

Pravilnik za upravljanje varnosti podatkov (DSOP)

Kot vodilno podjetje na področju varstva potrošnikov si družba American Express že dolgo prizadeva zaščititi podatke imetnika kartice in občutljive podatke za preverjanje pristnosti, s čimer zagotavlja njihovo varnost.

Ogroženi podatki negativno vplivajo na potrošnike, prodajalce, ponudnike storitev in izdajatelje kartic. Že en sam dogodek lahko resno škoduje ugledu družbe in s tem zmanjša zmožnost učinkovitega poslovanja. Tej nevarnosti se lahko izognemo z uvajanjem pravilnikov za upravljanje varnosti podatkov, kar prispeva k večjemu zaupanju strank, poveča dobičkonosnost in izboljša ugled podjetja.

Družba American Express se zaveda, da imate naši prodajalci in ponudniki storitev (skupaj, **vi**) enake pomisleke, zato zahtevamo, da kot del vaših odgovornosti zagotovite skladnost s predpisi o varstvu podatkov v vaši pogodbi za sprejemanje (za prodajalce) ali obdelavo (za ponudnike storitev) kartice American Express® (**pogodba** v obeh primerih) in s tem *pravilnikom za upravljanje varnosti podatkov*, ki se lahko občasno spremeni. Te zahteve veljajo za vso vašo opremo, sisteme in omrežja (in njihove komponente), v katerih se shranjujejo, obdelujejo ali prenašajo šifrirni ključi, podatki imetnika kartice ali občutljivi podatki za preverjanje pristnosti (ali kombinacija naštetih).

Pojmi, ki v tem besedilu niso opredeljeni, imajo pomene, kot so opredeljeni v slovarju na koncu pravilnika.

Poglavje 1 Standardi za zaščito šifrirnih ključev, podatkov imetnika kartice in občutljivih podatkov za preverjanje pristnosti

Vi in vaše pokrite stranke morate poskrbeti, da:

- podatke imetnika kartice shranjujete samo za izvajanje transakcij s kartico American Express skladno s pogodbo in kot zahteva pogodba;
- delujete skladno s trenutnim standardom PCI DSS in drugimi zahtevami PCI SSC, ki veljajo za vašo obdelavo, shranjevanje ali prenašanje podatkov imetnika kartice ali občutljivih podatkov za preverjanje pristnosti in niso starejše od dneva začetka veljavnosti za izvajanje te različice ustrezne zahteve;
- pri uvajanju novih ali nadomestnih naprav za vnos kode PIN ali zahtevkov za plačilo (ali obeh) na predvidenih mestih uporabljate samo tiste, ki jih je odobrila panoga PCI.

Zaščititi morate vse zapise o bremenitvah kartice American Express in kreditne zapise, pridobljene skladno s pogodbo in temi varnostnimi določili za podatke; te zapise smete uporabljati samo za namene pogodbe in jih skladno s tem varovati. Finančno in drugače ste družbi American Express odgovorni, da zagotovite skladnost delovanja vaših pokritih strank s temi določbami o varnosti podatkov (razen za izkazovanje skladnosti delovanja vaših pokritih strank s [Poglavje 4, »Pomembna redna validacija vaših sistemov«](#), razen če to poglavje določa drugače).

Poglavje 2 Obveznosti pri upravljanju incidentov, povezanih s podatki

Po odkritju incidenta, povezanega s podatki, morate o tem nemudoma oziroma najpozneje v štiriindvajsetih (24) urah obvestiti družbo American Express.

Za obveščanje družbe American Express se obrnite na Program družbe American Express za odziv na incidente (American Express Enterprise Incident Response Programme, *EIRP*) na telefonsko številko +1 (602) 537-3021 (+ pomeni mednarodno klicno številko »IDD«, velja mednarodna tarifa) ali pošljite elektronsko pošto na EIRP@aexp.com. Za posamezen incident, povezan s podatki, morate določiti posameznika za stike. Poleg tega morate storiti naslednje:

- Za vsak incident, povezan s podatki, morate izvesti temeljito forenzično preiskavo.
- Pri incidentih, povezanih s podatki, ki vključujejo 10.000 ali več enoličnih števil kartic, mora to preiskavo opraviti forenzični preiskovalec PCI (PFI) v petih (5) dneh po odkritju incidenta, povezanega s podatki.
- Neurejeno poročilo forenzične preiskave je treba družbi American Express predložiti v desetih (10) delovnih dneh po tem, ko se ga sestavi.
- Družbi American Express morate takoj sporočiti vse ogrožene številke kartic. Družba American Express si pridržuje pravico, da izvede svojo interno analizo za identifikacijo števil kartic, vključenih v incident, povezan s podatki.

Poročila forenzične preiskave morajo biti izpolnjena z uporabo trenutne predloge Forenzičnega končnega poročila o incidentu, ki je na voljo pri PCI. Ta poročila morajo vključevati forenzične preglede, poročila o skladnosti in vse druge informacije v zvezi z incidentom, povezanim s podatki; odkriti vzrok incidenta, povezanega s podatki; potrditi, ali ste v času incidenta, povezanega s podatki, delovali skladno s standardom PCI DSS ali ne; in preveriti vašo zmožnost preprečevanja nadaljnjih incidentov, povezanih s podatki, in to tako, da (i) vključujejo načrt za odpravljanje vseh pomanjkljivosti PCI DSS in (ii) sodelujejo v programu skladnosti družbe American Express (kot je opisano v nadaljevanju). Na zahtevo družbe American Express morate predložiti potrdilo pooblaščenega presojevalca varnosti (QSA) o tem, da so bile pomanjkljivosti odpravljene.

Ne glede na določila v zgoraj navedenih odstavkih [Poglavje 2, »Obveznosti pri upravljanju incidentov, povezanih s podatki«](#):

- lahko družba American Express po lastni presoji zahteva, da imenujete forenzičnega preiskovalca (PFI), da opravi preiskavo incidenta, povezanega s podatki, kadar gre za incidente, povezane s podatki, ki vključujejo manj kot 10.000 enoličnih števil kartic. Vse take preiskave morajo izpolnjevati zgornje zahteve, določene v [Poglavje 2, »Obveznosti pri upravljanju incidentov, povezanih s podatki«](#), in jih je treba dokončati v časovnem roku, ki ga določi družba American Express;
- lahko družba American Express po lastni presoji ločeno imenuje forenzičnega preiskovalca (PFI), da opravi preiskavo katerega koli incidenta, povezanega s podatki, ter vam zaračuna stroške take preiskave.

Strinjate se, da boste sodelovali z družbo American Express pri odpravljanju vseh težav, ki bodo izhajale iz incidenta, povezanega s podatki, med drugim se boste posvetovali z družbo American Express o komunikaciji z imetniki kartic, ki so bile zajete v incident, povezan s podatki, ter boste zagotavljali (in pridobili vse privolitve, potrebne za to, da boste zagotavljali) družbi American Express vse ustrezne informacije, s katerimi bo mogoče preveriti vašo zmožnost za preprečevanje nadaljnjih incidentov, povezanih s podatki, skladno s pogodbenimi določili.

Ne glede na kakršno koli nasprotno obveznost o zaupnosti v pogodbi ima družba American Express pravico, da informacije o katerem koli incidentu, povezanem s podatki, razkrije imetnikom kartic American Express, izdajateljem kartic, drugim udeležencem mreže družbe American Express in javnosti, kot to zahteva veljavna zakonodaja oziroma sodni, administrativni ali regulativni nalog, uredba, poziv, zahteva ali drug postopek, da se čim bolj zmanjša tveganje goljufije ali druge škode, oziroma je to treba storiti zaradi drugega razloga v obsegu, ustreznem za upravljanje mreže družbe American Express.

Poglavje 3 Odškodninske obveznosti za incident, povezan s podatki

[Poglavje 3, »Odškodninske obveznosti za incident, povezan s podatki«](#), določa vaše odškodninske obveznosti do družbe American Express skladno s pogodbo o incidentih, povezanih s podatki, ne da bi se družba American Express odpovedala katerim koli drugim svojim pravicam in pravnim sredstvom. Poleg vaših morebitnih odškodninskih obveznosti boste morda plačali nadomestilo za neskladnost ob incidentu, povezanem s podatki, kot je opisano v nadaljevanju v [Poglavje 3, »Odškodninske obveznosti za incident, povezan s podatki«](#).

Za incidente, povezane s podatki, ki vključujejo:

- 10.000 ali več števil kartic American Express z eno do teh dveh kategorij:
 - občutljivi podatki za preverjanje pristnosti ali
 - datum poteka veljavnosti,morate družbi American Express povrniti škodo v višini 5 USD na številko računa.

Toda družba American Express od vas ne bo zahtevala odškodnine zaradi incidenta, povezanega s podatki, ki vključuje:

- manj kot 10.000 števil kartic American Express ali
- več kot 10.000 števil kartic American Express, če ste izpolnili te pogoje:
 - družbo American Express ste obvestili o incidentu, povezanem s podatki, skladno s [Poglavje 3, »Odškodninske obveznosti za incident, povezan s podatki«](#),
 - v času incidenta, povezanega s podatki, ste delovali skladno s standardom PCI DSS (kot je forenzični preiskovalec PFI ugotovil s preiskavo incidenta, povezanega s podatki) in
 - incidenta, povezanega s podatki, ni povzročila vaša napaka ali napaka vaših pokritih strank.

Ne glede na določila v zgoraj navedenih odstavkih [Poglavje 3, »Odškodninske obveznosti za incident, povezan s podatki«](#), boste ne glede na število števil kartic American Express za vse incidente, povezane s podatki, plačali družbi American Express nadomestilo za neskladnost ob incidentu, povezanem s podatki, ki ne bo presegalo 100.000 USD na incident, povezan s podatki (kot bo po svoji presoji določila družba American Express), če ne boste izpolnili katere koli svoje obveznosti, določene v [Poglavje 2, »Obveznosti pri upravljanju incidentov, povezanih s podatki«](#). Da ne bo dvoma: skupno nadomestilo za neskladnost ob incidentu, povezanem s podatki, za kateri koli posamezni incident, povezan s podatki, ne sme presegati 100.000 USD.

Družba American Express bo iz svojih izračunov izključila vse številke računov kartic American Express, ki so bile vključene v odškodninski zahtevek, vložen za predhoden incident, povezan s podatki, v dvanajstih (12) mesecih pred prijavnim datumom. Vsi izračuni, ki jih družba American Express opravi skladno s to metodologijo, so končni.

Družba American Express vam lahko zaračuna celoten znesek vaših odškodninskih obveznosti za incidente, povezane s podatki, ali odšteje znesek od plačil, ki vam jih izplačuje družba American Express (ali ustrezno obremeni vaš bančni račun) skladno s pogodbo.

Odškodninske obveznosti prodajalca za incidente, povezane s podatki, opredeljene v tem poglavju, se ne bodo obravnavale kot naključna, posredna, spekulativna, posledična, posebna, kazenska ali eksemplarična odškodnina po pogodbi, če te obveznosti ne vključujejo škode, povezane z izgubljenim dobičkom ali prihodkom, izgubo dobrega imena ali izgubo poslovnih priložnosti.

Po svoji lastni presoji lahko družba American Express zmanjša odškodninske obveznosti za incidente, povezane s podatki, tistim prodajalcem, ki izpolnjujejo vsa naslednja merila:

- pred incidentom, povezanim s podatki, so bile uvedene ustrezne tehnologije za zmanjševanje tveganja in so se uporabljale med celotnim trajanjem incidenta, povezanega s podatki;
- izvedena je bila temeljita preiskava v skladu s programom PFI (razen če je bilo prej pisno dogovorjeno drugače);
- forenzično poročilo jasno navaja, da so se za obdelavo, shranjevanje in/ali prenos podatkov v času incidenta, povezanega s podatki, uporabljale tehnologije za zmanjševanje tveganja; in

- ne shranjujete (in niste shranjevali v času trajanja incidenta, povezanega s podatki) občutljivih podatkov za preverjanje pristnosti ali katerih koli podatkov imetnika kartice, ki niso bili pretvorjeni v neberljive.

Kadar je na voljo zmanjšanje odškodnine, se vaša odškodninska obveznost (brez vseh zneskov nadomestil za neskladnost) zmanjša na naslednji način:

Zmanjšanje odškodninske obveznosti	Zahtevana merila
Standardno zmanjšanje: 50 %	> 75 % od celotnih transakcij, obdelanih na napravah z omogočeno uporabo čipa ¹ ALI uporabljena tehnologija za zmanjševanje tveganja na > 75 % lokacij prodajalca ²
Povečano zmanjšanje: 75 % do 100 %	> 75 % vseh transakcij obdelanih na napravah z omogočeno uporabo čipa ¹ IN uporabljena dodatna tehnologija za zmanjševanje tveganja na > 75 % lokacij prodajalca ²

¹ Kot je ugotovljeno z notranjo analizo družbe American Express.

² Kot je ugotovljeno s preiskavo PFI.

- Povečano zmanjšanje (75 % do 100 %) se bo določilo na podlagi manjšega odstotka transakcij z uporabo naprav z omogočeno uporabo čipa IN lokacij prodajalca z uporabo tehnologije za zmanjševanje tveganja. Spodnji primeri prikazujejo izračun zmanjšanja odškodnine.
- Če želite uveljaviti uporabo tehnologije za zmanjševanje tveganja, morate dokazati učinkovito uporabo tehnologije skladno z njeno zasnovo in predvideno uporabo. Na primer, uporaba naprav z omogočeno uporabo čipa in obdelava kartic s čipom kot transakcij z magnetnim trakom ali transakcij z vnosom ključa NI učinkovita uporaba te tehnologije.
- Odstotek lokacij, ki uporabljajo tehnologijo za zmanjševanje tveganja, se ugotovi s preiskavo PFI.
- Zmanjšanje odškodninske obveznosti ne velja za nadomestila za neskladnost, ki jih je treba plačati v zvezi z incidentom, povezanim s podatki.

Primer	Uporabljene tehnologije za zmanjšanje tveganj	Upravičenost do povečanega zmanjšanja odškodninske obveznosti?	Zmanjšanje
1	80 % transakcij na napravah z omogočeno uporabo čipa	Ne	50 %: standardno zmanjšanje (manj kot 75-odstotna uporaba tehnologije za zmanjšanje tveganja ne upraviči povečanega zmanjšanja) ¹
	0 % lokacij uporablja drugo tehnologijo za zmanjšanje tveganja		
2	80 % transakcij na napravah z omogočeno uporabo čipa	Da	77 %: povečano zmanjšanje (na podlagi 77-odstotne uporabe tehnologije za zmanjšanje tveganja)
	77 % lokacij uporablja drugo tehnologijo za zmanjšanje tveganja		

Primer	Uporabljene tehnologije za zmanjšanje tveganj	Upravičenost do povečanega zmanjšanja odškodninske obveznosti?	Zmanjšanje
3	93 % transakcij na napravah z omogočeno uporabo čipa	Da	93 %: povečano zmanjšanje (na podlagi 93 % transakcij na napravah z omogočeno uporabo čipa)
	100 % lokacij uporablja drugo tehnologijo za zmanjšanje tveganja		
4	40 % transakcij na napravah z omogočeno uporabo čipa	Ne	50 %: standardno zmanjšanje (manj kot 75 % transakcij na napravah z omogočeno uporabo čipa ne upraviči povečanega zmanjšanja)
	90 % lokacij uporablja drugo tehnologijo za zmanjšanje tveganja		

¹ Incident, povezan s podatki, ki vključuje 10.000 računov kartic American Express, v višini 5 USD na številko računa (10.000 x 5 USD = 50.000 USD), je lahko upravičen do 50-odstotnega zmanjšanja, kar pomeni, da se odškodninska obveznost zmanjša s 50.000 USD na 25.000 USD, pri čemer pa so izključena nadomestila za neskladnost.

Poglavje 4 Pomembna redna validacija vaših sistemov

Kot je opisano spodaj, morate za letno in četrtletno validacijo stanja opreme, sistema in/ali mrež (in njihovih komponent), na katerih se shranjujejo, obdelujejo ali prenašajo podatki imetnikov kartic ali občutljivi podatki za preverjanje pristnosti pri vas in vaših franšizah skladno s standardom PCI DSS izvajati naslednje korake.

Za izvedbo validacije so potrebni štirje koraki:

Korak 1: sodelujte v programu skladnosti družbe American Express po tem pravilniku.

Korak 2: zavedajte se svoje stopnje in zahtev za validacijo.

Korak 3: izpolnite validacijsko dokumentacijo, ki jo je treba poslati družbi American Express.

Korak 4: pošljite validacijsko dokumentacijo družbi American Express v predpisanih časovnih okvirjih.

Korak 1: sodelujte v programu skladnosti družbe American Express po tem pravilniku

Prodajalci stopnje 1, prodajalci stopnje 2 in vsi ponudniki storitev, kot je opisano spodaj, morajo sodelovati v programu skladnosti PCI družbe American Express po tem pravilniku, v katerem navedejo polno ime, elektronski naslov, telefonsko številko in poštni naslov posameznika, ki bo njihov stik za varnost podatkov. Te informacije morate poslati družbi SecureTrust, podružnici družbe Trustwave (<https://portal.securetrust.com>), ki upravlja program v imenu družbe American Express, na enega od načinov, navedenih spodaj v **Korak 4: »pošljite validacijsko dokumentacijo družbi American Express«**. Družbo SecureTrust morate obvestiti, če se te informacije spremenijo, in ji predložiti posodobljene informacije, če je primerno. Če ne boste sporočili teh kontaktnih informacij, to ne bo vplivalo na naše pravice do določitve plačil zaradi odsotnosti validacije, kot je opisano v **Preglednica plačil zaradi odsotnosti validacije**.

Družba American Express lahko po lastni presoji s pošiljanjem pisnega obvestila določi, da se v program skladnosti družbe American Express po tem pravilniku vključijo nekateri prodajalci stopnje 3 in stopnje 4. Prodajalec se mora vključiti najpozneje v 90 dneh po prejemu obvestila.

Korak 2: zavedajte se svoje stopnje in zahtev za validacijo

Obstajajo štiri stopnje, ki se nanašajo na prodajalce, in dve stopnji, ki se nanašata na ponudnike storitev, glede na obseg transakcij s kartico American Express. Pri prodajalcih ta obseg predložijo njihove poslovalnice, ki poročajo do najvišje stopnje računov prodajalca American Express.* Vključeni boste v eno od stopenj, opredeljenih v spodnjih preglednicah za prodajalce in ponudnike storitev. Transakcije plačil, ki jih izvedejo kupci (BIP), niso vključene v obseg transakcij s karticami American Express za določanje stopnje prodajalca in zahtev validacije.

* Pri franšizorjih to vključuje obseg njihovih franšiznih poslovalnic. Franšizorji, ki zahtevajo, da njihove franšize uporabljajo specifičen sistem prodajnega mesta (POS) ali ponudnika storitev, morajo predložiti tudi validacijsko dokumentacijo za zadevne franšize.

Zahteve za prodajalce

Za prodajalce (ne ponudnike storitev) so na voljo štiri možne razvrstitve glede na stopnjo in validacijske zahteve. Po določitvi stopnje prodajalca skladno s spodnjim seznamom si oglejte preglednico za prodajalce, s katero določite zahteve za validacijsko dokumentacijo.

- **Prodajalec stopnje 1** – 2,5 milijona transakcij s kartico American Express ali več na leto ali kateri koli prodajalec, ki ga družba American Express po lastni presoji šteje kot prodajalca stopnje 1.
- **Prodajalec stopnje 2** – 50.000 do 2,5 milijona transakcij s kartico American Express na leto.
- **Prodajalec stopnje 3** – 10.000 do 50.000 transakcij s kartico American Express na leto.
- **Prodajalec stopnje 4** – manj kot 10.000 transakcij s kartico American Express na leto.

Preglednica za prodajalce

Stopnja prodajalca/Letne transakcije s kartico American Express	Validacijska dokumentacija		
	Interno poročilo o oceni skladnosti (ROC)	Samoocenjevalni vprašalnik (SAQ) IN četrtletno preverjanje mreže	Potrdilo STEP za prodajalce, ki izpolnjujejo pogoje
Stopnja 1/ 2,5 milijona ali več	Obvezno	Ni veljavno	Neobvezno (nadomesti ROC)
Stopnja 2/ od 50.000 do 2,5 milijona	Neobvezno	Obvezni SAQ (razen v primeru predložitve interne ocene); obvezno preverjanje pri nekaterih tipih SAQ	Neobvezno (nadomesti SAQ in preverjanje mreže ali ROC)
Stopnja 3/ 10.000 do 50.000	Neobvezno	Neobvezen SAQ (obvezen, če tako zahteva družba American Express); obvezno preverjanje pri nekaterih tipih SAQ	Neobvezno (nadomesti SAQ in preverjanje mreže ali ROC)
Stopnja 4/ 10.000 ali manj	Neobvezno	Neobvezen SAQ (obvezen, če tako zahteva družba American Express); obvezno preverjanje pri nekaterih tipih SAQ	Neobvezno (nadomesti SAQ in preverjanje mreže ali ROC)

* Da ne bo dvoma: prodajalcem stopnje 3 in stopnje 4 ni treba predložiti validacijske dokumentacije, razen če to po svoji presoji zahteva družba American Express, vendar morajo kljub temu delovati skladno z vsemi drugimi določili tega pravilnika za upravljanje varnosti podatkov.

Družba American Express si pridržuje pravico, da po potrebi preveri natančnost in ustreznost validacijske dokumentacije PCI, med drugim lahko to na svoje stroške stori s pooblaščenim presojevalcem varnosti (QSA) ali forenzičnim preiskovalcem (PFI), ki ga izbere družba American Express.

Program izboljšave varnostne tehnologije (STEP)

Prodajalci, skladni s standardom PCI DSS, so lahko po presoji družbe American Express upravičeni tudi do programa izboljšave varnostne tehnologije (STEP) družbe American Express, če v svojem okolju za obdelavo kartic uporabljajo nekatere dodatne varnostne tehnologije. Program STEP se uvede, samo če prodajalec ni imel incidenta, povezanega s podatki, v zadnjih 12 mesecih in če se 75 % vseh kartičnih transakcij prodajalca izvede z:

- **EMV** – na aktivni napravi z omogočeno uporabo čipa, ki ima veljavno in posodobljeno odobritev/potrdilo EMVCo (www.emvco.com) ter je sposobna obdelave transakcij s karticami s čipom, združitljivih z AEIPS (prodajalci iz ZDA morajo vključiti brezstične transakcije);
- **šifriranjem od točke do točke (P2PE)** – procesorju prodajalca se pošlje s sistemom za šifriranje od točke do točke, odobrenim s standardom PCI-SSC ali presojevalcem QSA.

Prodajalci, primerni za program STEP, imajo zmanjšane zahteve za validacijsko dokumentacijo PCI, kot je podrobneje opisano v nadaljevanju v [Korak 3: »izpolnite validacijsko dokumentacijo, ki jo je treba poslati družbi American Express«](#).

Zahteve za ponudnike storitev

Ponudniki storitev (ne prodajalci) imajo dve možni razvrstitvi glede na stopnjo in validacijske zahteve. Po določitvi stopnje ponudnika storitev skladno s spodnjim seznamom si oglejte preglednico za ponudnike storitev, s katero določite zahteve za validacijsko dokumentacijo.

Ponudnik storitev stopnje 1 – 2,5 milijona transakcij s kartico American Express ali več na leto ali kateri koli ponudnik storitev, ki ga družba American Express šteje kot ponudnika storitev stopnje 1.

Ponudnik storitev stopnje 2 – manj kot 2,5 milijona transakcij s kartico American Express na leto ali kateri koli ponudnik storitev, ki ga družba American Express ne šteje za ponudnika storitev stopnje 1.

Ponudnikom storitev ni na voljo program STEP.

Preglednica za ponudnike storitev

Stopnja	Validacijska dokumentacija	Zahteva
1	Letno interno poročilo o oceni varnosti glede skladnosti	Obvezno
2	Letni vprašalnik SAQ D (ponudnik storitev) in četrtletno preverjanje mreže ali letno interno poročilo o oceni varnosti glede skladnosti, poljubno.	Obvezno

Priporočeno je, da tudi ponudniki storitev upoštevajo dodatno validacijo za določena podjetja PCI.

Korak 3: izpolnite validacijsko dokumentacijo, ki jo je treba poslati družbi American Express

Za različne stopnje prodajalcev in ponudnikov storitev, kot je navedeno v zgornjih preglednicah za prodajalce in ponudnike storitev, so potrebni naslednji dokumenti.

Letna interna ocena varnosti – letna interna ocena varnosti je podrobna interna preiskava vaše opreme, sistemov in mrež (ter njihovih komponent), v katerih se shranjujejo, obdelujejo in prenašajo podatki imetnikov kartic ali občutljivi podatki za preverjanje pristnosti (ali oboji). Opraviti jo mora:

- QSA ali
- vi, kar mora potrditi vaš izvršni direktor, finančni direktor, direktor za varnost informacijskih sistemov ali upravnik in vsako leto predložiti družbi American Express na veljavnem potrdilu o skladnosti (AOC).

Potrdilo AOC mora izkazovati skladnost z vsemi zahtevami standarda PCI DSS in na zahtevo vključevati kopije celotnega poročila o skladnosti (prodajalci stopnje 1 in ponudniki storitev stopnje 1).

Letni samoocenjevalni vprašalnik – letna samoocena je proces, pri katerem se uporabi samoocenjevalni vprašalnik (SAQ) PCI DSS, ki omogoča samopregledovanje vaše opreme, sistemov in mrež (ter njihovih komponent) v katerih se shranjujejo, obdelujejo ali prenašajo podatki imetnikov kartic ali občutljivi podatki za preverjanje pristnosti (ali oboji). Izpolniti ga morate vi, potrditi pa ga mora vaš izvršni direktor, finančni direktor, direktor za varnost informacijskih sistemov ali upravnik. Potrdilo AOC, ki je del vprašalnika SAQ, je treba družbi American Express predložiti vsako leto. Potrdilo AOC, ki je del vprašalnika SAQ, mora potrjevati vašo skladnost z vsemi zahtevami standarda PCI DSS in na zahtevo vključevati popolne kopije vprašalnika SAQ (prodajalci stopnje 2, stopnje 3 in stopnje 4, ponudniki storitev stopnje 2).

Četrtno preverjanje mreže – četrtno preverjanje mreže je proces za oddaljeno testiranje vaših računalniških mrež, priključenih na internet, in spletnih strežnikov za morebitno šibkost in ranljivost. Opraviti ga mora odobreni ponudnik preverjanja (**ASV**). Potrdilo o skladnosti preverjanja (**AOSC**) s poročilom o preverjanju ASV morate pripraviti vsako četrtno in to potrdilo ali povzetek rezultatov preverjanja (in na zahtevo kopije celotnega preverjanja) poslati družbi American Express. Potrdilo AOSC ali povzetek mora potrditi, da rezultati izpolnjujejo zahteve za postopke preverjanja standarda PCI DSS, da niso bile ugotovljene nobene težave z velikim tveganjem in da je preverjanje uspešno ali skladno (vsi prodajalci, razen tistih, ki oddajo tudi interno poročilo o oceni varnosti, prodajalci, ki izpolnjujejo pogoje programa STEP, in vsi ponudniki storitev). Da ne bo dvoma, četrtno preverjanje mreže je obvezno, če tako zahteva ustrezeni vprašalnik SAQ.

Letna validacijska dokumentacija s potrdilom STEP – letno potrdilo za usposabljanje STEP družbe American Express (»potrdilo STEP«) je na voljo samo prodajalcem, ki izpolnjujejo merila, navedena pri zgornjem [Korak 2: »Zavedajte se svoje stopnje in zahtev za validacijo«](#). Potrdilo STEP vključuje proces z zahtevami standarda PCI DSS, ki omogoča samopregledovanje vaše opreme, sistemov in mrež (ter njihovih komponent) v katerih se shranjujejo, obdelujejo ali prenašajo podatki imetnikov kartic ali občutljivi podatki za preverjanje pristnosti (ali oboji). Izpolniti ga morate vi, potrditi pa ga mora vaš izvršni direktor, finančni direktor, direktor za varnost informacijskih sistemov ali upravnik. Postopek zaključite tako, da družbi American Express vsako leto predložite obrazec s potrdilom STEP. (Samo za prodajalce, ki izpolnjujejo pogoje programa STEP.) Letni obrazec s potrdilom STEP lahko prenesete z varnega portala družbe SecureTrust.

Povzetek skladnosti (SOC) – SOC je dokument, s katerim lahko franšizor ali ponudnik storitev poroča o stanju skladnosti PCI v svojih franšizah. Predlogo SOC lahko prenesete z varnega portala družbe SecureTrust.

Neskladnost s standardom PCI DSS – če ugotovite neskladnost s standardom PCI DSS, morate poslati enega izmed naslednjih dokumentov:

- potrdilo o skladnosti (AOC), vključno s »4. delom. Akcijski načrt za neskladno stanje«
- povzetek orodja s prednostnim pristopom PCI in potrdilo o skladnosti (PASAOC)
- predloga projektnega načrta (na voljo za prenos z varnega portala družbe SecureTrust)

Vsak od zgornjih dokumentov mora imeti določen datum odpravljanja neskladnosti, ki ne sme presegati 12 mesecev od datuma izpolnitve dokumenta. Ustrezni dokument morate predložiti družbi American Express na enega od načinov, navedenih v spodnjem [Korak 4: »Pošljite validacijsko dokumentacijo družbi American Express«](#). Za neskladno stanje boste družbi American Express pošiljali redne posodobitve napredka pri odpravljanju neskladnosti (prodajalci stopnje 1, stopnje 2, stopnje 3 in stopnje 4; vsi ponudniki storitev). Da ne bo dvoma: prodajalci, ki ne delujejo skladno s standardom PCI DSS, niso upravičeni do programa STEP. Družba American Express vam pred datumom odpravljanja neskladnosti ne bo zaračunala zneska zaradi odsotnosti validacije (opisanega spodaj) zaradi neskladnosti, vendar ste družbi American Express zavezani glede vseh odškodninskih obveznosti za incident, povezan s podatki, in dolžni izpolnjevati vsa druga določila tega pravilnika.

Korak 4: pošljite validacijsko dokumentacijo družbi American Express

Vsi prodajalci in ponudniki storitev, ki morajo sodelovati v programu skladnosti PCI družbe American Express, morajo predložiti validacijsko dokumentacijo, označeno »obvezno« v preglednicah v [Korak 2: »zavedajte se svoje stopnje in zahtev za validacijo«](#). Validacijsko dokumentacijo morate družbi SecureTrust poslati na enega od teh načinov:

- **Varen portal:** Validacijsko dokumentacijo lahko naložite na varen portal družbe SecureTrust na spletnem mestu <https://portal.securetrust.com>.

Obrnite se na družbo SecureTrust po telefonski številki za svojo državo ali pošljite elektronsko pošto na americanexpresscompliance@securetrust.com, če želite informacije o uporabi tega portala.

- **Varen faks:** Validacijsko dokumentacijo lahko po faksu pošljete na: +1 (312) 276-4019. (+ pomeni mednarodno klicno številko »IDD«, velja mednarodna tarifa).

Vključite svoje ime, ime DBA (Doing Business As – »poslovanje pod registriranim imenom«), ime svojega stika za varnost podatkov, svoj naslov in telefonsko številko ter 10-mestno številko prodajalca American Express, kar velja samo za prodajalce.

Če imate splošna vprašanja o programu ali zgornjem postopku, se obrnite na družbo SecureTrust na telefonsko številko + 800 9000 1140 ali +1 (312) 267-3208 ali pošljite elektronsko pošto na americanexpresscompliance@securetrust.com.

Skladnost in validacija se opravi na vaše stroške. S predložitvijo validacijske dokumentacije družbi American Express potrjujete in jamčite, da ste pooblaščen za razkrivanje informacij v njej in da validacijsko dokumentacijo družbi American Express pošiljate brez kršenja katerih koli pravic drugih strank.

Trgi	Telefonska številka SecureTrust	Trgi	Telefonska številka SecureTrust
Argentina	+ 800 9000 1140	Madžarska	+ 800 9000 1140
Avstralija	+ 800 9000 1140	Malta	+ 312 267 3208
Avstrija	+ 800 9000 1140	Mehika	+ 888 900 0114
Bolgarija	+ 312 267 3208	Nemčija	+ 800 9000 1140
Ciper	+ 800 9000 1140	Nizozemska	+ 312 267 3208
Češka republika	+ 800 144 316	Nova Zelandija	+ 800 9000 1140
Danska	+ 800 9000 1140	Norveška	+ 800 9000 1140
Estonija	+ 312 267 3208	Poljska	+ 800 9000 1140
Francija	+ 800 9000 1140	Portugalska	+ 312 267 3208
Grčija	+ 312 267 3208	Romunija	+ 312 267 3208
Hongkong	+ 800 9000 1140	Rusija	+ 312 267 3208
Hrvaška	+ 312 267 3208	Singapur	+ 800 9000 1140
IDC	+ 888 900 0114	Slovaška	+ 312 267 3208
Indija	+ 800 9000 1140	Slovenija	+ 312 267 3208
Irska	+ 800 9000 1140	Španija	+ 800 9000 1140
Islandija	+ 800 9000 1140	Švedska	+ 800 9000 1140
Italija	+ 800 9000 1140	Tajvan	+ 312 267 3208
Japonska	+ 312 267 3208	Tajska	+ 800 9000 1140
Kanada	1 866 659 9016	Združeno kraljestvo	+ 800 9000 1140
Latvija	+ 312 267 3208	Združene države Amerike	1 866 659 9016
Litva	+ 312 267 3208		

+ pomeni mednarodno klicno številko »IDD«, velja mednarodna tarifa

Plačila zaradi odsotnosti validacije in prenehanje pogodbe

Družba American Express ima pravico, da vam zaračuna zneske zaradi odsotnosti validacije in prekine pogodbo, če ne izpolnujete teh zahtev ali ne predložite obvezne validacijske dokumentacije družbi American Express do veljavnega roka. Družba American Express vas bo ločeno obveščala o veljavnih rokih za posamezna letna in četrletna poročila.

Družbi American Express pošljite dokumentacijo do veljavnega roka. Družba American Express vas bo ločeno obveščala o veljavnih rokih za posamezna letna in četrletna poročila. Glejte spodnjo preglednico plačil zaradi odsotnosti validacije za zneske, ki veljajo za vašo državo.

Opis	Prodajalec ali ponudnik storitev stopnje 1	Prodajalec ali ponudnik storitev stopnje 2 ali prodajalec STEP	Prodajalec stopnje 3 ali stopnje 4
Opravila se bo ocena za plačilo zaradi odsotnosti validacije, če se validacijska dokumentacija ne predloži do prvega roka.	Plačilo prvega meseca za stopnjo 1	Plačilo prvega meseca za stopnjo 2	Mesečno plačilo
Opravila se bo ocena za dodatno plačilo zaradi odsotnosti validacije, če se validacijska dokumentacija ne predloži v 30 dneh od prvega roka.	Plačilo drugega meseca za stopnjo 1	Plačilo drugega meseca za stopnjo 2	
Opravila se bo ocena za dodatno plačilo zaradi odsotnosti validacije, če se validacijska dokumentacija ne predloži v 60 dneh od prvega roka.	Plačilo tretjega meseca za stopnjo 1	Plačilo tretjega meseca za stopnjo 3	

Če družba American Express ne prejme obvezne validacijske dokumentacije v 60 dneh po prvem roku, ima pravico, da prekine pogodbo skladno z njenimi pogoji in vam kumulativno zaračuna zgoraj omenjene zneske zaradi odsotnosti validacije.

Preglednica plačil zaradi odsotnosti validacije

Trg	Stopnja	Vrsta	Valuta	Plačilo prvega meseca	Plačilo drugega meseca	Plačilo tretjega meseca
Avstralija	Stopnja 1	Prodajalec ali ponudnik storitev	AUD	35.000	49.000	63.000
	Stopnja 2	Prodajalec ali ponudnik storitev	AUD	7000	14.000	21.000
	Stopnja 3 in stopnja 4	Prodajalec	AUD	Mesečno plačilo: 20		
Bolgarija	Stopnja 1	Prodajalec ali ponudnik storitev	BGN	28.000	40.000	51.000
	Stopnja 2	Prodajalec ali ponudnik storitev	BGN	5500	11.000	16.500
	Stopnja 3 in stopnja 4	Prodajalec	BGN	Mesečno plačilo: 33		

Trg	Stopnja	Vrsta	Valuta	Plačilo prvega meseca	Plačilo drugega meseca	Plačilo tretjega meseca
Ciper, Estonija, Francija, Nemčija, Irska, Španija, Latvija, Litva, Portugalska, Slovaška, Slovenija	Stopnja 1	Prodajalec ali ponudnik storitev	EUR	19.000	26.000	34.000
	Stopnja 2	Prodajalec ali ponudnik storitev	EUR	4000	7500	11.000
	Stopnja 3 in stopnja 4	Prodajalec	EUR	Mesečno plačilo: 15		
Češka republika	Stopnja 1	Prodajalec ali ponudnik storitev	CZK	392.000	564.000	721.000
	Stopnja 2	Prodajalec ali ponudnik storitev	CZK	78.300	157.000	235.000
	Stopnja 3 in stopnja 4	Prodajalec	CZK	Mesečno plačilo: 440		
Danska	Stopnja 1	Prodajalec ali ponudnik storitev	DKK	110.000	156.000	200.000
	Stopnja 2	Prodajalec ali ponudnik storitev	DKK	22.000	42.000	65.000
	Stopnja 3 in stopnja 4	Prodajalec	DKK	Mesečno plačilo: 130		
Hongkong	Stopnja 1	Prodajalec ali ponudnik storitev	HKD	25.000	35.000	45.000
	Stopnja 2	Prodajalec ali ponudnik storitev	HKD	5000	10.000	15.000
	Stopnja 3 in stopnja 4	Prodajalec	HKD	Mesečno plačilo: 150		
Hrvaška	Stopnja 1	Prodajalec ali ponudnik storitev	HRK	105.000	152.000	195.000
	Stopnja 2	Prodajalec ali ponudnik storitev	HRK	21.000	42.000	63.000
	Stopnja 3 in stopnja 4	Prodajalec	HRK	Mesečno plačilo: 130		

Trg	Stopnja	Vrsta	Valuta	Plačilo prvega meseca	Plačilo drugega meseca	Plačilo tretjega meseca
Islandija	Stopnja 1	Prodajalec ali ponudnik storitev	ISK	3.070.000	4.300.000	5.500.000
	Stopnja 2	Prodajalec ali ponudnik storitev	ISK	615.000	920.000	1.227.200
	Stopnja 3 in stopnja 4	Prodajalec	ISK	Mesečno plačilo: 2400		
Madžarska	Stopnja 1	Prodajalec ali ponudnik storitev	HUF	4.650.000	6.700.000	8.600.000
	Stopnja 2	Prodajalec ali ponudnik storitev	HUF	930.000	1.860.000	2.800.000
	Stopnja 3 in stopnja 4	Prodajalec	HUF	Mesečno plačilo: 5500		
Nova Zelandija	Stopnja 1	Prodajalec ali ponudnik storitev	NZD	35.000	49.000	63.000
	Stopnja 2	Prodajalec ali ponudnik storitev	NZD	7000	14.000	21.000
	Stopnja 3 in stopnja 4	Prodajalec	NZD	Mesečno plačilo: 20		
Norveška	Stopnja 1	Prodajalec ali ponudnik storitev	NOK	135.000	195.000	249.000
	Stopnja 2	Prodajalec ali ponudnik storitev	NOK	27.000	54.000	81.000
	Stopnja 3 in stopnja 4	Prodajalec	NOK	Mesečno plačilo: 170		
Singapur	Stopnja 1	Prodajalec ali ponudnik storitev	SGD	38.000	53.000	68.000
	Stopnja 2	Prodajalec ali ponudnik storitev	SGD	7500	15.000	22.500
	Stopnja 3 in stopnja 4	Prodajalec	SGD	Mesečno plačilo: 25		

Trg	Stopnja	Vrsta	Valuta	Plačilo prvega meseca	Plačilo drugega meseca	Plačilo tretjega meseca
Švedska	Stopnja 1	Prodajalec ali ponudnik storitev	SEK	175.000	245.000	315.000
	Stopnja 2	Prodajalec ali ponudnik storitev	SEK	35.000	70.000	105.000
	Stopnja 3 in stopnja 4	Prodajalec	SEK	Mesečno plačilo: 135		
Združeno kraljestvo	Stopnja 1	Prodajalec ali ponudnik storitev	GBP	12.500	18.000	23.000
	Stopnja 2	Prodajalec ali ponudnik storitev	GBP	2500	5000	7500
	Stopnja 3 in stopnja 4	Prodajalec	GBP	Mesečno plačilo: 15		

Poglavje 5 Zaupnost

Družba American Express bo uvedla smiselne ukrepe za zaupno shranjevanje vaših poročil o skladnosti, vključno z validacijsko dokumentacijo (in bo poskrbela, da jih bodo njeni zastopniki in podizvajalci, vključno z družbo SecureTrust, tako shranjevali) in ne bo razkrila validacijske dokumentacije nobeni tretji osebi (ki ni pridružena družba, zastopnik, predstavnik, ponudnik storitev in podizvajalec družbe American Express) v obdobju treh let od prejema, razen kadar ta obveznost zaupnosti ne velja za validacijsko dokumentacijo, ki:

- je že znana družbi American Express pred razkritjem;
- je na voljo ali postane na voljo javnosti, ne da bi ob tem družba American Express kršila določila tega odstavka;
- jo je družba American Express zakonito prejela od tretje osebe, ki ni zavezana dolžnosti zaupnosti;
- jo samostojno razvije družba American Express; ali
- jo je treba razkriti po nalogu sodišča, upravne agencije ali vladnega organa ali skladno s katero koli zakonodajo, pravilom ali predpisom ali sodnim pozivom, zahtevo po razkritju, sodnim pozivom ali drugim administrativnim ali pravnim postopkom ali na podlagi kakršne koli uradne ali neuradne poizvedbe ali preiskave s strani vladne agencije ali organa (vključno s katerim koli upravnim organom, inšpektorjem, preiskovalcem ali organom kazenskega pregona).

Poglavje 6 Zavrnitev odgovornosti

DRUŽBA AMERICAN EXPRESS ZAVRAČA KAKRŠNA KOLI EKSPPLICITNA, IMPLICITNA, ZAKONSKO PREDPISANA ALI DRUGA ZASTOPANJA, JAMSTVA IN ODGOVORNOSTI, POVEZANE S TEM PRAVILNIKOM ZA UPRAVLJANJE VARNOSTI PODATKOV, STANDARDOM PCI DSS, SPECIFIKACIJAMI EMV IN IMENOVANJEM TER UČINKOVITOSTJO PREISKOVALCEV QSA, PONUDNIKOV ASV ALI PREISKOVALCEV PFI (ALI KATEREGA KOLI OD NJIH), VKLJUČNO S KAKRŠNIM KOLI JAMSTVOM ZA PRIMERNOST ZA PRODAJO ALI USTREZNOST ZA POSAMEZEN NAMEN. IZDAJATELJI KARTIC AMERICAN EXPRESS PO TEM PRAVILNIKU NISO UPRAVIČENI KOT TRETJE OSEBE.

Koristna spletna mesta

Varnost podatkov v družbi American Express: www.americanexpress.com/datasecurity

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

Slovar

Naslednje opredelitve veljajo samo za namene tega [Pravilnik za upravljanje varnosti podatkov \(DSOP\)](#) in imajo prednost, če niso usklajene z izrazi, navedenimi v *Pravila za prodajalce*.

Bremenitev pomeni plačilo ali nakup s kartico.

Čip pomeni integriran mikročip, vdelan v kartico, ki vsebuje informacije o imetniku kartice in računu.

Forenzični preiskovalec PCI (PFI) pomeni organ, ki ga je svet Payment Card Industry Security Standards Council, LLC odobril za opravljanje forenzičnih preiskav kršitev ali ogroženosti podatkov plačilne kartice.

Franšizor pomeni upravljavca podjetja, ki pooblasti osebe ali organe (franšize) za distribucijo blaga in/ali storitev pod znamko upravljavca ali z uporabo znamke upravljavca, nudi pomoč franšizam pri opravljanju posla ali vpliva na metodo delovanja franšize in za svoje storitve zahteva plačilo franšize.

Imetnik kartice pomeni posameznika ali organ, i) ki je sklenil pogodbo z izdajateljem, s katero je ustvaril kartični račun, ali ii) katerega ime je na kartici.

Incident, povezan s podatki, pomeni dogodek, ki vključuje ogroženost ali sum na ogroženost šifrirnih ključev American Express ali vsaj ene številke računa kartice American Express in pri katerem gre za:

- neodobren dostop ali uporabo šifrirnih ključev, podatkov imetnikov kartic ali občutljivih podatkov za preverjanje pristnosti (ali njihova kombinacija), ki se shranjujejo, obdelujejo ali prenašajo v vaši opremi, sistemih in/ali mrežah (ali njihovih komponentah) ali za katerih uporabo ste pooblaščen;
- uporabo takih šifrirnih ključev, podatkov imetnikov kartic ali občutljivih podatkov za preverjanje pristnosti (ali njihove kombinacije), ki ni skladna s pogodbo; in/ali
- domnevno ali potrjeno izgubo, krajo ali poneverbo s kakršnimi koli mediji, materiali, evidencami ali informacijami, ki vsebujejo take šifrirne ključe, podatke imetnikov kartic ali občutljive podatke za preverjanje pristnosti (ali njihovo kombinacijo).

Informacije o imetniku kartice pomenijo informacije o imetnikih kartice American Express in kartičnih transakcijah, vključno z imeni, naslovi, števkami kartičnih računov in kartičnimi identifikacijskimi števkami (CID).

Kartica družbe American Express ali kartica pomeni katero koli kartico, napravo za dostop do računa ali plačilno napravo ali storitev z imenom, logotipom, blagovno znamko, storitveno znamko, tržnim imenom ali drugim lastniškim znakom ali oznako družbe American Express ali pridružene družbe, ki jo izda izdajatelj ali številka računa kartice.

Kartica s čipom pomeni kartico, ki vsebuje čip in lahko zahteva PIN za potrjevanje identitete imetnika kartice ali informacij o računu, ki jih vsebuje čip, ali obojega (včasih se v našem gradivu imenuje »pametna kartica«, »kartica EMV« ali »ICC« ali »kartica z integriranim vezjem«).

Kredit pomeni vsoto bremenitve, ki jo povrnete imetnikom kartic za nakupe ali plačila s kartico.

Naprava za vnos kode PIN ima pomen, ki ji je dodeljen v takrat veljavnem slovarju izrazov za modularne varnostne zahteve za varnost transakcije PIN (PTS) na točki interakcije (POI) pri kartičnem poslovanju, ki so na voljo na spletnem mestu www.pcisecuritystandards.org.

Naprava z omogočeno uporabo čipa pomeni napravo poslovne enote, ki ima veljavno in posodobljeno odobritev/potrjeno EMVCo (www.emvco.com) ter je sposobna obdelave transakcij s karticami s čipom, združitljivih z AEIPS.

Občutljivi podatki za preverjanje pristnosti pomenijo, kot je opredeljeno v takrat veljavnem slovarju izrazov standarda PCI DSS.

Odobrena rešitev šifriranja od točke do točke (P2PE), ki je vključena na seznam PCI SSC za validirane rešitve ali jo je validirala družba P2PE s pooblaščenim presojevalcem varnosti PCI SSC.

Odobreni ponudnik preverjanja (ASV) pomeni organ, ki ga je pooblastil svet Payment Card Industry Security Standards Council, LLC za to, da validira skladnost z nekaterimi zahtevami standarda PCI DSS, in to tako, da izvaja preverjanje za odkrivanje ranljivosti v okoljih, povezanih z internetom.

Odobreno s PCI pomeni, da je naprava za vnos kode PIN ali zahtevke za plačilo (ali oba) v času uporabe na seznamu odobrenih podjetij in ponudnikov, ki ga vzdržuje PCI Security Standards Council, LLC, in je na voljo na spletnem mestu www.pcisecuritystandards.org.

Ogrožena številka kartice pomeni številko računa kartice American Express v zvezi z incidentom, povezanim s podatki.

PCI DSS pomeni Standard varnosti podatkov kartičnega poslovanja, ki je na voljo na spletnem mestu www.pcisecuritystandards.org.

Podatki imetnika kartice imajo pomen, ki jim je dodeljen v takrat veljavnem slovarju izrazov standarda PCI DSS.

Pokrite stranke pomenijo vse vaše zaposlene, zastopnike, predstavnike, podizvajalce, procesorje, ponudnike storitev, ponudnike vaše opreme v poslovnih enotah (POS) ali sistemov POS ali rešitev za obdelavo plačil, organe, povezane z vašim računom prodajalca American Express, in vse druge osebe, ki jim skladno s pogodbo omogočate dostop do informacij o imetnikih kartic.

Ponudniki storitev pomenijo pooblaščen procesorje, procesorje tretjih oseb, ponudnike portalov, postavljalce sistemov POS in katere koli druge ponudnike za prodajalce sistemov POS ali ponudnike drugih rešitev ali storitev za obdelavo plačil.

Ponudnik storitev stopnje 1 pomeni ponudnika storitev z 2,5 milijona transakcij s kartico American Express ali več na leto ali katerega koli ponudnika storitev, ki ga družba American Express šteje kot ponudnika storitev stopnje 1.

Ponudnik storitev stopnje 2 pomeni ponudnika storitev z manj kot 2,5 milijona transakcij s kartico American Express na leto ali katerega koli ponudnika storitev, ki ga družba American Express ne šteje za ponudnika storitev stopnje 1.

Pooblaščen presojevalec varnosti (QSA) pomeni organ, ki ga je pooblastil svet Payment Card Industry Security Standards Council, LLC, da validira skladnost s standardom PCI DSS.

Potrdilo o skladnosti (AOC) pomeni izjavo o stanju vaše skladnosti s standardom PCI DSS v obliki, ki jo zagotovi svet Payment Card Industry Security Standards Council, LLC.

Potrdilo o skladnosti preverjanja (AOSC) pomeni izjavo o stanju vaše skladnosti s standardom PCI DSS na podlagi preverjanja mreže in v obliki, ki jo zagotovi svet Payment Card Industry Security Standards Council, LLC.

Povzetek skladnosti (SOC) pomeni validacijski dokument PCI, ki ga franšizor ali ponudnik storitev uporabi za izkazovanje stanja skladnosti svojih zadevnih franšiz.

Prijavni datum pomeni datum, ki ga družba American Express določi izdajateljem v končnem obvestilu o incidentu, povezanem s podatki. Ta datum je odvisen od prejema končnega forenzičnega poročila ali interne analize s strani družbe American Express in se določi po lastni presoji družbe American Express.

Procesor pomeni ponudnika storitev prodajalcem, ki omogoča obdelavo pooblastil in vlog v mreži družbe American Express.

Prodajalec pomeni prodajalca in vse njegove pridružene družbe, ki sprejemajo kartice American Express po pogodbi z družbo American Express ali njenimi pridruženimi družbami.

Prodajalec stopnje 1 pomeni prodajalca z 2,5 milijona transakcij s kartico American Express ali več na leto ali katerega koli prodajalca, ki ga družba American Express šteje kot prodajalca stopnje 1.

Prodajalec stopnje 2 pomeni prodajalca s 50.000 do 2,5 milijona transakcij s kartico American Express na leto.

Prodajalec stopnje 3 pomeni prodajalca z 10.000 do 50.000 transakcij s kartico American Express na leto.

Prodajalec stopnje 4 pomeni prodajalca z manj kot 10.000 transakcij s kartico American Express na leto.

Program izboljšave varnostne tehnologije (STEP) pomeni program družbe American Express, s katerim prodajalce spodbuja, da uporabljajo tehnologije za izboljšavo varnosti podatkov. Da bi bili prodajalci upravičeni do programa STEP, ne smejo imeti incidenta, povezanega s podatki, v 12 mesecih pred predložitvijo letnega potrdila STEP in morajo vsaj 75 % vseh transakcij izvesti z uporabo šifriranja od točke do točke ali osebnimi transakcijami z uporabo naprav z omogočeno uporabo čipa EMV.

Samoocenjevalni vprašalnik (SAQ) pomeni orodje za samoocenjevanje, ki ga je ustvaril svet Payment Card Industry Security Standards Council, LLC, in je namenjeno ocenjevanju in potrjevanju skladnosti s standardom PCI DSS.

Sistem v poslovni enoti (POS) pomeni sistem ali opremo za obdelavo informacij, vključno s terminalom, osebnim računalnikom, elektronsko blagajno in brezstičnim čitalnikom, ali plačilni mehanizem ali postopek, ki ga prodajalec uporablja za pridobivanje pooblastil ali zbiranje transakcijskih podatkov ali oboje.

Specifikacije EMV pomenijo specifikacije, ki jih je izdala družba EMVCo, LLC, in so na voljo na spletnem mestu www.emvco.com.

Šifriranje od točke do točke (P2PE) pomeni rešitev, ki kriptografsko ščiti podatke računa od točke, kjer prodajalec sprejme plačilno kartico, do varne točke šifriranja.

Šifrirni ključ (šifrirni ključ American Express) pomeni vse ključe, ki se uporabljajo za obdelavo, ustvarjanje, nalaganje in/ali zaščito podatkov računa. Ti med drugim vključujejo:

- ključe za šifriranje ključev: univerzalne ključe za različne cone (ZMK) in ključe za šifriranje PIN za različne cone (ZPK)
- univerzalne ključe, ki se uporabljajo na varnih kriptografskih napravah: lokalne univerzalne ključe (LMK)
- kodirne ključe za varnost kartice (CSCK)
- ključe za šifriranje PIN: ključe za izpeljavo osnove (BDK), ključe za šifriranje PIN (PEK) in ZPK

Tehnologija za zmanjševanje tveganja pomeni tehnološke rešitve, ki izboljšajo varnost podatkov imetnikov kartic American Express in občutljivih podatkov za preverjanje pristnosti, kot jih določi družba American Express. Če želite uveljaviti uporabo tehnologije za zmanjševanje tveganja, morate dokazati učinkovito uporabo tehnologije skladno z njeno zasnovo in predvideno uporabo. Primeri vključujejo: EMV, šifriranje od točke do točke in tokenizacija.

Trajanje incidenta, povezanega s podatki pomeni obdobje, ki se začne na datum ogroženosti, če je znan, ali 365 dni pred prijavnim datumom, če dejanski datum ogroženosti ni znan. Trajanje incidenta, povezanega s podatki, poteče 30 dni po prijavnem datumu.

Transakcija pomeni bremenitev ali kredit, za katerega se uporabi kartica.

Transakcija EMV pomeni transakcijo s kartico z integriranim vezjem (včasih imenovano »kartica IC«, »kartica s čipom«, »pametna kartica«, »kartica EMV« ali »ICC«), ki se izvede na terminalu v poslovni enoti (POS), združljivem s kartico IC, z odobritvijo veljavnega in trenutnega tipa EMV. Odobritve tipa EMV so na voljo na spletnem mestu www.emvco.com.

Transakcije plačil, ki jih izvedejo kupci (BIP) pomenijo plačilno transakcijo, omogočeno prek datoteke za plačilna navodila, ki jo obdela BIP.

Validacijska dokumentacija pomeni potrdilo AOC, pridobljeno v povezavi z letno interno oceno varnosti ali SAQ, potrdilo AOSC in povzetke rezultatov, pridobljene v povezavi s četrtletnimi preverjanji mreže, ali letno potrdilo za program izboljšave varnostne tehnologije.

Varnostne zahteve PIN PCI pomenijo varnostne zahteve kartičnega poslovanja za PIN, ki so na voljo na spletnem mestu www.pcisecuritystandards.org.

Zahtevak za plačilo ima pomen, ki mu je dodeljen v takrat veljavnem slovarju izrazov za Standard varnosti podatkov kartičnega poslovanja, ki je na voljo na spletnem mestu www.pcisecuritystandards.org.

Zahteve sveta Payment Card Industry Security Standards Council (PCI SSC) pomenijo nabor standardov in zahtev v zvezi z varovanjem in zaščito podatkov plačilne kartice, vključno s standardoma PCI DSS in PA DSS, ki sta na voljo na spletnem mestu www.pcisecuritystandards.org.