adatvédelmi incidensből eredő bármely probléma orvoslása érdekében együttműködik az American Express-szel, ideértve az American Express-szel történő egyeztetést az Ön által az adatvédelmi incidenssel érintett kártyatulajdonosokkal folytatott kommunikációról, továbbá az American Express részére minden arra vonatkozó releváns információ átadását (és az átadáshoz szükséges bármely joglemondás biztosítását), hogy Ön a szerződésnek megfelelő módon meg tud akadályozni minden későbbi adatvédelmi incidenst.

A szerződésben foglalt bármely ellenkező tartalmú titoktartási kötelezettségtől függetlenül az American Expressnek jogában áll bármely adatvédelmi incidensről információt közzétenni az American Express-kártyatulajdonosok és -kártyakibocsátók, az American Express-hálózat más résztvevői, továbbá a vonatkozó jogszabályok által előírtak szerint a nyilvánosság részére; tekintettel bírósági, közigazgatási vagy egyéb hatósági végzésben, rendeletben, idézésben, felhívásban vagy egyéb eljárásban foglaltakra; hogy csökkentse a csalás vagy más kár bekövetkezésének kockázatát; vagy egyébként az American Express-hálózat működtetéséhez szükséges mértékben.

3. rész Kártalanítási kötelezettségek adatvédelmi incidens esetén

Az Ön szerződés szerinti, az American Express felé fennálló kártalanítási kötelezettségeit adatvédelmi incidens bekövetkezése esetén a jelen 3. rész, „Kártalanítási kötelezettségek adatvédelmi incidens esetén" határozza meg az American Express bármely más jogának és jogorvoslati lehetőségének sérelme nélkül. Kártalanítási kötelezettségein felül – ha van ilyen – előfordulhat, hogy a jelen 3. rész, „Kártalanítási kötelezettségek adatvédelmi incidens esetén" alább meghatározott kötbért kell fizetnie az adatvédelmi incidensre vonatkozóan.

Azon adatvédelmi incidensekért, amelyek:

- legalább 10 000 American Express-kártyaszámot érintenek a következők egyikével:
  - érzékeny hitelesítési adatok, vagy
  - lejárati dátum

  Ön köteles az American Expresst számlaszámonként 5 USD díjon kártalanítani.

Azonban az American Express nem követel Öntől kártérítést azon adatvédelmi incidensek esetén, amelyek:

- 10 000-nél kevesebb American Express-kártyaszámot érintenek, vagy
- 10 000-nél több American Express-kártyaszámot érintenek, amennyiben Ön teljesíti az alábbi feltételeket:
  - Ön értesítette az American Expresst az adatvédelmi incidensről a jelen 3. rész, „Kártalanítási kötelezettségek adatvédelmi incidens esetén" szerint,
  - az adatvédelmi incidens időpontjában Ön betartotta a PCI DSS-t (az adatvédelmi incidens PFI általi vizsgálatának megállapítása szerint), és
  - az adatvédelmi incidenst nem az Ön vagy az Ön szerződött feleinek jogellenes magatartása okozta.

A jelen 3. rész, „Kártalanítási kötelezettségek adatvédelmi incidens esetén" fenti bekezdéseitől függetlenül Ön bármely adatvédelmi incidensért – függetlenül az American Express-kártyaszámok számától – köteles az American Express részére adatvédelmi incidensenként legfeljebb 100 000 USD összegű adatvédelmi incidensre vonatkozó kötbért fizetni (az American Express által saját mérlegelési jogkörében meghatározottak szerint) abban az esetben, ha Ön nem tesz eleget a 2. rész, „Adatvédelmiincidens-kezelési kötelezettségek" szerinti valamely kötelezettségének. A félreértések elkerülése érdekében az egyes adatvédelmi incidensekért megállapítható adatvédelmi incidensre vonatkozó kötbér teljes összege nem haladhatja meg a 100 000 USD-t.

Az American Express nem veszi számításba azokat az American Express-kártyaszámlaszámokat, amelyek érintettek voltak egy korábbi adatvédelmi incidenssel kapcsolatban benyújtott kártérítési igényben az értesítési határidőt megelőző tizenkét (12) hónapon belül. Az American Express által ezzel a módszerrel végzett minden számítás végleges.

Az American Express a szerződésnek megfelelően kiszámlázhatja az adatvédelmi incidensekért fizetendő kártérítési kötelezettség teljes összegét, vagy le is vonhatja az összeget az American Express által Önnek fizetendő összegből (illetve ennek megfelelően megterhelheti az Ön bankszámláját).

A kereskedők kártalanítási kötelezettségei az itt foglalt adatvédelmi incidensek tekintetében nem tekintendők a szerződés szerinti járulékos, közvetett, spekulatív, következményi, rendkívüli, büntető jellegű vagy a károkozás kirívó jogellenessége miatt a kár tényleges összegét meghaladó kártérítési kötelezettségnek, feltéve, hogy ezen kötelezettségek nem kapcsolódnak elmaradt haszonnal, jó hírnév vagy üzleti lehetőségek elvesztésével kapcsolatos vagy ilyen jellegű károkhoz.

Az American Express saját jogkörében eljárva csökkentheti a kereskedők kártalanítási kötelezettségét, de kizárólag azon adatvédelmi incidensek vonatkozásában, amelyek megfelelnek az alábbi követelményeknek:

- a megfelelő kockázatcsökkentő technológiákat az adatvédelmi incidenst megelőzően igénybe vették, és az adatvédelmi incidens teljes eseményidőszaka alatt alkalmazták;
- a PFI-programmal összhangban lévő alapos vizsgálatot lefolytatták (amennyiben előzetesen írásban másként nem állapodtak meg);
- az igazságügyi vizsgálati jelentésből egyértelműen kiderül, hogy kockázatcsökkentő technológiát használtak az adatok feldolgozására, tárolására és/vagy továbbítására az adatvédelmi incidens bekövetkezésekor; és

- Ön nem tárol (és az adatvédelmi incidens eseményidőszakában sem tárolt) olyan érzékeny hitelesítési adatot vagy bármilyen kártyatulajdonosi adatot, amely nem olvashatatlanná alakított.

Ha lehetőség van a kártalanítás csökkentésére, az Ön kártalanítási kötelezettségének csökkentését – bármely fizetendő kötbért kivéve – az alábbiak szerint határozzák meg:

Kártalanítási kötelezettség csökkentése	Előírt követelmények
Általános csökkentés: 50%	összes tranzakció több mint 75%-át chippel ellátott eszközzel dolgozták fel[1] VAGY
	a kereskedői telephelyek több mint 75%-ánál kockázatcsökkentő technológiát alkalmaztak[2]
Fokozott csökkentés: 75% és 100% között	összes tranzakció több mint 75%-át chippel ellátott eszközzel dolgozták fel[1] ÉS a kereskedői telephelyek több mint 75%-ánál alkalmaztak egyéb kockázatcsökkentő technológiát[2]

[1] Az American Express belső elemzése szerint meghatározva

[2] A PFI-vizsgálat szerint meghatározva

- A Fokozott csökkentést (75% és 100% között) a chippel ellátott eszközzel folytatott tranzakciók ÉS az egyéb kockázatcsökkentő technológiát használó kereskedői telephelyek százalékos aránya közül a kisebbik alapján határozzák meg. Az alábbi példák a kártalanítás csökkentésének kiszámítását szemléltetik.
- A kockázatcsökkentő technológia minősítés eléréséhez Ön köteles bizonyítani a technológia tervezése és rendeltetése szerinti hatékony felhasználását. Például chippel ellátott eszközök telepítése és chipkártyák mágnescsíkos vagy kódbeviteles tranzakciókként történő feldolgozása NEM jelenti a technológia hatékony alkalmazását.
- A kockázatcsökkentő technológiát használó telephelyek százalékos arányát a PFI-vizsgálat állapítja meg.
- A kártalanítási kötelezettség csökkentése nem vonatkozik az adatvédelmi incidens kapcsán fennálló semmilyen kötbérfizetési kötelezettségre.

Pl.	Használatban lévő kockázatcsökkentő technológiák	Jogosult a kártalanítási kötelezettség fokozott csökkentésére?	Csökkentés
1	A tranzakciók 80%-át chippel ellátott eszközzel dolgozták fel	Nem	50%: Általános csökkentés (amennyiben a kockázatcsökkentő technológiák aránya 75%-nál kisebb, a fokozott csökkentés nem lehetséges)[1]
	A telephelyek 0%-a használ egyéb kockázatcsökkentő technológiát		
2	A tranzakciók 80%-át chippel ellátott eszközzel dolgozták fel	Igen	77%: Fokozott csökkentés (a kockázatcsökkentő technológia 77%-os igénybevétele alapján)
	A telephelyek 77%-a használ egyéb kockázatcsökkentő technológiát		

Pl.	Használatban lévő kockázatcsökkentő technológiák	Jogosult a kártalanítási kötelezettség fokozott csökkentésére?	Csökkentés
3	A tranzakciók 93%-át chippel ellátott eszközzel dolgozták fel A telephelyek 100%-a használ egyéb kockázatcsökkentő technológiát	Igen	93%: Fokozott csökkentés (chippel ellátott eszközzel feldolgozott tranzakciók 93%-os aránya alapján)
4	A tranzakciók 40%-át chippel ellátott eszközzel dolgozták fel A telephelyek 90%-a használ egyéb kockázatcsökkentő technológiát	Nem	50%: Általános csökkentés (amennyiben a chippel ellátott eszközzel feldolgozott tranzakciók aránya 75%-nál kisebb, a fokozott csökkentés nem lehetséges)

[1] A 10 000 American Express-kártyaszámlát érintő adatvédelmi incidensnél számlaszámonként 5 USD díj esetében (10 000 × 5 USD = 50 000 USD) elérhető csökkentés 50%, amely a kártalanítási kötelezettség összegét 50 000 USD-ról 25 000 USD-ra csökkenti, a kötbérkötelezettségeket nem számítva.

4. rész Az Ön rendszereinek fontos periodikus érvényesítése

Ön köteles elvégezni a lenti műveleteket, hogy az alábbiakban leírt módon, a PCI DSS szerint évente és negyedévente érvényesítse az Ön és az Ön jogbérletbe vevői azon berendezéseinek, rendszereinek és/vagy hálózatainak (és azok összetevőinek) státuszát, amelyeken kártyatulajdonosi adatokat vagy érzékeny hitelesítési adatokat tárolnak, dolgoznak fel vagy továbbítanak.

Az érvényesítéshez négy műveletet kell elvégezni:

1. művelet: Vegyen részt az American Express jelen szabályzat szerinti megfelelőségi programjában.

2. művelet: Ismerje meg a szintjét és az érvényesítési követelményeit.

3. művelet: Készítse el az érvényesítési dokumentációt, amelyet meg kell küldenie az American Expressnek.

4. művelet: Küldje el az érvényesítési dokumentációt az American Expressnek a megadott határidőn belül.

1. művelet: Vegyen részt az American Express jelen szabályzat szerinti megfelelőségi programjában

Az 1. szintű kereskedők, a 2. szintű kereskedők és minden szolgáltató – az alábbiakban leírtak szerint – köteles részt venni az American Express jelen szabályzat szerinti PCI-megfelelőségi programjában, megadva annak a személynek a teljes nevét, e-mail-címét, telefonszámát és postai levelezési címét, aki adatvédelmi kapcsolattartóként fog eljárni. Ön köteles ezen információkat a SecureTrust – a Trustwave egyik divíziója (https://portal.securetrust.com), amely szervezet a programot az American Express képviseletében kezeli – rendelkezésére bocsátani a lenti 4. művelet: „Küldje el az érvényesítési dokumentációt az American Expressnek” leírásában felsorolt módszerek valamelyikével. Ön köteles értesíteni a SecureTrustot, ha ezen információkban változások történnek, megadva a naprakész információt, ha van ilyen. Ha elmulasztja e kapcsolattartási adatok megadását, az nem befolyásolja a mi arra vonatkozó jogunkat, hogy az érvényesítés elmulasztásáért díjat állapítsunk meg az Érvényesítés elmaradásáért kirótt díjak táblázata szerint.

Az American Express írásbeli értesítés megküldésével előírhatja egyes 3. és 4. szintű kereskedők részvételét is az American Express jelen szabályzat szerinti megfelelőségi programjában. A kereskedő legkésőbb 90 nappal az értesítés átvételét követően köteles regisztrálni.

2. művelet: Ismerje meg a szintjét és az érvényesítési követelményeit

Négy szint létezik kereskedők számára, és két szint szolgáltatók számára, amelynek alapja az Ön által kezelt, American Express-kártyával végzett tranzakciók volumene. A kereskedők esetében ez az a volumen, amelyet azok a létesítményeik küldenek be, amelyek elérik az American Express kereskedői fiókok legmagasabb szintjét.* Ön az alábbi kereskedői és szolgáltatói táblázatban meghatározott szintek egyikébe tartozik. A Buyer Initiated Payment (BIP) tranzakciók nem számítanak bele az American Express-kártyával végzett tranzakciók volumenébe a kereskedői szint és az érvényesítési követelmények meghatározásakor.

* Jogbérletbe adók esetében ebbe beletartozik a jogbérletbe vevők létesítményeitől származó volumen is. Azok a jogbérletbe adók, amelyek kötelezően előírják, hogy jogbérletbe vevőik egy meghatározott értékesítési ponti (Point of Sale, POS) rendszert vagy szolgáltatót használjanak, kötelesek érvényesítési dokumentációt rendelkezésre bocsátani az érintett jogbérletbe vevőkről is.

Kereskedői követelmények

A kereskedőknél (nem a szolgáltatóknál) négy minősítés lehetséges a szintjük és az érvényesítési követelményeik kapcsán. Miután az alábbi felsorolásból meghatározta kereskedői szintjét, nézze meg a Kereskedői táblázatot, hogy meghatározza az érvényesítési dokumentáció követelményeit.

- **1. szintű kereskedő** – 2,5 millió vagy annál több American Express-kártyával végzett tranzakció évente; vagy bármely kereskedő, akit az American Express saját belátása szerint egyébként 1. szintűnek jelöl meg.
- **2. szintű kereskedő** – 50 000 és 2,5 millió közötti American Express-kártyával végzett tranzakció évente.
- **3. szintű kereskedő** – 10 000 és 50 000 közötti American Express-kártyával végzett tranzakció évente.
- **4. szintű kereskedő** – 10 000-nél kevesebb American Express-kártyával végzett tranzakció évente.

Kereskedői táblázat

	Érvényesítési dokumentáció		
Kereskedői szint/ Éves American Express-tranzakciók	Helyszíni értékelő jelentés a megfelelőségről (ROC)	Önértékelési kérdőív (SAQ) ÉS negyedéves hálózatátvilágítás	STEP-hitelesítés a jogosult kereskedők számára
1. szint/ 2,5 millió vagy több	Kötelező	Nem alkalmazható	Választható (az ROC-t helyettesíti)
2. szint/ 50 000 – 2,5 millió	Választható	SAQ kötelező (kivéve helyszíni értékelés benyújtása esetén); az átvilágítás bizonyos SAQ-típusoknál kötelező	Választható (helyettesíti az SAQ-t és a hálózati átvilágítást vagy az ROC-t)
3. szint/ 10 000 – 50 000	Választható	SAQ választható (akkor kötelező, ha azt az American Express előírja); az átvilágítás bizonyos SAQ-típusoknál kötelező	Választható (helyettesíti az SAQ-t és a hálózati átvilágítást vagy az ROC-t)

	Érvényesítési dokumentáció		
Kereskedői szint/ Éves American Express-tranzakciók	Helyszíni értékelő jelentés a megfelelőségről (ROC)	Önértékelési kérdőív (SAQ) ÉS negyedéves hálózatátvilágítás	STEP-hitelesítés a jogosult kereskedők számára
4. szint/ 10 000 vagy kevesebb	Választható	SAQ választható (akkor kötelező, ha azt az American Express előírja); az átvilágítás bizonyos SAQ-típusoknál kötelező	Választható (helyettesíti az SAQ-t és a hálózati átvilágítást vagy az ROC-t)

* A félreértések elkerülése végett a 3. szintű és a 4. szintű kereskedőknek nem kell benyújtaniuk érvényesítési dokumentációt, kivéve, ha azt az American Express saját hatáskörében kéri; azonban ettől függetlenül is kötelesek betartani a jelen adatvédelmi működési szabályzat rendelkezéseit, és annak minden más rendelkezésének betartásáért felelősség terheli őket.

Az American Express fenntartja a jogot, hogy ellenőrizze a szükség szerint benyújtott PCI-érvényesítési dokumentáció pontosságát és megfelelőségét, akár azáltal is, hogy saját költségén szerződtet egy választása szerinti QSA-t vagy PFI-t.

Biztonságitechnológia-fejlesztési program (STEP)

A PCI DSS-t betartó kereskedők az American Express belátása szerint jogosultak lehetnek az American Express STEP programjára is, ha bevezetnek bizonyos további biztonsági technológiákat kártyafeldolgozási környezetükben. A STEP csak akkor alkalmazandó, ha a kereskedőnél nem történt adatvédelmi incidens az elmúlt 12 hónap során, és ha az összes kártyatranzakció 75%-át az alábbiak alkalmazásával végezték:

- **EMV-technológia** – ahol egy aktív chippel ellátott eszköz rendelkezik érvényes és aktuális EMVCo (www.emvco.com) jóváhagyással/minősítéssel, és képes feldolgozni AEIPS-nek megfelelő chipkártyás tranzakciókat. (Az USA-beli kereskedők az érintés nélküli tranzakciókat is kötelesek ideérteni)
- **Pontok közötti titkosítás (Point to Point Encryption, P2PE)** – amelyet a kereskedő feldolgozójának adnak át egy PCI-SSC által jóváhagyott vagy QSA által jóváhagyott pontok közötti titkosítási rendszeren keresztül

A STEP programra jogosult kereskedőkre csökkentett mértékű követelmények vonatkoznak a PCI-érvényesítési dokumentáció terén a 3. művelet: „Készítse el az érvényesítési dokumentációt, amelyet meg kell küldenie az American Expressnek” szerint.

Szolgáltatói követelmények

A szolgáltatóknál (nem a kereskedőknél) két minősítés lehetséges a szintjük és az érvényesítési követelményeik kapcsán. Miután az alábbi felsorolásból meghatározta szolgáltatói szintjét, nézze meg a Szolgáltatói táblázatot, hogy meghatározza az érvényesítési dokumentáció követelményeit.

1. szintű szolgáltató – 2,5 millió vagy annál több American Express-kártyával végzett tranzakció évente; vagy bármely szolgáltató, akit az American Express egyébként 1. szintűnek tekint.

2. szintű szolgáltató – 2,5 milliónál kevesebb American Express-kártyával végzett tranzakció évente; vagy bármely szolgáltató, akit az American Express nem tekint 1. szintűnek.

A szolgáltatók nem vehetnek részt a STEP programban.

Szolgáltatói táblázat

Szint	Érvényesítési dokumentáció	Követelmény
1	Éves helyszíni biztonsági értékelő jelentés a megfelelőségről	Kötelező
2	Éves SAQ D (szolgáltató) és negyedéves hálózatátvilágítás vagy éves helyszíni biztonsági értékelő jelentés a megfelelőségről, ha azt preferálják.	Kötelező

A szolgáltatók részére is ajánlott, hogy tartsák be a kijelölt PCI-szervezetek kiegészítő érvényesítését is.

3. művelet: Készítse el az érvényesítési dokumentációt, amelyet meg kell küldenie az American Expressnek

Az alábbi dokumentumok kötelezők a fenti kereskedői táblázatban és szolgáltatói táblázatban felsorolt különböző kereskedői és szolgáltatói szinteknél.

Éves helyszíni biztonsági értékelés – Az éves helyszíni biztonsági értékelés az Ön olyan berendezéseinek, rendszereinek és hálózatainak (és azok összetevőinek) részletes helyszíni vizsgálata, amelyeknél kártyatulajdonosi adatokat vagy érzékeny hitelesítési adatokat (vagy mindkettőt) tárolnak, dolgoznak fel vagy továbbítanak. Ezt a következő személyek valamelyikének kell elvégeznie:

- egy QSA-nak, vagy
- Önnek, és az Ön ügyvezetőjének, pénzügyi vezetőjének, információbiztonsági vezetőjének vagy elöljárójának kell hitelesítenie, és az American Expressnek kell éves szinten benyújtani a vonatkozó megfelelőségi igazolási (Attestation of Compliance, AOC) dokumentumban.

Az AOC-dokumentumnak alá kell támasztania, hogy Ön megfelel a PCI DSS összes követelményének, és kérésre több példányban tartalmaznia kell a teljes megfelelőségi jelentést (1. szintű kereskedők és 1. szintű szolgáltatók).

Éves önértékelési kérdőív – Az éves önértékelés a PCI DSS önértékelési kérdőívének (Self-Assessment Questionnaire, SAQ) segítségével végzett eljárás, amely lehetővé teszi az Ön olyan berendezéseinek, rendszereinek és hálózatainak (és azok összetevőinek) önvizsgálatát, ahol kártyatulajdonosi adatokat vagy érzékeny hitelesítési adatokat (vagy mindkettőt) tárolnak, dolgoznak fel vagy továbbítanak. Ezt Önnek kell elvégeznie, és az Ön ügyvezetőjének, pénzügyi vezetőjének, információbiztonsági vezetőjének vagy elöljárójának kell hitelesítenie. Az SAQ AOC részét évente kell benyújtani az American Expressnek. Az SAQ AOC-részének igazolnia kell, hogy Ön megfelel a PCI DSS összes követelményének, és kérésre több példányban tartalmaznia kell a teljes SAQ-t (2. szintű, 3. szintű és 4. szintű kereskedők; 2. szintű szolgáltatók).

Negyedéves hálózatátvilágítás – A negyedéves hálózatátvilágítás egy olyan eljárás, amely távolról teszteli az Ön internetre csatlakozó számítógépes hálózatait és webszervereit az esetleges gyenge pontok és sérülékenységek tekintetében. Ezen eljárást egy jóváhagyott átvilágítási szállítónak (Approved Scanning Vendor, **ASV**) kell elvégeznie. Ön negyedévente köteles kitölteni és az American Express rendelkezésére bocsátani az ASV átvilágítási megfelelőségi igazolását (Attestation of Scan Compliance, **AOSC**) vagy az átvilágítás megállapításainak vezetői összefoglalóját (és kérésre több példányban a teljes átvilágítást). Az AOSC-nek vagy a vezetői összefoglalónak igazolnia kell, hogy az eredmények megfelelnek a PCI DSS átvilágítási eljárásának, hogy nem azonosítottak be nagy kockázatot jelentő problémákat, és hogy az átvilágítás kielégítő vagy megfelelő (minden kereskedő, kivéve a helyszíni biztonsági értékelő jelentést is benyújtó kereskedőket, a STEP programra jogosult kereskedőket és valamennyi szolgáltatót). Az egyértelműség kedvéért a negyedéves hálózatátvilágítás abban az esetben kötelező, ha azt a vonatkozó Önértékelési kérdőív előírja.

Éves STEP-hitelesítés érvényesítési dokumentáció – Az American Express éves STEP-minősítési hitelesítés („STEP-hitelesítés") keretébe kizárólag azok a kereskedők tartoznak, akik a 2. művelet: „Ismerje meg a szintjét és az érvényesítési követelményeit" fent felsorolt követelményeinek megfelelnek. A STEP-hitelesítés a PCI DSS-követelmények segítségével végzett eljárás, amely lehetővé teszi az Ön olyan berendezéseinek, rendszereinek és hálózatainak (és azok összetevőinek) önvizsgálatát, ahol kártyatulajdonosi adatokat vagy érzékeny hitelesítési adatokat (vagy mindkettőt) tárolnak, dolgoznak fel vagy továbbítanak. Ezt Önnek kell elvégeznie, és az Ön

ügyvezetőjének, pénzügyi vezetőjének, információbiztonsági vezetőjének vagy elöljárójának kell hitelesítenie. Ön úgy köteles végrehajtani a folyamatot, hogy évente benyújtja az American Expressnek a STEP-hitelesítési nyilatkozatot. (Csak STEP-re jogosult kereskedők.) Az éves STEP-hitelesítési nyilatkozat letölthető a SecureTrust védett portáljáról.

Megfelelőségi összefoglaló – A megfelelőségi összefoglaló (Summary of Compliance, SOC) az a dokumentum, amelyet használva egy jogbérletbe adó vagy szolgáltató jelentést tehet jogbérletbe vevői PCI-megfelelőségi státuszáról. Az SOC-minta letölthető a SecureTrust védett portáljáról.

PCI DSS megszegése – Ha Ön nem tartja be a PCI DSS-t, akkor az alábbi dokumentumok egyikét köteles benyújtani:

- Megfelelőségi igazolás (AOC), ideértve a 4. részt („Szabályszegési státusz akcióterve") is
- PCI kiemelt megközelítési eszköze – Összefoglaló és megfelelőségi igazolás (PASAOC)
- Projekttervsablon (amely letölthető a SecureTrust védett portáljáról)

Valamennyi fenti dokumentumban helyreállítási határidőt kell kitűzni, amely a megfelelés elérése érdekében nem haladhatja meg a dokumentum elkészítésének időpontját követő 12 hónapot. Ön köteles a megfelelő dokumentumot az American Express rendelkezésére bocsátani a lenti 4. művelet: „Küldje el az érvényesítési dokumentációt az American Expressnek" felsorolt módszereinek valamelyikével. Ön köteles a szabályszegési státuszának helyreállítása érdekében tett intézkedéseinek előrehaladásáról meghatározott időközönként az American Expresst értesíteni (1., 2., 3. és 4. szintű kereskedők; valamennyi szolgáltató). A félreértések elkerülése végett azok a kereskedők, akik nem tartják be a PCI DSS-t, nem jogosultak a STEP programra. Az American Express nem fog Önre terhelni nem-megfelelőség miatt (az alábbiakban meghatározott) érvényesítés elmaradásáért kirótt díjat a helyreállítási határidő előtt, de ez esetben Ön továbbra is felelősséggel tartozik az American Express felé az adatvédelmi incidensek vonatkozásában fennálló minden kártalanítási kötelezettség tekintetében és a jelen szabályzat összes egyéb rendelkezése szerint.

4. művelet: Küldje el az érvényesítési dokumentációt az American Expressnek

Az American Express PCI-megfelelőségi programjában kötelezően részt vevő valamennyi kereskedő és szolgáltató köteles benyújtani a 2. művelet: „Ismerje meg a szintjét és az érvényesítési követelményeit" táblázataiban „Kötelező" jelzéssel ellátott érvényesítési dokumentációt. Az érvényesítési dokumentációját a SecureTrustnak kell beküldenie az alábbi módok egyikével:

- **Védett portál**: Az érvényesítési dokumentáció feltölthető a SecureTrust védett portálján: https://portal.securetrust.com.

  Kérjük, a portál használati utasításáért lépjen kapcsolatba a SecureTrusttal az Ön országához tartozó telefonszámon, vagy érdeklődjön e-mailben az americanexpresscompliance@securetrust.com címen.
- **Védett fax**: Az érvényesítési dokumentáció küldhető faxon is a következő számra: +1 (312) 276-4019. (a + jelzi a nemzetközi direkt hívás („IDD") előtagot, nemzetközi hívásdíj vonatkozik rá).

  Kérjük, adja meg az Ön nevét, azt a nevet, amely alatt Ön üzleti tevékenységet folytat, az Ön adatvédelmi kapcsolattartójának nevét, az Ön címét és telefonszámát, és csak kereskedők esetén az Ön 10 számjegyű American Express kereskedői számát.

Ha általános kérdései vannak a programról vagy a fenti folyamatról, kérjük, forduljon a SecureTrusthoz a + 800 9000 1140 vagy az +1 (312) 267-3208 telefonszámon vagy e-mailben az americanexpresscompliance@securetrust.com címen.

A megfelelőség és az érvényesítés az Ön költségén jön létre. Az érvényesítési dokumentáció benyújtásával Ön kijelenti és szavatolja az American Express felé, hogy jogosult az abban foglalt információ közlésére, és az érvényesítési dokumentáció American Expressnek történő átadásával nem sérti semmilyen más fél jogait.

Piacok	SecureTrust Telefonszáma
Amerikai Egyesült Államok	1 866 659 9016
Argentína	+ 800 9000 1140
Ausztrália	+ 800 9000 1140
Ausztria	+ 800 9000 1140
Bulgária	+ 312 267 3208
Ciprus	+ 800 9000 1140
Csehország	+ 800 144 316
Dánia	+ 800 9000 1140
Egyesült Királyság	+ 800 9000 1140
Észtország	+ 312 267 3208
Franciaország	+ 800 9000 1140
Görögország	+ 312 267 3208
Hollandia	+ 312 267 3208
Hongkong	+ 800 9000 1140
Horvátország	+ 312 267 3208
IDC	+ 888 900 0114
India	+ 800 9000 1140
Írország	+ 800 9000 1140
Izland	+ 800 9000 1140
Japán	+ 312 267 3208

Piacok	SecureTrust Telefonszáma
Kanada	1 866 659 9016
Lengyelország	+ 800 9000 1140
Lettország	+ 312 267 3208
Litvánia	+ 312 267 3208
Magyarország	+ 800 9000 1140
Málta	+ 312 267 3208
Mexikó	+ 888 900 0114
Németország	+ 800 9000 1140
Norvégia	+ 800 9000 1140
Olaszország	+ 800 9000 1140
Oroszország	+ 312 267 3208
Portugália	+ 312 267 3208
Románia	+ 312 267 3208
Spanyolország	+ 800 9000 1140
Svédország	+ 800 9000 1140
Szingapúr	+ 800 9000 1140
Szlovákia	+ 312 267 3208
Szlovénia	+ 312 267 3208
Tajvan	+ 312 267 3208
Thaiföld	+ 800 9000 1140
Új-Zéland	+ 800 9000 1140

A + jelzi a nemzetközi direkt hívás („IDD") előtagot, nemzetközi hívásdíj vonatkozik rá

Érvényesítés elmaradásáért kirótt díjak és a szerződés felmondása

Az American Express jogosult Önre az érvényesítés elmaradásáért kirótt díjakat terhelni és a szerződést felmondani, ha Ön nem teljesíti a jelen követelményeket, vagy nem nyújtja be a kötelező érvényesítési dokumentációt az American Expressnek a vonatkozó határidőn belül. Az American Express külön értesítést fog Önnek küldeni minden éves és negyedéves bejelentési időszak vonatkozó határidejéről.

Küldje el a dokumentációt az American Express részére a vonatkozó határidőn belül. Az American Express külön értesítést fog Önnek küldeni minden éves és negyedéves bejelentési időszak vonatkozó határidejéről. Az alábbi érvényesítés elmaradásáért kirótt díjak táblázatában találja az Ön országára érvényes díjakat.

Leírás	1. szintű kereskedő vagy 1. szintű szolgáltató	2. szintű kereskedő, 2. szintű szolgáltató vagy STEP-kereskedő	3. szintű vagy 4. szintű kereskedő
Érvényesítés elmaradásáért kirótt díj akkor kerül megállapításra, ha az érvényesítési dokumentációt nem kapják kézhez az első határidőn belül.	1. szint 1. havi díja	2. szint 1. havi díja	Havi díj
További érvényesítés elmaradásáért kirótt díj kerül megállapításra, ha az érvényesítési dokumentációt nem kapják kézhez az első határidőt követő 30 napon belül.	1. szint 2. havi díja	2. szint 2. havi díja	
További érvényesítés elmaradásáért kirótt díj kerül megállapításra, ha az érvényesítési dokumentációt nem kapják kézhez az első határidőt követő 60 napon belül.	1. szint 3. havi díja	3. szint 3. havi díja	

Ha az American Express nem kapja kézhez az Ön kötelező érvényesítési dokumentációját az első határidő lejártától számított 60 napon belül, akkor az American Express jogosult felmondani a szerződést az abban foglalt feltételek szerint, továbbá jogosult a fentiek szerinti, az érvényesítés elmaradásáért kirótt díjakat halmozottan Önre terhelni.

Érvényesítés elmaradásáért kirótt díjak táblázata

Piac	Szint	Típus	Deviza	1. havi díj	2. havi díj	3. havi díj
Ausztrália	1. szint	Kereskedő vagy szolgáltató	AUD	35 000	49 000	63 000
	2. szint	Kereskedő vagy szolgáltató	AUD	7000	14 000	21 000
	3. szint és 4. szint	Kereskedő	AUD	Havi díj: 20		
Bulgária	1. szint	Kereskedő vagy szolgáltató	BGN	28 000	40 000	51 000
	2. szint	Kereskedő vagy szolgáltató	BGN	5500	11 000	16 500
	3. szint és 4. szint	Kereskedő	BGN	Havi díj: 33		

Piac	Szint	Típus	Deviza	1. havi díj	2. havi díj	3. havi díj
Ciprus, Észtország, Franciaország, Németország, Írország, Spanyolország, Lettország, Litvánia, Portugália, Szlovákia, Szlovénia	1. szint	Kereskedő vagy szolgáltató	EUR	19 000	26 000	34 000
	2. szint	Kereskedő vagy szolgáltató	EUR	4000	7500	11 000
	3. szint és 4. szint	Kereskedő	EUR		Havi díj: 15	
Csehország	1. szint	Kereskedő vagy szolgáltató	CZK	392 000	564 000	721 000
	2. szint	Kereskedő vagy szolgáltató	CZK	78 300	157 000	235 000
	3. szint és 4. szint	Kereskedő	CZK		Havi díj: 440	
Dánia	1. szint	Kereskedő vagy szolgáltató	DKK	110 000	156 000	200 000
	2. szint	Kereskedő vagy szolgáltató	DKK	22 000	42 000	65 000
	3. szint és 4. szint	Kereskedő	DKK		Havi díj: 130	
Egyesült Királyság	1. szint	Kereskedő vagy szolgáltató	GBP	12 500	18 000	23 000
	2. szint	Kereskedő vagy szolgáltató	GBP	2500	5000	7500
	3. szint és 4. szint	Kereskedő	GBP		Havi díj: 15	
Hongkong	1. szint	Kereskedő vagy szolgáltató	HKD	25 000	35 000	45 000
	2. szint	Kereskedő vagy szolgáltató	HKD	5000	10 000	15 000
	3. szint és 4. szint	Kereskedő	HKD		Havi díj: 150	
Horvátország	1. szint	Kereskedő vagy szolgáltató	HRK	105 000	152 000	195 000
	2. szint	Kereskedő vagy szolgáltató	HRK	21 000	42 000	63 000
	3. szint és 4. szint	Kereskedő	HRK		Havi díj: 130	

Piac	Szint	Típus	Deviza	1. havi díj	2. havi díj	3. havi díj
Izland	1. szint	Kereskedő vagy szolgáltató	ISK	3 070 000	4 300 000	5 500 000
	2. szint	Kereskedő vagy szolgáltató	ISK	615 000	920 000	1 227 200
	3. szint és 4. szint	Kereskedő	ISK	Havi díj: 2400		
Magyarország	1. szint	Kereskedő vagy szolgáltató	HUF	4 650 000	6 700 000	8 600 000
	2. szint	Kereskedő vagy szolgáltató	HUF	930 000	1 860 000	2 800 000
	3. szint és 4. szint	Kereskedő	HUF	Havi díj: 5500		
Norvégia	1. szint	Kereskedő vagy szolgáltató	NOK	135 000	195 000	249 000
	2. szint	Kereskedő vagy szolgáltató	NOK	27 000	54 000	81 000
	3. szint és 4. szint	Kereskedő	NOK	Havi díj: 170		
Szingapúr	1. szint	Kereskedő vagy szolgáltató	SGD	38 000	53 000	68 000
	2. szint	Kereskedő vagy szolgáltató	SGD	7500	15 000	22 500
	3. szint és 4. szint	Kereskedő	SGD	Havi díj: 25		
Svédország	1. szint	Kereskedő vagy szolgáltató	SEK	175 000	245 000	315 000
	2. szint	Kereskedő vagy szolgáltató	SEK	35 000	70 000	105 000
	3. szint és 4. szint	Kereskedő	SEK	Havi díj: 135		
Új-Zéland	1. szint	Kereskedő vagy szolgáltató	NZD	35 000	49 000	63 000
	2. szint	Kereskedő vagy szolgáltató	NZD	7000	14 000	21 000
	3. szint és 4. szint	Kereskedő	NZD	Havi díj: 20		

5. rész Titoktartás

Az American Express köteles észszerű intézkedéseket tenni annak érdekében, hogy az Ön megfelelőségi jelentéseit – az érvényesítési dokumentációval együtt – bizalmasan kezelje (és meghatalmazottait és alvállalkozóit is erre kötelezze, ideértve a SecureTrustot is), és ne bocsássa az érvényesítési dokumentációt harmadik fél rendelkezésére (kivéve az American Express kapcsolt vállalkozásait, meghatalmazottait, képviselőit, szolgáltatóit és alvállalkozóit) azok átvételétől számított három évig azzal, hogy ez a titoktartási kötelezettség nem vonatkozik arra az érvényesítési dokumentációra:

a. amelyről az American Expressnek már a rendelkezésre bocsátás előtt is tudomása volt;

b. amely a nyilvánosság számára már elérhető volt, vagy amely a nyilvánosság számára elérhetővé válik anélkül, hogy az American Express a jelen bekezdést megsértené;

c. amelyet az American Express jogszerűen kap kézhez harmadik féltől titoktartási kötelezettség nélkül;

d. amelyet az American Express önállóan hoz létre; vagy

e. amelynek közlése kötelező bírósági, közigazgatási, vagy egyéb hatósági végzésben foglaltak szerint, vagy amelynek közlése bármely jogszabályban, szabályban, rendeletben, idézésben foglaltakra tekintettel vagy egyéb közigazgatási vagy jogi eljárás folytán, vagy bármely kormányzati szerv vagy hatóság formális vagy informális megkeresése vagy vizsgálata miatt (ideértve bármely szabályozó, nyomozó, vizsgálati vagy bűnüldöző szervet) kötelező.

6. rész Felelősség kizárása

AZ AMERICAN EXPRESS EZÚTON KIJELENTI, HOGY NEM VÁLLAL FELELŐSSÉGET SEMMILYEN NYILATKOZAT, SZAVATOSSÁGVÁLLALÁS ÉS EGYÉB FELELŐSSÉG TEKINTETÉBEN – LEGYEN AZ KIFEJEZETT, VÉLELMEZETT, JOGSZABÁLYON ALAPULÓ VAGY EGYÉB – A JELEN ADATVÉDELMI MŰKÖDÉSI SZABÁLYZAT, A PCI DSS, AZ EMV-SPECIFIKÁCIÓK ÉS A QSA-K, ASV-K, VAGY PFI-K (VAGY EZEK BÁRMELYIKE) KIJELÖLÉSE ÉS TELJESÍTÉSE TEKINTETÉBEN, IDEÉRTVE A FORGALMAZHATÓSÁGRA VAGY BIZONYOS CÉLRA VALÓ ALKALMASSÁGRA VONATKOZÓ SZAVATOSSÁGVÁLLALÁST. AZ AMERICAN EXPRESS KÁRTYAKIBOCSÁTÓK NEM HARMADIK FÉL KEDVEZMÉNYEZETTEK A JELEN SZABÁLYZAT VONATKOZÁSÁBAN.

Hasznos weboldalak

American Express Adatvédelem: www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC: www.pcisecuritystandards.org

Szószedet

Kizárólag a jelen Adatvédelmi működési szabályzat (DSOP) alkalmazásában az alábbi meghatározások alkalmazandók és irányadók a következőben található kifejezésekkel fellépő esetleges ellentmondás esetén: *Kereskedői szabályzat*.

1. szintű kereskedő: évente 2,5 millió vagy annál több American Express-kártyával végzett tranzakcióval rendelkező kereskedő; vagy bármely kereskedő, akit az American Express egyébként 1. szintűnek ítél.

2. szintű kereskedő: évente 50 000 és 2,5 millió közötti American Express-kártyával végzett tranzakcióval rendelkező kereskedő.

3. szintű kereskedő: évente 10 000 és 50 000 közötti American Express-kártyával végzett tranzakcióval rendelkező kereskedő.

4. szintű kereskedő: évente 10 000-nél kevesebb American Express-kártyával végzett tranzakcióval rendelkező kereskedő.

1. szintű szolgáltató: évente 2,5 millió vagy annál több American Express-kártyával végzett tranzakcióval rendelkező szolgáltató; vagy bármely szolgáltató, akit az American Express egyébként 1. szintűnek tekint.

2. szintű szolgáltató: évente 2,5 milliónál kevesebb American Express-kártyával végzett tranzakcióval rendelkező szolgáltató; vagy bármely szolgáltató, akit az American Express nem tekint 1. szintűnek.

Adatvédelmi incidens: American Express titkosítási kulcsainak vagy legalább egy American Express-kártyaszámlaszámnak a vélt vagy valós feltörésével járó incidens, amelyben:

- illetéktelen hozzáférés vagy felhasználás történik olyan titkosítási kulcsok, kártyatulajdonosi adatok vagy érzékeny hitelesítési adatok (vagy ezek kombinációja) tekintetében, amelyeket az Ön berendezéseinek, rendszereinek és/vagy hálózatainak (vagy azok összetevőinek) használatával vagy az Ön által előírtak szerint használva tárolnak, dolgoznak fel vagy továbbítanak;
- ilyen titkosítási kulcsok, kártyatulajdonosi adatok vagy érzékeny hitelesítési adatok (vagy ezek kombinációja) olyan felhasználása történik, amely nincs összhangban a szerződéssel; és/vagy
- bármely olyan adathordozó, anyag, nyilvántartás vagy információ bármilyen vélt vagy valós elvesztése, ellopása vagy helytelen eltulajdonítása történik, amely ilyen titkosítási kulcsokat, kártyatulajdonosi adatokat vagy érzékeny hitelesítési adatokat (vagy ezekből álló kombinációt) tartalmaz.

Adatvédelmi incidens eseményidőszaka: az az időszak, amely a feltörés időpontjával kezdődik, ha ez az időpont ismert, vagy 365 nappal az értesítési határidő előtt, ha az incidens tényleges időpontja nem ismert. Az adatvédelmi incidens eseményidőszaka 30 nappal az értesítési határidő után ér véget.

American Express kártya vagy **kártya**: bármely kártya, számlaelérési eszköz, illetve fizetési eszköz vagy szolgáltatás, amely az American Express vagy bármely kapcsolt vállalkozása nevét, logóját, kereskedelmi vagy szolgáltatási védjegyét, kereskedelmi nevét vagy más saját tulajdonú dizájnját vagy megjelölését viseli, és kibocsátó által került kibocsátásra, vagy kártyaszámlaszám.

Átvilágítási megfelelőségi igazolás (AOSC): az Ön megfelelőségi státuszára vonatkozó nyilatkozat a PCI DSS tekintetében hálózati átvilágítás alapján a Payment Card Industry Security Standards Council, LLC által megadott formátumban.

Biztonságitechnológia-fejlesztési program (STEP): az American Express programja, amelyben a kereskedőket arra ösztönzik, hogy alkalmazzanak olyan technológiákat, amelyek javítják az adatvédelmet. A STEP programra jogosult kereskedők azok, akiknél nem történt adatvédelmi incidens az éves STEP-hitelesítés benyújtását megelőző 12 hónapban, és az összes tranzakció legalább 75%-ában használnak pontok közötti titkosítást, vagy ekkora arányban folytattak személyes tranzakciókat EMV-chippel ellátott eszközök használatával.

Buyer Initiated Payment (BIP) tranzakciók: a BIP-n keresztül feldolgozott fizetési megbízási fájlon keresztül engedélyezett fizetési tranzakció.

Chip: a kártyába beépített integrált mikrochip, amely tartalmazza a kártyatulajdonos és a számla adatait.

Chipkártya: az a kártya, amely chipet tartalmaz, és használatához szükséges lehet egy PIN, amellyel ellenőrizni lehet a kártyatulajdonos személyazonosságát vagy a chip által tartalmazott számlainformációkat vagy mindkettőt (erre néha „okos kártya", „EMV-kártya", vagy „ICC" vagy „integrált áramkörös kártya" néven hivatkozunk az anyagainkban).

Chippel ellátott eszköz: értékesítési ponti eszköz, érvényes és aktuális EMVCo (www.emvco.com) jóváhagyással/minősítéssel, amely képes feldolgozni az AEIPS szerinti chipkártyás tranzakciókat.

EMV-specifikációk: az EMVCo, LLC által kiadott specifikációk, amelyek elérhetők a www.emvco.com címen.

EMV-tranzakció: integrált áramkörös kártya (néha „IC-Kártya", „chip kártya", „okos kártya", „EMV-kártya" vagy „ICC" néven említik) segítségével végzett tranzakció egy IC-kártya leolvasására alkalmas, érvényes és aktuális EMV-típusjóváhagyással rendelkező értékesítési ponti (POS) terminálon. Az EMV-típusjóváhagyások elérhetők a www.emvco.com címen.

Értékesítési ponti (POS) rendszer: egy kereskedő által engedélyek megszerzésére vagy tranzakciós adatok gyűjtésére vagy mindkettőre használt információfeldolgozó rendszer vagy berendezés, ideértve a terminált, személyi számítógépet, elektronikus pénztárgépet, érintés nélküli leolvasót, illetve fizetési motort vagy folyamatot.

Értesítési határidő: az a dátum, amikor az American Express a kibocsátóknak megküldi az adott adatvédelmi incidensről az utolsó értesítést. Ez a dátum a végleges vizsgálati jelentés vagy a belső elemzés American Express általi kézhezvételétől függ, és az American Express saját jogkörében határozza meg.

Érvényesítési dokumentáció: az éves helyszíni biztonsági értékeléshez vagy SAQ-hoz tartozó AOC, a negyedéves hálózatátvilágításokhoz tartozó AOSC és a megállapítások vezetői összefoglalói, vagy az éves biztonságitechnológia-fejlesztési program hitelesítése.

Érzékeny hitelesítési adatok: a PCI DSS mindenkori szószedetében meghatározott jelentéssel bír.

Feldolgozó: a kereskedő szolgáltatója, aki/amely elősegíti az engedélyezés és benyújtás feldolgozását az American Express hálózatára.

Feltört kártyaszám: Adatvédelmi incidenshez kapcsolódó American Express-kártyaszámlaszám.

Fizetési alkalmazás: a Payment Card Industry Fizetési alkalmazásokra vonatkozó adatvédelmi szabványa (Payment Application Data Security Standard, PA DSS) mindenkori szószedetében meghatározott jelentéssel bír, amely elérhető a www.pcisecuritystandards.org címen.

Jogbérletbe adó: annak a vállalkozásnak az üzemeltetője, amely magánszemélyek vagy jogi személyek (a jogbérletbe vevők) számára engedélyezi, hogy árukat és/vagy szolgáltatásokat nyújtsanak az üzemeltető védjegye alatt, vagy az üzemeltető védjegye szerint működjenek; segítséget nyújt a jogbérletbe vevőknek az üzleti vállalkozásuk működtetésében, vagy befolyással van a jogbérletbe vevő működési módjára; és kifizetést vagy díjat szed be a jogbérletbe vevőktől.

Jóváhagyott pontok közötti titkosítási (P2PE) megoldás: a PCI SSC validált megoldásainak felsorolásában szerepel, vagy egy PCI SSC-minősített biztonsági felmérő P2PE vállalat által validált.

Jóváhagyott átvilágítási szállító (ASV): az a jogi személy, amelyet a Payment Card Industry Security Standards Council, LLC alkalmasnak nyilvánít arra, hogy bizonyos PCI DSS-követelmények betartását validálja internetes környezetek sérülékenységi átvilágításának lefolytatása útján.

Jóváírás: annak a terhelésnek az összege, amelyet Ön visszafizet a kártyatulajdonosoknak a kártyával végzett vásárlásokért vagy fizetésekért.

Kártyatulajdonosi adatok: a PCI DSS mindenkori szószedetében meghatározott jelentéssel bír.

Kártyatulajdonos: magánszemély vagy jogi személy, (i) aki/amely szerződést kötött kártyaszámla létesítésére egy kibocsátóval, vagy (ii) akinek/amelynek neve szerepel a kártyán.

Kártyatulajdonosi információ: információ az American Express-kártyatulajdonosokról és -kártyatranzakciókról, ideértve a neveket, címeket, kártyaszámlaszámokat és kártyaazonosítási számokat (CID-k).

Kereskedő: a kereskedő és valamennyi kapcsolt vállalkozása, amely az American Express-szel vagy kapcsolt vállalkozásaival kötött szerződés alapján American Express-kártyával elfogad.

Kockázatcsökkentő technológia: azon technológiai megoldások összessége, amelyek az American Express által meghatározott American Express-kártyatulajdonosi adatok és az érzékeny hitelesítési adatok biztonságát javítják. A kockázatcsökkentő technológia minősítés eléréséhez Ön köteles bizonyítani a technológia tervezése és rendeltetése szerinti hatékony felhasználását. Ide sorolhatók különösen: az EMV, a pontok közötti titkosítás és a tokenizálás.

Megfelelőségi igazolás (AOC): az Ön megfelelőségi státuszára vonatkozó nyilatkozat a PCI DSS tekintetében a Payment Card Industry Security Standards Council, LLC által megadott formátumban.

Megfelelőségi összefoglaló (SOC): egy jogbérletbe adó vagy szolgáltató által használt PCI-érvényesítési dokumentum, amelyen jelezheti az érintett jogbérletbe vevőinek PCI-megfelelőségi státuszát.

Minősített biztonsági felmérő (QSA): az a jogi személy, amelyet a Payment Card Industry Security Standards Council, LLC alkalmasnak nyilvánított arra, hogy a PCI DSS szabvány betartását validálja.

Önértékelési kérdőív (SAQ): a Payment Card Industry Security Standards Council, LLC által létrehozott önértékelési eszköz, amelynek rendeltetése a PCI DSS betartásának felmérése és hitelesítése.

Payment Card Industry Security Standards Council (PCI SSC) követelményei: a fizetésikártya-adatok biztonságához és védelméhez kapcsolódó szabványok és követelmények összessége, ideértve a PCI DSS és PA DSS szabványokat is, amelyek elérhetők a www.pcisecuritystandards.org címen.

PCI által jóváhagyott: a PIN-beviteli eszköz vagy a fizetési alkalmazás (vagy mindkettő) megjelenik a telepítés időpontjában a jóváhagyott vállalatok és szolgáltatók a PCI Security Standards Council, LLC által vezetett listáján, amely elérhető a www.pcisecuritystandards.org címen.

PCI DSS: a Payment Card Industry adatvédelmi szabványa (Data Security Standards), amely elérhető a www.pcisecuritystandards.org címen.

PCI-igazságügyi nyomozó (PFI): az a szervezet, amelyet a Payment Card Industry Security Standards Council, LLC jóváhagyott arra, hogy lefolytassa egy jogsértés vagy fizetésikártya-adatok feltörésének igazságügyi vizsgálatát.

PCI PIN-biztonsági követelményei: a Payment Card Industry PIN-biztonsági követelményei (PIN Security Requirements), amelyek elérhetők a www.pcisecuritystandards.org címen.

PIN-beviteli eszköz: a Payment Card Industry PIN-tranzakciók biztonsága (PIN Transaction Security, PTS), Interakciós pont (Point of Interaction, POI), Moduláris biztonsági követelmények (Modular Security Requirements) alatti mindenkori szószedetében meghatározott jelentéssel bír, amely elérhető a www.pcisecuritystandards.org címen.

Pontok közötti titkosítás (P2PE): az a megoldás, amely titkosítással védi a számlaadatokat attól a ponttól kezdve, ahol a kereskedő elfogadja a fizetési kártyát a titkosítás feloldásának védett pontjáig.

Szerződött felek: az Ön bármelyik vagy összes munkavállalója, meghatalmazottja, képviselője, alvállalkozója, feldolgozója, szolgáltatója, értékesítési ponti berendezéseinek vagy rendszereinek vagy fizetésfeldolgozó megoldásainak szolgáltatója, az Ön American Express-kereskedői számlájához tartozó jogi személyek és bármely más fél, akinek kártyatulajdonosi információihoz való hozzáférést adhat a szerződésnek megfelelően.

Szolgáltatók: meghatalmazott feldolgozók, harmadik fél feldolgozók, átjárók szolgáltatói, POS-rendszerek integrátorai és POS-rendszerek vagy egyéb fizetési feldolgozási megoldások vagy szolgáltatások szállítói a kereskedők számára.

Terhelés: kártyával végzett fizetés vagy vásárlás.

Titkosítási kulcs (American Express titkosítási kulcs): minden olyan kulcs, amelyet a számlaadatok feldolgozására, létrehozására, betöltésére és/vagy védelmére használnak. Ezek közé tartoznak többek között a következők:

- Kulcstitkosító kulcsok (Key Encryption Keys): Zóna mesterkulcsok (Zone Master Keys, ZMK-k) és Zóna PIN-kulcsok (Zone Pin Keys, ZPK-k)
- Biztonságos kriptográfiai eszközökben használt mesterkulcsok: Helyi mesterkulcsok (Local Master Keys, LMK-k)
- Kártyabiztonságikód-kulcsok (Card Security Code Keys, CSCK-k)
- PIN-kulcsok: Alap származtató kulcsok (Base Derivation Keys, BDK-k), PIN-titkosítási kulcsok (PIN Encryption Keys, PEK-k) és ZPK-k

Tranzakció: egy kártya útján végrehajtott terhelés vagy jóváírás.