AMERICAN EXPRESS

Pravilnik za upravljanje varnosti podatkov (DSOP)

Vrstice za spremembe

V preglednici povzetka sprememb so navedene pomembne posodobitve, ki so v pravilniku DSOP označene z vrstico za spremembe. Vrstice za spremembe so navpične črte na levem robu, ki označujejo revidirano, dodano ali odstranjeno besedilo. Vse spremembe v pravilniku DSOP so označene z vrstico za spremembe, ki je prikazana tukaj.

Preglednica povzetka sprememb

V spodnji preglednici so navedene pomembne posodobitve, ki so v pravilniku *DSOP* označene z vrstico za spremembe.

Poglavje/podpoglavje	Opis spremembe
Za to izdajo ni sprememb.	

Kaj moramo storiti, če pride do Incidenta, povezanega s podatki?

Če ste ugotovili, da je v vašem podjetju prišlo Incidenta, povezanega s podatki, sledite tem korakom.

1. korak:

Izpolnite obrazec za Prvo obvestilo o Incidentu, povezanem s podatki trgovca, in ga v najkasneje 72 urah po odkritju Incidenta, povezanega s podatki, pošljite po elektronski pošti na naslov EIRP@aexp.com.

2. korak:

Izvedite temeljito preiskavo; pri tem boste morda morali najeti Forenzičnega preiskovalca s področja kartičnega poslovanja (PCI).

3. korak:

Nemudoma nas obvestite o številkah vseh ogroženih Kartic American Express®.

4. korak:

Sodelujte z nami pri reševanju vseh težav, ki izhajajo iz Incidenta, povezanega s podatki.

Glejte Poglavje 3, »Obveznosti pri upravljanju Incidentov, povezanih s podatki« za podrobnosti glede obveznosti pri upravljanju Incidentov, povezanih s podatki.

Imate še dodatna vprašanja?

ZDA: (888) 732-3750 (brezplačna številka)

Druge države: +1 (602) 537-3021

EIRP@aexp.com

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 Program ciljnih analiz (TAP)

Vzrok za ogrožanje Podatkov imetnika Kartice so lahko varnostne vrzeli v Okolju Podatkov imetnika Kartice (CDE).

Primeri ogrožanja Podatkov imetnika Kartice so med drugim naslednji:

- **Skupna točka nakupa (CPP):** Imetniki Kartic družbe American Express poročajo o goljufivih Transakcijah na svojih računih Kartic, odkrili in ugotovili pa so, da te goljufive Transakcije izvirajo iz nakupov v vaših poslovalnicah.
- **Najdeni podatki Kartic:** Na svetovnem spletu so bili najdeni podatki Kartic družbe American Express in Podatki imetnikov Kartic, povezani s Transakcijami v vaših poslovalnicah.
- **Sum o zlonamerni programski opremi:** Družba American Express sumi, da uporabljate programsko opremo, ki je okužena s škodljivo kodo ali ji škodljiva koda lahko škoduje.

TAP je zasnovan za identifikacijo morebitnega ogrožanja Podatkov imetnika Kartice.

Ko vas družba American Express obvesti o morebitnem ogrožanju Podatkov imetnika Kartice, morate izpolniti spodnje zahteve in poskrbeti, da jih izpolnijo tudi vaše Pokrite stranke.

- Takoj morate preveriti, ali so se v okolju CDE pojavile pomanjkljivosti glede varnosti podatkov, in odpraviti te pomanjkljivosti, če jih odkrijete.
  - Če imate podizvajalce, ki so tretje osebe, jim morate naročiti, naj temeljito preverijo svoje okolje CDE.
- Ko prejmete obvestilo družbe American Express, morate pripraviti povzetek ukrepov, ki ste jih izvedli ali načrtovali po dejavnostih preverjanja, ocenjevanja in/ali odpravljanja pomanjkljivosti.
- Predložiti morate posodobljene validacijske dokumente PCI DSS skladno s spodaj navedenim Poglavjem 5, »Pomembna redna validacija vaših sistemov«.
- Skladno s tem morate imenovati usposobljenega Forenzičnega preiskovalca PCI (PFI), ki mora pregledati vaše okolje CDE, če vi ali vaša Pokrita stranka:
  - ne more razrešiti ogrožanja Podatkov imetnika Kartice v razumnem roku, kot ga določi družba American Express, ali
  - potrdi, da je prišlo do Incidenta, povezanega s podatki, in izpolni zahteve iz Poglavja 3, »Obveznosti pri upravljanju Incidentov, povezanih s podatki«.

Preglednica A-1: Nadomestilo za neskladnost s programom TAP

Opis	Prodajalec ali Ponudnik storitev stopnje 1	Prodajalec ali Ponudnik storitev stopnje 2	Prodajalec stopnje 3 ali stopnje 4
Nadomestilo za neskladnost je lahko ocenjeno, če obveznosti v zvezi programom TAP ne bodo izpolnjene do prvega roka.	25.000 USD	5000 USD	1000 USD
Nadomestilo za neskladnost je lahko ocenjeno, če obveznosti v zvezi programom TAP ne bodo izpolnjene do drugega roka.	35.000 USD	10.000 USD	2500 USD
Nadomestilo za neskladnost je lahko ocenjeno, če obveznosti v zvezi programom TAP ne bodo izpolnjene do tretjega roka. **OPOMBA:** *Nadomestila za neskladnost se lahko uveljavljajo, dokler niso obveznosti izpolnjene oziroma dokler pogoji iz programa TAP niso izpolnjeni.*	45.000 USD	15.000 USD	5000 USD

Če ne izpolnite svojih obveznosti v okviru programa TAP, ima družba American Express pravico, da vam kumulativno zaračuna nadomestila za neskladnost, zadrži plačila in/ali prekine pogodbo.

Poglavje 2 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) uporabljate samo tiste, ki so Odobreni s 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 iz Poglavja 5, »Pomembna redna validacija vaših sistemov«, razen če to poglavje določa drugače).

Poglavje 3 Obveznosti pri upravljanju Incidentov, povezanih s podatki

Po odkritju Incidenta, povezanega s podatki, morate o tem nemudoma oziroma najpozneje v dvainsedemdesetih (72) 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 Številk 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 zaključku poročila.
- Družbi American Express morate takoj sporočiti vse Ogrožene Številke Kartic. Družba American Express si pridržuje pravico, da izvede svojo interno analizo za identifikacijo Številk 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 Poglavja 3, »Obveznosti pri upravljanju Incidentov, povezanih s podatki«:

- lahko družba American Express po lastni presoji zahteva, da imenujete PFI, da opravi preiskavo Incidenta, povezanega s podatki, kadar gre za Incidente, povezane s podatki, ki vključujejo manj kot 10.000 enoličnih Številk Kartic. Vse take preiskave morajo izpolnjevati zgornje zahteve, določene v Poglavju 3, »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 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 preprečevanja 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, Izdajateljem, 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 4 Odškodninske obveznosti za Incident, povezan s podatki

Poglavjem 4, »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 Poglavju 4, »Odškodninske obveznosti za Incident, povezan s podatki«.

Za Incidente, povezane s podatki, ki vključujejo:

- 10.000 ali več Številk Kartic American Express z eno od 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 Številk Kartic American Express ali
- več kot 10.000 Številk Kartic American Express, če ste izpolnili te pogoje:
  - družbo American Express ste obvestili o Incidentu, povezanem s podatki, skladno s Poglavjem 3, »Obveznosti pri upravljanju Incidentov, povezanih 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 Poglavja 4, »Odškodninske obveznosti za Incident, povezan s podatki«, boste ne glede na število Številk 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 Poglavju 3, »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 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:

Preglednica A-2: Zahtevana merila za zmanjšanje odškodninske obveznosti

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.

Preglednica A-3: Povečano zmanjšanje odškodninske obveznosti

Primer	Uporabljene Tehnologije za zmanjševanje tveganja	Upravičenost	Zmanjšanje
1	80 % Transakcij na Napravah z omogočeno uporabo Čipa 0 % lokacij uporablja drugo Tehnologijo za zmanjševanje tveganja	Ne	50 %: standardno zmanjšanje (manj kot 75-odstotna uporaba Tehnologije za zmanjševanje tveganja ne upraviči povečanega zmanjšanja)[1]
2	80 % Transakcij na Napravah z omogočeno uporabo Čipa 77 % lokacij uporablja drugo Tehnologijo za zmanjševanje tveganja	Da	77 %: povečano zmanjšanje (na podlagi 77-odstotne uporabe Tehnologije za zmanjševanje tveganja)
3	93 % Transakcij na Napravah z omogočeno uporabo Čipa 100 % lokacij uporablja drugo Tehnologijo za zmanjševanje tveganja	Da	93 %: povečano zmanjšanje (na podlagi 93 % Transakcij na Napravah z omogočeno uporabo Čipa)

Primer	Uporabljene Tehnologije za zmanjševanje tveganja	Upravičenost	Zmanjšanje
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 zmanjševanje 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 5 Pomembna redna validacija vaših sistemov

Kot je opisano spodaj, morate za validacijo stanja vaše opreme, sistemov in/ali mrež (in njihovih komponent), na katerih se pri vas in v vaših franšizah shranjujejo, obdelujejo ali prenašajo Podatki imetnikov Kartic ali Občutljivi podatki za preverjanje pristnosti vsako leto in vsakih 90 dni izvajati naslednje korake.

Za izvedbo validacije so potrebni štirje koraki:

Korak 1: sodelujte v programu American Express za PCI skladnost (»Program«) po tem pravilniku.

Korak 2: zavedajte se svoje stopnje Prodajalca 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 po tem pravilniku. Družba American Express lahko po lastni presoji določi določene Prodajalce stopnje 3 in stopnje 4 za sodelovanje v Programu po tem pravilniku.

Prodajalec in Ponudniki storitev, ki morajo sodelovati v Programu, se morajo v predpisanih rokih prijaviti na Portalu, ki ga zagotavlja skrbnik Programa, ki ga je izbrala družba American Express.

- Sprejeti morate vse razumne pogoje, povezane z uporabo Portala.
- Na Portalu morate dodeliti in navesti točne podatke za vsaj eno kontaktno osebo za varnost podatkov. Zahtevani podatkovni elementi vključujejo:
  - ime in priimek,
  - e-poštni naslov,
  - telefonska številka,
  - fizični poštni naslov.
- Na Portalu morate zagotoviti posodobljene ali nove kontaktne podatke za dodeljeno kontaktno osebo za varnost podatkov, ko se ti podatki spremenijo.
- Zagotoviti morate, da so vaši sistemi posodobljeni tako, da omogočajo komunikacijo storitev iz domene, določene za Portal.

Če ne zagotovite ali vzdržujete aktualnih kontaktnih podatkov osebe za varnost podatkov ali ne omogočite e-poštnih komunikacij, to ne bo vplivalo na naše pravice do zaračunavanja pristojbin.

Korak 2: zavedajte se svoje stopnje Prodajalca 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.*
- Pri Ponudnikih storitev je to vsota obsega, ki ga predložijo Ponudnik storitev in Subjekti Ponudnika storitev, ki jim zagotavljate storitve.

Transakcije plačil, ki jih izvedejo kupci (BIP), niso vključene v obseg Transakcij s Karticami American Express za določanje stopnje Prodajalca in zahtev validacije. Vključeni boste v eno od stopenj, opredeljenih v spodnjih preglednicah za Prodajalce in Ponudnike storitev.

* Pri Franšizorjih to vključuje obseg njihovih Franšiznih poslovalnic. Franšizorji, ki zahtevajo, da njihove Franšize uporabljajo specifičen Sistem v poslovni enoti (POS) ali Ponudnika storitev, morajo predložiti tudi Validacijsko dokumentacijo za zadevne Franšize.

Zahteve Validacijske dokumentacije za Prodajalce

Za Prodajalce (ne Ponudnike storitev) so na voljo štiri možne razvrstitve stopnje Prodajalcev. Po določitvi stopnje Prodajalca skladno s spodnjim seznamom si oglejte Preglednica A-4: Validacijska dokumentacija 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 A-4: Validacijska dokumentacija za Prodajalce

Stopnja Prodajalca/ Letne Transakcije s Kartico American Express	Poročilo o skladnosti Potrdilo o skladnosti (ROC AOC)	Samoocenjevalni vprašalnik Potrdilo o skladnosti (SAQ AOC) IN Četrtletno preverjanje ranljivosti zunanje mreže (Scan)	Potrdilo STEP za Prodajalce, ki izpolnjujejo pogoje
Stopnja 1/ 2,5 milijona ali več	Obvezno	Ni veljavno	Neobvezno z odobritvijo družbe American Express (nadomesti ROC)
Stopnja 2/ od 50.000 do 2,5 milijona	Neobvezno	Obvezna SAQ AOC (razen v primeru predložitve ROC AOC); obvezno preverjanje pri nekaterih tipih SAQ	Neobvezno (nadomesti SAQ in preverjanje mreže ali ROC)
Stopnja 3/ 10.000 do 50.000	Neobvezno	Neobvezna SAQ AOC (obvezna, 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	Neobvezna SAQ AOC (obvezna, 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 preveri popolnost, točnost in ustreznost vaše Validacijske dokumentacije PCI. Družba American Express lahko v ta namen od vas zahteva, da predložite dodatna dokazila za oceno. Poleg tega ima družba American Express pravico, da od vas zahteva, da vključite QSA ali PFI, ki ga je odobril svet PCI Security Standards Council.

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 s kombinacijo naslednjih razširjenih izboljšanih varnostnih možnosti:

- **EMV, brezstična EMV ali digitalna denarnica** – z omogočeno uporabo Čipa, ki ima veljavno in posodobljeno odobritev/potrdilo EMVCo (www.emvco.com) ter je sposobna obdelave Transakcij s Karticami s Čipom, združljivih z AEIPS. (Prodajalci iz ZDA morajo vključiti brezstične Transakcije)
- **Šifriranje od točke do točke (P2PE)** – procesorju Prodajalca se pošlje s sistemom za Šifriranje od točke do točke, odobrenim s Standardom PCI SSC ali Pooblaščenim presojevalcem varnosti QSA.
- **Tokenizacija** – izvedena rešitev tokenizacije mora:
  - izpolnjevati specifikacije EMVCo,
  - biti varovana, obdelana, shranjena in prenesena ter biti v celoti upravljana s strani tretjega Ponudnika storitev, ki je skladen s PCI, in
  - žetona ni mogoče obrniti, da bi Prodajalcu razkril neodkrite primarne številke računa (PAN).

Prodajalci, primerni za program STEP, imajo zmanjšane zahteve za Validacijsko dokumentacijo PCI, kot je podrobneje opisano v nadaljevanju v Koraku 3: »izpolnite Validacijsko dokumentacijo, ki jo je treba poslati družbi American Express« spodaj.

Zahteve za Ponudnike storitev

Ponudniki storitev (ne Prodajalci) imajo dve možni razvrstitvi stopnje. Po določitvi stopnje Ponudnika storitev skladno s spodnjim seznamom si oglejte Preglednico A-5: Dokumentacija 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 A-5: Dokumentacija za Ponudnike storitev

Stopnja	Validacijska dokumentacija	Zahteva
1	Letno Poročilo o skladnosti Potrdilo o skladnosti (ROC AOC)	Obvezno
2	Letni SAQ D (Ponudnik storitev) in Četrtletno preverjanje mreže ali letno Poročilo o skladnosti (ROC AOC), 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.

Predložiti morate Potrdilo o skladnosti (AOC) za ustrezno vrsto ocenjevanja. AOC je izjava o vašem statusu skladnosti, zato jo mora podpisati in datirati ustrezno vodstvo vaše organizacije.

Družba American Express lahko poleg AOC od vas zahteva tudi kopijo celotne ocene in po naši presoji dodatna dokazila o skladnosti z zahtevami PCI DSS. Ta Validacijska dokumentacija se izpolni na vaše stroške.

Poročilo o skladnosti Potrdilo o skladnosti (ROC AOC) – (letna zahteva) – Poročilo o skladnosti dokumentira rezultate podrobnega pregleda vaše opreme, sistemov in omrežij (in njihovih komponent), kjer se shranjujejo, obdelujejo ali prenašajo podatki o imetnikih kartic ali občutljivi podatki za preverjanje pristnosti (ali oboje). Na voljo sta dve različici: ena za Prodajalce in druga za Ponudnike storitev. Poročilo o skladnosti mora izdelati:

- QSA ali
- vi, kar mora potrditi vaš izvršni direktor, finančni direktor, direktor za varnost informacijskih sistemov ali upravnik.

AOC mora podpisati in datirati QSA ali Ocenjevalec notranje varnosti (ISA) in pooblaščena raven vodstva v vaši organizaciji ter ga vsaj enkrat letno posredovati družbi American Express.

Samoocenjevalni vprašalnik Potrdilo o skladnosti (SAQ AOC) – (letna zahteva) – Samoocenjevalni vprašalniki omogočajo samopregledovanje vaše opreme, sistemov in mrež (in njihovih komponent), v katerih se shranjujejo, obdelujejo ali prenašajo Podatki imetnikov kartic ali Občutljivi podatki za preverjanje pristnosti (ali oboji). Obstaja več različic vprašalnika SAQ. Izbrali boste enega ali več glede na okolje Podatkov imetnikov kartic.

Vprašalnik SAQ lahko izpolni osebje v vašem podjetju, ki je usposobljeno za natančne in temeljite odgovore na vprašanja, lahko pa za pomoč vključite QSA. Potrdilo o skladnosti (AOC) mora podpisati in datirati pooblaščeno vodstvo v vaši organizaciji ter ga vsaj enkrat letno posredovati družbi American Express.

Odobreni ponudnik preverjanja Povzetek preverjanja ranljivosti zunanje mreže (Preverjanje ASV) – (90-dnevna zahteva) – Zunanje preverjanje ranljivosti je test na daljavo, ki pomaga ugotoviti morebitne slabosti, ranljivosti in napačne konfiguracije internetno dostopnih komponent vašega okolja Podatkov imetnikov kartic (npr. spletna mesta, aplikacije, spletni strežniki, poštni strežniki, javno dostopne domene ali gostitelji).

Opraviti ga mora Odobreni ponudnik preverjanja (ASV).

Če to zahteva vprašalnik SAQ, je treba Potrdilo o skladnosti preverjanja (AOSC) s poročilom o preverjanju ASV ali povzetek, ki vključuje število pregledanih ciljev, potrdilo, da rezultati izpolnjujejo postopke pregledovanja PCI DSS, in status skladnosti, ki ga je izpolnil ASV, predložiti družbi American Express vsaj enkrat na 90 dni.

ROC AOC ali STEP nista potrebna za zagotovitev povzetka AOSC ali preverjanja ASV, razen če se to izrecno zahteva. Da ne bo dvoma, četrtletno preverjanje mreže je obvezno, če tako zahteva ustrezni Samoocenjevalni vprašalnik SAQ.

Da ne bo dvoma, ASV je obvezno, če tako zahteva ustrezni Samoocenjevalni vprašalnik SAQ.

Validacijska dokumentacija s potrdilo STEP (STEP) – (letna zahteva) – STEP je na voljo samo Prodajalcem, ki izpolnjujejo merila, navedena pri zgornjem Koraku 2: »Zavedajte se svoje stopnje Prodajalca in zahtev za validacijo«. Če vaše podjetje izpolnjuje pogoje, morate družbi American Express vsako leto predložiti obrazec s potrdilom STEP. Letni obrazec s potrdilom STEP si lahko prenesete s Portala.

Neskladnost s Standardom PCI DSS – (letna, 90-dnevna in/ali priložnostna zahteva) – Če ugotovite neskladnost s Standardom PCI DSS, morate predložiti enega od naslednjih dokumentov:

- Potrdilo o skladnosti (AOC), vključno s »4. delom Akcijski načrt za neskladno stanje« (na voljo za prenos na spletni strani Sveta za varnostne standarde PCI)
- povzetek orodja s prednostnim pristopom PCI (na voljo za prenos na spletnem mestu Sveta za varnostne standarde PCI)

- predloga projektnega načrta (na voljo za prenos s Portala). Namesto letnega potrdila (SAQ/ROC) in/ali zahteve po preverjanju se lahko predloži projektni načrt.

Vsak od zgornjih dokumentov mora imeti določen datum odpravljanja neskladnosti, ki ne sme presegati dvanajst (12) mesecev od datuma izpolnitve dokumenta. 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). Sanacijske ukrepe, ki so potrebni za doseganje skladnosti s Standardom PCI DSS, je treba izvesti na vaše stroške.

Sanacijske ukrepe, ki so potrebni za doseganje skladnosti s Standardom PCI DSS, je treba izvesti na vaše stroške.

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.

Da ne bo dvoma: Prodajalci, ki ne delujejo skladno s Standardom PCI DSS, niso upravičeni do programa STEP.

Korak 4: pošljite Validacijsko dokumentacijo družbi American Express

Vsi Prodajalci in Ponudniki storitev, za katere se zahteva sodelovanje v Programu, morajo družbi American Express do ustreznih rokov predložiti Validacijsko dokumentacijo, ki je označena kot »obvezna« v preglednicah Koraka 2: »Zavedajte se svoje stopnje Prodajalca in zahtev za validacijo«.

Validacijsko dokumentacijo morate družbi American Express predložiti prek Portala, ki ga zagotovi Skrbnik Programa, ki ga izbere družba American Express. S predložitvijo Validacijske dokumentacije družbi American Express izjavljate in jamčite, da je naslednje (po vaših najboljših močeh) resnično:

- Vaša ocena je bila popolna in temeljita;
- Status PCI DSS je ob zaključku natančno predstavljen, in sicer kot skladen ali neskladen;
- Pooblaščeni ste za razkritje informacij, ki jih vsebuje, in zagotavljate Validacijsko dokumentacijo družbi American Express, ne da bi pri tem kršili pravice katere koli druge stranke.

Plačila zaradi odsotnosti validacije in prenehanje pogodbe

Družba American Express ima pravico, da vam zaračuna zneske zaradi odsotnosti validacije in prekine pogodbo, če ne izpolnjujete 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 četrtletna poročila.

Preglednica A-6: Plačilo zaradi odsotnosti validacije

Opis*	Prodajalec ali Ponudnik storitev stopnje 1	Prodajalec ali Ponudnik storitev stopnje 2 ali	Prodajalec stopnje 3 ali stopnje 4
Opravila se bo ocena za plačilo zaradi odsotnosti validacije, če se Validacijska dokumentacija ne predloži do prvega roka.	25.000 USD	5000 USD	50 USD
Opravila se bo dodatna ocena za plačilo zaradi odsotnosti validacije, če se Validacijska dokumentacija ne predloži do drugega roka.	35.000 USD	10.000 USD	100 USD

Opis*	Prodajalec ali Ponudnik storitev stopnje 1	Prodajalec ali Ponudnik storitev stopnje 2 ali	Prodajalec stopnje 3 ali stopnje 4
Opravila se bo dodatna ocena za plačilo zaradi odsotnosti validacije, če se Validacijska dokumentacija ne predloži do tretjega roka. **OPOMBA:** Plačilo zaradi odsotnosti validacije bo v veljavi, dokler ne bo predložena Validacijska dokumentacija.	45.000 USD	15.000 USD	250 USD

* Plačila zaradi odsotnosti validacije se ocenijo v protivrednostih lokalne valute.

* Ne velja v Argentini.

Če vaše obveznosti glede Validacijske dokumentacije PCI DSS niso izpolnjene, ima družba American Express pravico kumulativno zaračunati plačila zaradi odsotnosti validacije, zadržati plačila in/ali prekiniti pogodbo.

Poglavje 6 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 s ponudnikom Portala, 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:

a. je že znana družbi American Express pred razkritjem;

b. je na voljo ali postane na voljo javnosti, ne da bi ob tem družba American Express kršila določila tega odstavka;

c. jo je družba American Express zakonito prejela od tretje osebe, ki ni zavezana dolžnosti zaupnosti;

d. jo samostojno razvije družba American Express; ali

e. 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 7 Zavrnitev odgovornosti

DRUŽBA AMERICAN EXPRESS ZAVRAČA KAKRŠNA KOLI EKSPLICITNA, 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 Pravilnika 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.

Franšiza pomeni tretjo osebo, ki ima neodvisnega lastnika in posluje neodvisno (vključno s franšizo, imetnikom licence ali lokalno podružnico) ter ni pridružena družba, ki jo je Franšizor pooblastil za upravljanje franšize in je sklenila pisni sporazum s Franšizorjem, pri čemer nenehno razkriva zunanje znake identitete, s katerimi se izrazito identificira z znamkami Franšizorja ali se v javnosti predstavlja kot članica skupine podjetij Franšizorja.

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 pooblaščeni oziroma jih zagotavljate ali omogočate;
- 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, številkami kartičnih računov in kartičnimi identifikacijskimi številkami (CID).

Izdajatelj pomeni kateri koli organ (vključno z družbo American Express in njenimi pridruženimi družbami), ki ga družba American Express ali pridružena družba družbe American Express pooblasti za izdajo Kartic in poslovanje, povezano z izdajo Kartic.

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/potrdilo EMVCo (www.emvco.com) ter je sposobna obdelave Transakcij s Karticami s Čipom, združljivih z AEIPS.

Občutljivi podatki za preverjanje pristnosti pomenijo, kot je opredeljeno v takrat veljavnem slovarju izrazov za Standard 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 Zahtevek 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.

Okolje Podatkov imetnika Kartice (CDE) pomeni ljudi, procese in tehnologijo, ki shranjujejo, obdelujejo ali prenašajo Podatke imetnika Kartice ali Občutljive podatke za preverjanje pristnosti.

Payment Card Industry Data Security Standard (PCI DSS) pomeni Standard varnosti podatkov kartičnega poslovanja, ki je na voljo na spletnem mestu www.pcisecuritystandards.org.

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 za Standard PCI DSS.

Pokrite stranke pomenijo vse vaše zaposlene, zastopnike, predstavnike, podizvajalce, Procesorje, Ponudnike storitev, ponudnike vaše opreme v poslovnih enotah (POS) ali sistemov 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 pooblaščene Procesorje, Procesorje tretjih oseb, ponudnike portalov, postavljavce 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.

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

Portal pomeni sistem za poročanje, ki ga zagotovi Skrbnik programa PCI družbe American Express, ki ga izbere družba American Express. Prodajalci in Ponudniki storitev morajo uporabljati Portal za predložitev Validacijske dokumentacije PCI družbi American Express.

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.

Predloga končnega poročila o forenzičnem incidentu pomeni predlogo, ki je na voljo pri svetu PCI Security Standards Council na spletnem naslovu www.pcisecuritystandards.org.

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.

Primarna številka računa (PAN) ima pomen, ki je naveden v veljavnem slovarju izrazov za PCI DSS.

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 pomeni program American Express za skladnost s PCI.

Program ciljnih analiz (TAP) je program, ki omogoča zgodnjo identifikacijo potencialnega ogrožanja Podatkov imetnika Kartice v vašem Okolju Podatkov imetnika Kartice (CDE). Glejte Poglavje 1, »Program ciljnih analiz (TAP)«.

Program izboljšave varnostne tehnologije (STEP) pomeni program družbe American Express, s katerim Prodajalce spodbuja, da uporabljajo tehnologije za izboljšavo varnosti podatkov.

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

Številka Kartice pomeni enolično identifikacijsko številko, ki jo Izdajatelj ob izdaji dodeli Kartici.

Stopnja Prodajalca pomeni oznako, ki jo dodelimo prodajalcem v zvezi z njihovimi obveznostmi potrjevanja skladnosti s Standardom PCI DSS, kot je opisano v Poglavju 5: »Pomembna redna validacija vaših sistemov«.

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, vendar niso omejeni na: EMV, Šifriranje od točke do točke in tokenizacija.

Trajanje Incidenta, povezanega s podatki pomeni obdobje nastopa vdora (ali na podoben način določeno obdobje), opredeljeno v končnem forenzičnem poročilu (npr. poročilu PFI) ali, če ni znano, do 365 dni pred Prijavnim datumom obvestila o potencialno ogroženih številkah Kartic, vključenih v ogrožene Podatke, o katerih smo bili obveščeni.

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.

Zahtevek za plačilo ima pomen, ki mu je dodeljen v takrat veljavnem Slovarju izrazov Standarda za varno programsko opremo in Standarda za varen življenjski cikel programske opreme, 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.

Žeton pomeni kriptografski žeton, ki zamenja PAN na podlagi danega indeksa za nepredvidljivo vrednost.