AMERICAN EXPRESS

Retningslinjer for Datasikkerhet (DSOP)

AMERICAN EXPRESS

DSOP Sammendrag av endringer

Ikoner

Viktige oppdateringer er oppført i Tabellen over Sammendrag av Endringer, og er også angitt i *DSOP* med en endringsbar. En endringsbar er en vertikal linje, vanligvis i venstre marg, som identifiserer tekst som er lagt til eller revidert. Kun vesentlige endringer i *DSOP* med potensielle virkninger på en Forhandlers driftsprosedyrer er angitt med en endingsbar som vist i venstre marg.

Tekst som er fjernet er fremhevet med et søppelkurvikon i margen ved siden av vesentlige slettinger, inkludert punkter, tabeller, avsnitt, merknader og kulepunkter. Fjernet tekst er i dette Sammendraget av Endringer referert til ved hjelp av punktnummerering fra den forrige publikasjonen for å unngå forvirring.

Blå linjer på grensen til avsnitt indikerer regionsspesifikk informasjon.

Tabell over Sammendrag av Endringer

Viktige oppdateringer er oppført i følgende tabell og er også angitt i *DSOP* med en endringsbar.

Punkt/Underavsnitt	Endringsbeskrivelse
Det er ingen endringer for denne utgivelsen.	

Punkt 1 Introduksjon til DSOP og Beskyttelsesstandarder

Som ledende innen forbrukerbeskyttelse, har American Express en langvarig forpliktelse til å beskytte Kortholderdata og Sensitive autentiseringsdata, slik at de holdes sikre.

Kompromitterte data påvirker forbrukere, Forhandlere, Tjenesteleverandører og kortutstedere negativt. Selv bare én enkelt hendelse kan alvorlig skade et selskaps omdømme og svekke dets evne til effektivt å drive forretninger. Å håndtere denne trusselen ved å implementere retningslinjer for driftssikkerhet, kan bidra til å bedre kundetillit, øke lønnsomheten og forbedre et selskaps omdømme.

American Express vet at våre Forhandlere og Tjenesteleverandører (samlet du) deler vår bekymring og krever, som en del av ditt ansvar, at **du** overholder retningslinjene for datasikkerhet i ditt samtykke til å akseptere (når det gjelder Forhandlere) eller behandle (når det gjelder Tjenesteleverandører) American Express®-kortet (henholdsvis **Avtalen**) og disse Retningslinjer for Datasikkerhet (DSOP), som vi kan endre fra tid til annen. Disse kravene gjelder alt utstyr, systemer og nettverk (og deres komponenter) der krypteringsnøkler, Kortholderdata eller Sensitive autentiseringsdata (eller en kombinasjon av disse) lagres, behandles eller overføres.

Begreper skrevet med store forbokstaver, men som ikke er definert her, har betydningen som er tilskrevet dem i ordlisten på slutten av disse retningslinjene.

Retningslinjer for Datasikkerhet (DSOP) er en rekke omfattende retningslinjekrav som er utformet for å beskytte Kontodata i forbindelse med lagring, behandling og overføring.

American Express krever at alle Forhandlere og Tjenesteleverandører er i samsvar med Payment Card Industry Security Standard (PCI DSS). Som del av dette kravet, må du sørge for at dine Berørte parter:

- Lagrer Kortholderdata utelukkende for gjennomføring av American Express-korttransaksjoner i samsvar med og i henhold til kravene i Avtalen.
- Overholder gjeldende PCI DSS-krav og andre PCI Security Standards Council (PCI-SSC)-krav som gjelder behandling, lagring eller overføring av Krypteringsnøkler, Kortholderdata eller Sensitive autentiseringsdata, senest fra ikrafttredelsesdatoen for implementering av gjeldende krav.
- Sørger for at PCI-godkjente produkter brukes ved utrulling eller erstatning av teknologi for lagring, behandling eller overføring av data.

Du skal beskytte alle American Express Belastningsoversikter og Krediteringsoversikter, som oppbevares i henhold til Avtalen, i samsvar med disse datasikkerhetsbestemmelsene. Disse dokumentene skal bare brukes i samsvar med formålene som er fastsatt i Avtalen og beskyttes tilsvarende. Du er økonomisk, og på annen måte, ansvarlig overfor American Express for å sikre at de Berørte partene overholder disse datasikkerhetsbestemmelsene (i tillegg til å demonstrere de Berørte partenes overholdelse av disse retningslinjene i henhold til Punkt 2, «PCI DSS-samsvarsprogram (Viktig Regelmessig Validering av Systemene dine)», med mindre annet er avtalt under dette punktet). Detaljer angående PCI-standardene, og hvordan du overholder kravene, er tilgjengelig på www.pcisecuritystandards.org.

Punkt 2 PCI DSS-samsvarsprogram (Viktig Regelmessig Validering av Systemene dine)

For å godkjennes i samsvar med PCI DSS må du årlig og hver 90. dag utføre følgende tiltak for å validere statusen for ditt og dine Franchisetakeres utstyr, systemer og/eller nettverk (og deres komponenter) der Kortholderdata eller Sensitive autentiseringsdata lagres, behandles eller overføres.

Det kreves fire tiltak for å fullføre valideringen:

- Tiltak 1: Deltakelse i American Express' PCI-samsvarsprogram i henhold til disse retningslinjene.
- Tiltak 2: Forstå ditt Forhandler-Tjenesteleverandørnivå og dine krav til Valideringsdokumentasjon.
- Tiltak 3: Fullføre Valideringsdokumentasjonen som du skal sende til American Express.
- Tiltak 4: Sende Valideringsdokumentasjonen til American Express innen den fastsatte fristen.

Tiltak 1: Deltakelse i American Express' Samsvarsprogram i henhold til disse Retningslinjene

Forhandlere på Nivå 1 og 2, og alle Tjenesteleverandører, som beskrevet nedenfor, må delta i Programmet under disse retningslinjene. American Express kan, etter eget skjønn, peke ut spesifikke Nivå 3 og Nivå 4-Forhandlere for å delta i Programmet under disse retningslinjene.

Forhandlere og Tjenesteleverandører som skal delta i Programmet, må melde seg på i Portalen som tilbys av Programadministratoren valgt av American Express innen de foreskrevne tidslinjene.

- Du må godta alle rimelige vilkår og betingelser knyttet til bruken av Portalen.
- Du må tildele og gi nøyaktig informasjon for minst én datasikkerhetskontakt i Portalen. Den nødvendige informasjonen inkluderer:
  - Fullt navn
  - E-postadresse
  - Telefonnummer
  - Fysisk postadresse
- Du må gi oppdatert eller ny kontaktinformasjon for den tildelte datasikkerhetskontakten i Portalen når informasjonen endres.
- Du må sørge for at systemene dine er oppdatert for å tillate tjenestekommunikasjon fra Portalens utpekte domene.

Din unnlatelse av å gi eller opprettholde gjeldende kontaktinformasjon for datasikkerhet eller aktivere e-postkommunikasjon vil ikke påvirke våre rettigheter til å vurdere avgifter.

Tiltak 2: Forstå ditt Forhandler-/Tjenesteleverandørnivå og dine krav til Valideringsdokumentasjon

Det er fire Forhandlernivåer som gjelder for Forhandlere og to nivåer som gjelder for Tjenesteleverandører, avhengig av volumet på American Express-korttransaksjoner.

- For Forhandlere er dette volumet som sendes inn av deres Bedrifter som ruller opp til det høyeste American Express Forhandlerkontonivå.*
- For Tjenesteleverandører er dette det sammenlagte volumet som sendes inn av Tjenesteleverandøren og Enhetstjenesteleverandøren du leverer tjenester til.

Transaksjoner som er initiert av kjøpere (BIP) er ikke inkludert i volumet av American Express-korttransaksjoner for å bestemme Forhandlernivået og valideringskravene. Du vil falle inn under ett av Forhandlernivåene spesifisert i Tabell A-1: Forhandler- og Tjenesteleverandørnivåer.

* For Franchisegivere inkluderer dette volumet fra deres Franchisetakere. Franchisegivere som gir tillatelse til at deres Franchisetakere bruker et spesifisert Betalingssystem (POS) eller Tjenesteleverandør, må også levere Valideringsdokumentasjon for de berørte Franchisetakerne.

Tabell A-1: Forhandler- og Tjenesteleverandørnivåer

Forhandlernivå	Årlige American Express-transaksjoner
Nivå 1 Forhandler	2,5 millioner American Express-korttransaksjoner eller mer per år; eller enhver Forhandler som American Express, etter eget skjønn, tildeler Nivå 1.
Nivå 2 Forhandler	50 000 til færre enn 2,5 millioner American Express-korttransaksjoner per år.
Nivå 3 Forhandler	10 000 til færre enn 50 000 American Express-korttransaksjoner per år.
Nivå 4 Forhandler	Færre enn 10 000 American Express-korttransaksjoner per år.
Tjenesteleverandørnivå	**Årlige American Express-transaksjoner**
Nivå 1 Tjenesteleverandør	2,5 millioner American Express-korttransaksjoner eller mer per år; eller enhver Tjenesteleverandør som American Express etter eget skjønn vurderer som Nivå 1.
Nivå 2 Tjenesteleverandør	færre enn 2,5 millioner American Express-korttransaksjoner per år; eller enhver Tjenesteleverandør som anses ikke som Nivå 1 av American Express.

Krav til Valideringsdokumentasjon for Forhandlere

Forhandlere (ikke Tjenesteleverandører) har fire mulige Forhandlernivå-klassifiseringer. Etter å ha fastslått Forhandlernivå fra Tabell A-1: Forhandler- og Tjenesteleverandørnivåer (over), se Tabell A-2: Valideringsdokumentasjon for Forhandlere for å fastslå krav til Valideringsdokumentasjon.

Tabell A-2: Valideringsdokumentasjon for Forhandlere

Forhandlernivå/ Årlige American Express-transaksjoner	Rapport om samsvar Bekreftelse av samsvar (ROC AOC)	Egenvurderingsskjema for Bekreftelse av samsvar (SAQ AOC) OG Kvartalsvis eksternt sårbarhetsskanning av nettverket (skanning)	Security Technology Enhancement Programme (STEP) sertifisering for kvalifiserte Forhandlere
Nivå 1/ 2,5 millioner eller mer	Obligatorisk	Ikke relevant	Valgfritt med godkjenning fra American Express (erstatter ROC)
Nivå 2/ 50 000 til færre enn 2,5 millioner	Valgfritt	SAQ AOC obligatorisk (med mindre du sender inn en ROC AOC); skanning obligatorisk for visse SAQ-typer	Valgfritt med godkjenning fra American Express* (erstatter SAQ og nettverksskanning eller ROC)
Nivå 3**/ 10 000 til færre enn 50 000	Valgfritt	SAQ AOC valgfritt (obligatorisk hvis påkrevet av American Express); skanning obligatorisk for visse SAQ-typer	Valgfritt med godkjenning fra American Express* (erstatter SAQ og nettverksskanning eller ROC)
Nivå 4**/ Færre enn 10 000	Valgfritt	SAQ AOC valgfritt (obligatorisk hvis påkrevet av American Express); skanning obligatorisk for visse SAQ-typer	Valgfritt med godkjenning fra American Express* (erstatter SAQ og nettverksskanning eller ROC)

* **Merk:** American Express PCI-teamet vil gjennomgå forespørselen og kvalifikasjonen og bekrefte om du kvalifiserer for STEP-programmet. Kontakt din Client Manager og/eller AXPPCIComplianceProgram@aexp.com for å kontrollere kvalifikasjoner.

**For å unngå enhver tvil: Forhandlere fra Nivå 3 og Nivå 4 trenger ikke å sende inn Valideringsdokumentasjon med mindre det kreves av American Express, men må likevel overholde og er underlagt ansvar i henhold til alle andre bestemmelser i disse Retningslinjene for Datasikkerhet.

American Express forbeholder seg retten til å verifisere fullstendigheten, nøyaktigheten, and hensiktsmessigheten til din PCI-Valideringsdokumentasjon. American Express kan kreve at du oppgir ytterligere støttedokumenter for evaluering til støtte for dette formålet. American Express har dessuten rett til å kreve at du engasjerer en Qualified Security Assessor (QSA) eller PCI Forensic Investigator (PFI) godkjent av PCI Security Standards Council.

Krav til Valideringsdokumentasjon for Tjenesteleverandører

Tjenesteleverandører (ikke Forhandlere) har to mulige Nivå-klassifiseringer. Etter å ha fastslått Tjenesteleverandørnivå fra Tabell A-1: Forhandler- og Tjenesteleverandørnivåer (over), se Tabell A-3: Valideringsdokumentasjon for Tjenesteleverandører for å fastslå krav til valideringsdokumentasjon.

Tjenesteleverandører kan ikke delta STEP.

Tabell A-3: Valideringsdokumentasjon for Tjenesteleverandører

Nivå	Valideringsdokumentasjon	Krav
1	Årlig Rapport om samsvar Bekreftelse av samsvar (ROC AOC)	Obligatorisk
2	Årlig SAQ D (Tjenesteleverandør) og Kvartalsvis nettverksskanning eller Årlig Rapport om samsvar Bekreftelse av samsvar (ROC AOC), hvis foretrukket	Obligatorisk

Det anbefales at Tjenesteleverandører også overholder PCI-krav til tilleggsvalidering.

Security Technology Enhancement Programme (STEP) eller forbedringsprogram for sikkerhetsteknologi

Forhandlere som er i samsvar med PCI DSS kan også, etter American Express' skjønn, kvalifisere seg for American Express' Forbedringsprogram for sikkerhetsteknologi (STEP) hvis de har implementert visse ekstra sikkerhetsteknologier i alle deres systemer for Kortbehandling. STEP gjelder bare hvis Forhandleren ikke har hatt noen Datahendelser de siste 12 månedene, og forutsatt at 75 % av alle Forhandlerkorttransaksjoner utføres ved bruk av en kombinasjon av følgende forbedrede sikkerhetsalternativer:

- **EMV, EMV kontaktløs eller digital lommebok** - på en Chip-aktivert enhet som har en gyldig og gjeldende EMVCo (www.emvco.com) godkjenning/sertifisering og som kan behandle Korttransaksjoner med Chip i samsvar med AEIPS. (Forhandlere i USA må inkludere kontaktløs)
- **Punkt-til-punkt-kryptering (P2PE)** – kommunisert til Forhandlerens databehandler ved hjelp av et PCI-SSC-godkjent eller QSA-godkjent Punkt-til-punkt-krypteringssystem
- **Tokenised** – den implementerte tokeniseringsløsningen må:
  - møte EMVCo spesifikasjoner,
  - være sikret, behandlet, lagret, overført og fullstendig administrert av en PCI-kompatibel tredjeparts tjenesteleverandør, og
  - tokenet kan ikke reverseres for å avsløre demaskerte Primærkontonumre (PAN) til forhandleren.

Forhandlere som er kvalifisert for STEP har reduserte krav til PCI-valideringsdokumentasjon, som beskrevet i Tiltak 3: «Fullføre Valideringsdokumentasjonen som du skal sende til American Express» nedenfor.

Tiltak 3: Fullføre Valideringsdokumentasjonen som du skal sende til American Express

Følgende dokumenter kreves for ulike nivåer av Forhandlere og Tjenesteleverandører som oppført i Tabell A-2: Valideringsdokumentasjon for Forhandlere og Tabell A-3: Valideringsdokumentasjon for Tjenesteleverandører over.

Du må oppgi Bekreftelse av samsvar (AOC) for den aktuelle vurderingstypen. AOC er en erklæring om din samsvarsstatus og må som sådan signeres og dateres av det riktige ledernivået innen din organisasjon.

I tillegg til AOC, kan American Express kreve at du leverer en kopi av den fullstendige vurderingen og, etter vårt skjønn, ytterligere støttedokumenter som viser samsvar med PCI DSS-kravene. Denne Valideringsdokumentasjonen fullføres for din regning.

Rapport om samsvar Bekreftelse av samsvar (ROC AOC) - (Årlig krav) – Rapporten om Samsvar dokumenterer resultatene av en detaljert undersøkelse på stedet av utstyret ditt, systemene og nettverkene dine

(og deres komponenter) der Kortholderdata eller Sensitive autentiseringsdata (eller begge deler) lagres, behandles eller overføres. Det er to versjoner: en for Forhandlere og en annen for Tjenesteleverandører. Rapporten om Samsvar må utføres av:

- et QSA eller
- en Intern sikkerhetsvurderer (ISA) og attestert av din administrerende direktør, finansdirektør, informasjonssikkerhetssjef eller leder

ROC AOC må være signert og datert av en QSA eller ISA og det autoriserte lederskapsnivået innen organisasjonen din og leveres til American Express minst én gang årlig.

Self-Assessment Questionnaire Bekreftelse av samsvar (SAQ AOC) - (Årlig krav) – Self-Assessment Questionnaires tillater selvundersøkelse av utstyret ditt, systemene og nettverkene dine (og deres komponenter) der Kortholderdata eller Sensitive autentiseringsdata (eller begge deler) lagres, behandles eller overføres. Det finnes flere versjoner av SAQ. Du ønsker å velge en eller flere basert på ditt Kortholderdatamiljø.

SAQ kan fylles ut av ansatte i ditt firma som er kvalifisert til å svare nøyaktig og grundig på spørsmålene, eller du kan engasjere en QSA for å assistere. SAQ AOC må være signert og datert av det autoriserte lederskapsnivået innen organisasjonen din og leveres til American Express minst én gang årlig.

Approved Scanning Vendor for ekstern sårbarhetsskanning av nettverket (ASV Scan) - (90 dager krav) – En ekstern sårbarhetsskanning er en ekstern test for å avdekke potensielle svakheter, sårbarheter og feilkonfigurasjoner av internettvendte komponenter i ditt Kortholderdatamiljø (f.eks. nettsteder, applikasjoner, webservere, e-postservere, offentlige domener eller verter).

ASV-skanningen må utføres av en Approved Scanning Vendor (ASV).

Om det kreves av SAQ, må ASV Scan Report Attestation of Scan Compliance (AOSC) eller kortfattet sammendrag inkludert en telling av skannede mål, sertifisering av at resultatene tilfredsstiller PCI DSS skanningsprosedyrer og samsvarsstatus fullført av ASV sendes til American Express minst én gang hver 90. dag.

Hvis du sender inn ROC AOC eller STEP, er du ikke pålagt å gi et AOSC eller ASV kortfattet skanningssammendrag med mindre det er spesifikt bedt om det. For å unngå enhver tvil, Skanning er obligatorisk hvis dette kreves av gjeldende SAQ.

Valideringsdokumentasjon for STEP-sertifisering (STEP) - (Årlig krav) – STEP er kun tilgjengelig for Forhandlere som oppfyller kriteriene oppført i Tiltak 2: «Forstå ditt Forhandler-/Tjenesteleverandørnivå og dine krav til Valideringsdokumentasjon» ovenfor. Om bedriften din kvalifiserer, må du årlig fylle ut og sende inn STEP-sertifiseringsskjemaet til American Express. Det årlige STEP-sertifiseringsskjemaet er tilgjengelig for nedlasting fra Portalen. Du kan også kontakte din Client Manager eller skrive til American Express på AXPPCIComplianceProgram@aexp.com.

Manglende samsvar med PCI DSS - (Årlig krav, 90 dager og/eller ad hoc-krav) – Hvis du ikke er i overensstemmelse med PCI DSS, må du sende inn et PCI-prioritert tilnærmingsverktøyssammendrag (PAT) (tilgjengelig for nedlasting via nettstedet til PCI-sikkerhetsstandardrådet).

PAT-sammendraget må gis en dato for utbedring som ikke må være senere enn tolv (12) måneder etter dokumentets dato for ferdigstillelse for å oppnå samsvar. Du skal gi American Express regelmessige oppdateringer på fremgang i forbindelse med utbedring av manglende samsvar (Forhandlere på Nivå 1, Nivå 2, Nivå 3 og Nivå 4 og alle Tjenesteleverandører). Utbedringstiltak som er nødvendige for å oppnå samsvar med PCI DSS skal være fullført på din bekostning.

American Express vil ikke pålegge avgifter for manglende samsvar før utbedringsdatoen. I henhold til Tabell A-4: Avgift for manglende samsvar, forblir du ansvarlig for alt erstatningsansvar for en Datahendelse og er underlagt alle andre bestemmelser i disse retningslinjene.

American Express bevarer, etter eget skjønn, retten til å pålegge avgifter for manglende samsvar hvis:

- en PCI-prioritert tilnærmingsmal ikke har blitt sendt inn i samsvar med kravene angitt i dette punktet,
- utbedringstrinnene skissert i PCI-prioritert tilnærmingsmal for ikke-samsvarsstatus ikke ble oppfylt,
- kravene i PCI-prioritert tilnærmingsmal for ikke-samsvarsstatus ikke ble oppfylt, eller

- den obligatoriske samsvarsdokumentasjonen ikke ble levert til American Express innen den gjeldende fristen eller ved forespørsel.

Forhandlere/Tjenesteleverandører som ikke overholder kravene fastsatt i Tiltak 2: Forstå ditt Forhandler-/Tjenesteleverandørnivå og dine krav til Valideringsdokumentasjon, kan være underlagt avgifter som angitt i Tiltak 4: Sende Valideringsdokumentasjonen til American Express.

For å unngå enhver tvil, Forhandlere som ikke oppfyller kravene til PCI DSS er ikke kvalifisert for STEP-sertifisering.

Tiltak 4: Sende Valideringsdokumentasjonen til American Express

Alle Forhandlere og Tjenesteleverandører som er pålagt å delta i Programmet må sende inn Valideringsdokumentasjonen merket «obligatorisk» i tabellene i Tiltak 2: «Forstå ditt Forhandler-/Tjenesteleverandørnivå og dine krav til Valideringsdokumentasjon» til American Express innen gjeldende frister.

Du må sende inn Valideringsdokumentasjonen til American Express ved å bruke Portalen som tilbys av Programadministratoren valgt av American Express. Ved å sende inn Valideringsdokumentasjon bekrefter og garanterer du overfor American Express at følgende er sant (etter beste evne):

- Din evaluering var fullstendig og grundig;
- PCI DSS-statusen er nøyaktig representert på fullføringstidspunktet, uansett om man sender inn Attestation of Compliance (AOC) eller et PCI Prioritised Approach Tool (PAT)-sammendrag for manglende samsvar;
- Du er autorisert til å avdekke informasjonen deri og leverer Valideringsdokumentasjonen til American Express uten å krenke noen annen parts rettigheter.

Manglende samsvar med Avgifter og Oppsigelse av Avtalen

American Express har rett til å pålegge avgifter for manglende samsvar og si opp Avtalen hvis du ikke oppfyller disse kravene, eller unnlater å sende den obligatoriske Valideringsdokumentasjonen til American Express innen den gjeldende fristen. American Express vil forsøke å varsle datasikkerhetskontakten om den relevante tidsfristen for hver årlige og kvartalsvise rapporteringsperiode.

Tabell A-4: Avgift for manglende samsvar

Beskrivelse*	Nivå 1 Forhandler eller Nivå 1 Tjenesteleverandør	Nivå 2 Forhandler eller Nivå 2 Tjenesteleverandør	Nivå 3 eller Nivå 4 Forhandler
Det kan pålegges en avgift for manglende samsvar hvis Valideringsdokumentasjonen ikke er mottatt innen utløp av første frist.	25 000 USD	5000 USD	50 USD
Det kan pålegges en ytterligere avgift for manglende samsvar hvis Validerings-dokumentasjonen ikke er mottatt innen utløp av andre frist.	35 000 USD	10 000 USD	100 USD
Det kan pålegges en ytterligere avgift for manglende samsvar hvis Validerings-dokumentasjonen ikke er mottatt innen utløp den tredje fristen. **MERK:** Avgifter for manglende samsvar vil fortsette å gjelde inntil Validerings-dokumentasjonen er sendt inn.	45 000 USD	15 000 USD	250 USD

* Avgifter for manglende samsvar blir vurdert i lokale valutaekvivalenter.

* Gjelder ikke i Argentina.

Hvis forpliktelsene til PCI DSS-samsvarsdokumentasjon ikke er oppfylt, har American Express rett til å pålegge avgifter for manglende samsvar kumulativt, holde tilbake betalinger og/eller si opp Avtalen.

Punkt 3 Forpliktelser for håndtering av Datahendelser

Du skal varsle American Express umiddelbart og senest syttito (72) timer etter at en Datahendelse er oppdaget.

For å varsle American Express, kan du kontakte American Express Enterprise Incident Response Programme (*EIRP*) gratis på 1.888.732.3750 eller 1.602.537.3021, eller send e-post til EIRP@aexp.com. Det skal oppnevnes en kontaktperson for slike Datahendelser. I tillegg gjelder følgende:

- Du må gjennomføre en grundig undersøkelse av hver Datahendelse og umiddelbart overlevere alle Kompromitterte Kortnumre til American Express. American Express forbeholder seg retten til å gjennomføre egne interne analyser for å identifisere data som er involvert i Datahendelsen.

For Datahendelser som involverer færre enn 10 000 unike Kortnumre, må et undersøkelsessammendrag leveres til American Express innen ti (10) arbeidsdager etter fullføring.

- Undersøkelsessammendrag bør inneholde følgende informasjon: hendelsessammendrag, beskrivelse av de berørte miljø(ene), tidslinje for hendelser, nøkkeldatoer, virkning og dataeksponeringsdetaljer, oppdemming og utbedrende tiltak og bekreftelse på at ytterligere American Express-data ikke står i fare.

For Datahendelser som involverer 10 000 eller flere unike Kortnumre, må du engasjere en PFI for å gjennomføre denne undersøkelsen senest fem (5) dager etter Datahendelsen ble oppdaget.

- Den uredigerte etterforskningssrapporten skal overleveres til American Express innen ti (10) arbeidsdager etter at den er fullført.
- Kriminaltekniske etterforskningssrapporter skal fullføres i samsvar med den gjeldende malen for sluttrapporter for Datahendelser (Forensic Incident Final Report) som er tilgjengelig fra PCI. En slik rapport må inneholde kriminaltekniske gjennomganger, Sammendrag av samsvarer og all annen informasjon relatert til Datahendelsen; identifisere årsaken til Datahendelsen; bekrefte om du/dere overholdt PCI DSS-kravene på tidspunktet for Datahendelsen og verifisere din/deres evne til å forhindre fremtidige Datahendelser ved å (i) fremlegge en plan for å avhjelpe alle PCI DSS-mangler og (ii) delta i American Express' samsvarsprogram (beskrevet nedenfor). På anmodning fra American Express skal du fremlegge validering fra et kvalifisert selskap for sikkerhetsvurdering, også kalt Qualified Security Assessor (QSA), om at manglene har blitt utbedret.

Til tross for de foregående avsnittene i dette Punkt 3, «Forpliktelser for håndtering av Datahendelser»:

- American Express kan, etter eget skjønn, kreve at du engasjere en PFI til å utføre en undersøkelse av en Datahendelse for Datahendelser som involverer færre enn 10 000 unike Kortnumre eller der flere hendelser har funnet sted i løpet av en periode på 12 måneder. Enhver slik etterforskning må være i samsvar med kravene angitt ovenfor i dette Punkt 3, «Forpliktelser for håndtering av Datahendelser» og må fullføres innen de tidsrammer som kreves av American Express.
- American Express kan, etter eget skjønn, engasjere sin egen PFI og kan kreve at du må dekke eventuelle kostnader for en slik etterforskning.

Du må vurdere Datahendelsen i henhold til gjeldende lover for varsling om databrudd globalt og, der det anses som nødvendig, varsle gjeldende regulatorer og berørte Kortmedlemmer i samsvar med slike lover for varsling om databrudd. Hvis du har fastslått at din Tjenesteleverandør eller en annen enhet er ansvarlig for å rapportere Datahendelsen, skal du råde slik Tjenesteleverandør eller enhet om dens plikt til å vurdere rapporteringsforpliktelsene i henhold til gjeldende lover for varsling om databrudd. Du samtykker til å innhente skriftlig samtykke fra American Express før du refererer til eller navngir American Express i kommunikasjon til Kortmedlemmer om Datahendelsen. Du samtykker til å samarbeide med American Express for å gi detaljer og rette opp eventuelle problemer som oppstår som følge av Datahendelsen, inkludert å gi American Express all relevant informasjon for å verifisere din evne til å forhindre fremtidige Datahendelser på en måte som er i samsvar med Avtalen.

Til tross for eventuell motstridende taushetsplikt i henhold til Avtalen, har American Express rett til å utlevere informasjon om eventuelle Datahendelser American Express-kortmedlemmer Utstedere, andre deltakere i American Express-nettverket og allmennheten dersom dette kreves som følge av gjeldende lov; rettsavgjørelse eller forskriftsmessig pålegg, dekret, stevning, forespørsel eller annen prosess; for å redusere risikoen for svindel eller annen skade; eller på annen måte og i den grad det er hensiktsmessig for driften av American Express-nettverket.

Hva gjør du hvis du har en Datahendelse?

Følg disse trinnene hvis du har identifisert en Datahendelse i virksomheten din.

Trinn 1:

Fyll ut innledende varslingsskjema for Datahendelser for Forhandlere og send det som e-post til EIRP@aexp.com innen 72 timer etter at Datahendelsen er oppdaget.

Trinn 2:

Gjennomfør en grundig undersøkelse – dette kan kreve at du ansetter en Payment Card Industry (PCI) Forensic Investigator.

Trinn 3:

Gi oss umiddelbart alle kompromitterte American Express®-kortnumre.

Trinn 4:

Samarbeid med oss for å hjelpe deg med å løse eventuelle problemer som oppstår fra Datahendelsen.

Se Punkt 3, «Forpliktelser for håndtering av Datahendelser» for flere detaljer om forpliktelser for håndtering av Datahendelser.

Har du flere spørsmål?

US: (888) 732-3750 (avgiftsfritt)

Internasjonalt: +1 (602) 537-3021

EIRP@aexp.com

Punkt 4 Erstatningsansvar for Datahendelser

Ditt erstatningsansvar overfor American Express i henhold til Avtalen for Datahendelser skal avgjøres, uten frafall av noen av American Express' andre rettigheter og rettsmidler, i henhold til dette Punkt 4, «Erstatningsansvar for Datahendelser». I tillegg til Erstatningsansvaret ditt (hvis gjeldende), kan du være underlagt en avgift for manglende overholdelse i forbindelse med en Datahendelse, som beskrevet nedenfor i Punkt 4, «Erstatningsansvar for Datahendelser».

Du skal kompensere American Express 5 USD per kontonummer, for Datahendelser som involverer:

- 10 000 eller flere American Express-kortnumre med en av følgende:
  - Sensitive autentiseringsdata eller
  - Utløpsdato

American Express vil imidlertid ikke søke skadeserstatning fra deg for en Datahendelse som involverer:

- færre enn 10 000 American Express-kortnumre, eller
- mer enn 10 000 American Express-kortnumre, forutsatt at du oppfyller følgende betingelser:
  - du varslet American Express om Datahendelsen i henhold til Punkt 3, «Forpliktelser for håndtering av Datahendelser»,
  - du var i samsvar med PCI DSS-kravene på tidspunktet for Datahendelsen (som fastsatt av PFIs etterforskning av Datahendelsen), og
  - Datahendelsen var ikke forårsaket av uriktig oppførsel gjennom deg eller de Berørte partene.

Til tross for de foregående avsnittene i dette Punkt 4, «Erstatningsansvar for Datahendelser», skal du betale American Express for enhver Datahendelse, og uavhengig av antallet American Express-kortnumre, en

erstatningsavgift for manglende overholdelse i forbindelse med en Datahendelse som ikke overskrider USD 100 000 per Datahendelse (fastsatt etter eget skjønn av American Express) i tilfelle det påvises manglende overholdelse av eventuelle forpliktelser som er spesifisert i avsnitt Punkt 3, «Forpliktelser for håndtering av Datahendelser». For å unngå enhver tvil, den totale erstatningsavgiften for manglende overholdelse i forbindelse med en Datahendelse skal ikke overstige USD 100 000 per Datahendelse.

American Express vil ikke ta med i beregningen American Express-kortkontonummer som har vært inkludert i tidligere erstatningskrav som er fremsatt av oss i løpet av de siste tolv (12) måneder før Varslingsdatoen. Alle beregninger gjort av American Express i henhold til denne metoden er endelige.

American Express kan fakturere deg for hele beløpet som du er skyldig på grunnlag av ditt erstatningsansvar for Datahendelser eller trekke beløpet fra American Express' betalinger til deg (eller belaste Bankkontoen din tilsvarende) i samsvar med Avtalen.

Ditt erstatningsansvar for Datahendelser i henhold til dette skal ikke anses som tilfeldige, indirekte, spekulative, betingede, spesielle, straffende eller eksemplariske skader i henhold til Avtalen; forutsatt at slike forpliktelser ikke inkluderer skader relatert til eller i form av tapt fortjeneste eller inntekter, tap av goodwill eller tap av forretningsmuligheter.

American Express kan etter eget skjønn redusere erstatningsansvaret for Forhandlere for Datahendelser som utelukkende oppfyller følgende kriterier:

- Gjeldende Risikoreduserende teknologier ble brukt før Datahendelsen og vær i bruk under hele Hendelsesvinduet for Datahendelsen,
- Det ble gjennomført en grundig etterforskning i henhold til kravene til PCI-programmet (med mindre annet var skriftlig avtalt på forhånd),
- Etterforskningsrapporten erklærer tydelig at Risikoreduserende teknologier ble brukt til å behandle, lagre og/eller overføre på tidspunktet for Datahendelsen, og
- Du ikke lagrer (og ikke lagret under Hendelsesvinduet for Datahendelsen) Sensitive autentiseringsdata og Kortholderdata som ikke er gjort uleselige.

Når en erstatningsreduksjon er tilgjengelig, bestemmes reduksjonen av ditt erstatningsansvar (med unntak av eventuelle avgifter for manglende overholdelse) som følger:

Tabell A-5: Kriterier for Reduksjon av erstatningsansvar

Reduksjon av Erstatningsansvar	Nødvendige Kriterier
Standard Reduksjon: 50 %	>75 % av totalt antall transaksjoner behandlet på Chip-aktiverte enheter[1] ELLER
	Risikoreduserende teknologi i bruk på >75 % av stedene til Forhandlerne[2]
Utvidet Reduksjon: 75 % til 100 %	>75 % av alle transaksjoner behandlet på Chip-aktiverte enheter[1] OG en annen Risikoreduserende teknologi i bruk på >75 % av stedene til Forhandlerne[2]

[1] I henhold til American Express' interne analyse

[2] I henhold til PFI-undersøkelse

- Utvidet Reduksjon (75 % til 100 %) skal bestemmes basert på den minste prosentandelen av transaksjoner som bruker Chip-aktiverte enheter OG Utsalgssteder som bruker annen Risikoreduserende teknologi. Eksemplene i Tabell A-6: Utvidet Reduksjon av Erstatningsansvar illustrerer beregningen av erstatningsreduksjonen.

- For å kvalifiseres som bruker av Risikoreduserende teknologi må du demonstrere effektiv bruk av teknologien i samsvar med dens design og tiltenkte formål.
- Prosentandelen av steder som bruker en Risikoreduserende teknologi avgjøres av PFI.
- Reduksjonen av erstatningsansvaret gjelder ikke for erstatningsavgifter som skal betales i forhold til Datahendelsen.

Tabell A-6: Utvidet Reduksjon av Erstatningsansvar

Eks.	Risikoreduserende teknologi i bruk	Kvalifisert	Reduksjon
1	• 80 % av Transaksjoner på Chip-aktiverte enheter • 0 % av stedene bruker Risikoreduserende teknologi	Nei	50 %: Standard Reduksjon (mindre enn 75 % bruk av Risikoreduserende teknologi gir ikke rett til Utvidet Reduksjon)[1]
2	• 80 % av Transaksjoner på Chip-aktiverte enheter • 77 % av stedene bruker Risikoreduserende teknologi	Ja	77 %: Utvidet Reduksjon (basert på 77 % bruk av Risikoreduserende teknologi)
3	• 93 % av Transaksjoner på Chip-aktiverte enheter • 100 % av stedene bruker Risikoreduserende teknologi	Ja	93 %: Utvidet Reduksjon (basert på 93 % av Transaksjoner på Chip-aktiverte enheter)
4	• 40 % av Transaksjoner på Chip-aktiverte enheter • 90 % av stedene bruker Risikoreduserende teknologi	Nei	50 %: Standard Reduksjon (mindre enn 75 % av Transaksjoner på Chip-aktiverte enheter gir ikke rett til Utvidet Reduksjon)

[1] En Datahendelse som involverer 10 000 American Express-kortkontoer, med en sats på USD 5 per kontonummer (10 000 x USD 5 = USD 50 000) kan være kvalifisert for en reduksjon på 50 %, noe som reduserer erstatningsansvaret fra USD 50 000 til USD 25 000, med unntak av eventuelle avgifter for manglende samsvar.

Punkt 5 Målrettet analyse-program (TAP)

Kompromitterte Kortholderdata kan være forårsaket av datasikkerhetshull i Kortholderens Datamiljø (CDE).

Eksempler på Kompromitterte Kortholderdata inkluderer, men er ikke begrenset til:

- **Vanlig kjøpested (CPP):** American Express-kortmedlemmer rapporterer falske Transaksjoner på deres Kortkontoer og er identifisert og bestemt å stamme fra kjøp fra Virksomhetene dine.
- **Kortdata funnet:** American Express-kort og kortholderdata funnet på nettet knyttet til transaksjoner hos Virksomhetene dine.
- **Mistenkt for skadelig programvare:** American Express mistenker at du bruker programvare infisert med eller sårbar for skadelig kode.

TAP er designet for å identifisere potensielle kompromitteringer av Kortholderdata.

Du må, og du må få Berørte parter til å overholde følgende krav ved varsel fra American Express om en potensiell kompromittering av Kortholderdata.

- Du må umiddelbart gjennomgå CDE-en din for datasikkerhetshull og rette opp eventuelle funn.
  - Du må få tredjepartsleverandøren(e) dine til å foreta en grundig undersøkelse av CDE-en din hvis den blir outsourcet.

- Du må gi et sammendrag av tiltak som er tatt eller planlagt for din gjennomgang, evaluering og/eller dine tiltak for utbedring etter melding fra American Express.
- Du må levere oppdaterte PCI DSS-valideringsdokumenter i samsvar med Punkt 2, «PCI DSS-samsvarsprogram (Viktig Regelmessig Validering av Systemene dine)».
- Hvis det er aktuelt, må du engasjere en kvalifisert PCI PFI for å undersøke CDI-en din hvis du eller din Berørte part:
  - Ikke kan løse Kompromitterte kortholderdata innen rimelig tid, bestemt av American Express, eller
  - Bekrefter at det har oppstått en datahendelse, og overholder kravene som er fremsatt i Punkt 3, «Forpliktelser for håndtering av Datahendelser».

Tabell A-7: Avgift for manglende overholdelse for TAP

Beskrivelse	Nivå 1 Forhandler eller Nivå 1 Tjeneste-leverandør	Nivå 2 Forhandler eller Nivå 2 Tjeneste-leverandør	Nivå 3 eller Nivå 4 Forhandler
Avgift for manglende samsvar kan vurderes når TAP-forpliktelser ikke tilfredsstilles innen den første fristen.	25 000 USD	5000 USD	1000 USD
Avgift for manglende samsvar kan vurderes når TAP-forpliktelser ikke tilfredsstilles innen den andre fristen.	35 000 USD	10 000 USD	2500 USD
Avgift for manglende samsvar kan vurderes når TAP-forpliktelser ikke tilfredsstilles innen den tredje fristen. **MERK:** *Avgifter for manglende overholdelse kan påføres månedlig til forpliktelsene er oppfylt eller TAP er løst.*	45 000 USD	15 000 USD	5000 USD

Hvis TAP-forpliktelsene ikke er oppfylt, har American Express rett til å pålegge avgifter for manglende overholdelse kumulativt, holde tilbake betalinger og/eller si opp Avtalen.

Punkt 6 Taushetsplikt

American Express skal treffe rimelige tiltak for å holde (og påse at agenter og underleverandører, inkludert Portalleverandøren, holder) rapporter om samsvar, inkludert Valideringsdokumentasjon konfidensielle og ikke avslører Valideringsdokumentasjonen til tredjeparter (annet enn American Express' datterselskap, agenter, representanter, Tjenesteleverandører og underleverandører) for en periode på tre år fra dato for mottak; denne taushetsplikten gjelder ikke i tilfeller der Valideringsdokumentasjonen:

a. allerede er kjent for American Express før utlevering;

b. er eller blir tilgjengelig for allmennheten uten at American Express har brutt dette punkt;

c. er rettmessig mottatt fra en tredjepart av American Express uten pålagt taushetsplikt;

d. er uavhengig utviklet av American Express; eller

e. er nødvendig å utlevere som følge av pålegg fra domstol, forvaltningsorgan eller offentlig myndighet, eller av lov, regel eller forskrift, eller ved begjæring, stevning eller annen administrativ eller juridisk prosess, eller ved en formell eller uformell henvendelse eller etterforskning av offentlige etater eller myndigheter (herunder lovgiver, inspektør, gransker, eller politimyndighet).

Punkt 7 Ansvarsfraskrivelse

AMERICAN EXPRESS FRASKRIVER SEG ALLE REPRESENTASJONER, GARANTIER OG FORPLIKTELSER MED HENSYN TIL DISSE RETNINGSLINJER FOR DATASIKKERHET, PCI DSS, EMV-KRAV OG UTPEKELSE OG YTELSE AV QSA, ASV ELLER PFI (ELLER NOEN AV DEM), ENTEN UTTRYKKELIG, UNDERFORSTÅTT, LOVFESTET ELLER

ANNET, INKLUDERT GARANTIER OM SALGBARHET ELLER EGNETHET FOR ET SPESIELT FORMÅL. AMERICAN EXPRESS-KORTUTSTEDERE ER IKKE TREDJEPARTSBEGUNSTIGEDE ETTER DISSE RETNINGSLINJENE.

Punkt 8 Ordliste

Følgende definisjoner er kun gjeldende og styrende i forbindelse med disse *Retningslinjer for Datasikkerhet*:

American Express-kort, eller **Kort**, ethvert kort, enhet for kontotilgang, betalingsenhet eller tjeneste som bærer American Express' eller et datterselskaps navn, logo, varemerke, servicemerke, handelsnavn eller annen merkevarebeskyttet design eller benevnelse og er utstedt av en utsteder eller et kortnummer.

Approved Scanning Vendor (ASV) betyr en Enhet som har blitt kvalifisert av Payment Card Industry Security Standards Council, LLC til å validere overholdelse av visse PCI DSS-krav ved å utføre eksterne sårbarhetsskanninger av datanettverk.

Attestation of Scan Compliance (AOSC) er en sertifisering om samsvar med PCI DSS basert på en ekstern nettverksskanning i henhold til Payment Card Industry Security Standards Council, LLC.

Avtale betyr de Generelle bestemmelsene, Forhandlerforskriftene og eventuelle ledsagende planer og fremvisninger, kollektivt (noen ganger referert til som Kortakseptavtalen i våre materialer).

Bekreftelse av samsvar (AOC) er en erklæring om samsvar med kravene til PCI DSS, utstedt av Payment Card Industry Security Standards Council, LLC.

Belastning betyr en betaling eller kjøp gjort med et Kort.

Belastningsoversikt betyr en reproduserbar (både på papir og elektronisk) registrering av en Belastning som samsvarer med våre krav og inneholder Kortnummer, Transaksjonsdato, dollarbeløp, Godkjenning, Kortmedlemssignatur (hvis aktuelt) og annen informasjon.

Berørte parter betyr enhver og alle av dine ansatte, agenter, representanter, underleverandører, Behandlere, Tjenesteleverandører, leverandører av utstyr eller systemer for salgssteder (POS) eller betalingsløsninger, Enheter knyttet til din Express-forhandlerkonto, og enhver annen part som du gir tilgang til Kortholderdata eller Sensitive autentiseringsdata (eller begge deler) i samsvar med Avtalen.

Betalingsapplikasjon har meningen som er fastsatt i den gjeldende ordlisten for sikre programvarestandarder og sikker livsforløpstandard for programvare i betalingskortindustrien, som er tilgjengelig på www.pcisecuritystandards.org.

Betalingssystemer (POS) betyr et informasjonsbehandlingssystem eller -utstyr, herunder en terminal, personlig datamaskin, elektronisk kassaapparat, kontaktløs kortleser, betalingsterminal eller -prosess som brukes av en Forhandler, for å få autorisasjon eller samle inn Transaksjonsdata eller begge deler.

Chip betyr en mikrobrikke integrert i et Kort som inneholder informasjon om Kortmedlemmet og kontoen.

Chip-aktivert enhet betyr en betalingsterminal som har en gyldig og gjeldende EMVCo-godkjenning/sertifisering (www.emvco.com) og som kan behandle Korttransaksjoner med Chip i samsvar med AEIPS.

Chip-kort betyr et Kort som inneholder en Chip, og som kan kreve en PIN-kode for å verifisere identiteten til Kortmedlemmet eller kontoinformasjon i Chipn, eller begge deler (noen ganger kalt et «smart-kort», «EMV-kort», «ICC» eller «integrert kretskort» i våre dokumenter).

Databehandler betyr en Tjenesteleverandør til Forhandleren som tilrettelegger for autorisasjon og rapportering til American Express-nettverket.

Datahendelse betyr en hendelse som involverer en kompromittering av eller en mistenkt kompromittering av American Express-krypteringsnøkler, eller minst ett American Express-kortnummer der det har vært:

- uautorisert tilgang til eller bruk av Krypteringsnøkler, Kortholderdata eller Sensitive autentiseringsdata (eller en kombinasjon av disse) som lagres, behandles eller overføres på ditt utstyr, dine systemer og/eller nettverk (eller dets komponenter) eller som brukes av andre med din godkjenning eller via deg;

- bruk av slike Krypteringsnøkler, Kortholderdata eller Sensitive autentiseringsdata (eller en kombinasjon av disse) i strid med denne avtalen; og/eller
- mistenkt eller bekreftet tap, tyveri eller enhver feil bruk av medier, materialer, oppføringer eller informasjon som inneholder slike Krypteringsnøkler, Kortholderdata eller Sensitive autentiseringsdata (eller en kombinasjon av disse).

EMV-spesifikasjoner betyr spesifikasjonene utstedt av EMVCo, LLC, som er tilgjengelige på www.emvco.com.

EMV-transaksjon betyr en integrert kretskorttransaksjon (noen ganger kalt et «IC-kort», «smart-kort», «EMV-kort» eller «ICC») gjennomført på en betalingsterminal som er aktivet for IC-kort og har en gyldig EMV-godkjenning. EMV-godkjenninger er tilgjengelig på www.emvco.com.

Forbruker er definert som en kortholder som kjøper varer, tjenester eller begge deler.

Forhandler betyr Forhandleren og alle dens datterselskap som aksepterer American Express-kort i henhold til en Avtale med American Express eller dets datterselskap.

Forhandlernivå betyr betegnelsen vi tildeler forhandlere knyttet til deres PCI DSS-samsvarsvalideringsforpliktelser, som beskrevet i Punkt 2, «PCI DSS-samsvarsprogram (Viktig Regelmessig Validering av Systemene dine)».

Franchisegiver betyr en person som driver en virksomhet som lisensierer personer eller enheter (Franchisetakere) til å distribuere varer og/eller tjenester under Franchisegiverens varemerke, gir støtte til Franchisetakere i forbindelse med drift av deres virksomhet eller påvirker Franchisetakerens driftsmåte og krever betaling i form av gebyr fra Franchisetakerne.

Franchisetaker betyr en uavhengig eid og drevet tredjepart (inkludert en franchisetaker, lisensinnehaver eller kapittel) annet enn et Tilknyttet selskap, som er lisensiert av en Franchisegiver til å drive en franchise og som har inngått en skriftlig avtale med Franchisegiveren, der den konsekvent viser ekstern identifikasjon og tydelig identifiserer seg med Franchisor's Marks eller utgir seg for publikum som medlem av en Franchise-gruppe av selskaper.

Godkjent punkt-til-punkt-kryptering (P2PE) inkludert i PCI SSC-listen over godkjente løsninger eller godkjent av et PCI SSC-kvalifisert selskap for sikkerhetsvurdering – Qualified Security Assessor P2PE.

Hendelsesvindu for Datahendelse betyr vinduet for inntrenging (eller en lignende begrenset tidsperiode) som fastsatt i den endelige rettsvitenskapelige rapporten (dvs. PFI-rapporten), opp til 365 dager før siste Varslingsdato for potensielt Kompromitterte kortnummerer involvert i en Datakompromittering som er rapportert til oss.

Informasjon om Kortmedlem betyr informasjon om American Express-kortmedlemmer og Korttransaksjoner, inkludert navn, adresser, kortnumre, og numre for kortidentifikasjon (CID).

Kompromittert kortnummer betyr et American Express-kortnummer knyttet til en Datahendelse.

Kontodata består av Kortholderdata og/eller Sensitive autentiseringsdata. Se Kortholderdata og Sensitive autentiseringsdata.

Kortholder betyr en kunde som betalingskortet utstedes til, eller enhver person autorisert til å bruke betalingskortet.

Kortholderdata betyr som et minimum, fullstendig Primært kontonummer (PAN) for seg selv eller fullstendig PAN pluss ethvert av det følgende: kortholderdata, utløpsdato og/eller servicekode. Se Sensitive autentiseringsdata for ekstra dataelementer som kan overføres eller behandles (men ikke lagres) som del av en betalingstransaksjon.

Kortholderens datamiljø (CDE) betyr personene, prosessene og teknologien som lagrer, behandler eller overfører kortholderdata eller sensitive autentiseringsdata.

Kortmedlem betyr en enkeltperson eller enhet (i) som har inngått en avtale om å etablere en Kortkonto med en utsteder eller (ii) hvis navn vises på Kortet.

Kortnummer betyr det unike identifikasjonsnummeret som utstederen tildeler Kortet når det utstedes.

Kortutsteder betyr enhver Enhet (inkludert American Express og dets tilknyttede selskaper) som er lisensiert av American Express eller et tilknyttet American Express-selskap til å utstede kort og å engasjere seg i kortutstedende virksomhet.

Kravene til Payment Card Industry Security Standards Council (PCI SSC) henviser til standarder og krav knyttet til sikring og beskyttelse av betalingskortdata, inkludert PCI DSS og PA DSS, tilgjengelig på www.pcisecuritystandards.org.

Kreditering betyr et Belastningsbeløp som du tilbakebetaler til Kortmedlemmer for kjøp eller betalinger på et Kortet.

Krediteringsoversikt betyr en registrering av en Kreditering som er i samsvar med kravene våre.

Krypteringsnøkkel (American Express-krypteringsnøkkel) betyr alle nøkler som brukes i behandling, generasjon, lasting og/eller beskyttelse av onto ata. Dette inkluderer, men er ikke begrenset til, følgende:

- Nøkkel-krypteringsnøkler: Zone Master-nøkler (ZMK) og Zone Pin-nøkler (ZPK)
- Masternøkler som brukes i sikre kryptografiske enheter: Lokale Master-nøkler (LMK)
- Kode-nøkler for kortsikkerhet (CSCK)
- PIN-nøkler: Base Derivation-nøkler (BDK), PIN-krypteringsnøkler (PEK) og ZPK

Målrettet analyse-program betyr et program som gir tidlig identifisering av potensielt Kompromitterte kortholderdata i Kortholderens datamiljø (CDE). Se Punkt 5, «Målrettet analyse-program (TAP)».

Nivå 1 Forhandler betyr en Forhandler som har 2,5 millioner American Express-korttransaksjoner eller mer per år; eller enhver Forhandler som American Express etter eget skjønn vurderer som Nivå 1.

Nivå 2 Forhandler betyr en Forhandler med 50 000 til færre enn 2,5 millioner American Express-korttransaksjoner per år.

Nivå 3 Forhandler betyr en Forhandler med 10 000 til færre enn 50 000 American Express-korttransaksjoner per år.

Nivå 4 Forhandler betyr en Forhandler med færre enn 10 000 American Express-korttransaksjoner per år.

Nivå 1 Tjenesteleverandør betyr en Tjenesteleverandør som har 2,5 millioner American Express-korttransaksjoner eller mer per år; eller enhver Tjenesteleverandør som American Express etter eget skjønn vurderer som Nivå 1.

Nivå 2 Tjenesteleverandør betyr en Tjenesteleverandør med færre enn 2,5 millioner American Express-korttransaksjoner per år; eller enhver Tjenesteleverandør som American Express etter eget skjønn ikke vurderer som Nivå 1.

Payment Card Industry Data Security Standard (PCI DSS) betyr Payment Card Industry Data Security Standard, som er tilgjengelig på www.pcisecuritystandards.org.

PCI DSS betyr Payment Card Industry Data Security Standard, som er tilgjengelig på www.pcisecuritystandards.org.

PCI-godkjent betyr at en PIN-enhet eller en Betalingsterminal (eller begge deler) på tidspunktet for levering på var oppført på listen over godkjente bedrifter og leverandører som vedlikeholdes av PCI Security Standards Council, LLC og som er tilgjengelig på www.pcisecuritystandards.org.

PCI PIN-sikkerhetskrav henviser til kravene til Payment Card Industry PIN Security, som er tilgjengelige på www.pcisecuritystandards.org.

PCI-sertifisert kriminaletterforsker (PFI) betyr en leverandør som har blitt godkjent av Payment Card Industry Security Standards Council, LLC til å utføre kriminaltekniske etterforskninger ved brudd på eller kompromittering av betalingskortdata.

PIN-enhet skal forstås i henhold til beskrivelsen som er gitt i den gjeldende Ordliste for Payment Card Industry PIN Transaction Security (PTS) Point of Interaction (POI), Modular Security Requirements, som er tilgjengelig på www.pcisecuritystandards.org.

Portalen betyr rapporteringssystemet som er levert av American Express PCI-programadministratoren valgt av American Express. Forhandlere og tjenesteleverandører er pålagt å bruke Portalen til å sende inn PCI-valideringsdokumentasjon til American Express.

Primært kontonummer (PAN) har betydningen gitt til det i den da gjeldende Vilkårordlisten for PCI DSS.

Programmet betyr American Express PCI Samsvarsprogram.

Punkt-til-punkt-kryptering (P2PE) betyr en løsning som kryptografisk beskytter kontoinformasjon fra det punktet en Forhandler godtar et betalingskort til det sikre punktet for dekryptering.

Qualified Security Assessor (QSA) betyr en enhet som har blitt kvalifisert av Payment Card Industry Security Standards Council, LLC til å validere samsvar med PCI DSS.

Risikoreduserende teknologi betyr Teknologiløsninger som forbedrer sikkerheten til American Express' Kortholderdata og Sensitive autentiseringsdata, fastsatt av American Express. For å kvalifiseres som bruker av Risikoreduserende teknologi, må du demonstrere effektiv bruk av teknologien i samsvar med dens design og tiltenkte formål. Eksempler inkluderer, men er ikke begrenset til: EMV, Punkt-til-punkt-kryptering, and tokenisering.

Security Technology Enhancement Programme (STEP) er American Express' forbedringsprogram for sikkerhetsteknologi der Forhandlerne oppfordres til å bruke teknologier som forbedrer datasikkerheten.

Self-Assessment Questionnaire (SAQ) betyr et verktøy for egenvurdering opprettet av Payment Card Industry Security Standards Council, LLC, utarbeidet for evaluering og bekreftelse av samsvar med PCI DSS.

Sensitive autentiseringsdata betyr sikkerhetsrelatert informasjon brukt for å autentisere kortholdere og/eller autorisere betalingskorttransaksjoner. Denne informasjonen inkluderer, men er ikke begrenset til, kortverifiseringskoder, fullstendige spordata (fra magnetstripe eller tilsvarende på en chip), PIN-koder og PIN-blokker.

Sluttrapportmal for rettsmedisinsk hendelse betyr malen som er tilgjengelig fra PCI Security Standards Council, som er tilgjengelig på www.pcisecuritystandards.org.

Tjenesteleverandører betyr autoriserte databehandlere, tredjeparts databehandlere, gateway-leverandører, installatører av betalingssystemer og andre leverandører til Forhandlere av Betalingssystemer, betalingsløsninger eller -tjenester.

Token betyr det kryptografiske tokenet som erstatter PAN, basert på en gitt indeks for en uforutsigbar verdi.

Transaksjon betyr en Belastning, Kreditering, Kontantforskudd (eller annen kontanttilgang) eller minibanktransaksjon fullført med en Kort.

Transaksjonsdata betyr enhver informasjon som kreves av American Express, som dokumenterer en eller flere transaksjoner, inkludert informasjon innhentet på salgspunktet, informasjon innhentet eller generert under Autorisering og Innsending, samt eventuell Tilbakeføring.

Transaksjoner som er initiert av kjøpere (BIP) betyr en digital betalingsløsning som lar kjøpere raskt og effektivt planlegge betalinger til leverandører (koblet til bedritskort).

Valideringsdokumentasjon betyr en AOC som er gitt i forbindelse med en årlig sikkerhetsvurdering på stedet eller SAQ, AOSC og kortfattet sammendrag av funnene gjengitt i forbindelse med Kvartalsvise nettverksskanninger eller den årlige Security Technology Enhancement Programme-sertifiseringen (forbedringsprogram for sikkerhetsteknologi).

Varslingsdato betyr datoen som American Express gir utstedere det endelige varselet om en Datahendelse. En slik dato er betinget av at American Express mottar den endelige etterforskningsrapporten eller den interne analysen og bestemmes utelukkende etter American Express' eget skjønn.

Punkt 9 Nyttige nettsteder

American Express Data Security: www.americanexpress.com/datasecurity

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

EMVCo: www.emvco.com