FORSKRIFTER FOR SALG MOT BETALING
MED KONTOKORT
DISTANSEHANDEL (Card Not Present)
(Oktober 2015)

Disse forskriftene, "Distansehandelsforskriftene", gjelder for salg mot betaling med Kontokort ved Distansehandel. Med "Distansehandel" menes Salgsmåter der Kontokort ikke er til stede i betalingssituasjonen. De "Salgsmåtene" som omfattes av Distansehandelsforskriftene, er for eksempel salg over Internett, salg mot postordre og/eller telefonbestilling, mobilbetaling, regelmessige betalinger som lagret kortnummer (såkalt "Account on File") og abonnementsbetalinger (såkalt "Recurring Payments").

Distansehandelsforskriftene supplerer de Generelle vilkårene for innløsning av kontokorttransaksjoner som gjelder for den avtalen om Innløsning av Kontokorttransaksjoner ("Hoveddokumentet") som er inngått mellom Salgsforetaket og Bambora. Ved eventuelle konflikter mellom Hoveddokumentet og Distansehandelsforskriftene skal Distansehandelsforskriftene ha fortrinnsrett. Ord som skrives med stor forbokstav, er ord som har fått særlig betydning/definisjon i Hoveddokumentet, og som i disse Distansehandelsforskriftene skal ha samme betydning som de har i Hoveddokumentet.

1. Generelt om salg mot betaling med Kontokort ved Distansehandel

Ved salg med Kontokort via Internett godtas samtlige Kontokort i henhold til Avtalen samt, der det er hensiktsmessig, MasterPass og V.me, bortsett fra Maestro-kort, som bare kan godtas dersom 3D Secure er installert og aktivert. Ved Telefonbestilling og Postordre godtas imidlertid aldri Maestro.

2. Særlige forpliktelser ved Distansehandel

Salgsforetaket påtar seg følgende:

- På bestillingsskjemaet eller Internett-siden tydelig å informere kortinnehaveren, før betalingsinstruksjonene, om hvilket land Transaksjonen skjer i samt hvilket land Salgsforetaket betaler merverdiavgift i,
- Ikke å ha informasjon eller lenker på sin hjemmeside til hjemmesider med ulovlig og/eller etter Bamboras vurdering uetisk virksomhet eller til virksomhet som av objektive årsaker må anses å skade Bamboras anseelse,
- Umiddelbart å underrette Bambora om hjemmesiden der Salgsforetakets salg skjer, der www-adresser byttes og/eller nye www-adresser innføres som Salgsforetaket bruker til sitt salg med kontokort.

3. Kontroller

Før Salgsforetaket debiterer kortinnehaveren, skal Salgsforetaket utføre kontrollene angitt under:

3.1 Autorisering
Autorisering skal alltid skje i betalingssituasjonen, uansett kjøpsbeløp. Autoriseringen skal kodes med korrekt Salgsmåte.

Ved kontroll av status på Kortinnehaverens Kontokort (kontroll av kortstatus) skal det alltid brukes en såkalt "nullverdiautorisasjon".

3.2 Identifisering av Kortinnehaver

3.2.1 Internett
Korttransaksjon skal være gjennomført i henhold til 3D Secure dersom ikke annet er avtalt mellom partene.

3.2.2 Telefonbestilling og Postordre
Ved Telefonbestilling og Postordre kan ikke Salgsforetaket sikre Kortinnehaverens identitet. Salgsforetaket står derfor alltid for risikoen for samtlige kjøpstransaksjoner ved Telefonbestilling og Postordre. Dette betyr at Bambora har rett til å tilbakedebitere Salgsforetaket for beløp som Kortinnehaver reklamerer på. Dette gjelder uansett om Kortinnehaverens innvending er berettiget eller ikke.

3.2.3 Postordre
Postordregrunnlaget skal sendes i lukket forsendelse til Salgsforetaket og inneholde:

- Salgsforetakets navn, sted og organisasjonsnummer,
- Kortinnehaverens navn,
- Kortinnehaverens adresse (leveringsadresse),
- Kortinnehaverens telefonnummer,
- Navn på Kortutsteder,
- Kontokortnummer,
- Kontokortets gyldighetstid,
- Bestillingsdato,
- Totalbeløp for bestillingen,
- Opplysninger om merverdiavgift,
- Beskrivelse av bestilte varer, samt
- Kortinnehaverens signatur.

3.2.4 Lagring
Salgsforetaket skal i minst 18 måneder arkivere bestillingsskjema/bestillingsgrunnlag i samsvar med Payment Card Industry (PCI) Data Security Standard (DSS). På forespørsel fra Bambora skal Salgsforetaket innen fem (5) bankdager legge frem bestillingsskjema/bestillingsgrunnlag som gjelder enkelte Transaksjoner.

3.3 Mottaksbevis
Ved levering av varer eller billetter som kan leveres fysisk, anbefales leveringsmåter, for eksempel postpakke eller brev, der det kan utstedes signert mottaksbevis med Legitimasjonskontroll ved utleveringen. Ved levering av høyrisikovarer kreves imidlertid mottaksbevis, se punkt 5.2. Dersom Kortinnehaver reklamerer på kjøp og det er benyttet mottaksbevis, forenkler det den senere utredningen. Utredning kan imidlertid påvise at Bambora likevel har rett til Tilbakedebitering av innløst Korttransaksjon i henhold til reglene i Generelle vilkår.

Salgsforetaket står for all risiko for Tilbakedebiteringer av innløste Korttransaksjoner i henhold til reglene i Generelle vilkår dersom Kortinnehaveren bestrider at vare eller tjeneste er mottatt, uansett hvordan Kortinnehaveren har identifisert seg i henhold til punkt 3.3.

4. Rapportering

4.1 Innsending av kjøpstransaksjoner m.m.
Elektronisk innsamlede kjøpstransaksjoner skal overføres til Bambora senest innen to (2) dager fra betalingsdatoen. Med "betalingsdatoen" menes datoen for autoriseringen. For miljøer som for eksempel hoteller, der det skjer en såkalt forhåndsautorisasjon, skal kjøpstransaksjonen være mottatt av Bambora innen tretti (30) dager.

4.2 Transaksjonsinformasjon
Salgsforetaket skal ved levering av vare eller tjeneste gi Kortinnehaveren Kundekvittering via e-post eller sammen med vare/tjeneste ved levering. Kundekvitteringen skal inneholde følgende informasjon:

- Ordet "kvittering" i overskriften,
- Salgsforetakets navn. Navnet skal være det samme som er oppgitt i Avtalen til Bambora, og som dermed angis på Kortinnehaverens kontoutdrag,
- Telefonnummer og e-postadresse til Salgsforetakets kundeservice,
- Der det er hensiktsmessig, Salgsforetakets hjemmeside (webadresse),
- Trunkert Kontokortnummer,
- Korttransaksjonens beløp sammen med transaksjonsvaluta,
- Transaksjonsdato og klokkeslett,
- Unikt transaksjonsnummer/ordrenummer som identifiserer transaksjonen,
- Mottatt Kontrollnummer fra Autorisering,
- Der det er hensiktsmessig, opplysning om at det gjelder en Internett-transaksjon,
- Transaksjonstype (kjøp eller retur),
- Beskrivelse av bestilte varer og tjenester,
- Retur- og tilbakebetalingsregler,
- Andre opplysninger i henhold til de til enhver tid gjeldende lover,
- Ved Telefonbestilling skal Salgsforetaket på Kortinnehaverens kvittering skrive "TO" eller "Telephone Order" og
- Ved Postordre skal Salgsforetaket skrive "MO" eller "Mailorder".

I de tilfellene der fysisk kvittering på gjennomført og rapportert Korttransaksjon ikke foreligger, for eksempel ved visse former for Internett-handel, skal Salgsforetaket opprette og lagre Transaksjonslogg og på forespørsel fra Bambora utlevere følgende informasjon om:

Korttransaksjonen:
- Salgsforetakets navn,
- Salgsforetakets rapporteringsnummer hos Bambora,
- Der det er hensiktsmessig, Salgsforetakets hjemmeside (webadresse),
- Beskrivelse av varer og tjenester,
- Mottakerens navn og leveringsadresse og, der det er hensiktsmessig, mottakerens metode for å autentisere seg, for eksempel 3D Secure-kode,
- Trunkert Kontokortnummer,
- Korttransaksjonens beløp sammen med transaksjonsvaluta og mva.,
- Transaksjonsdato og klokkeslett,
- Unikt transaksjonsnummer/ordrenummer som identifiserer transaksjonen,
- Mottatt Kontrollnummer fra Autorisering,

- Transaksjonstype (kjøp eller retur),
- Indikator for elektronisk handel,
- Bestillerens IP-adresse.

Transaksjonsloggen skal oppfylle kravene i henhold til PCI DSS.

Salgsforetaket skal på forespørsel fra Bambora legge frem informasjon om Korttransaksjonen fra system som håndterer 3D Secure. Dersom dette systemet håndteres av Payment Service Provider (PSP), skal Salgsforetaket sikre at PSP kan forevise denne informasjonen på oppdrag fra Salgsforetaket. Dette gjelder også ved forespørsel om informasjon om Korttransaksjon i Transaksjonslogg.

5. Annet

5.1 Salgssted
Stedet der Salgsstedets salg foregår på Internett, skal minst inneholde følgende informasjon:

- Salgsforetakets navn. Navnet skal være det samme som er oppgitt til Bambora i Avtalen, og som dermed angis på Kortinnehaverens kontoutdrag,
- Landet der Salgsforetaket er registrert,
- Beskrivelse av varer og tjenester som tilbys,
- Priser,
- Transaksjonsvaluta,
- Skatter og andre myndighetspålegg,
- Reklamasjonsregler, retur- og tilbakebetalingsregler samt leveringsvilkår,
- Fraktkostnader,
- Kundeservicekontakt, e-postadresse og telefonnummer,
- Salgsforetakets besøksadresse,
- Eventuelle eksportrestriksjoner,
- Logotyper for Kontokort som Salgsforetaket godtar,
- Der det er hensiktsmessig, logotyper for Verified by Visa og MasterCard SecureCode samt V.me og MasterPass samt
- Andre opplysninger i henhold til de lover som til enhver tid gjelder for Salgsforetaket.

Salgsforetaket påtar seg å stille til rådighet korrekt informasjon og løpende oppdatere informasjonen på hjemmesiden med tanke på punktene over.

5.2 Risikoreduksjon
Aktivert støtte for 3D Secure, MasterPass og V.me på Salgsforetakets hjemmeside på Internett betyr at Salgsforetaket får en såkalt risikoreduksjon, som betyr at Kortutstederen vanligvis ikke kan reklamere på svindel i forbindelse med Korttransaksjoner.

Denne risikoreduksjonen gjelder for Kontokort med varemerkene Visa, MasterCard og Maestro samt hvis MasterPass og V.me godtas. For Kontokort med varemerket Visa

omfatter risikoreduksjonen imidlertid for tiden ikke foretakskort og innkjøpskort (såkalte corporate/commercial cards) utstedt av Kortutsteder utenfor Europa.

Bambora er ikke ansvarlig for å informere Salgsforetaket om korttyper og utstedelsesland eller for advarsler og/eller kontroller dersom Kontokort omfattes av risikoreduksjonen.

Bambora har rett til å oppheve retten til risikoreduksjon dersom svindelnivåene ifølge Kortnettverkets vurdering overskrider de til enhver tid tillatte nivåene.

Salgsforetaket er klar over at 3D Secure, MasterPass og V.me ikke er noen garanti for å beskytte seg mot svindel i forbindelse med Korttransaksjoner.

Ved salg av høyrisikovarer som for eksempel hjemmeelektronikk, klokker, smykker og gavekort, er Salgsforetaket klar over sin risikoeksponering for svindel i forbindelse med Korttransaksjoner, siden dette er varer som ofte utsettes for kortsvindel. Det kreves mottaksbevis for leveringene.

Salgsforetaket skal på egen bekostning implementere eller skaffe til veie systemer for å forhindre svindel ved bestillinger.

Salgsforetaket står for all risiko for Korttransaksjoner, dersom det ikke anvendes risikoreduksjon som finnes i henhold til 3D Secure, MasterPass og V.me.

5.3 Særskilt for Recurring Payments (regelmessige betalinger) ved salg over Internett

- Når Salgsforetaket knytter til seg en ny Kortinnehaver for regelmessige betalinger og debitering ikke er aktuelt ved tilknytningen, skal det gjennomføres en såkalt kontroll av statusen på Kortinnehaverens Kontokort, en såkalt "nullverdiautorisasjon".
- Når Salgsforetaket knytter til seg en ny Kortinnehaver som betaler med Kontokort, sender Salgsforetaket den første debiteringstransaksjonen i henhold til 3D Secure. For denne transaksjonen gjelder den til enhver tid gjeldende risikoreduksjonen i henhold til 3D Secure.
- Ved etterfølgende regelmessige kortbetalinger (debiteringer) gjelder ikke risikoreduksjonen i henhold til 3D Secure, og dermed står Salgsforetaket for all risiko, dersom ikke annet er avtalt.
- Når en Kortinnehaver registrerer seg og inngår avtale om regelmessig kortbetaling, skal Kortinnehaveren motta kvittering på e-post. Kvitteringen skal inneholde teksten "regelmessig kortbetaling" og inneholde informasjon om beløpets størrelse, hvor ofte debitering skjer og hvor lenge avtalen gjelder. Det skal fremgå om det gjelder et fast eller et variabelt beløp.
- Når en Kortinnehaver betaler for varer og/eller tjenester hos Salgsforetaket, kan ikke Salgsforetaket knytte Kortinnehaveren til Recurring Payments uten at dette tydelig fremgår og Kortinnehaveren godtar dette.
- Kortinnehaveren skal motta en e-postmelding før hver debitering.
- Kortinnehaver skal motta en e-postmelding før utgangen av eventuelle "gratisperioder" eller andre typer introduksjonstilbud.
- Kortinnehaver skal løpende informeres på e-post om eventuelle endringer i debiteringene, for eksempel endring av for eksempel beløp eller dato for debitering.

- Kortinnehaveren skal kunne avbryte den regelmessige kortbetalingen med umiddelbar virkning.
- Salgsforetaket kan ikke lagre Kontokortnummer og annen Kontokortinformasjon i eget system dersom ikke sikkerhetskontroll og, der det er hensiktsmessig, sertifisering i henhold til Kortnettverkets krav (PCI DSS) er gjennomført og godkjent.
- Salgsforetaket skal kunne legge frem dokumentasjon fra programvaren som håndterer 3D Secure, og Kundekvittering som gjelder Kortinnehaverens valg av debiteringsfrekvens og hvor lang tidsperiode Kortinnehaveren har tillatt Recurring Payments for.
- Korttransaksjon skal inneholde informasjon om Recurring Payment. Salgsforetaket er ansvarlig for å stille krav til PSP, slik at korttransaksjonenes innhold samsvarer med Generelle vilkår, Forskrifter og Instruksjoner.
- Korttransaksjon skal alltid kontrolleres gjennom Autorisering før hver debitering. Dersom Autorisering avslås, kan ikke debitering gjennomføres.
- Det beløpet som ifølge avtale med Kortinnehaver skal debiteres, kan ikke endres uten samtykke fra Kortinnehaver.

5.4 Spesielt for Account on File ved salg over Internett

- Når Salgsforetaket knytter til seg en ny Kortinnehaver som betaler med Kontokort, sender Salgsforetaket den første transaksjonen i henhold til 3D Secure. For denne transaksjonen gjelder den til enhver tid gjeldende risikoreduksjonen i henhold til 3D Secure.
- Når salgsforetaket knytter til seg en ny Kortinnehaver for regelmessige betalinger og debitering ikke er aktuelt ved tilknytningen, skal det gjennomføres en såkalt kontroll av statusen på Kortinnehaverens Kontokort, en såkalt "nullverdiautorisasjon".
- Ved etterfølgende kortbetalinger (debiteringer) gjelder ikke risikoreduksjonen i henhold til 3D Secure, og dermed står Salgsforetaket for all risiko, dersom ikke annet er avtalt.

6. Sikkerhet

6.1 Håndtering av visse typer kontokortinformasjon

For dels å beholde et høyt sikkerhetsnivå i de globale kortbetalingssystemene og dels å styrke tilliten til Kontokort som betalingsmiddel er det ytterst viktig at alle som håndterer Kontokortinformasjon, gjør det på en sikker måte. Med "Kontokortinformasjon" menes slik informasjon som er preget eller trykt på Kontokortets frem- og bakside, inkludert informasjon som ligger lagret på Kontokortets magnetspor og chip. Av denne grunn har Kortnettverket blitt enige om en felles standard for håndtering av Kontokortinformasjon. Standarden kalles Payment Card Industry (PCI) Data Security Standard (DSS) og er utarbeidet av de internasjonale kortnettverkene Visa og MasterCard.

Salgsforetaket forplikter seg til å følge standarden PCI DSS i den versjonen som til enhver tid finnes publisert på www.pcisecuritystandards.org.

6.2 Godkjenning av system

System som leverer transaksjoner til Bambora, skal være godkjent av Bambora eller annen tredjepart som Bambora utpeker. Bambora kan stille krav til særlig kontroll av

komponenter som ut fra et sikkerhetssynspunkt er sensitive. Denne kontrollen eller skanningen utføres av en aktør utvalgt i samråd med Bambora.

6.3 Særskilt om Payment Service Providers
Bruker Salgsforetaket en tredjepart (såkalt Payment Service Provider) til deler av eller all Distansehandel, må Salgsforetaket sikre at denne oppfyller alle krav i henhold til PCI DSS.

6.4 Endringer i system m.m.
Endringer i systemet som påvirker de forutsetningene som gjaldt på tidspunktet for godkjenning, kan ikke gjennomføres uten godkjenning fra Bambora.

Salgsforetaket skal gjennomføre en test anvist av Bambora av oppkoblingen mot Bamboras mottakssystem før Transaksjoner kan sendes inn til Bambora. Salgsforetaket skal informere Bambora før hver installasjon, omflytting eller avvikling av utstyr som er teknisk tilkoblet til Bambora eller annen innsamler av Transaksjoner som fungerer på oppdrag fra Salgsforetaket innenfor rammene av denne avtalen.

6.5 Datainnbrudd og IT-rettslige undersøkelser
Dersom Bambora mistenker at Salgsforetakets kassesystem, datasystem e.l. har vært utsatt for innbrudd, manipulasjon e.l. som etter Bamboras vurdering på noen måte angår Partenes samarbeid i henhold til denne Avtalen, har Bambora rett til å gjennomføre en IT-rettslig undersøkelse ("Undersøkelsen") av det aktuelle utstyret. Undersøkelsen skal gjennomføres av Bambora eller av et IT-rettslig foretak utpekt av Bambora.

Tidspunkt, og spørsmål/rutiner som henger sammen med dette og som kan henføres til gjennomføringen av Undersøkelsen, skal, dersom Bambora ikke vurderer dette som u-passende, så langt det er mulig avtales mellom Partene. Bambora kan imidlertid også, dersom dette etter Bamboras mening er det mest formålstjenlige, besøke Salgsforetaket og gjennomføre Undersøkelsen uten at Salgsforetaket har blitt underrettet om dette på forhånd.

Salgsforetaket plikter i rimelig omfang å medvirke ved Undersøkelsen og tilrettelegge for gjennomføringen slik at formålet med Undersøkelsen, dvs. å konstatere om det har forekommet innbrudd/manipulasjon, kan oppnås.

Dersom Undersøkelsen fører til at det konstateres at Salgsforetakets kassesystem, datasystem e.l. har blitt utsatt for innbrudd, manipulasjon e.l., plikter Salgsforetaket på forespørsel fra Bambora å dekke Bamboras kostnader til Undersøkelsen.