

FORSKRIFTER FOR SALG MOT BETALING MED KONTOKORT ¹
UBEMANNET TERMINAL
(Juli 2010)

Disse forskrifter, "Forskrifter for ubemannet terminal", gjelder ved salg mot betaling med Kontokort i ubemannede terminaler, som bensinpumper, parkeringsautomater og veibommer.

Forskriftene utfyller de alminnelige vilkårene som gjelder for den avtalen om Innløsning av Kontokorttransaksjoner ("Hoveddokumentet") som er inngått mellom Salgsforetaket og Euroline. Ved eventuelle konflikter mellom Hoveddokumentet og Kontantuttaksforskriftene, skal Kontantuttaksforskriftene gå foran.

1. Typer av Terminaler for ubemannet miljø

Type 1 gjelder ubemannet terminal, som f eks vareautomat eller bensinpumpe der verifisering gjøres med PIN-kode og autorisering fra 0 kr. Dersom sluttbeløpet ikke er kjent når autoriseringen skjer, gjelder Eurolines til enhver tid gjeldende rutinebeskrivelse. Beløpet ved betaling med Kontokort i dette miljøet må ikke overstige SEK 600.

Type 2 gjelder ubemannet terminal som mangler mulighet til verifisering med PIN-kode, men med autorisering fra 0 kr.

Type 3 gjelder ubemannet terminal der sperrekontroll skjer mot lokalt sperreregister i Salgsforetakets system. Rutiner for slik sperrehåndtering spesifiseres i bilag til Avtalen. Beløpet ved betaling med Kontokort i dette miljøet må ikke overstige SEK 500.

Chip og Pin-terminaler

Fra og med 1. januar 2011 skal terminaler som anvendes for å gjennomføre transaksjoner med Kontokort, støtte så vel magnetsporlest som EMV-chip teknologi. MasterCard og VISA kan komme til å ilegge Euroline en avgift dersom Salgsselskapet ikke overholder det ovenstående. Salgsselskapet er i dette tilfellet i henhold til punkt 6.3 og 6.4 i Hoveddokumentet forpliktet til å godtgjøre Euroline for slike avgifter.

2. Kundekvittering

Kundekvittering skal alltid leveres og inneholde følgende opplysninger:

- Salgsforetakets navn, sted og organisasjonsnummer
 - Dato
 - Kontokortets nummer skal angis i trunkert form, dvs at bare de 4 (fire) siste sifrene skrives ut, innledende posisjoner trunkeres med "***"
 - Beløp
 - Opplysninger om merverdiavgift
 - Referanse / gjenfinningsnummer (unik identitet for Transaksjonen),
-

3. Bruk av PIN

Dersom Terminalen håndterer PIN, skal kortinnehaveren skal gis 3 (tre) forsøk på å identifisere seg ved hjelp av PIN-kode. Dersom gal PIN-kode tastes inn 3 (tre) ganger i rekkefølge, skal utstyret om mulig beholde kortet. Disse kortene klippes i stykker og sendes vedkommende kortutsteder. Kortinnehaveren skal ha mulighet til å avbryte en Transaksjon i stedet for å gjøre flere forsøk med PIN-kode.

4. Transaksjonsinnsamling

Innsamling av kjøpstransaksjoner med Kontokort der navn og/eller nummer ikke er preget (f eks Kontokort med varemerkene Maestro eller Electron) kan bare skje i Terminal type 1.

5. Regnskap

5.1 Innsending av kjøpstransaksjoner

Elektronisk innsamlede kjøpstransaksjoner skal senest innen 2 (to) dager fra dagen for betalingen overføres til Euroline. Med "dagen for betalingen" menes dagen for autoriseringen.

5.2 Transaksjonsjournal

Salgsforetaket skal føre en særskilt journal over samtlige Transaksjoner der et Kontokort er brukt, dvs. så vel gjennomførte som avbrutte Transaksjoner. Journalen skal vise:

- på hvilken måte Transaksjonen er gjennomført,
- Salgsforetakets navn (firma), sted og organisasjonsnummer
- dato og klokkeslett
- Kontokortets nummer (forutsatt at Terminalen støtter det, skal det skje i trunkert form)
- betalingsmåte (se punkt 2.1 annet avsnitt ovenfor)
- transaksjonstype (uttak eller retur/kreditering) i klartekst,
- kasseidentitet,
- kontrollnummer som bevis på autorisering,
- beløp som skal debiteres,
- referanse/gjenfinningsnummer,
- svarkode.

5.3 Lagring

Salgsforetaket skal i minst 18 (atten) måneder arkivere Transaksjonsjournalen i henhold til de sist gjeldende reglene for PCI DSS (se punkt 6.1 nedenfor). På Eurolines anmodning skal Salgsforetaket innen 5 (fem) dager kunne fremlegge en signaturkvittering når det gjelder en enkelt Transaksjon. Dette gjelder selv om Salgsforetakets innløsningsavtale med Euroline ellers har opphørt

6. Sikkerhet

6.1 Håndtering av Kontokortopplysninger

For dels å beholde et høyt sikkerhetsnivå i de globale kortbetalingssystemene, dels å styrke tilliten til Kontokort som betalingsmiddel, er det av ytterste viktighet at alle som håndterer Kontokortopplysninger gjør det på en sikker måte. "Kontokortopplysninger" betyr opplysninger som er preget eller trykket på Kontokortets for- og/eller bakside, herunder opplysninger som finnes lagret i Kontokortets magnetspor og chip. Av denne grunn har kortbransjen blitt enige om en felles standard for håndtering av Kontokortopplysninger. Standarden kalles Payment Card Industry (PCI) Data Security Standard (DSS) og er utviklet av de internasjonale kortnettverkene Visa og MasterCard.

Salgsforetaket forplikter seg til å følge standarden PCI DSS i den utgave den til enhver tid finnes offentliggjort i på www.pcisecuritystandards.org.

Dette innebærer bl.a. at Salgsforetaket:

- ikke under noen som helst omstendigheter må lagre eller skrive ut i) CVV/CVC (dvs. kortverifiseringsverdien i Kontokortets magnetstripe), ii) CVV2/CVC2 (dvs. den sikkerhetskode som normalt finnes i slutten av signaturfeltet på Kontokortets bakside) eller iii) iCVV/iCVC (dvs. verifiseringsverdien i et Kontokort som er utstyrt med chip). Salgsforetaket forplikter seg også til ikke å lagre eller skrive ut PVV (dvs. verifiseringsverdien for PIN-koder)
- bare kan lagre Kontokortopplysninger som er absolutt nødvendig for Salgsforetakets virksomhet (dvs. navn, Kontokortets nummer og Kontokortets gyldighetstid)
- må oppbevare/lagre media som inneholder Kontokortopplysninger (f eks logger, transaksjonsrapporter, elektroniske kvitteringer eller avtaler) på et sikkert sted og på slik måte at bare personer som har behov for tilgang til vedkommende materiale gis slik tilgang
- må håndtere all Kontokortopplysninger konfidensielt og ikke meddele utenforstående noe om de personopplysninger (f eks navn og personnummer) som Salgsforetaket kan komme i besittelse av
- må oppbevare opplysninger om Kontokortets nummer på slik måte at ingen uberettiget bruk kan forekomme
- må påse at elektroniske kvitteringer og andre medier er beskyttet mot uberettiget tilgang
- umiddelbart melder fra til Euroline dersom Salgsforetaket oppdager, eller har mistanke om, at informasjon om et Kontokort er brukt på uberettiget måte eller på annen måte er misbrukt. Ved mistanke om misbruk skal Salgsforetaket på Eurolines anmodning også politianmelde hendelsen
- må påse at Kontokortets nummer ikke vises for andre personer enn de personer hos Salgsforetaket som har behov for tilgang til det
- må påse at det dokumenteres hvordan Kontokortopplysninger beskyttes i Salgsforetakets tekniske utstyr
- må påse at det finnes rutiner for sikker håndtering og distribuering av Kontokortopplysninger og at disse rutinene regelmessig følges opp og kontrolleres. Rutinene, eller informasjon om dem, skal ødelegges på sikker måte, f eks ved hjelp av makuleringsmaskin, når rutinene/informasjonen ikke lenger behøves i henhold til gjeldende lovgivning og/eller Instruksjonene
- må påse at det finnes en fortegnelse over alt teknisk utstyr og at dette utstyret oppbevares på sikker måte
- må påse at teknisk utstyr og/eller annet medium som inneholder Kontokortopplysninger og/eller opplysninger om kortinnehaver, gjøres ubrukbart så snart slike opplysninger ikke lenger skal anvendes av Salgsforetaket.

6.2 Godkjenning av system

Terminaler som leverer Transaksjoner til Euroline må være godkjent av Euroline eller av tredjepart som Euroline utpeker. Euroline kan stille krav om særskilt undersøkelse av følsomme komponenter fra et sikkerhetsmessig synspunkt.

6.3 Særskilt om s.k. Noder og Payment Service Providers

Anvender Salgsforetaket en tredjepart (s.k. node eller Payment Service Provider) som del av sin betalingsløsning for håndtering av Transaksjoner, må Salgsforetaket sikre at denne oppfyller alle krav i henhold til PCI DSS

6.4 Endringer av utstyr m.m.

Salgsforetaket må informere Euroline før hver installasjon, flytting eller avvikling av utstyr som er teknisk tilkoblet Euroline eller annen innsamler av Transaksjoner.

Endringer i Terminaler som påvirker de forutsetninger som gjaldt på tidspunktet for godkjenningen, må ikke foretas uten Eurolines samtykk.

Salgsforetaket må innen Transaksjoner kan overføres til Euroline, gjennomføre en test anvist av Euroline av sin oppkobling mot Euroline mottakssystem.

6.5 Særskilt om kassesystemer med integrert kortleser/Sikkerhetsregler

Salgsforetaket som anvender kassesystemer med integrert kortleser, må også påse at de Sikkerhetsregler som til enhver tid er fastsatt av Euroline følges.

6.6 Datainntrengning og IT-teknisk undersøkelse

Dersom Euroline har mistanke om at Salgsforetakets kassesystem, datasystem e.l. er utsatt for inntrengning, manipulasjon e.l. som etter Eurolines mening på noen måte berører Partenes samarbeid i henhold til denne Avtale, har Euroline rett til å gjennomføre en s.k. IT-teknisk undersøkelse ("Undersøkelsen") av vedkommende utstyr. Undersøkelsen kan gjennomføres av Euroline eller av et IT-teknisk foretak engasjert av Euroline.

Tidspunkt, og spørsmål/rutiner i den forbindelse som gjelder gjennomføringen av Undersøkelsen, skal dersom Euroline ikke anser det som uegnet, i størst mulig utstrekning avtales mellom Partene. Euroline har allikevel rett til, dersom det etter Euroline mening er mest formålstjenlig, å besøke Salgsforetaket og gjennomføre Undersøkelsen uten at Salgsforetaket på forhånd underrettes om dette.

Det påligger Salgsforetaket i rimelig utstrekning å medvirke ved Undersøkelsen og lette gjennomføringen, slik at hensikten med Undersøkelsen, dvs. å fastslå hvordan inntrengning /manipulasjon har skjedd, kan oppnås.

Dersom det gjennom Undersøkelsen konstateres at Salgsforetakets kassesystem, datasystem e.l. har vært utsatt for inntrengning, manipulasjon e.l., skal Salgsforetaket på Eurolines anmodning erstatte Euroline kostnadene for Undersøkelsen.

7. Liability Shift

For Transaksjoner foretatt fra og med 1. januar 2009 kommer Euroline til å anvende et såkalt Liability Shift. Dette innebærer at Salgsforetaket fra og med samme dato i forhold til Euroline i følge Avtalen bærer risikoen for samtlige tap som kan henføres til magnetporleste Transaksjoner foretatt med uberettiget fremstilte kort der det korrekte Kontokortet, dvs det Kontokort som er utferdiget av berettiget/lisensiert kortutgiver med samme kortnummer som det uberettiget fremstilte, er utstyrt med en såkalt EMV-chip.