American Express
Data Security Operating Policy – Nederland

Als toonaangevende onderneming op het gebied van consumentenbescherming legt American Express zich er reeds lang op toe Kaarthouderinformatie te beschermen om ervoor te zorgen dat deze zodat deze informatie vertrouwelijk bewaard wordt.

Gecompromitteerde gegevens hebben een negatieve invloed op consumenten, Kaartaccepterende bedrijven, Serviceproviders en kaartuitgevende bedrijven Zelfs één incident kan de reputatie van een onderneming ernstige schade toebrengen en de mogelijkheden tot effectieve bedrijfsvoering beperken. Het beperken van dit risico door een beveiligingsbeleid te implementeren, kan het consumentenvertrouwen bevorderen, de winstgevendheid vergroten en de reputatie van een onderneming verbeteren.

*American Express erkent dat onze Kaartaccepterende bedrijven en Serviceproviders (gezamenlijk **u**) onze zorgen delen en vereist, als onderdeel van uw verantwoordelijkheden, dat u zich houdt aan de bepalingen betreffende gegevensbeveiliging in uw Overeenkomst voor de acceptatie (voor Kaartaccepterende bedrijven) of de verwerking (voor Serviceproviders) van de American Express®-kaart (voor beide respectievelijk de **Overeenkomst**) en deze Data Security Operating Policy, die wij mogelijk van tijd tot tijd aanpassen. Deze vereisten gelden voor al uw apparatuur, systemen en netwerken (en onderdelen daarvan) waarop Coderingssleutels, Kaarthouderinformatie en/of Gevoelige verificatiegegevens (of een combinatie daarvan) worden opgeslagen, verwerkt of verzonden.*

Termen die hier met een hoofdletter worden geschreven zonder bijgaande definitie, hebben de betekenis die daaraan wordt toegekend in de woordenlijst opgenomen aan het einde van dit document.

Paragraaf 1 – Normen voor de beveiliging van Coderingssleutels, Kaarthouderinformatie en Gevoelige verificatiegegevens

U en partijen waar u mee werkt dienen zorg te dragen dat:

- Kaarthouderinformatie alleen opgeslagen wordt ter vereenvoudiging van American Express-kaarttransacties conform en zoals vereist door de Overeenkomst;
- U voldoet aan de huidige versie van de Payment Card Industry Data Security Standard (***PCI DSS***) en PCI PIN Security Requirements, en dan niet later dan de ingangsdatum van de implementatie van die versie; en
- Op bemande locaties alleen door de PCI goedgekeurde nieuwe of vervangende Pinapparaten en/of Betaaltoepassingen gebruikt worden.

U dient alle American Express-Betalingsoverzichten en kredietoverzichten te beschermen die conform de Overeenkomsten in overeenstemming met deze bepalingen betreffende beveiliging van gegevens worden aangereikt; u dient deze overzichten alleen te gebruiken voor doeleinden die in deze Overeenkomst aan de orde komen en deze op gepaste wijze te beveiligen. U bent zowel financieel als anderszins aansprakelijk tegenover American Express om ervoor te zorgen dat uw Derde partijen zich houden aan deze bepalingen voor gegevensbeveiliging (naast aantonen dat uw Derde partijen zich aan dit beleid houden, zoals wordt beschreven in paragraaf 4 hieronder, tenzij anderszins bepaald in deze paragraaf).

Paragraaf 2 – Verplichtingen omtrent beheer van Gegevensincidenten

U dient American Express onmiddellijk op de hoogte te stellen binnen vierentwintig (24) uur nadat het Gegevensincident is ontdekt.

Indien u American Express op de hoogte wilt stellen, neemt u contact op met het American Express Enterprise Incident Response Program (***EIRP***). Dit kan telefonisch via +1 (602) 537-3021 ('+' duidt de internationale toegangscode aan, waar internationale belkosten gelden) of per e-mail via EIRP@aexp.com. U dient bij een dergelijk Gegevensincident iemand aan te wijzen als contactpersoon.

- U dient elk Gegevensincident te onderwerpen aan een grondig forensisch onderzoek. In geval van een Gegevensincident waarmee 10.000 of meer unieke American Express-kaartrekeningnummers zijn gemoeid (of op verzoek van American Express), dient dit onderzoek te worden uitgevoerd door een PCI Forensic Investigator (PFI) binnen vijf dagen nadat het Gegevensincident is ontdekt of zoals American Express naar eigen inzicht kan verzoeken. Het

onbewerkte rapport van forensisch onderzoek dient binnen tien werkdagen na voltooiing te worden verstrekt aan American Express. Indien vereist, kan American Express apart een PFI inschakelen om een onderzoek uit te voeren en de kosten van dit onderzoek voor u te beoordelen.

- U dient American Express direct te voorzien van alle Gecompromitteerde kaartnummers en het rapport van het forensisch onderzoek van het Gegevensincident. American Express behoudt zich het recht voor een eigen interne analyse uit te voeren om kaartnummers te identificeren die bij het Gegevensincident zijn betrokken.
- U dient met American Express samen te werken om alle problemen ten gevolgen van een Gegevensincident te rectificeren. Dit houdt onder meer in dat u met American Express dient te overleggen over uw communicatie met American Express-Kaarthouders op wie het Gegevensincident betrekking heeft; bovendien dient u aan American Express alle relevante informatie te verstrekken (en enige noodzakelijke ontheffingen te verkrijgen) om te verifiëren dat u toekomstige Gegevensincidenten kunt voorkomen op een wijze die in overeenstemming is met deze Overeenkomst.

Rapporten van het forensisch onderzoek dienen te worden opgesteld volgens de huidige Forensic Incident Final Report Template, die beschikbaar is bij PCI. Het PFI-rapport dient de volgende informatie te bevatten: forensische overzichten, nakomingsrapporten en alle andere informatie die betrekking heeft op het Gegevensincident. Bovendien dient in de rapporten de oorzaak van het Gegevensincident worden geïdentificeerd, er dient te worden vastgesteld of u ten tijde van het Gegevensincident heeft gehandeld conform de PCI DSS en er dient te worden geverifieerd of u in de toekomst Gegevensincidenten kunt voorkomen door (i) een plan op te nemen voor het oplossen van tekortkomingen op het vlak van PCI DSS en (ii) deel te nemen aan het nakomingsprogramma van American Express (zoals hieronder is beschreven). Op verzoek van American Express dient u een Qualified Security Assessor (*QSA*) te laten bevestigen dat de tekortkomingen zijn opgelost.

Onverminderd enige andersluidende verplichting met betrekking tot vertrouwelijkheid in de Overeenkomst heeft American Express het recht informatie over een Gegevensincident openbaar te maken aan American Express-Kaarthouders en -uitgevers, andere deelnemers van het American Express-netwerk en aan openbare instellingen, zoals vereist door toepasselijke wetgeving of door een juridisch(e), administratief(-ve) of wettelijk(e) bevel, verordening, dagvaarding, verzoek of ander proces om het risico van fraude, andere schade of anderszins zo klein mogelijk te maken, voor zover van toepassing op het gebruik van het American Express-netwerk.

Paragraaf 3 – Schadeloosstellingsverplichtingen voor een Gegevensincident

Uw schadeloosstellingsverplichtingen voor Gegevensincidenten richting American Express worden in de Overeenkomst bepaald in paragraaf 3, zonder afstand te nemen van andere rechten en rechtsmiddelen van American Express. In de volgende gevallen dient u aan American Express een boete voor niet-nakoming met betrekking tot een Gegevensincident te betalen:

- U heeft American Express niet onmiddellijk binnen vierentwintig (24) uur na ontdekking van een Gegevensincident hiervan op de hoogte gesteld.
- U heeft geen PFI ingeschakeld binnen vijf dagen nadat een Gegevensincident is ontdekt of op verzoek van American Express; of
- U heeft geen onbewerkt rapport van forensisch onderzoek ingediend binnen tien werkdagen nadat dit is voltooid.
- U heeft American Express niet alle Gecompromitteerde kaartnummers verstrekt.
- U heeft problemen die voortvloeien uit het Gegevensincident niet rechtgezet, met inbegrip van de verificatie of u toekomstige Gegevensincidenten kunt voorkomen.

Behalve een boete voor niet-nakoming met betrekking tot een Gegevensincident op basis van factoren in de voorgaande paragraaf vereist American Express verder geen schadeloosstelling.

Van u indien het Gegevensincident (a) minder dan 10.000 unieke Gecompromitteerde kaartnummers betreft of (b):

- U American Express op de hoogte heeft gesteld van het Gegevensincident conform paragraaf 2 van dit document,
- U ten tijde van het Gegevensincident heeft gehandeld conform de PCI DSS (zoals vastgesteld in het onderzoek van het Gegevensincident door de PFI) en
- Het Gegevensincident niet is veroorzaakt door foutief handelen van u of uw Derde partijen.

U bent als volgt aansprakelijk jegens American Express: Voor een Gegevensincident dat zich beperkt tot American Express-kaartrekeningnummers, dient u American Express direct te compenseren door middel van een boete voor niet-nakoming met betrekking tot het Gegevensincident, waarbij een maximum geldt van

USD 100.000 per Gegevensincident. Voor een Gegevensincident waarbij American Express-kaartrekeningnummers met Gevoelige verificatiegegevens zijn gemoeid, dient u American Express direct het volgende te compenseren:

- Een boete voor niet-nakoming van de regelgeving inzake een Gegevensincident, waarvoor een maximumboete van USD 100.000 per Gegevensincident geldt (zoals vastgesteld door American Express, waarbij rekening kan worden gehouden met aanvullende factoren naast de factoren in de tweede alinea in deze paragraaf);
- USD 5 per rekeningnummer (deze berekening is van toepassing op alle Gegevensincidenten die bij American Express zijn gemeld na 14 april 2016),

Voor de berekening hiervan telt American Express geen American Express-kaartrekeningnummers mee die betrokken waren bij een ander Gegevensincident met American Express-kaartrekeningnummers met Gevoelige verificatiegegevens, onder voorbehoud dat American Express binnen twaalf (12) maanden vóór de Notificatiedatum op de hoogte is gesteld van het andere Gegevensincident. Alle berekeningen die American Express met deze methodologie maakt, zijn definitief.

Schadeloosstellingsverplichtingen van Kaartaccepterende bedrijven voor Gegevensincidenten zoals hierin bepaald, worden niet beschouwd als incidentele schade, indirecte schade, speculatieve schade, gevolgschade, speciale schade, schade door strafmaatregelen of smartengeld op grond van deze Overeenkomst, mits dergelijke verplichtingen geen schade berokkenen die is gerelateerd aan of de aard heeft van inkomsten- of winstderving, verlies van goodwill of verlies van zakelijke mogelijkheden.

American Express kan naar eigen inzicht de schadeloosstellingsverplichtingen verlagen voor Kaartaccepterende bedrijven bij Gegevensincidenten die op of na 13 oktober 2017 zijn ontdekt en die voldoen aan alle onderstaande criteria:

- De toepasselijke Preventieve technologieën zijn gebruikt voorafgaand aan het Gegevensincident en werden toegepast tijdens de volledige Gegevensincidentperiode,
- Er wordt een gedegen onderzoek naar de maatstaven van het PFI-programma (Payment Card Industry Forensic Investigator) uitgevoerd (tenzij voorheen anderszins schriftelijk is overeengekomen),
- In het forensisch verslag wordt duidelijk vermeld welke Preventieve technologieën werden gebruikt om de gegevens te verwerken, op te slaan en/of te verzenden op het moment van het Gegevensincident, en
- U slaat geen Gevoelige verificatiegegevens of Kaarthoudergegevens op zonder te beveiligen (en heeft deze niet opgeslagen via de Gegevensincidentperiode)

Indien er een schadeloosstellingsverlaging beschikbaar is, wordt de verlaging op uw schadeloosstellingsverplichting als volgt vastgesteld:

Verlaging van schadeloosstellingsverplichting	Verplichte criteria
Standaardverlaging: 50%	>75% van totale aantal transacties die zijn verwerkt op apparaten met een chipfunctie[1] OF
	Preventieve technologie in gebruik op >75% van Kaartaccepterende bedrijfslocaties[2]
Extra verlaging: 75% tot 100%	>75% van alle transacties die zijn verwerkt op apparaten met een chipfunctie[1] EN een andere Preventieve technologie in gebruik op >75% van Kaartaccepterende bedrijfslocaties[2]

[1]Zoals vastgesteld door een interne analyse van American Express

[2]Zoals vastgesteld door een onderzoek van de PFI

- De extra verlaging (75% tot 100%) zal worden vastgesteld op basis van het percentage transacties op apparaten met een chipfunctie OF, indien lager, Kaartaccepterende bedrijfslocaties die een andere risicoverlagende technologie gebruiken. De onderstaande voorbeelden illustreren de berekening van de schadeloosstellingsverlaging.
- Indien u in aanmerking wilt komen voor Preventieve technologie, dient u aan te tonen dat de technologie effectief wordt toegepast in overeenstemming met het ontwerp en het beoogde doel. De installatie van apparaten met een chipfunctie en de verwerking van chipkaarten als transacties met een magnetische strip of een invoercode zijn geen voorbeelden van een effectieve toepassing van deze technologie.
  - Het percentage van uw locaties dat een Preventieve technologie gebruikt, wordt vastgesteld via een onderzoek van de PFI.
  - De verlaging van de schadeloosstellingsverplichting is niet van toepassing op boetes voor niet-nakoming in verband met het Gegevensincident

Bijv.:	Risicoverlagende technologieën in gebruik	In aanmerking voor extra verlaging van schadeloosstellingsverplichting?	Verlaging
1	80% van transacties op apparaten met een chipfunctie 0% van de locaties gebruikt een andere Preventieve technologie	Nee	50%: Standaardverlaging (minder dan 75% gebruik van Preventieve technologie komt niet in aanmerking voor extra verlaging)[1]
2	80% van transacties op apparaten met een chipfunctie 77% van de locaties gebruikt een andere Preventieve technologie	Ja	77%: Extra verlaging (gebaseerd op 77% gebruik van Preventieve technologie)
3	93% van transacties op apparaten met een chipfunctie 100% van de locaties gebruikt een andere Preventieve technologie	Ja	93%: Extra verlaging (gebaseerd op 93% van transacties op apparaten met een chipfunctie)
4	40% van transacties op apparaten met een chipfunctie 90% van de locaties gebruikt een andere Preventieve technologie	Nee	50%: Standaardverlaging (minder dan 75% van transacties op apparaten met een chipfunctie komt niet in aanmerking voor extra verlaging)

[1]Een Gegevensincident waarbij 10.000 American Express-kaartrekeningen zijn gemoeid, tegen USD 5 per rekeningnummer (10.000 x USD 5 = USD 50.000), kan in aanmerking komen voor een verlaging van 50%, waarmee de schadeloosheidsverplichtingen worden verlaagd van USD 50.000 naar USD 25.000, exclusief boetes voor niet-nakoming.

Paragraaf 4 – BELANGRIJK! Periodieke validering van uw systemen

U dient de volgende stappen te nemen om in overeenstemming met de PCI DSS om jaarlijks en elk kwartaal de status te valideren van apparatuur, systemen en/of netwerken (en de onderdelen daarvan) van u en uw franchisenemer waarop Kaarthouderinformatie of Gevoelige verificatiegegevens worden opgeslagen, verwerkt of verzonden, zoals hieronder wordt beschreven.

Er zijn vier stappen vereist voor een volledige validering:

Stap 1 – Deelnemen aan het nakomingsprogramma van American Express conform dit beleid.

Stap 2 – Uw niveau en valideringsvereisten begrijpen.

Stap 3 – De Valideringsdocumentatie invullen die u dient te verzenden naar American Express.

Stap 4 – De Valideringsdocumentatie verzenden naar American Express binnen de voorgeschreven deadlines.

Stap 1 – Deelnemen aan het nakomingsprogramma van American Express conform dit beleid

Kaartaccepterende bedrijven van niveau 1, Kaartaccepterende bedrijven van niveau 2 en alle Serviceproviders, zoals hieronder beschreven, dienen conform dit beleid te participeren aan het nakomingsprogramma van American Express door de volledige naam, het e-mailadres, het telefoonnummer en het fysieke postadres te verstrekken van een persoon die als algemeen contactpersoon voor gegevensbeveiliging zal dienen. U dient deze informatie in te dienen bij Trustwave, het bedrijf dat het programma namens American Express uitvoert, middels een van de methoden onder Stap 4 hieronder. U dient Trustwave op de hoogte te stellen indien deze informatie verandert, en waar van toepassing bijgewerkte informatie verstrekken.

American Express kan mogelijk naar eigen oordeel van bepaalde Kaartaccepterende bedrijven van niveau 3 en niveau 4 vereisen dat zij participeren aan het nakomingsprogramma van American Express conform dit beleid door hen schriftelijk in kennis te stellen. Het Kaartaccepterende bedrijf dient zich binnen 90 dagen vanaf ontvangst van de kennisgeving in te schrijven.

American Express kan de resultaten van uw PCI-valideringsproces controleren. Indien nodig kunt u op kosten van American Express een Qualified Security Assessor (QSA) naar uw keuze inschakelen.

Stap 2 – Uw niveau en valideringsvereisten begrijpen

Er zijn vier niveaus voor Kaartaccepterende bedrijven en twee niveaus voor Serviceproviders op basis van het aantal American Express-kaarttransacties. Voor een Kaartaccepterend bedrijf is dit het opgetelde volume dat is ingediend door diens vestigingen, welke op het hoogste klantniveau van het American Express-Kaartaccepterend bedrijf wordt samengevoegd.* U behoort tot een van de niveaus van de onderstaande tabellen voor Kaartaccepterende bedrijven en Serviceproviders.

BIP-transacties (Buyer Initiated Payments) worden niet in het aantal American Express-kaarttransacties

opgenomen voor het vaststellen van het niveau van het Kaartaccepterende bedrijf en de valideringsvereisten.

*In het geval van franchisegevers, omvat dit het aantal van de vestigingen van franchisenemers. Franchisegevers die opleggen dat franchisenemers een gespecificeerd Point of Sale-systeem (POS-systeem) of gespecificeerde Serviceprovider gebruiken, dienen ook Valideringsdocumentatie te verstrekken aan de betreffende franchisenemers.

Vereisten voor Kaartaccepterende bedrijven

Voor Kaartaccepterende bedrijven (niet voor Serviceproviders) zijn er vier mogelijke classificaties voor het niveau en de valideringsvereisten. Zodra u het niveau van het Kaartaccepterende bedrijf heeft vastgesteld aan de hand van de onderstaande lijst, raadpleegt u de tabel met Kaartaccepterende bedrijven om de vereisten van Valideringsdocumentatie vast te stellen.

- **Kaartaccepterend bedrijf van niveau 1** – 2,5 miljoen of meer American Express-kaarttransacties per jaar; of een Kaartaccepterend bedrijf dat anderszins naar het oordeel van American Express onder niveau 1 valt.
- **Kaartaccepterend bedrijf van niveau 2** – 50.000 tot 2,5 miljoen American Express-kaarttransacties per jaar.
- **Kaartaccepterend bedrijf van niveau 3** – 10.000 tot 50.000 miljoen American Express-kaarttransacties per jaar
- **Kaartaccepterend bedrijf van niveau 4 –** Minder dan 10.000 American Express-kaarttransacties per jaar.

Tabel met Kaartaccepterende bedrijven

	Valideringsdocumentatie		
Niveau van Kaartaccepterend bedrijf/jaarlijkse American Express-transacties	Nakomingsrapport (ROC) voor beoordeling ter plaatse	Enquête voor zelfbeoordeling (SAQ) EN driemaandelijkse netwerkscan	STEP-attest voor in aanmerking komende Kaartaccepterende bedrijven
Niveau 1/ 2,5 miljoen of meer	Verplicht	Niet van toepassing	Optioneel (vervangt ROC)
Niveau 2/ 50.000 tot 2,5 miljoen	Optioneel	SAQ verplicht (tenzij een beoordeling ter plaatse wordt ingediend). Scan verplicht bij bepaalde SAQ-typen	Optioneel (vervangt SAQ en netwerkscan of ROC)
Niveau 3/ 10.000 tot 50.000	Optioneel	SAQ optioneel (verplicht indien vereist door American Express). Scan verplicht bij bepaalde SAQ-typen	Optioneel (vervangt SAQ en netwerkscan of ROC)
Niveau 4/ 10.000 of minder	Optioneel	SAQ optioneel (verplicht indien vereist door American Express). Scan verplicht bij bepaalde SAQ-typen	Optioneel (vervangt SAQ en netwerkscan of ROC)

*Ter voorkoming van twijfel: Kaartaccepterende bedrijven van niveau 3 en niveau 4 hoeven geen Valideringsdocumentatie in te dienen, tenzij American Express hen daartoe naar eigen oordeel verplicht, maar dienen te voldoen aan en zijn aansprakelijk voor alle andere bepalingen van dit Data Security Operating Policy.

Programma voor verbeteringen van beveiligingstechnologie (STEP)

Kaartaccepterende bedrijven die voldoen aan PCI DSS, kunnen ook, naar het oordeel van American Express, in aanmerking komen voor het programma voor verbeteringen van beveiligingstechnologie (STEP) indien ze overal in hun kaartverwerkende omgeving bepaalde aanvullende beveiligingstechnologieën implementeren. STEP is uitsluitend van toepassing wanneer er bij het Kaartaccepterende bedrijf in de afgelopen twaalf maanden geen Gegevensincident heeft plaatsgevonden en wanneer 75% van alle kaarttransacties van Kaartaccepterende bedrijven wordt uitgevoerd met behulp van:

- **EMV** – op een actief chipapparaat met een geldige en actuele EMVCo-goedkeuring/-certificering (www.emvco.com) dat voor AEIPS geschikte transacties met Chipkaarten kan verwerken. (Amerikaanse Kaartaccepterende bedrijven dienen ook contactloos te gebruiken)
- **Point-to-Point-codering** (P2PE, Point to Point Encryption) – gecommuniceerd naar de processor van het Kaartaccepterende bedrijf met behulp van een door de PCI-SSC of QSA goedgekeurd point-to-point-coderingssysteem

Voor Kaartaccepterende bedrijven die in aanmerking komen voor het programma voor verbeteringen van beveiligingstechnologie zijn verlaagde vereisten voor te valideren PCI-documentatie van toepassing, zoals hieronder beschreven in stap 3.

Vereisten voor Serviceproviders

Voor Serviceproviders (niet voor Kaartaccepterende bedrijven) zijn er twee mogelijke classificaties voor het niveau en de valideringsvereisten. Zodra u het niveau van de Serviceprovider heeft vastgesteld aan de hand van de

onderstaande lijst, raadpleegt u de tabel met Serviceproviders om de vereisten van Valideringsdocumentatie vast te stellen.

Serviceprovider van niveau 1 – 2,5 miljoen of meer American Express-kaarttransacties per jaar; of een Serviceprovider die naar het oordeel van American Express onder niveau 1 valt.

Serviceprovider van niveau 2 – minder dan 2,5 miljoen American Express-kaarttransacties per jaar; en elke andere Serviceprovider die naar het oordeel van American Express niet onder niveau 1 valt.

Serviceproviders komen niet in aanmerking voor het programma voor verbeteringen van beveiligingstechnologie.

Tabel met Serviceproviders

Niveau	Valideringsdocumentatie	Vereiste
1	Jaarlijks rapport van beveiligingstoetsing op locatie	Verplicht
2	Jaarlijkse Enquête voor zelfbeoordeling D (Serviceprovider) en driemaandelijkse netwerkscan OF desgewenst jaarlijks nakomingsrapport van beveiligingstoetsing op locatie	Verplicht

Het wordt aanbevolen dat Serviceproviders ook voldoen aan de aanvullende validering van aangewezen entiteiten door de PCI

Stap 3 – De Valideringsdocumentatie invullen die u dient te verzenden naar American Express

De volgende documenten zijn verplicht voor verschillende niveaus van Kaartaccepterende bedrijven en Serviceproviders, zoals weergegeven in de tabel met Kaartaccepterende bedrijven en de tabel met Serviceproviders hierboven.

Jaarlijkse beveiligingstoetsing op locatie – De jaarlijkse beveiligingstoetsing op locatie is een gedetailleerde inspectie op locatie van uw apparatuur, systemen en netwerken (en de onderdelen daarvan) waarop Kaarthouderinformatie en/of Gevoelige verificatiegegevens worden opgeslagen, verwerkt of verzonden. De beoordeling dient te worden uitgevoerd door

- een QSA of
- u en officieel worden bevestigd door uw Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer of Principal Officer en jaarlijks worden ingediend bij American Express voor het desbetreffende Attest van nakoming (AOC).

Het AOC dient de nakoming aan te tonen van alle vereisten van de PCI DSS en op verzoek kopieën van het volledige nakomingsrapport opnemen (Kaartaccepterende bedrijven van niveau 1 en Serviceproviders van niveau 1).

Jaarlijkse Enquête voor zelfbeoordeling– De jaarlijkse zelfbeoordeling is een proces waarbij de Enquête voor zelfbeoordeling (***SAQ***) van PCI DSS wordt gebruikt en waarmee u zelf een inspectie kunt uitvoeren van uw apparatuur, systemen en netwerken (en de onderdelen daarvan) waarop u Kaarthouderinformatie en/of Gevoelige verificatiegegevens opslaat, verwerkt of verzendt. Deze toetsing dient te worden uitgevoerd door u en officieel worden bevestigd door uw Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer of Principal Officer. Het AOC-gedeelte van de SAQ dient jaarlijks te worden ingediend bij American Express. Het AOC-gedeelte van de SAQ dient de nakoming aan te tonen van alle vereisten van de PCI DSS en op verzoek kopieën bevatten van de volledige SAQ (Kaartaccepterende bedrijven van niveau 2, niveau 3 en niveau 4; Serviceproviders van niveau 2).

Driemaandelijkse netwerkscan – De driemaandelijkse netwerkscan is een proces waarmee op afstand uw met internet verbonden computernetwerken en webservers worden getest op potentiële zwaktes en kwetsbaarheden. Deze dient te worden uitgevoerd door een goedgekeurde scanprovider (***ASV***). U dient elk kwartaal het Scanrapport met attest van nakoming van scanregels van de ASV (***AOSC***) of de executive summary van de bevindingen van de scan (en op aanvraag kopieën van de volledige scan) te voltooien en in te dienen bij American Express. Uit de AOSC of executive summary dient te blijken dat de resultaten voldoen aan de PCI DSS-scanprocedures, dat er geen grote risico's zijn geïdentificeerd en dat de scan voldoet aan de regels (alle Kaartaccepterende bedrijven, behalve degenen die ook een rapport van beveiligingstoetsing op locatie indienen, Kaartaccepterende bedrijven die voor STEP in aanmerking komen, en alle Serviceproviders). Ter voorkoming van twijfel: driemaandelijkse netwerkscans zijn verplicht indien ze vereist zijn volgens de Enquête voor zelfbeoordeling.

Valideringsdocumentatie voor het jaarlijkse attest van het programma voor verbeteringen van beveiligingstechnologie (STEP) – Het jaarlijkse STEP-kwalificatieattest van American Express ('STEP-attest') is alleen beschikbaar voor Kaartaccepterende bedrijven die voldoen aan de criteria in stap 2 hierboven. Het STEP-attest omvat een proces waarbij de PCI DSS-vereisten worden gebruikt en waarmee u zelf een inspectie kunt uitvoeren van uw apparatuur, systemen en netwerken (en de onderdelen daarvan) waarop Kaarthouderinformatie en/of Gevoelige

verificatiegegevens worden opgeslagen, verwerkt of verzonden. Deze toetsing dient te worden uitgevoerd door u en officieel worden bevestigd door uw Chief Executive Officer, Chief Financial Officer, Chief Information Security Officer of Principal Officer. U dient het proces te voltooien door het STEP-attestformulier jaarlijks in te dienen bij American Express. (Alleen Kaartaccepterende bedrijven die in aanmerking komen voor STEP.) Het document voor het jaarlijkse attest van het programma voor verbeteringen van beveiligingstechnologie is beschikbaar op www.trustwave.com.

Samenvatting van nakoming – De Samenvatting van nakoming ('SOC', Summary of Compliance) is een document waarmee een franchisegever of Serviceprovider de PCI-nakomingsstatus van zijn franchisenemers kan verwerken. Het SOC-sjabloon kan worden gedownload via de veilige portal van Trustwave.

Niet-nakoming van PCI DSS – Indien u niet voldoet aan de PCI DSS, dient u een van de volgende documenten in te dienen:

- een Attest van nakoming (AOC), met inbegrip van deel 4, Actieplan in geval van niet-nakoming
- een Geprioriteerde aanpaksamenvatting en Attest van nakoming van de PCI DSS (PASAOC)
- een projectplansjabloon (kan worden gedownload via de veilige portal van Trustwave)

In elk van de bovenstaande documenten dient u aan te geven op welke datum het probleem is verholpen. Deze datum dient voor succesvolle nakoming binnen twaalf maanden van de datum van het document te liggen. U dient het betreffende document in te dienen bij American Express middels een van de methoden onder stap 4 hieronder. U dient American Express periodiek op de hoogte te houden van uw voortgang met betrekking tot het oplossen van de niet-nakoming (Kaartaccepterende bedrijven van niveau 1, niveau 2 en niveau 4; alle Serviceproviders). Ter voorkoming van twijfel: Kaartaccepterende bedrijven die niet aan PCI DSS voldoen, komen niet in aanmerking voor het programma voor verbeteringen van beveiligingstechnologie (STEP).

American Express legt u geen boetes voor niet-nakoming op (zoals hieronder beschreven) voor zover het niet naleven betrekking heeft tot de periode vóór de gestelde vervaldatum. U blijft echter aansprakelijk tegenover American Express voor alle schadeloosstellingsverplichtingen voor een Gegevensincident en u bent onderhevig aan alle andere bepalingen in dit beleid.

Stap 4 – De Valideringsdocumentatie verzenden naar American Express

Alle Kaartaccepterende bedrijven en Serviceproviders dienen de Valideringsdocumentatie in te dienen die in de tabellen van stap 2 zijn gemarkeerd als 'verplicht'.

U dient uw Valideringsdocumentatie volgens een van de volgende methoden in te dienen bij Trustwave:

Beveiligde portal: Valideringsdocumentatie kan worden geüpload via de veilige portal van Trustwave op https://login.trustwave.com.

Neem contact op met Trustwave door te bellen naar +1 (312) 267-3208 ('+' duidt de internationale toegangscode aan; internationale gesprekskosten zijn van toepassing) of een e-mail te sturen naar AmericanExpressCompliance@trustwave.com voor instructies over het gebruik van deze portal.

Beveiligde fax: Valideringsdocumentatie kan per fax worden verzonden naar: +1 (312) 276-4019. ('+' duidt de internationale toegangscode aan; internationale gesprekskosten zijn van toepassing). Geef uw naam, bedrijfsnaam, de naam van uw contactpersoon voor gegevensbeveiliging, uw adres en telefoonnummer op. Kaartaccepterende bedrijven dienen ook hun tiencijferige American Express Merchant-aansluitnummer op te geven.

Indien u algemene vragen heeft over het programma of het bovenstaande proces, kunt u contact opnemen met Trustwave door te bellen naar +1 (312) 267-3208 (+ geeft de internationale toegangscode aan; internationale gesprekskosten zijn van toepassing) of een e-mail te sturen naar AmericanExpressCompliance@trustwave.com.

Nakoming en validering geschieden op uw kosten. Door Valideringsdocumentatie in te dienen geeft u aan en garandeert u American Express dat u gemachtigd bent de informatie daarin bekend te maken en dat u de Valideringsdocumentatie aan American Express verstrekt zonder de rechten van derden te schenden.

Boetes en beëindiging van de Overeenkomst bij niet valideren

American Express heeft het recht u boetes op te leggen voor niet valideren en de Overeenkomst te beëindigen indien u niet voldoet aan deze vereisten of niet vóór de gestelde deadline de verplichte Valideringsdocumentatie verstrekt aan American Express. American Express stelt u afzonderlijk op de hoogte van de deadlines voor elke jaarlijkse en driemaandelijkse rapportageperiode.

Beschrijving (Valuta EUR (€))	Kaartaccepterend bedrijf van niveau 1 of Serviceprovider van niveau 1	Kaartaccepterend bedrijf van niveau 2, Serviceprovider van niveau 2 of STEP-Kaartaccepterend bedrijf	Kaartaccepterend bedrijf van niveau 3 of niveau 4
Er wordt een boete voor niet valideren vastgesteld als de Valideringsdocumentatie niet wordt ontvangen voor de eerste deadline.	€19.000	€4.000	
Er wordt een extra boete voor niet valideren vastgesteld als de Valideringsdocumentatie niet wordt ontvangen binnen 30 dagen na de eerste deadline.	€26.000	€7.500	€15 per maand
Er wordt een extra boete voor niet valideren vastgesteld als de Valideringsdocumentatie niet wordt ontvangen binnen 60 dagen na de eerste deadline.	€34.000	€11.000	

Lokale valuta

Indien American Express uw verplichte Valideringsdocumentatie niet binnen 60 dagen van de eerste deadline ontvangt, heeft American Express het recht de Overeenkomst te beëindigen in overeenstemming met de voorwaarden en u de bovenstaande cumulatieve boetes voor niet valideren op te leggen.

Paragraaf 5 – Vertrouwelijkheid

American Express zal redelijke maatregelen treffen om gedurende een periode van drie jaar vanaf de ontvangstdatum uw nakomingsrapporten, inclusief de Valideringsdocumentatie, vertrouwelijk te houden (en ervoor te zorgen dat agenten en onderaannemers van American Express, inclusief Trustwave, dat ook doen) en de Valideringsdocumentatie niet openbaar te maken aan een derde partij (anders dan gelieerde bedrijven, agenten, vertegenwoordigers, Serviceproviders en onderaannemers van American Express). Deze vertrouwelijkheidsverplichting geldt niet op Valideringsdocumentatie die:

i. Al vóór bekendmaking bekend was bij American Express;
ii. Zonder inbreuk van deze paragraaf door American Express openbaar toegankelijk is of wordt;
iii. Door American Express rechtmatig is ontvangen van een derde partij zonder vertrouwelijkheidsverplichting;
iv. Onafhankelijk is ontwikkeld door American Express; of
v. Verplicht bekend dient te worden gemaakt wegens een gerechtelijk bevel, bevel van een overheidsinstantie, wegens een wet, regel, dagvaarding, verzoek voor inzage van stukken, sommering of ander bestuursproces of juridische proces of wegens een formeel of informeel onderzoek door een overheidsinstantie (inclusief toezichthouders, inspecteurs of wetshandhavingsinstanties).

Paragraaf 6 – Disclaimer

AMERICAN EXPRESS NEEMT HIERBIJ AFSTAND VAN ENIGE EN ALLE VOORSTELLINGEN, GARANTIES EN AANSPRAKELIJKHEDEN MET BETREKKING TOT DEZE DATA SECURITY OPERATING POLICY, DE PCI DSS, DE EMV-SPECIFICATIES EN DE AANDUIDING EN PRESTATIES VAN QSA's, ASV's EN PFI's, ZOWEL UITDRUKKELIJK, IMPLICIET, KRACHTENS DE WET ALS ANDERSZINS, INCLUSIEF ENIGE GARANTIE MET BETREKKING TOT DE VERHANDELBAARHEID OF GESCHIKTHEID VOOR EEN SPECIFIEK DOEL. UITGEVERS VAN AMERICAN EXPRESS-KAARTEN ZIJN IN DIT BELEID GEEN BEGUNSTIGDEN.

Nuttige websites

American Express-gegevensbeveiliging:

http://www.americanexpress.com/datasecurity

PCI Security Standards Council, LLC:

http://www.pcisecuritystandards.org

Woordenlijst

Uitsluitend voor dit beleid zijn de volgende definities van toepassing:

American Express-kaart of kaart betekent elk(e) kaart, apparaat voor rekeningtoegang of betaalapparaat of -service met de naam, het logo, het handelsmerk, het dienstmerk, de handelsnaam of andere bedrijfseigen ontwerpen of aanduidingen van American Express of een van diens gelieerde bedrijven die/dat is uitgegeven door een uitgever of een kaartrekeningnummer

Attest van nakoming (of AOC) betekent een verklaring over de status van uw nakoming van de PCI DSS in de vorm die is

bepaald door de Payment Card Industry Security Standards Council, LLC.

Goedgekeurde oplossing voor point-to-point-codering (P2PE), inbegrepen in de PCI SSC-lijst van gevalideerde oplossingen of gevalideerd door een PCI SSC Qualified Security Assessor P2PE-bedrijf.

Goedgekeurde scanprovider (of ASV) betekent een entiteit die volgens de Payment Card Industry Security Standards Council, LLC gekwalificeerd is voor de validering van nakoming van specifieke PCI DSS-vereisten door kwetsbaarheidsscans uit te voeren op omgevingen die in contact staan met internet.

Attest van nakoming van scanregels (of AOSC) betekent een nakoming over de status van uw nakoming van de PCI DSS op basis van een netwerkscan in de vorm die is bepaald door de Payment Card Industry Security Standards Council, LLC.

Kaarthouderinformatie heeft de betekenis die de term 'Cardholder Data' kreeg in de toen actuele verklarende woordenlijst van de PCI DSS.

Kaarthouder betekent een persoon of entiteit (i) die of dat een overeenkomst is aangegaan waarin een kaartrekening is gemaakt bij een uitgever of (ii) wiens naam op de kaart staat.

Kaarthouderinformatie betekent informatie over American Express-Kaarthouders en kaarttransacties, inclusief namen, adressen, kaartrekeningnummers en kaartidentificatienummers (CID's).

Betaling betekent een betaling of aankoop die met de kaart wordt gedaan.

Chip betekent een microchip die in de kaart is geïntegreerd en die Kaarthouderinformatie en rekeninginformatie bevat.

Chipkaart betekent een kaart met een Chip waarvoor mogelijk een pincode nodig is om de identiteit van de Kaarthouder en/of de rekeninginformatie op de Chip te verifiëren (in onze documentatie ook wel 'smartcard', 'EMV-kaart', 'ICC' (integrated circuit card) genoemd).

Chipapparaat betekent een apparaat op een Point of Sale met een geldige en actuele EMVCo-goedkeuring/-certificering (www.emvco.com) dat voor AEIPS geschikte transacties met Chipkaarten kan verwerken.

Gecompromitteerd kaartnummer betekent een American Express-kaartrekeningnummer dat betrokken is bij een Gegevensincident.

Derde partijen betekent al uw werknemers, agenten, vertegenwoordigers, subcontractanten, Processors, Serviceproviders, leveranciers van uw Point of Sale-apparatuur of -systemen of oplossingen voor de verwerking van betalingen, entiteiten die zijn gekoppeld aan uw bedrijfsaccount van American Express, plus elke andere partij die u toegang tot Kaarthouderinformatie en/of Gevoelige verificatiegegevens geeft conform de Overeenkomst.

Krediet betekent het bedrag van de Betaling dat u terugstort aan Kaarthouders voor aankopen of betalingen die met de kaart zijn gedaan.

Gegevensincident betekent een incident waarbij coderingssleutels van American Express zijn of vermoedelijk zijn betrokken, of ten minste één American Express-kaartrekeningnummer waarbij sprake is van:

- Ongeautoriseerd(e) toegang of gebruik van Coderingssleutels, Kaarthouderinformatie en/of Gevoelige verificatiegegevens (of een combinatie daarvan) die worden opgeslagen, verwerkt of verzonden op apparatuur, systemen en/of netwerken (of de onderdelen daarvan) van u of waarvan u het gebruik oplegt;
- Gebruik van deze Coderingssleutels, Kaarthouderinformatie en/of Gevoelige verificatiegegevens (of een combinatie daarvan) dat niet in overeenstemming is met de Overeenkomst; en/of
- Vermoed(e) of bevestigd(e) verlies, diefstal of verduistering op welke wijze dan ook van enige media, materialen, records of informatie die deze Coderingssleutels, Kaarthouderinformatie en/of Gevoelige verificatiegegevens bevatten (of een combinatie daarvan).

Gegevensincidentperiode betekent de periode die begint op de datum van de betrokkenheid of de periode vanaf 365 dagen vóór de Notificatiedatum indien de feitelijke datum van de betrokkenheid onbekend is. De Gegevensincidentperiode betekent de periode vanaf 365 dagen vóór de Notificatiedatum tot 30 dagen na de Notificatiedatum.

EMV-specificaties betekent de specificaties die zijn uitgegeven door EMVCo, LLC; deze zijn beschikbaar op http://www.emvco.com.

EMV-transactie betekent een transactie met een chipkaart (ook wel 'IC-kaart', 'integrated circuit card', 'smartcard', 'EMV-kaart' of 'ICC' genoemd) die wordt uitgevoerd bij een terminal van een Point of Sale (POS) die geschikt is voor chipkaarten en van een geldig en actueel goedgekeurd EMV-type is. Goedgekeurde EMV-typen vindt u op http://www.emvco.com.

Coderingssleutel (Coderingssleutel van American Express) **betekent** een sleutel die wordt gebruikt bij het verwerken, genereren, laden en/of beveiligen van rekeninggegevens. Dit omvat maar is niet beperkt tot:

- Sleutelcoderingssleutels (KEK's, Key Encryption Keys): Zonehoofdsleutels (ZMK's, Zone Master Keys) en zonepincodesleutels (ZPK's, Zone PIN Keys)
- Hoofdsleutels die worden gebruikt in veilige cryptografische apparaten: Lokale hoofdsleutels (LMK's, Local Master Keys)
- Kaartbeveiligingscodesleutels (CSCK's, Card Security Code Keys)
- Pincodesleutels: basisderivatiesleutels (BDK's, Base Derivation Keys), pincodecoderingssleutels (PEK's, PIN Encryption Key) en ZPK's

Forensic Incident Final Report Template betekent de sjabloon die de PCI Security Standards Council beschikbaar heeft gesteld op https://www.pcisecuritystandards.org.

Franchisenemer betekent een derde partij in onafhankelijk eigendom en beheer (met inbegrip van een franchisenemer, licentiehouder of afdeling), behalve een Gelieerde onderneming waaraan een Franchisegever een franchiselicentie is verstrekt en die een schriftelijke overeenkomst met de Franchisegever

heeft gesloten en daarbij zichzelf steeds in het openbaar identificeert met Merken van de Franchisegever of zichzelf naar het publiek toe presenteert als lid van de bedrijvengroep van de Franchisegever.

Franchisegever betekent de operator van een bedrijf die personen of entiteiten (Franchisenemers) licentie verstrekt om onder het merk van de operator goederen en/of diensten te verstrekken of onder dit merk werkzaam te zijn. De Franchisegever biedt ondersteuning bij de uitvoering van bedrijfsactiviteiten of beïnvloedt de werkmethode van de Franchisenemer en vereist betaling van de Franchisenemer.

Kaartaccepterend bedrijf van niveau 1 – 2,5 miljoen of meer American Express-kaarttransacties per jaar; of een Kaartaccepterend bedrijf dat naar het oordeel van American Express onder niveau 1 valt.

Kaartaccepterend bedrijf van niveau 2 – 50.000 tot 2,5 miljoen American Express-kaarttransacties per jaar.

Kaartaccepterend bedrijf van niveau 3 – 10.000 tot 50.000 miljoen American Express-kaarttransacties per jaar.

Kaartaccepterend bedrijf van niveau 4 – Minder dan 10.000 American Express-kaarttransacties per jaar.

Serviceprovider van niveau 1 – 2,5 miljoen of meer American Express-kaarttransacties per jaar; of een Serviceprovider die naar het oordeel van American Express onder niveau 1 valt.

Serviceprovider van niveau 2 – minder dan 2,5 miljoen American Express-kaarttransacties per jaar; en elke andere Serviceprovider die naar het oordeel van American Express niet onder niveau 1 valt.

Kaartaccepterend bedrijf - betekent het Kaartaccepterende bedrijf en al zijn gelieerde bedrijven die American Express-kaarten accepteren onder een Overeenkomst met American Express of zijn gelieerde bedrijven.

Notificatiedatum betekent een door American Express vastgestelde datum waarop uitgevers een melding ontvangen van het Gegevensincident. Deze datum hangt af van de ontvangst door American Express van het definitieve forensische verslag of de interne en zal volledig naar het oordeel van American Express worden vastgesteld.

Betaaltoepassing heeft de betekenis die de term 'Payment Application' kreeg in de toen actuele verklarende woordenlijst van de Payment Card Industry Payment Application Data Security Standard; deze vindt u op https://www.pcisecuritystandards.org.

Door de PCI goedgekeurd betekent dat een Pinapparaat en/of Betaaltoepassing ten tijde van het gebruik op de lijst staat met goedgekeurde bedrijven en leveranciers die wordt onderhouden door de PCI Security Standards Council, LLC; deze is beschikbaar op https://www.pcisecuritystandards.org.

PCI DSS staat voor de Payment Card Industry Data Security Standard; deze is beschikbaar op https://www.pcisecuritystandards.org.

PCI Forensic Investigator (PFI) betekent een entiteit die is goedgekeurd door de Payment Card Industry Security Standards Council, LLC voor het uitvoeren van forensisch onderzoek naar een lek of gecompromitteerde betaalkaartgegevens.

PCI PIN Security Requirements betekent de vereisten van de Payment Card Industry voor pincodebeveiliging; deze zijn beschikbaar op https://www.pcisecuritystandards.org.

Pinapparaat heeft de betekenis die de term 'PIN Entry Device' kreeg in de toen actuele verklarende woordenlijst van de Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements; deze is beschikbaar op https://www.pcisecuritystandards.org.

Point of Sale-systeem (POS-systeem) betekent een systeem of apparaat voor informatieverwerking, waaronder een terminal, pc, elektronische kassa, contactvrije scanner of betaalautomaat of -proces, gebruikt door een Kaartaccepterend bedrijf om autorisatie te verkrijgen en/of transactiegegevens te verzamelen.

Point-to-point-codering (P2PE) betekent een oplossing die cryptografische bescherming biedt voor rekeninggegevens vanaf het punt waar een Kaartaccepterend bedrijf de betaalkaart accepteert naar een veilig punt voor decodering

Processor betekent een Serviceprovider voor Kaartaccepterende bedrijven die verwerking van autorisatie en indiening biedt aan het American Express-netwerk.

Qualified Security Assessor (QSA) betekent een entiteit die door de Payment Card Industry Security Standards Council, LLC is gekwalificeerd voor het valideren van nakoming van de PCI DSS.

Preventieve technologie betekent technologieoplossingen waarmee de veiligheid van de gegevens en Gevoelige verificatiegegevens van American Express-kaarthouders wordt verbeterd, zoals wordt vastgesteld door American Express. Indien u in aanmerking wilt komen als Preventieve technologie, dient u aan te tonen dat de technologie effectief wordt toegepast in overeenstemming met het ontwerp en het beoogde doel. Voorbeelden zijn: EMV, point-to-point-codering en tokenisatie.

Enquête voor zelfbeoordeling (SAQ) betekent een hulpmiddel voor zelfbeoordeling dat is ontwikkeld door de Payment Card Industry Security Standards Council, LLC en dat is bestemd voor het evalueren en attesteren van nakoming van de PCI DSS.

Gevoelige verificatiegegevens heeft de betekenis die de term 'Sensitive Authentication Data' kreeg in de toen actuele verklarende woordenlijst van de PCI DSS.

Serviceprovider betekent een geautoriseerde processor, externe processor, gatewayleverancier, integratoren van POS-systemen of een andere entiteit die aan Kaartaccepterende bedrijven van POS-systemen of andere oplossingen of services voor de verwerking van betalingen levert.

Samenvatting van nakoming of SOC betekent een te valideren PCI-document gebruikt door een franchisegever om de PCI-nakomingsstatus van zijn betreffende franchisenemers aan te duiden.

Programma voor verbeteringen van beveiligingstechnologie (STEP) betekent het programma van American Express waarin Kaartaccepterende bedrijven worden gestimuleerd

technologieën in te zetten die gegevensbeveiliging verbeteren. Indien Kaartaccepterende bedrijven in aanmerking willen komen voor STEP, mogen ze geen Gegevensincident hebben gehad in de twaalf maanden voorafgaand aan de indiening van het jaarlijkse STEP-attest en dienen ze minimaal 75% van alle transacties uit te voeren via point-to-point-codering of persoonlijke transacties op een EMV-apparaat met chipfunctie.

Transactie betekent een betaling of krediet die of dat wordt voltooid met een kaart.

Valideringsdocumentatie betekent het AOC dat is opgesteld in verband met een jaarlijkse beveiligingstoetsing op locatie of SAQ, het AOSC en executive summary's van de bevindingen die zijn opgesteld in verband met driemaandelijkse netwerkscans of het jaarlijkse attest van het programma voor verbeteringen van beveiligingstechnologie.