AMERICAN EXPRESS

Adatvédelmi működési szabályzat (DSOP)

AMERICAN EXPRESS

DSOP Változásösszesítő

Ikonok

A fontos változtatásokat a Változásösszesítő táblázatban soroltuk fel, illetve a *DSOP-ban* a változtatásjelző sávval jelöltük. A változtatásjelző sáv egy függőleges vonal, általában a bal oldali margón, amely a hozzáadott vagy módosított szöveget jelöli. Csak a *DSOP-ban* bekövetkező, a Kereskedői működési eljárásokat potenciálisan befolyásoló lényeges változásokat jelzi a bal oldali margón látható változtatási sáv.

Az eltávolított szöveget a margón elhelyezett szemeteskuka ikon jelzi minden jelentős törölt szöveg mellett, beleértve a részeket, táblázatokat, bekezdéseket, jegyzeteket és felsoroláspontokat. Az eltávolított szövegre ebben a Változásösszefoglalóban a korábbi kiadvány részeinek számozását használva hivatkozunk a félreértések elkerülése érdekében.

A bekezdéseket határoló kék vonalak a régióra vonatkozó információkat jelzik.

Változásösszesítő táblázat

A fontos változtatásokat az alábbi táblázatban soroltuk fel, illetve a *DSOP-ban* a változtatásjelző sávval jelöltük.

Pont/Alpont	A változtatás leírása
Ebben a kiadásban nincsenek változások.	

1. rész Bevezetés a DSOP-ba és a védelmi szabványokba

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 (DSOP) 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.

Az Adatvédelmi működési szabályzat (DSOP) a számlaadatok védelmét szolgáló átfogó irányelvi követelmények összessége, amelyek célja a számlaadatok védelme minden olyan esetben, amikor ilyen adatokat tárolnak, feldolgoznak vagy továbbítanak.

American Express megköveteli, hogy minden Kereskedő és szolgáltató megfeleljen a Payment Card Industry Data Security Standard (PCI DSS) szabványnak. 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.
- Megfeleljen a Titkosítási kulcsok, 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.
- Biztosítsa, hogy az adatok tárolására, feldolgozására vagy továbbítására szolgáló technológia telepítésekor vagy cseréjekor a PCI által jóváhagyott termékeket használjanak.

Ön köteles a jelen adatvédelmi rendelkezéseknek megfelelően védeni a Szerződés szerint megőrzött American Express Terhelési és Jóváírási 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 2. rész, „A PCI DSS Megfelelőségi Program (Az Ön Rendszereinek fontos periodikus érvényesítése)" szerint, kivéve, ha ez a rész másként nem rendelkezik). A PCI-szabványokkal és a követelmények teljesítésével kapcsolatos részletek a következő weboldalon találhatók: www.pcisecuritystandards.org.

2. rész A PCI DSS Megfelelőségi Program (Az Ön Rendszereinek fontos periodikus érvényesítése)

Ön köteles elvégezni a lenti műveleteket, hogy az alábbiakban leírt módon, a PCI DSS szerint évente és 90 naponta érvényesítse az Ön és az Ön Jogbérletbe vevői olyan 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 PCI megfelelőségi programjában.

- 2. művelet: A Kereskedői/Szolgáltatói szint és a Érvényesítési dokumentációs követelmények megértése.
- 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

1. szintű Kereskedőknek, 2. szintű Kereskedőknek és minden az alábbiakban leírt Szolgáltatónak részt kell vennie a jelen Szabályzat Szerinti Programban. Az American Express saját belátása szerint kijelölhet bizonyos 3. és 4. szintű Kereskedőket a Programban való részvételre a jelen szabályzat szerint.

A Programban való részvételre kötelezett Kereskedőknek és Szolgáltatóknak az American Express által kiválasztott Programfelügyelő által biztosított Portálon kell regisztrálniuk az előírt határidőn belül.

- Önnek el kell fogadnia a Portál használatához kapcsolódó valamennyi észszerű feltételt.
- A Portálon belül legalább egy adatbiztonsági kapcsolattartót kell kijelölnie és pontos adatokat kell megadnia. Az előírt adatok közé a következők tartoznak:
  - Teljes név
  - E-mail-cím
  - Telefonszám
  - Levelezési cím
- A Portálon belül meg kell adnia a kijelölt adatvédelmi kapcsolattartó frissített vagy új elérhetőségi adatait, amennyiben az adatok megváltoznak.
- Biztosítania kell, hogy rendszerei frissítve legyenek, hogy lehetővé tegyék a szolgáltatás kommunikációját a Portál kijelölt tartományából.

Amennyiben Ön nem ad meg vagy nem tart fenn aktuális adatvédelmi kapcsolattartási adatokat, illetve nem teszi lehetővé az e-mailen keresztüli kommunikációt, az nem érinti a díjmegállapítási jogainkat.

2. művelet: A Kereskedői/Szolgáltatói szint és a Érvényesítési dokumentációs követelmények megértése

Négy szint létezik Kereskedők számára, és két Szint Szolgáltatók számára, amelynek alapja az Ön által kezelt, American Express kártyával végzett Tranzakciók volumene.

- A Kereskedők számára ez a Fióktelepeik által benyújtott volumen, amely a legmagasabb American Express Kereskedői számlaszintre emelkedik.*
- Szolgáltatók esetében ez a Szolgáltató és a Szolgáltatást nyújtó szervezetek által benyújtott volumenek összege, amelyeknek Ön szolgáltatást nyújt.

A Buyer Initiated Payment (BIP) Tranzakciók nem számítanak bele az American Express Kártyával végzett Tranzakciók volumenébe a Kereskedői szint és az érvényesítési követelmények meghatározásakor. Ön a következő táblázatban meghatározott Kereskedői szintek valamelyikébe tartozik: A-1 táblázat: Kereskedői és Szolgáltatói szintek.

* 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.

A-1 táblázat: Kereskedői és Szolgáltatói szintek

Kereskedői szintek	Éves American Express Tranzakciók
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	Kevesebb, mint 10 000 American Express Kártyával végzett Tranzakció évente.
Szolgáltatói Szint	**Éves American Express Tranzakciók**
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.

Kereskedői Érvényesítési Dokumentációs Követelmények

A Kereskedők (nem a Szolgáltatók) négy lehetséges Kereskedői Szint besorolással rendelkeznek. Miután meghatározta a Kereskedői szintet az A-1 táblázat: Kereskedői és Szolgáltatói szintek (fent), nézze meg az A-2 táblázat: Kereskedői Érvényesítési Dokumentációs Követelmények az Érvényesítési dokumentációs követelmények meghatározásához.

A-2 táblázat: Kereskedői Érvényesítési Dokumentációs Követelmények

Kereskedői szint/ Éves American Express Tranzakciók	Megfelelőségi jelentés Megfelelőségi igazolás (ROC AOC)	Önértékelési Kérdőíves Megfelelőségi igazolás (SAQ AOC) ÉS negyedévente Külső hálózati sebezhetőségi vizsgálat (Scan)	Biztonságitechnológia-fejlesztési program (STEP) Igazolás a jogosult kereskedők számára
1. Szint/ 2,5 millió vagy annál több	Kötelező	Nem alkalmazható	Választható az American Express jóváhagyásával (ROC helyébe lép)
2. Szint/ 50 000 és 2,5 millió között	Választható	SAQ AOC kötelező (hacsak nem nyújtanak be ROC AOC-ot); az átvilágítás bizonyos SAQ-típusoknál kötelező	Választható az American Express jóváhagyásával* (helyettesíti az SAQ-t és a hálózati átvilágítást vagy az ROC-t)
3. Szint**/ 10 000 és 50 000 között	Választható	SAQ AOC választható (akkor kötelező, ha azt az American Express előírja); az átvilágítás bizonyos SAQ-típusoknál kötelező	Választható az American Express jóváhagyásával* (helyettesíti az SAQ-t és a hálózati átvilágítást vagy az ROC-t)
4. Szint**/ Kevesebb, mint 10 000	Választható	SAQ AOC választható (akkor kötelező, ha azt az American Express előírja); az átvilágítás bizonyos SAQ-típusoknál kötelező	Választható az American Express jóváhagyásával* (helyettesíti az SAQ-t és a hálózati átvilágítást vagy az ROC-t)

* **Megjegyzés:** Az American Express PCI csapata megvizsgálja a kérelmet és a jogosultságot, és megerősíti, hogy Ön jogosult-e a STEP programra. Kérjük, forduljon ügyfélmenedzseréhez és/vagy AXPPCIComplianceProgram@aexp.com a jogosultság ellenőrzésére.

**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 az Ön PCI Érvényesítési dokumentációjának a teljességét, pontosságát és megfelelőségét. Az American Express kérheti, hogy e cél érdekében további igazoló

dokumentumokat nyújtson be az értékeléshez. Továbbá, az American Express jogosult arra kötelezni Önt, hogy a PCI Biztonsági Szabványok Tanácsa által jóváhagyott Minősített biztonsági felmérőt (Qualified Security Assessor, QSA) vagy PCI Igazságügyi nyomozót (PCI Forensic Investigator, PFI) bízzon meg.

Szolgáltatói Érvényesítési dokumentáció követelmények

A Szolgáltatóknak (nem a Kereskedőknek) két lehetséges Szint besorolásuk van. Miután meghatározta a Szolgáltatói szintet az A-1 táblázat: Kereskedői és Szolgáltatói szintek (fent), nézze meg az A-3 táblázat: Szolgáltatói Érvényesítési dokumentáció az Érvényesítési dokumentációs követelmények meghatározásához.

A Szolgáltatók nem vehetnek részt a STEP programban.

A-3 táblázat: Szolgáltatói Érvényesítési dokumentáció

Szint	Érvényesítési dokumentáció	Követelmény
1	Éves Megfelelőségi jelentés Megfelelőségi igazolás (ROC AOC)	Kötelező
2	Éves SAQ D (Szolgáltató) és negyedéves hálózati vizsgálat vagy Éves Megfelelőségi jelentés Megfelelőségi igazolás (ROC AOC), ha előnyösebb	Kötelező

A Szolgáltatók részére is ajánlott, hogy tartsák be a PCI Kijelölt szervezetek kiegészítő érvényesítését is.

Biztonságitechnológia-fejlesztési program (STEP)

A PCI DSS-t betartó Kereskedők az American Express belátása szerint jogosultak lehetnek az American Express STEP (Security Technology Enhancement Programme) programjára is, amennyiben 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 amennyiben az összes Kártyatranzakció 75%-a a következő fokozott biztonsági opciók kombinációjával történik:

- **EMV, EMV érintés nélküli vagy Digitális pénztárca** – 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 amerikai 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
- **Tokenizált** - a bevezetett tokenizációs megoldásnak:
  - meg kell felelnie az EMVCo specifikációnak,
  - PCI-kompatibilis harmadik fél szolgáltatónak kell biztosítania, feldolgoznia, tárolnia, továbbítania és teljes egészében kezelnie, és
  - a Token nem fordítható vissza, hogy a Kereskedő számára feltárja az Elsődleges számlaszámokat (PAN).

A STEP programra jogosult Kereskedőknek csökkentett PCI Érvényesítési dokumentációs követelményeik vannak, amelyet a 3. művelet: „Készítse el az Érvényesítési dokumentációt, amelyet el kell küldenie az American Express számára" alább.

3. művelet: Készítse el az Érvényesítési dokumentációt, amelyet el kell küldenie az American Express számára

A következő dokumentumok szükségesek a különböző szintű Kereskedők és Szolgáltatók számára, amint az az A-2 táblázat: Kereskedői Érvényesítési Dokumentációs Követelmények és az A-3 táblázat: Szolgáltatói Érvényesítési dokumentáció fentebb szerepel.

Be kell nyújtania a Megfelelőségi igazolást (Attestation of Compliance, AOC) a vonatkozó értékelési típushoz. Az AOC az Ön megfelelőségi státuszáról szóló nyilatkozat, és mint ilyet, a szervezet megfelelő szintű vezetőjének alá kell írnia és dátummal kell ellátnia.

Az American Express az AOC mellett a teljes értékelés egy példányát és, saját belátásunk szerint, további, a PCI DSS követelményeinek való megfelelést igazoló dokumentumokat is kérhet Öntől. Ezt az Érvényesítési dokumentációt az Ön költségére töltjük ki.

Megfelelőségi jelentés Megfelelőségi igazolás (ROC AOC) - (Éves követelmény) – A Megfelelőségi jelentés dokumentumok az Ön berendezései, rendszerei és hálózatai részletes helyszíni vizsgálatának az eredményei (és azok összetevői), ahol a Kártyatulajdonosok adatait vagy az Érzékeny hitelesítési adatokat (vagy mindkettőt) tárolják, feldolgozzák vagy továbbítják. Két verziója van: egy a Kereskedők és egy másik a Szolgáltatók számára. A Megfelelőségi jelentést az alábbi személyek valamelyikének kell elvégeznie:

- egy QSA-nak, vagy
- egy Belső biztonsági értékelő (ISA), és a vezérigazgató, a pénzügyi vezető, az információbiztonsági vezető vagy a főigazgató igazolja

A ROC AOC-t a QSA-nak vagy ISA-nak és a szervezeten belüli felhatalmazott vezetői szintnek alá kell írnia és dátummal kell ellátnia, és évente legalább egyszer be kell nyújtania az American Express felé.

Önértékelési kérdőív Megfelelőségi igazolás (SAQ AOC) - (Éves követelmény) – Az Önértékelési kérdőívek lehetővé teszik azon berendezések, rendszerek és hálózatok (és azok összetevőinek) önellenőrzését, ahol a Kártyatulajdonosok adatait vagy az Érzékeny hitelesítési adatokat (vagy mindkettőt) tárolják, feldolgozzák vagy továbbítják. Az SAQ-nak több változata is létezik. Ön a Kártyatulajdonosi adatkörnyezetétől függően választ egyet vagy többet.

Az SAQ-ot kitölthetik a vállalaton belüli, a kérdések pontos és alapos megválaszolására képesített munkatársak, vagy megbízhat egy QSA-t a segítségnyújtással. A SAQ AOC-ot a szervezeten belüli felhatalmazott vezetői szintnek alá kell írnia és dátummal kell ellátnia, és évente legalább egyszer be kell nyújtania az American Express felé.

Külső hálózati sebezhetőségi átvizsgálás összefoglalója (ASV átvizsgálás) - (90 napos követelmény) – A külső sebezhetőségi átvizsgálás egy távoli teszt, amely segít azonosítani a Kártyatulajdonosok adatkörnyezete internetre néző összetevőinek (pl. weboldalak, alkalmazások, webszerverek, levelezőszerverek, nyilvános domainek vagy hosztok) potenciális gyengeségeit, sebezhetőségeit és hibás konfigurációit.

Az ASV átvilágítást egy Jóváhagyott átvilágítási szállítónak (Approved Scanning Vendor, ASV) kell elvégeznie.

Amennyiben a SAQ megköveteli, az ASV vizsgálatról szóló jelentést (Attestation of Scan Compliance, AOSC) vagy a vezetői összefoglalót, amely tartalmazza a vizsgált célpontok számát, annak igazolását, hogy az eredmények megfelelnek a PCI DSS vizsgálati eljárásainak, valamint az ASV által kitöltött megfelelőségi státuszt, legalább 90 naponként egyszer be kell nyújtani az American Express felé.

Ha ROC AOC vagy STEP dokumentumot nyújt be, nem szükséges AOSC vagy ASV átvilágítási összefoglalót benyújtania, kivéve, ha külön kérik. Az egyértelműség kedvéért az Átvilágítás abban az esetben kötelező, ha azt a vonatkozó SAQ előírja.

STEP Hitelesítés érvényesítési dokumentáció (STEP) - (Éves követelmény) – A STEP csak azon Kereskedők számára érhető el, akik megfelelnek a fenti 2. művelet: „A Kereskedői/Szolgáltatói szint és a Érvényesítési dokumentációs követelmények megértése” részben előírt követelményeknek. Amennyiben az Ön vállalata megfelel a követelményeknek, akkor évente ki kell töltenie és be kell nyújtania az American Expressnek a STEP-Hitelesítési formanyomtatványt. Az éves STEP igazolási űrlap letölthető a Portálol. Keresse fel ügyfélmenedzserét, vagy írjon az American Expressnek a következő e-mail-címre: AXPPCIComplianceProgram@aexp.com.

A PCI DSS-nek történő nem megfelelőség - (Éves, 90 napos és/vagy Eseti követelmény) – Amennyiben nem felel meg a PCI DSS-nek, akkor a PCI Prioritised Approach Tool (PAT) összefoglalót (letölthető a PCI Biztonsági Szabványügyi Tanács weboldaláról) kell benyújtani.

A PAT összefoglalóban helyreállítási határidőt kell kitűzni, amely a megfelelés elérése érdekében nem haladhatja meg a dokumentum elkészítésének időpontját követő tizenkettő (12) hónapot. Ön köteles a szabályszegési státuszának helyreállítása érdekében tett intézkedéseinek előrehaladásáról meghatározott időközönként az

American Expresst értesíteni (1., 2., 3. és 4. Szintű Kereskedők; minden Szolgáltató). A PCI DSS-nek való megfelelés eléréséhez szükséges javítási intézkedéseket az Ön költségén kell elvégezni.

Az American Express nem szab ki meg nem felelési díjat a helyreállítási határidő előtt. Az A-4 táblázat: Meg nem felelési díj értelmében Ön továbbra is felelős az American Express-szel szemben az Adatvédelmi incidenssel kapcsolatos valamennyi kártérítési kötelezettségért, és a jelen szabályzat minden egyéb rendelkezése vonatkozik Önre.

American Express, saját belátása szerint fenntartja magának a jogot, hogy meg nem felelésért díjakat szabjon ki, ha:

- a PCI Prioritised Approach sablonját nem az e szakaszban meghatározott követelményeknek megfelelően nyújtották be,
- nem teljesültek a nem megfelelő státuszra vonatkozó, a PCI Prioritised Approach sablonjában felvázolt helyreállítási lépések,
- a nem megfelelő státuszra vonatkozó PCI Prioritised Approach sablonjának bármelyik követelménye nem teljesült, vagy
- a kötelező megfelelési dokumentációt nem nyújtották be az American Expressnek a vonatkozó határidőig vagy kérésre.

Azok a Kereskedők/Szolgáltatók, akik nem felelnek meg a 2. művelet: A Kereskedői/Szolgáltatói szint és a Érvényesítési dokumentációs követelmények megértése részletezett követelményeknek, 4. művelet: Küldje el az Érvényesítési dokumentációt az American Expressnek című részben meghatározott díjakkal sújthatók.

A félreértések elkerülése végett azok a Kereskedők, akik nem tartják be a PCI DSS-t, nem jogosultak a STEP programra.

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

Minden, a Programban való részvételre kötelezett Kereskedőnek és Szolgáltatónak a vonatkozó határidőkön belül be kell nyújtania az American Expressnek a 2. művelet: „A Kereskedői/Szolgáltatói szint és a Érvényesítési dokumentációs követelmények megértése" című táblázatban „Kötelező" jelzéssel ellátott érvényesítési dokumentációt.

Az Érvényesítési dokumentációt az American Expressnek kell benyújtania az American Express által kiválasztott Programfelügyelő által biztosított Portálon keresztül. Az Érvényesítési dokumentáció benyújtásával Ön kijelenti és garantálja az American Expressnek, hogy a következők igazak (legjobb tudása szerint):

- Az Ön értékelése teljes és alapos volt;
- A PCI DSS státusza a befejezéskor pontosan megjelenik, akár a megfelelőségi igazolást (Attestation of Compliance, AOC) vagy a PCI Prioritised Approach Tool (PAT) összefoglalóját nyújtja be a meg nem felelés miatt;
- Ön jogosult az abban foglalt információk nyilvánosságra hozatalára, és az Érvényesítési dokumentációt úgy bocsátja az American Express rendelkezésére, hogy az nem sérti más felek jogait.

Nem megfelelési díjak és a Szerződés felmondása

Az American Express jogosult Önre a Meg nem felelésért 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 megkísérli értesíteni az adatbiztonsági kapcsolattartót az egyes éves és negyedéves jelentési időszakokra vonatkozó határidőkről.

A-4 táblázat: Meg nem felelési díj

Leírás*	1. Szintű Kereskedő vagy 1. Szintű Szolgáltató	2. Szintű Kereskedő vagy 2. Szintű Szolgáltató	3. Szintű vagy 4. Szintű Kereskedő
A meg nem felelésért kirótt díj akkor kerül megállapításra, ha az Érvényesítési dokumentációt nem kapják kézhez az első határidőn belül.	USD 25 000	USD 5 000	USD 50
A meg nem felelésért kirótt további díj akkor kerül megállapításra, ha az Érvényesítési dokumentációt nem kapják kézhez a második határidőn belül.	USD 35 000	USD 10 000	USD 100
A meg nem felelésért kirótt további díj akkor kerül megállapításra, ha az Érvényesítési dokumentációt nem kapják kézhez a harmadik határidőn belül. **MEGJEGYZÉS:** A Meg nem felelésért kirótt díjakat addig alkalmazzák, amíg az Érvényesítési dokumentáció nem kerül benyújtásra.	USD 45 000	USD 15 000	USD 250

* A Meg nem felelésért kirótt díjakat a Helyi pénznem alapján számoljuk.

* Argentínára nem vonatkozik.

Amennyiben a PCI DSS megfelelőségi dokumentációs kötelezettségei nem teljesülnek, az American Express jogosult a meg nem felelési díjakat halmozottan felszámítani, a kifizetéseket visszatartani és/vagy a Szerződést felmondani.

3. rész Adatvédelmiincidens-kezelési kötelezettségek

Ön köteles haladéktalanul értesíteni az American Expresst, de legfeljebb hetvenkét (72) órával azt követően, hogy Adatvédelmi incidensről szerez tudomást.

Az American Express értesítéséhez lépjen kapcsolatba az American Express Enterprise Incident Response Programmal (*EIRP*) díjmentesen: 1.888.732.3750, vagy 1.602.537.3021, vagy e-mailben: EIRP@aexp.com. Az Adatvédelmi incidens vonatkozásában Önnek kötelessége kijelölni egy személyt kapcsolattartóként. Ezenfelül:

- Önnek minden egyes Adatvédelmi incidenst alaposan ki kell vizsgálnia, és haladéktalanul át kell adnia az American Expressnek az összes Kompromittált Kártyaszámot. Az American Express fenntartja a jogot, hogy saját belső elemzést végezzen az Adatvédelmi incidens által érintett adatok azonosítása érdekében.

A 10 000-nél kevesebb egyedi Kártyaszámot érintő Adatvédelmi incidensek esetében a vizsgálat befejezését követő tíz (10) munkanapon belül összefoglalót kell küldeni az American Express számára.

- A vizsgálati összefoglalóknak a következő információkat kell tartalmazniuk: az incidens összefoglalása, az érintett környezet(ek) leírása, az események idővonala, a legfontosabb dátumok, a hatás és az adatok kitettségének részletei, a korlátozási és helyreállítási intézkedések, valamint annak igazolása, hogy nincs jele annak, hogy további American Express adatok veszélyben lennének.

A 10 000 vagy annál több egyedi Kártyaszámot érintő Adatvédelmi incidens esetében egy Ön által alkalmazott PCI Igazságügyi nyomozónak (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.
- A törvényszéki vizsgálati jelentéseket a PCI-nél elérhető, aktuális törvényszéki esemény zárójelentés-sablon felhasználásával kell kitölteni. A jelentésnek tartalmaznia kell a törvényszéki vizsgálatokat, a megfelelőségi jelentéseket és az adatvédelmi incidenssel kapcsolatos minden egyéb információt; azonosítania kell az adatvédelmi incidens okát; meg kell erősítenie, hogy az adatvédelmi incidens idején megfelelt-e a PCI DSS-nek; és igazolnia kell, hogy képes megelőzni a jövőbeni adatvédelmi incidenseket azáltal, hogy (i) tervet nyújt be a PCI DSS hiányosságainak orvoslására, és (ii) részt vesz az American Express megfelelőségi programban (az alábbiakban leírtak szerint). Az American Express kérésére Ön köteles a hiányosságok orvoslásáról szóló, Minősített biztonsági felmérő (Qualified Security Assessor, QSA) által készített igazolást rendelkezésre bocsátani.

A jelen 3. rész, „Adatvédelmiincidens-kezelési kötelezettségek” előző bekezdései ellenére:

- Az American Express saját belátása szerint kérheti Öntől, hogy bízzon meg egy PFI-t az adatvédelmi incidens kivizsgálásának lefolytatására olyan adatvédelmi incidensek esetében, amelyek kevesebb mint 10 000 egyedi Kártyaszámot érintenek, vagy amikor 12 hónapon belül több incidens is történt. Minden ilyen vizsgálatnak meg kell felelnie a jelen 3. 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.

Az Adatvédelmi incidenst az alkalmazandó adatvédelmi incidensről szóló törvények szerint kell értékelnie világszerte, és amennyiben szükségesnek ítéli, az adatvédelmi incidensről szóló törvényeknek megfelelően értesítenie kell az alkalmazandó szabályozó hatóságokat és az érintett Kártyatagokat. Amennyiben Ön úgy döntött, hogy a Szolgáltatója vagy más szervezet felelős az Adatvédelmi incidens bejelentéséért, akkor tájékoztatnia kell az ilyen Szolgáltatót vagy szervezetet arról, hogy köteles felmérni az alkalmazandó adatvédelmi incidensről szóló törvények szerinti bejelentési kötelezettségeit. Ön vállalja, hogy az American Express írásbeli jóváhagyását megszerzi, mielőtt a Kártyatagoknak szóló, az Adatvédelmi incidenssel kapcsolatos kommunikációban hivatkozna vagy megnevezné az American Express-t. Ön vállalja, hogy együttműködik az American Express-szel az Adatvédelmi incidensből eredő problémák részletezése és orvoslása érdekében, beleértve az összes releváns információ megadását (és a szükséges lemondások megszerzését) az American Express számára annak igazolására, hogy Ön képes a jövőbeni Adatvédelmi incidensek megelőzésére a Szerződéssel összhangban lévő módon.

A Szerződésben foglalt bármely ellenkező tartalmú titoktartási kötelezettségtől függetlenül az American Expressnek jogában áll bármely Adatvédelmi incidensről információt közzétenni az American Express Kártyatulajdonosok, Kibocsátók, 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.

Mi a teendő Adatvédelmi incidens esetén?

Kérjük, kövesse az alábbi lépéseket, amennyiben Adatvédelmi incidenst azonosított a vállalkozása vonatkozásában.

1. lépés:

Töltse ki a Kereskedői Adatvédelmi incidens kezdeti bejelentési űrlapot és küldje el az EIRP@aexp.com e-mail-címre az Adatvédelmi incidens felfedezésétől számított 72 órán belül.

2. lépés:

Folytasson alapos vizsgálatot; ez lehet azt igényli, hogy fel kell bérelnie egy Payment Card Industry (PCI) Igazságügyi nyomozót.

3. lépés:

Azonnal adja meg nekünk a veszélybe került American Express® Kártyaszámokat.

4. lépés:

Működjön együtt velünk az Adatvédelmi incidensből származó problémák megoldása érdekében.

Olvassa el a 3. rész, „Adatvédelmiincidens-kezelési kötelezettségek" hogy további információt tudjon meg az Adatvédelmiincidens-kezelési kötelezettségekről.

További kérdései vannak?

US: (888) 732-3750 (díjmentes)

Nemzetközi: +1 (602) 537-3021

EIRP@aexp.com

4. rész Kártalanítási kötelezettségek Adatvédelmi incidens esetén

Az Ön Szerződés szerinti, az American Express felé fennálló kártalanítási kötelezettségeit Adatvédelmi incidens bekövetkezése esetén a jelen 4. 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 4. rész, „Kártalanítási kötelezettségek Adatvédelmi incidens esetén" alább meghatározott kötbért kell fizetnie az Adatvédelmi incidensre vonatkozóan.

Ön köteles az American Expresst számlaszámonként 5 USD díjon kártalanítani azokért az Adatvédelmi incidensekért, amelyek:

- legalább 10 000 American Express Kártyaszámot érintenek a következők egyikével:
  - Érzékeny hitelesítési adatok, vagy
  - Lejárati dátum

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 az American Express-t az Adatvédelmi incidensről a 3. rész, „Adatvédelmiincidens-kezelési kötelezettségek" résznek megfelelően értesítette,
  - 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 4. 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 meg nem felelési díjat fizetni (az American Express által saját mérlegelési jogkörében meghatározottak szerint) abban az esetben, amennyiben Ön nem tesz eleget a 3. rész, „Adatvédelmiincidens-kezelési kötelezettségek" részben foglalt valamely kötelezettségének. A félreértések elkerülése érdekében az egyes Adatvédelmi incidensekért megállapítható Adatvédelmi incidensre vonatkozó meg nem felelési díj 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 kapcsolatosan 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).

Az Ön 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:

A-5 táblázat: Kártalanítási kötelezettség csökkentésének követelményei

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. A példák az A-6 táblázat: Kártalanítási kötelezettség fokozott csökkentése a kártalanítás csökkentés kiszámítását szemléltetik.
- A Kockázatcsökkentő technológia használatával történő minősítés eléréséhez Ön köteles bizonyítani a technológia tervezése és rendeltetése szerinti hatékony felhasználását.
- 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.

A-6 táblázat: Kártalanítási kötelezettség fokozott csökkentése

Pl.	Használatban lévő Kockázatcsökkentő technológiák	Jogosult	Csökkentés
1	• A Tranzakciók 80%-át Chippel ellátott eszközzel dolgozták fel • A telephelyek 0%-a használ egyéb Kockázatcsökkentő technológiát	Nem	50%: Általános csökkentés (amennyiben a Kockázatcsökkentő technológiák aránya 75%-nál kisebb, a fokozott csökkentés nem lehetséges)[1]
2	• A Tranzakciók 80%-át Chippel ellátott eszközzel dolgozták fel • A telephelyek 77%-a használ egyéb Kockázatcsökkentő technológiát	Igen	77%: Fokozott csökkentés (a Kockázatcsökkentő technológia 77%-os igénybevétele alapján)
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 5,00 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.

5. rész Célzott elemzési program (Targeted Analysis Programme, TAP)

Kártyatulajdonosi adatokat veszélyeztető incidenst például a Kártyatulajdonosi adatkörnyezetben (Cardholder Data Environment, CDE) lévő adatbiztonsági rések okozhatnak.

Kártyatulajdonosi adatokat veszélyeztető incidensek lehetnek többek között az alábbiak is:

- **Közös vásárlási pont (Common Point of Purchase, CPP):** Az American Express Kártyatagok hamis Tranzakciókat jelentenek Kártyaszámlájukon, és ezekről az azonosítást követően azt állapítjuk meg, hogy az Ön Létesítményeiben tett vásárlásokból származnak.

- **Közzétett kártyaadatok:** American Express Kártya- vagy Kártyatulajdonosi adatokat találunk a világhálón, amelyek az Ön Létesítményeiben végbement Tranzakciókhoz kapcsolhatók.
- **Kártevőveszély:** Az American Express azt gyanítja, hogy Ön kártevő kóddal fertőzött vagy azzal szemben védtelen szoftvert használ.

A TAP célja a Kártyatulajdonosi adatokat veszélyeztető potenciális incidensek felismerése.

Önnek és Szerződött feleinek meg kell felelniük az alábbi követelményeknek, amint az American Express értesítést kap a Kártyatulajdonosi adatokat veszélyeztető potenciális incidensről.

- Ön köteles azonnal átvizsgálni a CDE-t adatbiztonsági rések jelenléte után, és orvosolni minden fellelt hibát.
  - Ön köteles minden külső beszállítóját arra kötelezni, hogy alaposan vizsgálják át az ÖN CDE-jét, ha azt kiszervezi.
- Ön köteles az American Express kérésére a vizsgálatra, kiértékelésre és/vagy hibaorvoslásra vonatkozóan megtett vagy tervezett intézkedésekkel kapcsolatos erőfeszítéseiről összesített jelentést küldeni.
- Ön köteles frissített PCI DSS hitelesítő dokumentumokat küldeni részünkre az 2. rész, „A PCI DSS Megfelelőségi Program (Az Ön Rendszereinek fontos periodikus érvényesítése)" leírtak szerint.
- Adott esetben fel kell kérnie egy képzett PCI PFI, hogy vizsgálja meg a CDE-t, ha Ön vagy a Szerződött fél:
  - Nem tudja megoldani a Kártyatulajdonosi adatokat veszélyeztető potenciális incidenst az American Express által meghatározott észszerű időn belül, vagy
  - Megerősíti, hogy Adatvédelmi incidens történt és követi a 3. rész, „Adatvédelmiincidens-kezelési kötelezettségek" részben leírtakat.

A-7 táblázat: TAP nem megfelelési díj

Leírás	1. Szintű Kereskedő vagy 1. Szintű Szolgáltató	2. Szintű Kereskedő vagy 2. Szintű Szolgáltató	3. Szintű vagy 4. Szintű Kereskedő
Meg nem felelési díj kivethető, ha a TAP-kötelezettségeket nem teljesítik az első határidőig.	USD 25 000	USD 5 000	USD 1 000
Meg nem felelési díj kivethető, ha a TAP-kötelezettségeket nem teljesítik a második határidőig.	USD 35 000	USD 10 000	USD 2 500
Meg nem felelési díj kivethető, ha a TAP-kötelezettségeket nem teljesítik a harmadik határidőig. **MEGJEGYZÉS:** *A meg nem felelési díj a kötelezettségek teljesítéséig vagy a TAP megoldásáig tovább számlázható.*	USD 45 000	USD 15 000	USD 5 000

Amennyiben Ön nem teljesíti a TAP-által előírt kötelezettséget, az American Express jogosult a meg nem felelési díjakat halmozottan felszámítani, a kifizetéseket visszatartani és/vagy a Szerződést felmondani.

6. 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 Portál szolgáltatót 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.

7. 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.

8. rész Szószedet

Kizárólag a jelen Adatvédelmi működési szabályzat alkalmazásában a következő fogalommeghatározások alkalmazandók és irányadók:

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 kulcsok vagy legalább egy American Express Kártyaszámlaszám 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, megadottak vagy elérhetővé tettek 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: a behatolásnak a végleges igazságügyi incidens jelentésben (pl. PFI-jelentés) meghatározott időszaka (vagy hasonlóan meghatározott időszak), vagy amennyiben ismeretlen, a nekünk bejelentett, potenciálisan veszélyeztetett Kártyaszámok utolsó bejelentési dátumát megelőző 365 nap

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.

Buyer Initiated Payment (BIP) tranzakciók: olyan digitális fizetési megoldást jelent, amely lehetővé teszi a vevők számára, hogy gyorsan és hatékonyan ütemezzék a beszállítóknak történő kifizetéseket (vállalati kártyákhoz kapcsolódva).

Célzott elemzési program: olyan program, amely lehetővé teszi a kártyatulajdonosi adatokat veszélyeztető potenciális incidensek korai felismerését biztosítja a Kártyatulajdonosi adatkörnyezetben (CDE). Lásd 5. rész, „Célzott elemzési program (Targeted Analysis Programme, TAP)”.

Chip: a Kártyába beépített integrált mikrochip, amely tartalmazza a kártyatag és a számla adatait.

Chipkártya: az a Kártya, amely chipet tartalmaz, és használatához szükséges lehet egy PIN, amellyel ellenőrizni lehet a Kártyatag 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.

Elsődleges számlaszámok (PAN): a PCI DSS mindenkor hatályos fogalomjegyzékében meghatározott jelentéssel bír.

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 kártyatulajdonosok hitelesítésére és/vagy a fizetési kártyatranzakciók engedélyezésére használt, biztonsággal kapcsolatos információk. Ezek az információk magukban foglalják többek között a kártya ellenőrző kódjait, az összes nyomkövetési adatot (mágnescsíkról vagy azzal egyenértékű chipről), PIN-kódokat és PIN-blokkokat.

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 A biztonságos szoftverszabványhoz (Secure Software Standard) és a biztonságos szoftveréletciklus szabványa (Secure Software Life Cycle Standard) mindenkori Szószedetében meghatározott jelentéssel bír, amely elérhető a www.pcisecuritystandards.org címen.

Fogyasztónak: minősül a kártyatulajdonos, aki árut, szolgáltatást vagy mindkettőt vásárol.

Igazságügyi incidens végleges jelentés sablonja: a PCI Security Standards Council által rendelkezésre bocsátott sablon, amely a www.pcisecuritystandards.org weboldal címen érhető el.

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.

Jogbérletbe vevő: egy független tulajdonban lévő és függetlenül üzemeltetett külső fél (ideértve a jogbérletbe vevőt, licencbe vevőt vagy fejezetet) – bármely Jogbérletbe adó által a jogbérlet üzemeltetésére licencelt Kapcsolt vállalkozások kivételével –, amely írásos szerződést kötött a Jogbérletbe adóval, miszerint köteles következetesen és feltűnő módon külső azonosító jelekkel – a Jogbérletbe adó márkajelével – azonosítani magát vagy a nyilvánosság előtt a Jogbérletbe adó vállalatcsoportjának tagjaként tüntetni fel magát.

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 Kártyatagoknak a Kártyával végzett vásárlásokért vagy fizetésekért.

Jóváírás nyilvántartás: a Jóváírások követelményeink szerinti nyilvántartása.

Kártyakibocsátó: olyan Jogi személy (ideértve az American Expresst és annak Kapcsolt vállalkozásait), akit az American Express vagy annak egy Kapcsolt vállalkozása licencel a Kártyák kibocsátására és a Kártyakibocsátó üzletágban való tevékenységre.

Kártyaszám: egyedi azonosító szám, amelyet a kibocsátó a Kártyához rendel annak kibocsátásakor.

Kártyatulajdonosi adatkörnyezet (CDE): a kártyatulajdonosok adatait vagy érzékeny hitelesítési adatokat tároló, feldolgozó vagy továbbító személyeket, folyamatokat és technológiák.

Kártyatulajdonos adatai: legalább a teljes Elsődleges számlaszámot (PAN) önmagában vagy a teljes PAN-t és az alábbiak bármelyikét jelentik: kártyatulajdonos neve, lejárati dátum, és/vagy szolgáltatói kód. A fizetési művelet részeként továbbított vagy feldolgozott (de nem tárolt) további adatelemekért lásd az Érzékeny hitelesítési adatok című részt.

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

Kártyatulajdonos: olyan ügyfél, akinek fizetési kártyát bocsátottak ki, vagy a fizetési kártya használatára jogosult bármely személy.

Kártyatag információ: információ az American Express Kártyatagokról 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 Kártyát elfogad.

Kereskedő Szint: az a megnevezés, amelyet a Kereskedők PCI DSS-megfelelőségi érvényesítési kötelezettségeihez rendelünk, az 2. rész, „A PCI DSS Megfelelőségi Program (Az Ön Rendszereinek fontos periodikus érvényesítése)”.

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 többek között de nem kizárólag: 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.

Minősített biztonsági felmérő (QSA): az a jogi személy, amelyet a Payment Card Industry Security Standards Council, LLC alkalmasnak nyilvánított arra, hogy 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 Data Security Standard (PCI DSS): amely elérhető a www.pcisecuritystandards.org címen.

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.

Portál: azt a jelentési rendszert takarja, amelyet az American Express által kiválasztott American Express PCI Program adminisztrátorai biztosítanak. A Kereskedők és a Szolgáltatók kötelesek a Portált használni a PCI érvényesítési dokumentáció American Express felé történő benyújtása érdekében.

Program: az American Express PCI megfelelőségi Programot jelenti.

Számlaadatok: a Kártyatulajdonos adataiból és/vagy érzékeny hitelesítési adatokból állnak. Lásd Kártyatulajdonos adatai és Érzékeny hitelesítési adatok.

Szerződés: az Általános rendelkezések, a Kereskedői szabályzat, valamint a kísérő ütemtervek és mellékletek együttesen (anyagainkban néha Kártyaelfogadási megállapodásként hivatkozunk rájuk).

Szerződött felek: az Ön bármelyik vagy összes munkavállalója, meghatalmazottja, képviselője, alvállalkozója, Feldolgozója, Szolgáltatója, értékesítési ponti (POS) berendezéseinek vagy rendszereinek vagy fizetésfeldolgozó megoldásainak szolgáltatója, az Ön American Express Kereskedői számlájához tartozó Jogi személyek és bármely más fél, akinek Kártyatulajdonosi információihoz vagy Érzékeny hitelesítési adatokhoz (vagy mindkettőhöz) 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.

Terhelési nyilvántartás: a Terhelésekről készült reprodukálható (papíralapú és elektronikus) nyilvántartás, amely megfelel a követelményeinknek, és tartalmazza a Kártyaszámot, a tranzakció dátumát, a dollárösszeget, a jóváhagyást, a Kártyatag aláírását (ha van ilyen) és egyéb információkat.

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

Token: az a kriptográfiai token, amely egy adott index alapján egy kiszámíthatatlan értékre cseréli a PAN-t.

Tranzakció: egy Kártya útján végrehajtott Terhelés, Jóváírás, Készpénzelőleg (vagy egyéb készpénz-hozzáféréses), ATM-Tranzakció, amelyet Kártyával hajtottak végre.

Tranzakció adatai: az American Express által kért minden olyan információ, amely egy vagy több Tranzakciót igazol, beleértve az eladási ponton kapott információkat, az Engedélyezés és benyújtás során kapott vagy generált információkat, valamint bármely Visszaterhelést.

9. rész Hasznos weboldalak

American Express Adatvédelem: www.americanexpress.com/datasecurity

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

EMVCo: www.emvco.com