American Express®

Radni pravilnik za sigurnost podataka – Hrvatska

Kao lider u zaštiti potrošača, tvrtka American Express oduvijek se zalaže za zaštitu „podataka vlasnika kartice“ i „osjetljivih podataka za provjeru autentičnosti“ i osiguravanje njihove zaštite.

Kompromitiranje podataka negativno utječe na potrošače, „trgovce“, „davatelje usluga“ i „izdavatelje kartica“. Čak i samo jedan incident može značajno naštetiti reputaciji tvrtke i pogoršati njezinu mogućnost učinkovitog poslovanja. Hvatanje u koštac s tom prijetnjom i uvođenje radnih pravilnika za sigurnost mogu pridonijeti poboljšanju povjerenja stranaka, povećanju profitabilnosti i reputacije tvrtke.

*Tvrtka American Express zna da naši „trgovci“ i „davatelji usluga“ (zajedno, **vi**) dijele našu zabrinutost i zahtijeva da, kao dio naših odgovornosti, budete u skladu s odredbama za sigurnost podataka u vašem ugovoru za prihvaćanje (u slučaju „trgovaca“) ili obradu (u slučaju „davatelja usluga“) kartice American Express® (svaki se naziva **ugovor**) te ovog „radnog pravilnika za sigurnost podataka“ koji možemo promijeniti s vremena na vrijeme. Ti se zahtjevi odnose na svu vašu opremu, sustave i mreže (i njihove komponente) putem koje se „ključevi za šifriranje“, „podaci vlasnika kartice“ ili „osjetljivi podaci za provjeru autentičnosti“ (ili njihova kombinacija) spremaju, obrađuju ili prenose.*

Značenje izraza u navodnicima koji ovdje nisu definirani navode se u pojmovniku na kraju ovog pravilnika.

ODJELJAK 1 – STANDARDI ZA ZAŠTITU „KLJUČEVA ZA ŠIFRIRANJE“, „PODATAKA VLASNIKA KARTICE“ I „OSJETLJIVIH PODATAKA ZA PROVJERU AUTENTIČNOSTI“

Vi i vaše „pokrivene stranke“ morate sljedeće:

- spremati „podatke vlasnika kartice“ samo za vršenje „transakcija“ putem kartice American Express i u skladu s i kako je zahtijevano ugovorom
- biti u skladu sa standardom za sigurnost podataka u industriji platnih kartica (Payment Card Industry Data Security Standard, PCI DSS) i zahtjevima za sigurnost PCI PIN najkasnije na datum stupanja na snagu te verzije i
- koristiti samo na mjestu prisustva koja su „PCI odobrena“ prilikom uvođenja novih ili zamjene „uređaja za unos PIN-a“ ili „aplikacija za plaćanje“ (ili oboje).

Morate zaštiti sve zapise o „naplati“ American Express i zadržane „kreditne“ zapise u skladu s ugovorom te u skladu s ovim odredbama za sigurnost podataka. Te zapise smijete koristiti samo za svrhe ugovora i morate ih čuvati na primjeren način. Financijski i na drugi način odgovarate tvrtki American Express za osiguravanje sukladnosti svojih „pokrivenih stranaka“ s ovim odredbama za sigurnost podataka (umjesto iskazivanja sukladnosti vaših „pokrivenih stranaka“ s ovim pravilnikom u okviru odjeljka 4 u nastavku, osim ako se u tom odjeljku ne navodi drugačije).

ODJELJAK 2 – OBVEZE ZA UPRAVLJANJE PODATKOVNIM INCIDENTIMA

Morate odmah obavijestiti tvrtku American Express, u svakom slučaju ne kasnije od dvadeset i četiri (24) sata, nakon otkrivanja „podatkovnog incidenta“.

Kako biste kontaktirali tvrtku American Express, kontaktirajte program za odziv na incidente tvrtke American Express (American Express Enterprise Incident Response Program, *EIRP*) na +1 (602) 537-3021 (+ označava prefiks za izravno međunarodno biranje „IDD“, naplaćuje se naknada za međunarodne pozive) ili putem e-pošte na EIRP@aexp.com. Morate imenovati osobu za kontaktiranje u vezi s takvim „podatkovnim incidentom“.

- Morate provesti temeljitu forenzičku istragu takvog podatkovnog incidenta. Za podatkovne incidente koji obuhvaćaju 10.000 ili više jedinstvenih brojeva računa kartice American Express (ili drugačije na zahtjev tvrtke American Express) tu istragu treba provesti „PCI forenzički istražitelj“ (PCI Forensic Investigator, PFI). Nerevidirano izvješće treba proslijediti tvrtki American Express u roku od 10 radnih dana nakon dovršetka.
  Tvrtki American Express morate što prije poslati sve „kompromitirane brojeve kartica“ i izvješće o forenzičkoj istrazi „podatkovnog incidenta“. Tvrtka American Express zadržava pravo na provođenje vlastite interne analize za identificiranje brojeva kartica zahvaćenih „podatkovnim incidentom“.

- Morate surađivati s tvrtkom American Express kako biste otklonili sve probleme proizašle iz „podatkovnog incidenta“, uključujući i savjetovanje s tvrtkom American Express o vašim komunikacijama prema „korisnicima usluge kartičnog plaćanja“ American Express zahvaćenim „podatkovnim incidentom“ (i pribavljanju svih neophodnih odricanja od odgovornosti) koje sadrže za American Express sve relevantne podatke za provjeru vaše sposobnosti za sprječavanje budućih podatkovnih incidenata na način sukladan ugovoru.

Izvješća o forenzičkom istraživanju moraju sadržavati forenzičke osvrte, izvješća o sukladnosti i sve druge informacije o „podatkovnom incidentu“; identificirajte uzrok podatkovnog incidenta, potvrdite jeste li bili u skladu ili ne s PCI DSS-om u trenutku „podatkovnog incidenta“; i potvrdite svoju sposobnost sprječavanja budućih „podatkovnih incidenata“ navođenjem plana za otklanjanje svih nedostataka u vezi s PCI DSS-om. Na zahtjev tvrtke American Express morate osigurati validaciju koju će provesti „kvalificirani procjenitelj sigurnosti“ (Qualified Security Assessor, ***QSA***) kako biste dokazali da su nedostaci otklonjeni.

Bez obzira na bilo kakvu proturječnu obvezu u ugovoru, tvrtka American Express ima pravo na otkrivanje informacija o bilo kojem „podatkovnom incidentu“ korisnicima „usluge kartičnog plaćanja“ American Express, izdavateljima i drugim sudionicima mreže American Express te općoj javnosti u skladu s primjenjivim zakonom; sudskim, administrativnim ili pravnim nalogom, proglasom, sudskim pozivom, zahtjevom ili drugim postupkom radi smanjenja opasnosti od prijevare ili drugih ugroza ili na drugi način do obima prikladnog za upravljanje mrežom American Express.

ODJELJAK 3 – OBVEZE OBEŠTEĆENJA ZBOG PODATKOVNOG INCIDENTA

Vaše obveze obeštećenja prema tvrtki American Express utvrđene su ugovorom s tvrtkom American Express za „podatkovne incidente“, bez poništavanja bilo kojih drugih prava ili mjera tvrtke American Express u okviru ovog odjeljka 3.

Tvrtka American Express neće od vas zahtijevati obeštećenje za „podatkovne incidente“ (a) koji obuhvaćaju manje od 10.000 jedinstvenih „kompromitiranih brojeva kartice“ ili (b) ako:

- obavijestite tvrtku American Express o „podatkovnom incidentu“ u skladu s odjeljkom 2 ovog pravilnika,
- ste bili u skladu s PCC DSS-om u vrijeme „podatkovnog incidenta“ (što se utvrđuje istragom PFI-ja o „podatkovnom incidentu“) i
- podatkovni incident nije bio uzrokovan pogrešnim postupanjem vas ili vaših „pokrivenih stranaka“.

Odgovorni ste za sve ostale „podatkovne incidente“ kako slijedi. Za „podatkovni incident“ koji obuhvaća samo brojeve računa kartica American Express tvrtku American Express što prije ćete obeštetiti plaćanjem naknade za „podatkovni incident“ zbog nesukladnosti koja neće premašivati 100.000 USD po „podatkovnom incidentu“. Za „podatkovni incident“ koji obuhvaća brojeve računa kartica American Express s „osjetljivim podacima za provjeru autentičnosti“ tvrtku American Express što prije ćete obeštetiti:

- po cijeni od 5 USD po broju računa
- naknadom za „podatkovni incident“ zbog nesukladnosti koja neće premašivati 100.000 USD po „podatkovnom incidentu“.

Tvrtka American Express iz svojih će izračuna isključiti sve brojeve računa kartica American Express koji su bili uključeni u drugi „podatkovni incident“ koji obuhvaća brojeve računa kartica American Express s osjetljivim podacima za provjeru autentičnosti, pod uvjetom da tvrtka American Express zaprimi obavijest o drugom „podatkovnom incidentu“ u roku od dvanaest (12) mjeseci prije datuma obavijesti. Svi izračuni koje ovom metodologijom izvrši tvrtka American Express konačni su.

Ovdje navedene obveze „trgovca“ za obeštećenjem za „podatkovne incidente“ ne smatraju se slučajnim, neizravnim, spekulativnim, posljedičnim, posebnim, kaznenim ili primjernim štetama u okviru ugovora, pod uvjetom da takve obveze ne obuhvaćaju štete povezane s ili koje su u naravi gubitka dobiti ili prihoda, dobre volje ili poslovnih prilika.

(Vrijedi samo za „podatkovne incidente“ otkrivene na dan ili nakon 13. listopada 2017). Tvrtka American Express po vlastitoj procjeni može smanjiti obvezu za obeštećenjem za „trgovca“ koji zadovoljava sljedeći kriterij:

- Prije „podatkovnog incidenta“ uporabljene su primjenjive tehnologije za izbjegavanje rizika i koristile su se tijekom cijelog „vremenskog okvira podatkovnog incidenta“, i
- Provedena je temeljita istraga u skladu s programom forenzičke istrage u industriji platnih kartica (Payment Card Industry Forensic Investigator, PFI) (osim ako je prethodno pismenim putem ugovoreno drugačije), i

- U forenzičkom izvješću jasno se navodi da su se za obradu spremanje i/ili prijenos podataka u vrijeme „podatkovnog incidenta“ koristile tehnologije za izbjegavanje rizika, i
- Ne spremate (i da niste spremali tijekom „vremenskog okvira podatkovnog incidenta“) „osjetljive podatke za provjeru autentičnosti“ i podatke vlasnika kartica koje nisu bile nečitljive

Kada je dostupno smanjenje obeštećenja, smanjenje vaše obveze za obeštećenjem (osim svih naplativih naknada za nesukladnost) utvrđuju se kako slijedi:

Smanjenje obveze za obeštećenjem	Potrebni kriterij
Standardno smanjenje: 50 %	>75 % ukupnih „transakcija“ obrađenih na „uređaju koji podržava čip“[1] ILI
	Tehnologija za izbjegavanje rizika koristi na >75 % lokacija trgovca[2]
Poboljšano smanjenje: 75 % do 100 %	>75 % svih „transakcija“ obrađenih na „uređaju koji podržava čip“[1] I druga tehnologija za izbjegavanje rizika koja se koristi na >75 % lokacija „trgovca“[2]

[1]Utvrđuje se internom analizom tvrtke American Express

[2]Utvrđuje se PFI istragom

- Poboljšano smanjenje (75 % do 100 %) utvrđuje se na temelju manjeg postotka „transakcija“ s pomoću „uređaja koji podržavaju čip“ I lokacija „trgovca“ na kojima se koristi druga tehnologija za izbjegavanje rizika. Primjeri u nastavku prikazuju izračun smanjenja obeštećenja.
- Kako biste ispunjavali uvjete za uporabu tehnologije za izbjegavanje rizika, morate dokazati učinkovitu primjenu tehnologije u skladu s njezinim dizajnom i namjenom. Na primjer, uporaba „uređaja koji podržava čip“ i obrada „kartica sa čipom“ kao „transakcije“ s magnetskom trakom ili unosom ključa NIJE učinkovita uporaba te tehnologije.
- Postotak lokacija na kojima se koristi tehnologija za izbjegavanje rizika utvrđuje se PFI istragom
- Smanjenje obveze za obeštećenjem ne vrijedi ni za kakve naplative naknade zbog nesukladnosti u vezi s „podatkovnim incidentom“

Primjer.	Uporaba tehnologije za izbjegavanje rizika	Jesu li ispunjeni uvjeti za smanjenje obveze za obeštećenjem?	Smanjenje
1	80 % ukupnih „transakcija“ na „uređaju koji podržava čip“ 0 % lokacija koristi tehnologiju za izbjegavanje rizika	Ne	50 %: Standardno smanjenje (uporaba manje od 75 % tehnologije za izbjegavanje rizika ne ispunjava uvjete za poboljšano smanjenje)[1]
2	80 % ukupnih „transakcija“ na „uređaju koji podržava čip“ 77% lokacija koristi tehnologiju za izbjegavanje rizika	Da	77 %: Poboljšano smanjenje (na temelju 77 % uporabe tehnologije za izbjegavanje rizika)
3	93% ukupnih „transakcija“ na „uređaju koji podržava čip“ 100% lokacija koristi tehnologiju za izbjegavanje rizika	Da	93 %: Poboljšano smanjenje (na temelju 93% „transakcija“ na uređajima koji podržavaju čip)
4	40% ukupnih „transakcija“ na „uređaju koji podržava čip“ 90 % lokacija koristi tehnologiju za izbjegavanje rizika	Ne	50 %: Standardno smanjenje (manje od 75 % „transakcija“ na „uređajima koji podržavaju čip“ ne ispunjava uvjete za poboljšano smanjenje)

[1]“Podatkovni incident“ koji obuhvaća 10.000 računa kartica American Express, po cijeni od 5 USD po broju računa (10.000 x 5 USD = 50.000 USD) može ispunjavati uvjete za smanjenje od 50 %, smanjujući obveze za obeštećenjem s 50.000 USD na 25.000 USD, isključujući sve naknade za nesukladnost.

ODJELJAK 4 – VAŽNO! POVREMENA PROVJERA VALJANOSTI VAŠIH SUSTAVA

Trebate izvršiti sljedeće korake godišnje i tromjesečno kako biste u okviru PCI DSS-a na način opisan u nastavku provjerili valjanost statusa opreme vaših primatelja franšize, sustava i/ili mreže (i njihovih komponenti) na kojima se spremanju, obrađuju ili prenose podaci vlasnika kartica ili „osjetljivi podaci za provjeru autentičnosti“.

Za dovršenje provjere valjanosti potrebna su:

Korak 1 – uključivanje u program sukladnosti tvrtke American Express u okviru ovog pravilnika

Korak 2 – utvrđivanje vaše razine i zahtjeva za „provjeru valjanosti“

Korak 3 – utvrđivanje dokumentacije za „provjeru valjanosti“ koju morate poslati tvrtki American Express

Korak 4 – slanje dokumentacije za „provjeru valjanosti“ tvrtki American Express

Korak 1 – uključivanje u program sukladnosti tvrtke American Express u okviru ovog pravilnika

„Trgovci razine 1“, „trgovci razine 2“, „trgovci razina 3“ i 4 koje je tvrtka American Express obavijestila te svi „davatelji usluge“, kako je opisano u nastavku, moraju se uključiti u program sukladnosti tvrtke American Express u okviru ovog pravilnika navodeći ime i prezime, adresu e-pošte, broj telefona i fizičku poštansku adresu pojedinaca koji će postupati kao njihovi općeniti kontakti za sigurnost podataka. Te informacije morate na jedan od načina navedenih u koraku 4 dolje poslati tvrtki Trustwave koja upravlja programom u ime tvrtke American Express. Tvrtku Trustwave morate obavijestiti ako se te informacije promijene i posredovati ažurirane informacije kada je to primjenjivo.

Tvrtka American Express može po vlastitoj prosudbi zatražiti da se određeni „trgovci“ razina 3 i 4 uključe u program sukladnosti tvrtke American Express u okviru ovog pravilnika, tako da im pošalje pismenu obavijest. „Trgovac“ se mora uključiti ne kasnije od 90 dana od zaprimanja obavijesti.

Tvrtka American Express može provjeriti rezultate vaše postupka PCI provjere valjanosti angažiranjem o svom trošku „kvalificiranog procjenitelja sigurnosti“ (Qualified Security Assessor, QSA) po vlastitom izboru.

Korak 2 – utvrđivanje vaše razine i zahtjeva za „provjeru valjanosti“

Postoje četiri razine za „trgovce“ i dvije razine za „davatelje usluge“. Većina razina temelji se na količini vaših „transakcija“ putem kartica American Express. Za „trgovce“ to je količina koju šalju njihove organizacije koja se proteže do najviše razine računa „trgovca“ za American Express. * Svrstat ćete se u jednu od razina specificiranih u tablicama za „trgovce“ i „davatelje usluge“ u nastavku.

„Transakcije“ za isplate koje pokreću tvrtke (Business Initiated Payments, BIP) nisu uključene u količinu „transakcija“ putem kartica American Express za utvrđivanje razine „trgovca“ i zahtjeve za „provjeru valjanosti“.

*To u slučaju „franšizodavaca“ uključuje količinu iz jedinica u njihovoj franšizi. „Franšizodavci“ koji svojim primateljima franšize nalažu primjenu specificiranog „sustava točke prodaje“ (Point of Sale, POS) ili „davatelji usluge“ također moraju pružiti „dokumentaciju za provjeru valjanosti“ za zahvaćene primatelje franšize.

Zahtjevi za „trgovce“

„Trgovci“ (ne „davatelji usluge“) imaju pet mogućih klasifikacija u vezi sa svojom razinom i zahtjevima za ovjerom valjanosti. Nakon utvrđivanja razine „trgovca“ s popisa u nastavku pogledajte tablicu „Trgovac“ kao biste utvrdili zahtjeve za „dokumentaciju za provjeru valjanosti“.

„Trgovac razine 1“ – 2,5 milijuna ili više „transakcija“ putem kartice American Express na godinu ili „trgovac“ kojeg tvrtka American Express inače smatra „trgovcem razine 1“.

„Trgovac razine 2“ – od 50.000 do 2,5 milijuna „transakcija“ putem kartice American Express na godinu

„Trgovac razine 3“ – od 10.000 do 50.000 „transakcija“ putem kartice American Express na godinu

„Trgovac razine 4“ – manje od 10.000 „transakcija“ putem kartice American Express na godinu

Tablica Trgovac

Razina	Obvezna dokumentacija za provjeru valjanosti	Opcijska dokumentacija za provjeru valjanosti
1	Godišnje izvješće o procjeni sigurnosti na lokaciji	Tromjesečno skeniranje mreže ILI Ovjera programa STEP
2	Godišnji „upitnik za samoprocjenu“ i tromjesečno skeniranje mreže	Godišnje izvješće o procjeni sigurnosti na lokaciji ILI Ovjera programa STEP
3*	(Godišnji „upitnik za samoprocjenu“ i tromjesečno skeniranje mreže mogu biti obvezni u skladu s procjenom tvrtke American Express)	Godišnji „upitnik za samoprocjenu“ i tromjesečno skeniranje mreže ILI Godišnje izvješće o procjeni sigurnosti na lokaciji ILI Ovjera programa STEP
4*	(Godišnji „upitnik za samoprocjenu“ i tromjesečno skeniranje mreže mogu biti obvezni u skladu s procjenom tvrtke American Express)	Godišnji „upitnik za samoprocjenu“ i tromjesečno skeniranje mreže ILI Godišnje izvješće o procjeni sigurnosti na lokaciji ILI Ovjera programa STEP

*Radi otklanjanja sumnje, trgovci razina 3 i 4 ne trebaju slati „dokumentaciju za provjeru valjanosti“, osim ako to zatraži tvrtka American Express po vlastitoj procjeni, ali svakako moraju biti sukladni i odgovorni u pogledu svih drugih odredbi ovog radnog pravilnika za sigurnost podataka.

„Program za unaprjeđenje sigurnosne tehnologije“

„Trgovci“ koji su sukladni s PCI DSS-om moraju ispunjavati i uvjete „programa za unaprjeđenje sigurnosne tehnologije“ (STEP) tvrtke American Express ako koriste određene dodatne sigurnosne tehnologije u svojim okruženjima za obradu kartica. Program STEP primjenjuje se samo ako se „trgovcu“ nije dogodio „podatkovni incident“ tijekom proteklih 12 mjeseci i ako se 75 % svih kartičnih „transakcija“ „trgovca“ vrši:

- **EMV** – na aktivnom „uređaju koji podržava čip“ s valjanim i trenutačnim EMVCo (www.emvco.com) odobrenjem/certifikatom i koji može obrađivati „transakcije“ s „karticama sa čipom“ u skladu s AEIPS-om. („Trgovci“ u SAD-u moraju uključivati breskontaktne „transakcije“)
- **„Šifriranje od točke do točke“** (Point-to-Point Encryption, P2PE) – komuniciranje s „procesorom“ „trgovca“ putem PCI-SSC ili QSA odobrenog sustava „šifriranja od točke do točke“.

„Trgovci“ koji zadovoljavaju uvjete za „program za unaprjeđenje sigurnosne tehnologije“ imaju smanjene potrebe za PCI „dokumentaciju za provjeru valjanosti", kao što je dodatno opisano u koraku 3 u nastavku.

Zahtjevi za „davatelje usluge“

„Davatelji usluge“ (ne „trgovci“) imaju dvije moguće klasifikacije u vezi sa svojom razinom i zahtjevima za ovjerom valjanosti. Nakon utvrđivanja razine „davatelja usluge“ s popisa u nastavku pogledajte tablicu „Davatelj usluge“ kao biste utvrdili zahtjeve za „dokumentaciju za provjeru valjanosti“.

„Davatelj usluge razine 1“ – 2,5 milijuna ili više „transakcija“ putem kartice American Express na godinu ili davatelj usluge kojeg tvrtka American Express inače smatra „davateljem usluge razine 1“.

„Davatelj usluge razine 2“ – manje od 2,5 milijuna „transakcija“ putem kartice American Express na godinu ili svi „davatelji usluge“ koje tvrtka American Express ne smatra „davateljima usluge razine 1“.

„Davatelji usluge“ ne moraju zadovoljavati „program za unaprjeđenje sigurnosne tehnologije“.

Tablica „Davatelj usluge“

Razina (definirano gore)	Provjera valjanosti Dokumentacija (definirano u koraku 3 gore)	Zahtjev
1	• Godišnje izvješće o procjeni sigurnosti na lokaciji	Obvezno
2	• Godišnji „upitnik za samoprocjenu“ • Tromjesečno skeniranje mreže	Obvezno

Preporučuje se da „davatelji usluge“ budu u skladu i s PCI dodatnom provjerom valjanosti za namjenske subjekte

Korak 3 – utvrđivanje „dokumentacije za provjeru valjanosti“ koju morate poslati tvrtki American Express

Sljedeći dokumenti potrebni su za različite razine „trgovaca“ i „davatelja usluge“, kako je navedeno u tablicama „Trgovac“ i „Davatelj usluge“ gore.

Godišnja procjena sigurnosti na lokaciji – godišnja procjena sigurnosti na lokaciji podroban je pregled na lokaciji vaše opreme, sustava i mreža (i njihovih komponenti) na kojima se spremanju, obrađuju ili prenose

podaci vlasnika kartica ili „osjetljivi podaci za provjeru autentičnosti“. Postupak treba provesti

- QSA ili
- vi i mora ga certificirati vaš izvršni voditelj, glavni financijski voditelj, glavni voditelj za informacijsku sigurnost ili ravnatelj i izvješće treba godišnje slati tvrtki American Express u ovjeri sukladnosti (Attestation of Compliance, ***AOC***).

AOC mora certificirati sukladnost sa svim zahtjevima PCI DSS-a i na zahtjev uključiti kopije cjelovitog izvješća o sukladnosti („trgovci“ i „davatelji usluge razine 1“)

„Godišnji upitnik za samoprocjenu“ – „godišnji upitnik za samoprocjenu“ postupak je u kojem se koristi PCI DSS „Upitnik za samoprocjenu“ (Self-Assessment Questionnaire, ***SAQ***) koji omogućuje samostalan pregled vaše opreme, sustava i mreža (i njihovih komponenti) na kojima se spremanju, obrađuju ili prenose podaci vlasnika kartica ili „osjetljivi podaci za provjeru autentičnosti“. Morate ga provesti vi i mora ga certificirati vaš izvršni voditelj, glavni financijski voditelj, glavni voditelj za informacijsku sigurnost ili ravnatelj. Odjeljak AOC upitnika SAQ treba godišnje slati tvrtki American Express. Odjeljak AOC upitnika SAQ mora certificirati vašu sukladnost sa svim zahtjevima PCI DSS i uključivati cjelovite kopije upitnika SAQ na zahtjev („Trgovci“ razina 2, 3 i 4 te „davatelji usluge razine 2“).

Tromjesečno skeniranje mreže – tromjesečno skeniranje mreže postupak je daljinskog testiranja vaših računalnih mreža i web poslužitelja povezanih s internetom radi pronalaženja mogućih nedostataka i ranjivosti. To treba izvršiti „odobreni skeniratelj (Approved Scanning Vendor, ***ASV***). Morate ispuniti i tvrtki American Express poslati ASV izvješće o skeniranju za „ovjeru sukladnosti skeniranja“ (Attestation of Scan Compliance, ***AOSC***) ili izvršni sažetak nalaza skeniranja (i na zahtjev kopije cjelovitog skeniranja). AOSC ili izvršni sažetak mora certificirati da rezultati zadovoljavaju postupke PCI DSS skeniranja, da nisu identificirani vrlo rizični problemi te da je skeniranje prolazno ili sukladno („davatelji usluge razine 2“, „trgovci“ razina 2, 3 i 4, osim „trgovaca“ koji zadovoljavaju uvjete za „program za unaprjeđenje sigurnosne tehnologije“).

Dokumentacija za godišnju provjeru valjanosti „programa za unaprjeđenje sigurnosne tehnologije“ (STEP) – godišnja ovjera kvalifikacije programa STEP za American Express („ovjera programa STEP“) dostupna je samo za „trgovce“ koji zadovoljavaju uvjete navedene u koraku 2 gore. Ovjera programa STEP uključuje postupak je u kojem se koristi PCI DSS koji omogućuje samostalan pregled vaše opreme, sustava i mreža (i njihovih komponenti) na kojima se spremanju, obrađuju ili prenose podaci vlasnika kartica ili „osjetljivi podaci za provjeru autentičnosti“ (ili oboje). Morate ga provesti vi i mora ga certificirati vaš izvršni voditelj, glavni financijski voditelj, glavni voditelj za informacijsku sigurnost ili ravnatelj. Morate dovršiti postupak godišnjim slanjem obrasca za ovjeru programa STEP tvrtki American Express. (Samo za „trgovce“ koji zadovoljavaju uvjete programa STEP). Obrazac za godišnju ovjeru „programa za unaprjeđenje sigurnosne tehnologije“ dostupan je za preuzimanje putem sigurnog portala tvrtke Trustwave.

„Saželak sukladnosti“ – „saželak sukladnosti“ (Summary of Compliance, „SOC“) dokument je putem kojeg „franšizodavac“ ili „davatelj usluge“ može poslati izvješće o statusu PCI sukladnosti svojih primatelja franšiza. Predložak SOC-a dostupan je za preuzimanje putem sigurnog portala tvrtke Trustwave.

Nesukladnost s PCI DSS-om – ako niste sukladni s PCI DSS-om, morate ispuniti AOC, uključujući „Dio 4. akcijski plan za status nesukladnosti” ili predložak projektnog plana (dostupan je za preuzimanje putem sigurnog portala tvrtke Trustwave) i odrediti datum za otklanjanje problema koji ne smije biti kasnije od dvanaest mjeseci od datuma AOC-a kako bi postigli sukladnost. AOC s „akcijski plan za status nesukladnosti“ trebate poslati tvrtki American Express na jedan od načina navedenih u koraku 4 dolje. Tvrtki American Express morate slati povremena ažuriranja svog napretka prema otklanjanju problema u okviru „akcijskog plana za status nesukladnosti“ („trgovci“ razina 1, 2, 3 i 4 te svi „davatelji usluge“). Radi otklanjanja svake sumnje, „trgovci“ koji nisu sukladni s PCI DSS-om ne ispunjavaju uvjete za „program za unaprjeđenje sigurnosne tehnologije“ (Security Technology Enhancement Program, STEP).

Tvrtka American Express neće vam nametati naknade koje nisu povezane s ovjerom (opisano u nastavku) prije datuma za otklanjanje problema, ali ćete i dalje biti odgovorni tvrtki American Express u pogledu svih obveza za obeštećenjem za „podatkovni incident“ i morat ćete poštivati sve druge odredbe iz ovog pravilnika.

Korak 4 – slanje „dokumentacije za provjeru valjanosti“ tvrtki American Express

„Trgovci“ razina 1 i 2, po vlastitoj procjeni tvrtke American Express „trgovci“ razina 3 i 4, „trgovci“ koji zadovoljavaju uvjete programa STEP i svi „davatelji usluge“ moraju slati „dokumentaciju za provjeru valjanosti“ označenu kao „obvezno“ u tablicama u koraku 2.

Svoju dokumentaciju trebate poslati tvrtki Trustwave na jedan od sljedećih načina:

Sigurni portal: „Dokumentaciju za provjeru valjanosti“ možete prenijeti putem sigurnog portala tvrtke Trustwave na https://login.trustwave.com.

Kontaktirajte tvrtku Trustwave na + 1 (312) 267-3208 (+ označava prefiks za izravno međunarodno biranje „IDD“, naplaćuje se naknada za međunarodne pozive) ili putem e-pošte na AmericanExpressCompliance@trustwave.com za upute za uporabu tog portala.

Sigurni faks: „Dokumentaciju za provjeru valjanosti“ možete faksirati na: +1 (312) 276-4019. (+ označava prefiks za izravno međunarodno biranje „IDD“, naplaćuje se naknada za međunarodne pozive). Navedite svoje ime, DBA (poslovanje kao) naziv, ime kontakta za sigurnost podataka, adresu i broj telefona te, samo za „trgovce“, 10-znamenkasti broj „trgovca“ American Express.

U slučaju općenitih pitanja o programu ili postupku opisanom gore obratite se tvrtki Trustwave na +1 (312) 267-3208 (+ označava prefiks za izravno međunarodno biranje „IDD“, naplaćuje se naknada za međunarodne pozive) ili putem e-pošte na AmericanExpressCompliance@trustwave.com

Sukladnost i ovjera vrše se o vašem trošku. Slanjem „dokumentacije za provjeru valjanosti“ tvrtki American Express izjavljujete i jamčite da imate ovlasti za otkrivanje sadržanih informacija i da tvrtki American Express pružate „dokumentaciju za provjeru valjanosti“ bez kršenja oprava bilo koje druge stranke.

Naknade za nesukladnost i raskidanje ugovora

Tvrtka American Express ima pravo naplate naknada za nesukladnost i raskidanje ugovora ako ne ispunite te zahtjeve ili ako ne isporučite obveznu „dokumentaciju za provjeru valjanosti“ tvrtki American Express do važećeg roka. Tvrtka American Express posebno će vas obavijestiti o važećem roku za svako godišnje i tromjesečno razdoblje.

Opis (Valuta HRK kn)	Trgovac ili davatelj usluge razine 1	Trgovac ili davatelj usluge razine 2, trgovac STEP	Trgovac razine 3 ili 4
Naknada za nesukladnost procijenit će se ako se „dokumentacija za provjeru valjanosti“ ne zaprimi do prvog roka.	HRK 105,000	HRK 21,000	130 kn na mjesec
Dodatna naknada za nesukladnost procijenit će se ako se „dokumentacija za provjeru valjanosti“ ne zaprimi u roku od 30 dana od prvog roka.	HRK 152,000	HRK 42,000	
Dodatna naknada za nesukladnost procijenit će se ako se „dokumentacija za provjeru valjanosti“ ne zaprimi u roku od 60 dana od prvog roka.	HRK 195,000	HRK 63,000	

Ako tvrtka American Express ne zaprimi vašu obveznu „dokumentaciju za provjeru valjanosti“ u roku od 60 dana od prvog roka, tada tvrtka American Express ima pravo na raskidanje ugovora u skladu s njegovim odredbama kao i na kumulativnu naplatu tekućih naknada za nesukladnost.

ODJELJAK 5 – POVJERLJIVOST

Tvrtka American Express poduzet će razumne mjere da vaša izvješća o sukladnosti, uključujući „dokumentaciju za provjeru valjanosti“ zadrže (što vrijedi i za njihove predstavnike i podugovorene stranke, uključujući tvrtku Trustwave) povjerljivima i „dokumentaciju za provjeru valjanosti“ neće otkrivati nijednoj trećoj strani (osim pridruženih tvrtki, agenata, predstavnika, „davatelja usluge“ i podugovorenih stranki) u razdoblju od tri godine od datuma zaprimanja, osim što ova obveza o povjerljivosti ne vrijedi za „dokumentaciju za provjeru valjanosti“:

i. koja je tvrtki American Express već bila poznata prije otkrivanja,
ii. koja jest ili postane dostupna javnosti od strane tvrtke American Express bez kršenja ovog članka,
iii. koju je tvrtka American Express valjano zaprimila bez obveze za povjerljivošću,
iv. koju je neovisno razvila tvrtka American Express ili,
v. koju treba otkriti po nalogu suda, upravnog organa ili vladinog tijela, ili tako nalaže bilo koji zakon, propis ili uredba ili sudski poziv, zahtjev za otkrivanjem, opoziv ili drugi upravni ili pravni postupak ili bilo koji službeni ili neslužbeni zahtjev ili istraga bilo koje vladine agencije ili

tijela (uključujući sve regulatore, inspektore, revizore ili agencije za provedbu zakona).

ODJELJAK 6 – POVJERLJIVOST

TVRTKA AMERICAN EXPRESS OVIM SE PUTEM ODRIČE BILO KOJIH I SVIH REPREZENTACIJA, JAMSTAVA I ODGOVORNOSTI U POGLEDU OVOG RADNOG PRAVILNIKA ZA SIGURNOST PODATAKA, PCI DSS-a, „EMV SPECIFIKACIJE“ I NAMJENE TE IZVEDBE QSA-ova, ASV-ova ILI PFI-ova (ILI BILO KOJEG OD NJIH), BILO IZREČENO, PODRAZUMIJEVANO, ZAKONSKI ILI DRUGAČIJE, UKLJUČUJUĆI SVA JAMSTVA O MOGUĆNOSTI PRODAJE ILI ODGOVARANJA ODREĐENOJ SVRSI. IZDAVATELJI KARTICA AMERICAN EXPRESS NISU KORISNICI TREĆE STRANE U OKVIRU OVOG PRAVILNIKA.

Korisna web-mjesta

Sigurnost podataka tvrtke American Express: http://www.americanexpress.com/datasecurity

Payment Card Industry Security Standards Council, LLC:

http://www.pcisecuritystandards.org

POJMOVNIK

Za svrhu ovog pravilnika primjenjuju se sljedeće definicije:

Kartica American Express ili kartica odnosi se na bilo koju karticu, uređaj za pristup računu, platni uređaj ili uslugu s nazivom, logotipom, zaštitnim znakom, znakom usluge, trgovačkim nazivom ili drugim vlasničkim dizajnom ili oznakom tvrtke American Express ili pridružene tvrtke koje izdaje izdavatelj ili se nalaze na računu kartice

Ovjera sukladnosti ili AOC označava izjavu o statusu vaše sukladnosti s PCI DSS-om u obrascu koji pribavlja Payment Card Industry Security Standards Council, LLC.

Rješenje za odobreno šifriranje od točke do točke (Approved Point-to-Point Encryption, P2PE), uključeno je na PCI SSC popisu ovjerenih rješenja ili koje ovjerava P2PE tvrtka PCI SSC kvalificiranog procjenitelja sigurnosti.

Odobreni skeniratelj, ASV, označava subjekt koji je kvalificiralo Payment Card Industry Security Standards Council, LLC za ovjeru ispunjavanja određenih zahtjeva PCI DSS-a provođenjem skeniranja ranjivosti okruženja povezanih s internetom.

Ovjera sukladnosti skeniranja ili AOSC označava izjavu o statusu vaše sukladnosti s PCI DSS-om na temelju mrežnog skeniranja, u obrascu koji pribavlja Payment Card Industry Security Standards Council, LLC.

„Podaci vlasnika kartice“ ima značenje navedeno u trenutačnom pojmovniku PCI DSS-a.

Korisnik usluge kartičnog plaćanja označava pojedinca ili subjekt (i) koji je sklopio ugovor otvaranjem kartičnog računa s izdavateljem ili (ii) čije se ime nalazi na kartici.

Informacije o korisniku usluge kartičnog plaćanja odnosi se na informacije o korisnicima usluge kartičnog plaćanja American Express i kartičnim transakcijama, uključujući imena, adrese, brojeve kartičnih računa i identifikacijske brojeve kartica (card identification numbers, ***CID-ovi***).

Naplata se odnosi na plaćanje izvršeno karticom.

Čip se odnosi na integrirani mikročip na kartici koji sadrži informacije o korisniku usluge kartičnog plaćanja i računu.

Kartica sa čipom odnosi se na karticu koja sadrži čip i za koju može biti potreban PIN kao sredstvo ovjere identiteta korisnika usluge kartičnog plaćanja ili informacija o računu koje čip sadrži ili ovoje (ponekad se u našim materijalima naziva „pametna kartica“ „EMV kartica“, kartica s integriranim krugom“).

Uređaj koji podržava čip – odnosi se na uređaj na točki prodaje s valjanim i trenutačnim EMVco (www.emvco.com) odobrenjem/certifikatom i koji može obrađivati transakcije s karticama sa čipom u skladu s AEIPS-om.

Kompromitirani broj kartice odnosi se na broj kartičnog računa American Express povezan s podatkovnim incidentom.

Pokrivene stranke odnosi se na sve vaše zaposlenike, agente, predstavnike, podugovaratelje, „procesore“, davatelje usluge, dobavljače vaše opreme na točki prodaje ili sustave ili rješenja za obradu plaćanja, subjekte povezane s vašim trgovačkim računom American Express i sve druge stranke kojima možete posredovati informacije o korisnicima usluge kartičnog plaćanja u skladu s ugovorom.

Kredit se odnosi na iznos koji vraćate korisnicima usluge kartičnog plaćanja za kupnje ili plaćanja izvršena karticom.

Podatkovni incident odnosi se na incident koji uključuje kompromitiranje ili sumnju na kompromitiranje ključeva za šifriranje American Express ili barem jednog kartičnog računa American Express na kojem je došlo do:

- neovlaštenog pristupa ili uporabe ključeva za šifriranje, podataka vlasnika kartice ili „osjetljivih podataka za provjeru autentičnosti“ (ili kombinacija navedenog) koji se spremaju obrađuju ili šalju putem vaše opreme, sustava i/ili mreža (i njihovih komponenti) ili čijom uporabom upravljate,
- uporabe „ključeva za šifriranje“, podataka vlasnika kartice ili „osjetljivih podataka za provjeru autentičnosti“ (ili kombinacija navedenog) koja nije u skladu s ugovorom, i/ili
- mogućeg ili potvrđenog gubitka, krađe, pronevjere na bilo koji način putem bilo kojeg medija, materijala, zapisa ili informacija sadržanih u takvim „ključevima za šifriranje“, podacima vlasnika kartice ili osjetljivim podacima za provjeru autentičnosti (ili kombinacija navedenog).

Vremenski okvir podatkovnog incidenta odnosi se na razdoblje koje počinje s datumom kompromitiranja, ako je poznat, ili 365 dana prije „datuma obavijesti“ ako stvarni datum

kompromitiranja nije poznat. Vremenski okvir podatkovnog incidenta završava 30 dana nakon "datuma obavijesti".

EMV specifikacije odnose se na specifikacije koje izdaje EMVCo, LLC i koje su dostupne na http://www.emvco.com.

EMV transakcija odnosi se na transakciju putem kartice s integriranim krugom (ponekad se naziva i „IC kartica", „kartica sa čipom", „pametna kartica", „EMV kartica" ili „ICC") izvršenu na terminalu na točki prodaje (POS) koja podržava IC karticu s valjanim odobrenjem EMV tipa. Odobrenja EMV tipa dostupna su na http://www.emvco.com.

Ključ za šifriranje („Ključ za šifriranje American Express") odnosi se na sve ključeve koji se koriste u obradi, generiranju, učitavanju i/ili zaštiti podataka računa. To uključuje između ostalog sljedeće:

- Ključevi za šifriranje: Glavni ključevi zone (Zone Master Keys, ZMK-ovi)i PIN ključevi zone (Zone Pin Keys, ZPK-ovi)
- Glavni ključevi koji se koriste za osiguravanje kriptografskog uređaja: Lokalni glavni ključevi (Local Master Keys, LMK-ovi)
- Ključevi sigurnosnog koda kartice (Card Security Code Keys, CSCK-ovi)
- PIN ključevi: Osnovni derivirani ključevi (Base Derivation Keys, BDK-ovi), ključevi za šifriranje PIN-a (PIN Encryption Key, PEK-ovi) i ZPK-ovi

Franšizodavac se odnosi na operatera tvrtke koja licencira osobe ili subjekte (**primatelji franšize**) za distribuciju robe i/ili usluga pod ili s uporabom operaterove oznake, pomažu primateljima franšize u poslovanju ili utječu na način poslovanja franšize i d primatelja franšize zahtijeva plaćanje naknade.

Trgovac razine 1 – 2,5 milijuna ili više transakcija putem kartice American Express na godinu ili trgovac kojeg tvrtka American Express inače smatra trgovcem razine 1.

Trgovac razine 2 – od 50.000 do 2,5 milijuna transakcija putem kartice American Express na godinu.

Trgovac razine 3 – od 10.000 do 50.000 transakcija putem kartice American Express na godinu

Trgovac razine 4 – manje od 10.000 transakcija putem kartice American Express na godinu

Davatelj usluge razine 1 – 2,5 milijuna ili više transakcija putem kartice American Express na godinu ili davatelj usluge kojeg tvrtka American Express inače smatra trgovcem razine 1.

Davatelj usluge razine 2 – manje od 2,5 milijuna transakcija putem kartice American Express na godinu ili svi davatelji usluge koje tvrtka American Express ne smatra davateljima usluge razine 1.

Trgovac – odnosi se na trgovca i sve njegove pridružene tvrtke koje prihvaćaju karticu American Express u skladu s ugovorom s tvrtkom American Express i njezinim pridruženim tvrtkama.

Datum obavijesti odnosi se na datum na koji tvrtka American Express izdavateljima pošalje završnu obavijest o podatkovnom incidentu. Takav datum ovisi o tome kada tvrtka American Express zaprimi završno forenzičko izvješće ili rezultate interne analize i po vlastitoj ga prosudbi određuje tvrtka American Express.

Aplikacija za plaćanje ima značenje kako je navedeno u rječniku pojmova za aplikaciju za plaćanje u standardu za sigurnost podataka u industriji platnih kartica koji je dostupan na https://www.pcisecuritystandards.org.

PCI odobreno znači da se „uređaj za unos PIN-a" ili aplikaciju za plaćanje (ili oboje) u vrijeme uporabe nalaze na popisu odobrenih tvrtki i davatelja usluge koji održava PCI Security Standards Council, LLC, koji je dostupan na https://www.pcisecuritystandards.org.

PCI DSS odnosi se na standard za sigurnost podataka u industriji platnih kartica koji je dostupan na https://www.pcisecuritystandards.org.

PCI forenzički istražitelj, PFI odnosi se na subjekt koji je odobrilo Payment Card Industry Security Standards Council, LLC za vršenje forenzičkih istraga u slučaju kršenja ili kompromitiranja podataka platnih kartica.

Sigurnosni zahtjevi za PCI PIN odnosi se na sigurnosne zahtjeve za PIN u industriji platnih kartica koji je dostupan na https://www.pcisecuritystandards.org.

Uređaj za unos PIN-a ima značenje kako je navedeno u rječniku pojmova za sigurnost transakcija s PIN-om u industriji platnih kartica (PIN Transaction Security, PTS), točku interakcije (Point of Interaction, POI), zahtjeve za modularnu sigurnost, koji je dostupan na https://www.pcisecuritystandards.org.

Sustav točaka prodaje (Point of Sale, POS) odnosi se na sustav ili opremu za obradu informacija, uključujući terminal, osobno računalo, elektroničku blagajnu, beskontaktni čitač ili platni mehanizam ili postupak koji koristi trgovac za pribavljanje autorizacije ili prikupljanje podataka transakcije ili oboje.

Šifriranje od točke do točke (Point-to-Point Encryption, P2PE) odnosi se na rješenje koje kriprografski štiti podatke računa od točke u kojoj trgovac prihvaća platnu karticu do sigurne točke dešifriranja.

Procesor se odnosi na davatelja usluge koji trgovcu obavlja autorizaciju i obradu slanja u mrežu American Express.

Kvalificirani procjenitelj sigurnosti ili QSA, označava subjekt koji je kvalificiralo Payment Card Industry Security Standards Council, LLC za ovjeru ispunjavanja PCI DSS-a.

Tehnologija za izbjegavanje rizika – tehnološka rješenja koja unaprjeđuju sigurnost podataka vlasnika kartice American Express i osjetljivih podataka za provjeru autentičnosti, kao utvrđuje tvrtka American Express. Kako biste ispunjavali uvjete za uporabu tehnologije za izbjegavanje rizika, morate dokazati učinkovitu primjenu tehnologije u skladu s njezinim dizajnom i namjenom. Primjeru uključuju: EMV, šifriranje od točke do točke i tokenizacija.

Upitnik za samoprocjenu ili SAQ odnosi se na alat za samoprocjenu koji je izradilo Vijeće za standarde za sigurnost podataka u industriji platnih kartica, LLC, namijenjen procjeni i ovjeri sukladnosti s PCI DSS-om.

Osjetljivi podaci za provjeru autentičnosti imaju značenje navedeno u trenutačnom pojmovniku PCI DSS-a.

Davatelji usluge odnosi se na procesore, procesore trećih strana, davatelje usluge pristupnika, integratore POS sustava i sve druge davatelje usluga trgovcima ili POS sustavima ili druga rješenja ili usluge za obradu plaćanja.

Sažetak sukladnosti ili SOC odnosi se na PCI dokument za provjeru valjanosti koji koristi franšizodavac ili davatelj usluge za iskazivanje PCI statusa sukladnosti svojih zahvaćenih primatelja franšize.

Program za unaprjeđenje sigurnosne tehnologije (Security Technology Enhancement Program, STEP) odnosi se na program tvrtke American Express kojim se trgovci potiču na razvoj tehnologija koje unaprjeđuju sigurnost podataka. Kako bi zadovoljili uvjete za program STEP, trgovci ne smiju imati podatkovni incident u proteklih 12 mjeseci prije slanja godišnje ovjere za program STEP i moraju vršiti najmanje 75 % svih transakcija putem šifriranja od točke do točke ili osobnih transakcija putem EMV uređaja koji podržavaju čip.

Transakcija se odnosi na naplatu ili kredit izvršen putem kartice.

Dokumentacija za provjeru valjanosti odnosi se na AOC dobivenim u vezi s godišnjom procjenom sigurnosti na lokaciji ili SAQ-om, AOSC-om i izvršnim sažecima nalaza dobivenim u vezi s tromjesečnim skeniranjima mreže ili godišnjom ovjerom programa za unaprjeđenje sigurnosne tehnologije.