Kammeradvokaten

5. NOVEMBER 2015

7512099 JKA/MSO/BHA

Notat om Rejsekort A/S' behandling af personoplysninger

Kammeradvokaten
Vester Farimagsgade 23
DK-1606 København V

Telefon +45 33 15 20 10
Fax +45 33 15 61 15
www.kammeradvokaten.dk

Indhold

1. INDLEDNING

Transportministeriet har bedt om min vurdering af, hvorvidt Rejsekort A/S overholder sine persondataretlige forpligtelser ved selskabets administration af "Rejsekortet". Ministeriet har endvidere bedt mig komme med forslag til fremadrettede initiativer til forbedring af selskabets håndtering af personoplysninger i rejsekortsystemet.

Efter aftale med Transportministeriet vil min vurdering navnlig vedrøre spørgsmålene om, hvordan og i hvilket omfang Rejsekort A/S indsamler personoplysninger om sine kunder, hvilken adgang der er hos Rejsekort A/S og de tilsluttede trafikselskaber til de opbevarede personoplysninger og hvor længe Rejsekort A/S må opbevare personoplysningerne.

Som led i mit arbejde har jeg modtaget og gennemgået en betydelig mængde dokumentation fra Rejsekort A/S vedrørende virksomhedens behandling af personoplysninger (se bilag 1). Jeg har herudover afholdt en række møder med Rejsekort A/S, hvor virksomheden har oplyst mig om dens behandling af personoplysninger. Jeg har desuden afholdt møder med henholdsvis Finanstilsynet og Erhvervsstyrelsen vedrørende spørgsmålet om opbevaringsperioden for de registrerede personoplysninger efter særlovgivningen. Mit notat er udarbejdet på baggrund af de tilsendte dokumenter, samt de oplysninger, som er fremkommet på de afholdte møder.

2. SAMMENFATNING OG ANBEFALINGER

Persondataloven finder anvendelse i forhold til Rejsekort A/S' behandling af de indsamlede oplysninger om kunderne til rejsekortet, da der derved foretages elektronisk behandling af personoplysninger i personhenførbar form. Rejsekort A/S er dataansvarlig i forhold til de behandlede oplysninger. Persondatalovens forpligtelser påhviler derfor i første række Rejsekort A/S.

Rejsekort A/S' indsamling og øvrige behandling af personoplysninger, som et led i driften af rejsekortet, er ganske omfattende. Rejsekort A/S behandler primært almindelige personoplysninger, men også i begrænset omfang følsomme personoplysninger. På grund af den måde Rejsekort A/S har tilrettelagt sin drift, har et stort antal personer (efter det oplyste mere end 1.100 personer) adgang til personoplysninger, herunder økonomiske oplysninger og rejseoplysninger, jf. nedenfor.

Overordnet set er det min vurdering, at Rejsekort A/S behandler personoplysninger i overensstemmelse med persondatalovens regler. Jeg har imidlertid på baggrund af min gennemgang konstateret en række punkter, hvor Rejsekort A/S kan forbedre deres overholdelse af persondataretten. Jeg kommer derfor i det følgende med en række anbefalinger til ændringer i Rejsekort A/S' indsamling, behandling og sletning af personoplysninger i rejsekortsystemet.

…….

Efter persondatalovens § 5, stk. 1, skal oplysninger behandles i overensstemmelse med god databehandlingsskik. Efter § 5, stk. 2, 1. pkt., må indsamling af oplysninger alene ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål. Det følger af § 5, stk. 3, at behandling af oplysninger skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Formålene med Rejsekort A/S' behandling af personoplysningerne er således udtrykkeligt opregnet som formålet om at administrere og betjene kunderne, at overholde gældende lovgivning, at kunne dokumentere rejsernes pris overfor kunderne i tilfælde af uenighed herom, samt at opdage og forhindre overtrædelse af regler, vilkår m.v., hvilket må anses for saglige formål. Der er endvidere ikke grundlag for at antage, at Rejsekort A/S foretager en senere behandling af personoplysningerne, der i almindelighed er uforenelig med disse formål.

Rejsekort A/S indsamler og behandler endvidere efter min opfattelse i almindelighed kun de relevante og nødvendige oplysninger, som er et led i driften af rejsekortet som rejsehjemmel. Jeg har således ikke i min gennemgang fået grundlag for at antage, at Rejsekort A/S systematisk indsamler og behandler personoplysninger i videre omfang end Rejsekort A/S' behov tilsiger, jf. dog nedenfor om opbevaringsperioden. Rejsekort A/S har endvidere efter min opfattelse etableret en række adækvate procedurer, der sikrer at oplysningerne er ajourførte og korrekte.

Rejsekort A/S har desuden efter min opfattelse i almindelighed tilstrækkelig behandlingshjemmel til at indsamle og behandle både de almindelige og ikke-fortrolige personoplysninger samt de følsomme personoplysninger, fordi Rejsekort A/S får samtykke til behandlingen fra de registrerede kunder, jf. henholdsvis persondatalovens § 6, stk. 1, nr. 1, og § 7, stk. 2, nr. 1, og § 8, stk. 4. Tilsvarende gælder i forhold til Rejsekort A/S' behandling af oplysninger om kundernes CPR-numre, jf. lovens § 11, stk. 2, nr. 2.

Det kræver dog imidlertid, at samtykkeerklæringerne er fyldestgørende udformet, således at der foreligger et informeret samtykke fra den, som oplysningerne vedrører. Det er ikke på alle punkter tilfældet. Jeg anbefaler derfor en række udbygninger i samtykkeerklæringen nedenfor.

Endelig har jeg overvejet, om samtykket kan anses for frivilligt under hensyn til om der reelt eksisterer andre alternative rejsehjemler end rejsekortet. Det er for så vidt korrekt, at

der ikke eksisterer en alternativ rejsehjemmel med samme opbygning og funktion som rejsekortet. Dog er der et udvalg af andre rejsehjemler, kunderne kan benytte sig af, hvis de ikke ønsker at anvende et rejsekort. Der er således mulighed for – afhængig af hvilken landsdel, man befinder sig i – at købe enkeltbilletter, klippekort samt at benytte et periodekort (eventuel via en app til smartphone). Derudover er det muligt at købe et rejsekort anonymt, jf. afsnit 3 nedenfor, hvis man som kunde ikke ønsker at give samtykke til registrering og opbevaring af personoplysninger.

Jeg mener på den baggrund ikke, at samtykket fra kunderne til, at Rejsekort A/S kan behandle personoplysninger, ikke kan anses for frivilligt på grund af mangel på alternative rejsehjemler. Hvis der derimod vil opstå en situation, hvor rejsekortet reelt er eneste mulighed for at købe rejsehjemmel til kollektiv transport (busser, tog, metro) kan der imidlertid rejses spørgsmål om, hvorvidt samtykket fortsat er frivilligt.

For så vidt angår spørgsmålet om adgang til oplysningerne, medens de er registreret hos Rejsekort A/S eller dets databehandlere, bemærkes, at Rejsekort A/S' procedurer og systemer efter min opfattelse lever op til kravene om autorisation og adgangskontrol i § 11-12 i sikkerhedsbekendtgørelsen. Overordnet set, er det min vurdering, at Rejsekort A/S opfylder de formelle krav i §§ 11, stk. 1, idet Rejsekort A/S har fastlagt en autorisationsordning og -arbejdsgang, både for så vidt angår medarbejdere hos Rejsekort A/S, de tilsluttede trafikselskaber og IT-leverandøren East-West.

I revisionsrapporter til Rejsekort A/S om efterlevelse af disse procedurer mv. er det dog konstateret, at procedurerne i en række tilfældet ikke har været overholdt.

Efter sikkerhedsbekendtgørelsens § 11, stk. 2, må kun personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles, autoriseres. I den formelle autorisationsprocedure indgår en forudgående vurdering af, hvad den enkelte bruger har behov for at være autoriseret til.

Rejsekort A/S har imidlertid oplyst, at ca. 1.100 medarbejdere hos Rejsekort A/S, de tilsluttede trafikselskaber, herunder f.eks. også fysiske salgssteder, og i East-West per april 2015 har adgang til alle personoplysninger i Rejsekortsystemet, dvs. oplysninger om kunder (dvs. navn, adresse samt oplysning om kundetype) og samtlige rejse- og betalingstransaktioner i 13 måneder fra transaktionsdatoen. Disse medarbejdere har herunder adgang til følsomme personoplysninger omfattet af lovens § 7 (handicap).

Uanset, at jeg er bekendt med, at der kan være en driftsøkonomisk begrundelse for, at medarbejdere i kundeservicecentrene har adgang til data i Rejsekortsystemet, er det høje antal personer med adgang til kundernes data efter min opfattelse betænkeligt og kan give anledning til kritik af Rejsekortet A/S.

Det forhold, at det kan føre til overkapacitet i kundeservicecentre at nedsætte antallet af personer med adgang til data, hvis den samme service skal opretholdes, kan efter min opfattelse ikke i tilstrækkelig grad opveje den omfattende adgang til rejse- og transaktionsoplysninger i 13 måneder, der eksisterer p.t.. Ud fra et hensyn om at minimere adgang til personoplysninger, herunder følsomme oplysninger, mest muligt, anbefaler jeg derfor, at Rejsekortet A/S tager skridt til at sikre, at et færre antal personer har adgang til rejsekortsoplysninger.

Vedrørende spørgsmålet om opbevaringsperiodens længde bemærkes, at efter persondatalovens § 5, stk. 5, må de indsamlede oplysninger ikke opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Det er min vurdering, at der ikke er retligt grundlag for, at Rejsekort A/S behandler oplysninger om de rejsendes konkrete rejser (rejsedata) i mere end den periode, hvor den konkrete kunde kan gøre indsigelser mod rejsen. I særlige tilfælde, hvor der f.eks. på grund af en klage- eller retssag er konkret behov herfor, kan oplysningerne dog lovligt forblive registreret i længere tidsrum. Oplysninger om kundernes betalingstransaktioner (tidspunkt for betaling, valgt kundetype, rejsepris og kortsaldo) må dog af hensyn til bogføringsloven fortsat opbevares i 5 år. Persondataloven er endvidere ikke til hinder for, at Rejsekort A/S opbevarer ikke personhenførbare oplysninger - f.eks. om kundernes rejsemønstre i anonymiseret form.

Endelig har jeg gennemgået Rejsekort A/S procedurer for håndtering af underretningspligten (§ 28), indsigtsretten (§ 31) og indsigelsesretten (§ 35), og jeg finder, at de lever op til persondatalovens regler.

I notatet kommer jeg med følgende anbefalinger:

1) Det bør efter min opfattelse fremgå af samtykkeerklæringen, at de foretagne transaktioner på rejsekortet (dvs. rejsemønsteret) overvåges med det formål at opdage og forhindre snyd og bedrageri. Samtykkeerklæringen bør endvidere indeholde oplysning om opbevaringsperioden for oplysningerne om kundernes rejsemønster (transaktionsoplysningerne).

2) Rejsekort A/S skal i udgangspunktet slette alle personhenførbare rejseoplysninger (rejsedata) senest på det tidspunkt, hvor kunderne ikke længere har adgang til at gøre indsigelser mod rejsen. Rejsekort A/S er hverken efter betalingstjenesteloven, hvidvaskningsloven eller bogføringsloven forpligtet til at opbevare oplysninger om kundernes rejser (rejsedata) i 5 år. I særlige tilfælde, hvor der f.eks. på grund af en

klage- eller retssag er konkret behov herfor, kan oplysningerne forblive registreret i længere tid. Oplysninger om kundernes betalingstransaktioner (tidspunkt for betaling, valgt kundetype, rejsepris og kortsaldo) må af hensyn til bogføringsloven fortsat opbevares i 5 år.

3) Rejsekort A/S bør tage initiativ til at få reduceret antallet af personer, der har adgang til personoplysninger gennem rejsekortet, herunder bl.a. i forhold til personer i kundeservice og salgsrettede funktioner. Rejsekort A/S bør således overveje, hvordan understøttelsen og organiseringen af kundeservice og salg kan omlægges, så færre samlet set har adgang til oplysningerne om kunder og deres rejse- og betalingstransaktioner.

4) Rejsekort A/S skal sikre korrekt dokumentation af databehandleraftaler. Rejsekort A/S bør navnlig være opmærksom på at modtage kopi af de underdatabehandleraftaler, som databehandlerne indgår med underdatabehandlere, så Rejsekort A/S er bekendt med underdatabehandlerne og de indgåede aftaler.

5) Rejsekort A/S bør udarbejde og implementere et bedre tilsyn med trafikselskaberne gennem en konkret handlingsplan herfor. I handlingsplanen bør mulighederne for anvendelse af tilsynsmidler såsom kontrolbesøg eller stikprøvekontroller mv. inddrages. Det anbefales, at tilsynet navnlig fokuserer på at styre tildeling af medarbejderadgang til personoplysninger.

DEL I – BESKRIVELSE AF REJSEKORT A/S' BEHANDLING AF PERSONOPLYSNINGER

3. REJSEKORTET

Rejsekortet består af et landsdækkende rejsekortsystem, hvorved et elektronisk chipkort (rejsekortet) fungerer som kombineret rejsehjemmel til og betaling for en persons rejser med bus, tog og metro hos de tilsluttede trafikselskaber. Formålet med rejsekortsystemet er at tilvejebringe mulighed for, at passagerer, der benytter den kollektive persontrafik, kan anvende samme rejsehjemmel til tog, busser, Metro og andre kollektive transportmidler, der er omfattet af det landsdækkende rejsekortsystem.

Der findes 3 former for rejsekort:

(1) Rejsekort personligt, som er et personligt rejsekort, hvor kortindehaveren altid skal være med på de rejser, hvor kortet benyttes.

(2) Rejsekort flex, som er et rejsekort, der også kan benyttes af andre, som har fået det overdraget af kortindehaveren.

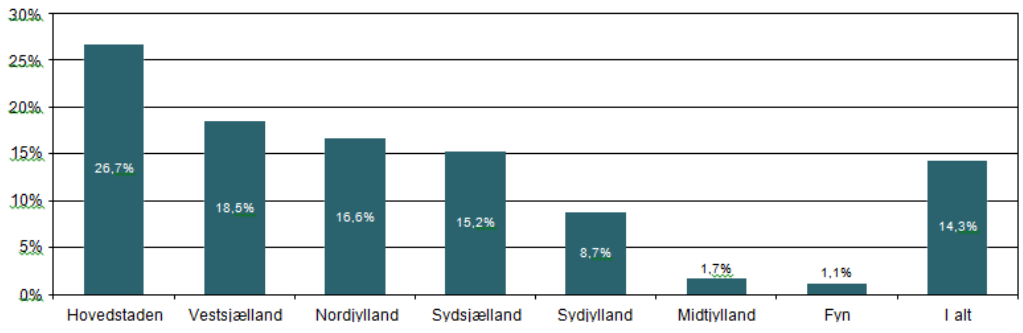
(3) Rejsekort anonymt, som er et rejsekort, der ikke er knyttet til en bestemt person og derfor kan benyttes af alle, der har kortet i hænde.

Rejsekortet kan både udstedes til private og til erhvervskunder (virksomheder, institutioner, myndigheder eller organisationer).

Ved køb og brug af et rejsekort registreres og opbevares en række personoplysninger, jf. afsnit 5.1. nedenfor. Såfremt en kunde ikke ønsker, at dennes personoplysninger behandles, er der mulighed for at købe et anonymt rejsekort, jf. pkt. 3.

Det fremgår af pkt. 8 i Rigsrevisionens beretning til Statsrevisorerne om driften af rejsekortet, april 2015, at der primo 2015 er udstedt ca. 1,1 mio. rejsekort, og at der hver uge foretages ca. 1,2 mio. rejser på rejsekort. Der er ca. 700.000 aktive rejsekortkunder, hvilket vil sige kunder, som anvender deres rejsekort til mindst én rejse hver 3. måned. Figur 1 viser andelen af rejsekortkunder i forhold til befolkningen opdelt på trafikselskabernes områder i februar 2015. (Figur 1 er gengivet fra Rigsrevisionens beretning, s. 4).

Figur 1. Andel af rejsekortkunder i forhold til befolkningen i februar 2015



Kilde: Rejsekort A/S.

4. REJSEKORT A/S OG DE TILSLUTTEDE TRAFIKSELSKABER

Rejsekort A/S' virksomhed består i at etablere, drive, vedligeholde og udvikle det landsdækkende rejsekortsystem og varetage opgaver i forbindelse hermed.

Rejsekort A/S er et aktieselskab, som ejes af det statsejede DSB, det stats- og kommunalejede Metroselskab og de regionale trafikselskaber Movia, Midttrafik, Nordjyllands Trafikselskab og Sydtrafik. I 2015 vil FynBus også tilslutte sig rejsekortet og dermed blive medejer af selskabet. Rejsekort A/S ledes af en bestyrelse og en direktion.

Rejsekort A/S skal som led i sin virksomhed give trafikselskaber muligheder for på visse vilkår at være tilsluttet rejsekortsystemet. Betingelserne for et trafikselskabs tilslutning reguleres i den såkaldte tilslutningsaftale, som tiltrædes af Rejsekort A/S og det enkelte trafikselskab.

Trafikselskaberne har ansvaret for kundeservice, produkter, priser mv. Det fremgår af tilslutningsaftalen, at trafikselskaberne er forpligtet til at servicere alle kunder, som er indehavere af et rejsekort, uanset hvilket trafikselskab, der konkret har distribueret kortet, jf. tilslutningsaftalen, s. 11.

Rejsekort A/S har oplyst, at en kunde, der har spørgsmål relateret til rejsekort, således kan henvende sig til kundebetjeningen i et hvilket som helst trafikselskab, der er tilsluttet rejsekortsystemet. Det gælder, uanset hvilket konkret trafikselskab, der har distribueret kortet til kunden, og uanset at den konkrete rejse, som kunden vil spørge ind til, f.eks. er foretaget med et andet trafikselskab, end det, som kunden tager kontakt til.

Dog skal spørgsmål vedrørende indgåede betalingsaftaler, rettes til det trafikselskab, som administrerer den pågældende aftale.

5. HVILKE OPLYSNINGER REGISTRERER OG OPBEVARER REJSEKORT A/S?

5.1 Overblik over oplysninger, der registreres i Rejsekort A/S' databaser

Følgende personoplysninger registreres i Rejsekort A/S' databaser:

- Kundens stamdata
    - Navn
    - Kundenummer
    - CPR-nummer
    - Kontaktoplysninger
        - Postadresse (adresse, postnr., by og land)
        - Fastnet- og/eller mobiltelefonnummer
        - E-mail adresse
    - Om der er afgivet samtykke til modtagelse af markedsføringsmateriale, herunder hvilket eller hvilke trafikselskaber, samtykket vedrører

- Stamdata - Kundens kort (der kan være flere)
    - Rejsekortnummer
    - Rejsekorttype
    - Passagertype

- Stamdata – Betalingsaftaler (tank-op-aftale)
    - Betalingsaftalenummer
    - Betalingsaftaletype
    - Dato for oprettelse
    - Dato for udløb
    - Valgt administrator, dvs. trafikselskab, der administrerer betalingsaftalen
    - Oplysninger om betalingsaftalen, tank-op beløb
    - Betalingskorttype, der benyttes i forbindelse med betalingsaftalen
    - Betalingskortnummer – maskeret
    - Dato for udløb af betalingskort

- Rejsekortsaldo
- Eventuel registrering i advarsels- og spærrelisterne
- Rejseoplysninger
- Betalingsoplysninger

5.2 Oplysninger, der registreres ved bestilling af et rejsekort og optankning af rejsekort

Når en kunde bestiller et rejsekort – enten ved udfyldelse af et fysisk bestillingsskema eller ved bestilling via rejsekort.dk – skal kunden give oplysninger om CPR-nummer, navn og adresse, evt. mailadresse, samt telefonnummer.

I forbindelse med eventuel brug af betalingskort, registreres desuden information om betalingskorttypen og udløbsdatoen. Selve betalingskortoplysningerne gemmes alene af NETS.

Herudover registreres en række oplysninger om selve rejsekortet, herunder korttype, valgt kundetype, dato for oprettelse, udløbsdato og eventuelle tank-op-aftaler.

Oplysninger om tank-op-aftaler omfatter oplysninger om det valgte beløb for optankning, type af tilknyttet betalingskort eller andre betalingsmåder, f.eks. Betalingsservice, samt hvilket trafikselskab, der har modtaget betalingen. Ved den enkelte optankning, registreres oplysninger om optankningstidspunkt og -sted.

5.3 Oplysninger, der registreres ved rejser

Når kunden herefter anvender sit rejsekort til at rejse med, registreres oplysninger om tidspunkt og sted for check ind og ud og kontrol undervejs på rejsen, valgt kundetype, rejsepris og kortsaldo. Der registreres således oplysninger om kundernes rejsemønster, dvs. den tilbagelagte rejse fra check ind til ud.

5.4 Oplysninger, der registreres i Rejsekort A/S' kunderegister eller kortdatabase

Hvis kunden har en ubetalt gæld til et af trafikselskaberne bag rejsekort eller flere gange har undladt at checke ud, kan kunden opføres i kunderegisteret med angivelse af årsag og dato.

I kortdatabasen registreres rejsekort, der er spærret af kortindehaveren eller af Rejsekort A/S, med angivelse af kortnummer, dato for spærring, oplysning om hvem, der har spærret kortet, samt årsag til spærringen.

5.5 Oplysninger om brug af tjenesterne på rejsekort.dk

Oplysninger, om hvilke dele af hjemmesiden, der besøges, opsamles i logfiler sammen med IP-adressen og oplysningerne bruges i forbindelse med videreudvikling af hjemmesiden. Ved brug af selvbetjeningsdelen, f.eks. ved køb af rejsekort, registreres endvidere en række oplysninger, jf. ovenfor afsnit 5.1 om registrering af oplysninger ved bestilling af rejsekort).

Herudover registreres ved hjælp af cookies og brug af Google Analytics oplysninger om bl.a. antallet af brugere på hjemmesiden (IP-adresser) og besøg af undersider.

5.6 Følsomme oplysninger om handicap

Rejsekort A/S behandler endvidere i visse tilfælde personfølsomme oplysninger, nemlig hvor en kundes handicap eller førtidspension giver ret til en særlig rabat. Her registreres alene oplysningen om, at kunden har ret til et rejsekort med kundetypen "handicap", men ikke yderligere informationer.

Oplysning om, at en kunde er hjemløs registreres som led i legitimationsproceduren i henhold til hvidvaskningsloven.

5.7 Anonymiserede oplysninger

Rejsekort A/S registrerer endelig oplysninger i anonymiseret form.

Selve anonymiseringen af oplysninger sker ved, at forbindelsen mellem registreringen af identitetsoplysninger (dvs. kundens navn, adresse, mv.) og de registrerede transaktioner (rejser og betalinger) fjernes. Transaktionerne er almindeligvis ikke direkte personhenførbare, men kan indirekte via kortnummeret kædes sammen med kortejeren. Ved anonymisering fjernes kortnummeret således fra transaktionerne.

6. MED HVILKET FORMÅL REGISTRERER OG OPBEVARER REJSEKORT A/S PERSONOPLYSNINGERNE?

Rejsekort A/S har oplyst, at personoplysningerne registreres og opbevares for at kunne administrere og betjene kunderne samt for at overholde gældende lovgivning, herunder reglerne om opbevaringspligt af visse oplysninger efter bogføringsloven, betalingstjenesteloven og hvidvaskningsloven.

Oplysninger om kundernes rejser registreres således bl.a. for at kunne betjene kunderne, når disse henvender sig til Rejsekort A/S' kundebetjening eller logger ind på selvbetjeningsfunktionen på rejsekort.dk.

Derudover anvender Rejsekort A/S oplysningerne til at dokumentere rejsernes pris overfor kunderne, hvis der opstår uenighed herom.

Rejsekort A/S foretager endvidere overvågning af foretagne transaktioner på rejsekortet. Dette sker med henblik på at opdage og forhindre overtrædelse af regler, vilkår m.v.(såkaldt "Rejsekort A/S' Fraud Management" (RFM)).

Oplysningerne om de foretagne rejser bruges desuden i anonymiseret form af trafikselskaberne til planlægningsformål, herunder for at planlægge trafikken, det vil sige hvordan ruteplaner, antal busser, tog mv. skal tilrettelægges. De anonymiserede oplysninger om foretagne rejser anvendes endvidere i forbindelse med overvejelser om prissætning, samt i forbindelse med fordeling af indtægter mellem trafikvirksomhederne.

7. SAMTYKKE TIL BEHANDLING AF PERSONOPLYSNINGER

Ved bestilling af rejsekort giver kortindehaveren samtykke til behandling af personoplysninger. Samtykketeksten lyder således:

> *"Jeg giver hermed mit samtykke til, at Rejsekort A/S og de tilsluttede trafikvirksomheder behandler, herunder indsamler, registrerer, opbevarer og udveksler 1) oplyste personlige oplysninger, herunder CPR-nr. i rejsekortsystemet med det formål at administrere mig som kunde, og eventuelt registrere mig i advarselsregisteret, jf. afsnit 6 i Rejsekort kortbestemmelser og 2) oplysninger om bevægelser på mit rejsekort samt mine rejser til afregning af min brug af rejsekortet. […] Jeg erklærer at have læst og accepteret Rejsekort A/S' kortbestemmelser samt politik om behandling af personoplysninger. Jeg kan til enhver tid tilbagekalde mit samtykke, jf. persondatalovens § 38. […]."*

Når Rejsekort A/S skal behandle personfølsomme oplysninger om en kunde, der er omfattet af en rabatordning for handicappede eller førtidspensionister, indhentes der særligt samtykke hertil. Samtykkeerklæringen for handicappede lyder således:

> *"Da jeg ønsker at gøre brug af rabatordning for handicappede, giver jeg hermed mit samtykke til, at Rejsekort A/S og de tilsluttede trafikvirksomheder behandler, herunder indsamler, registrerer, opbevarer og udveksler oplysningen om, at jeg er berettiget til rabatordningen til handicappede, herunder en kopi af den*

dokumentation, som jeg har forevist for at opnå adgang til rabatordningen. Jeg accepterer, at behandlingen sker med henblik på at administrere mig som kunde."

Ved udstedelse af rejsekort, får kunden desuden lejlighed til at gøre sig bekendt med Rejsekort A/S' kortbestemmelser. Afhængig af, hvordan rejsekortet bestilles, sker det enten ved fysisk udlevering af kortbestemmelserne, adgang til at gennemgå og angive sin accept af kortbestemmelserne, eller ved en generel henvisning til, at kortbestemmelserne kan findes på rejsekort.dk.

8. HVOR OPBEVARES PERSONOPLYSNINGERNE?

Rejsekortrelaterede data lagres i "Rejsekortsystemet", i et datawarehouse og i Rejsekort Kundecenters sagssystem (RESS).

8.1 Rejsekortsystemet

Rent fysisk består Rejsekortsystemet af en stor mængde servere og supportsystemer, der dog rent funktionelt kan opdeles i to forskellige komponenter: (1) Rejsekortudstyr, der findes på stationer, i busser og på salgssteder, og (2) BackOffice, der udgør det centrale rejsekortsystem.

Rejsekortsystemet opsamler i systemet BackOffice bl.a. data om kunder (dvs. navn, adresse, CPR nummer samt oplysning om kundetype: voksen, barn, pensionist, handicap), salg af rejsekort, salg af optankninger (e-penge på rejsekortet) og kontantbilletter og rejseforbrug. Salg, der håndteres af trafikselskaberne via salgsudstyr (kaldet RVM, Boris, DC m.m), registreres ligeledes i BackOffice. Samtlige kunde-, rejse- og betalingstransaktioner registreres altså i BackOffice.

IT-leverandøren East-West har leveret og står for drift af Rejsekortsystemet.

8.2 Datawarehouse

Baseret på data fra Rejsekortsystemet har Rejsekort A/S i samarbejde med Bus & Tog, som er et samarbejdsorgan for den kollektive trafik, desuden etableret et Datawarehouse, som giver Rejsekort A/S og trafikselskaberne mulighed for at producere analyser af data til forskellige formål, herunder kontroller og fraud-overvågning, rapportering mv.

I Datawarehouse ligger udvalgte data overført fra Rejsekortsystemet, herunder salgsdata (kortsalg, optankninger mv.), rejsetransaktioner (rejsedata), økonomidata (opkrævninger og betalinger) og kundestamdata. Kundestamdata indeholder, navn, adresse, CPR og oplysning om kundetype (voksen, barn, pensionist, handicap).

Rejsekort A/S er sammen med Bus & Tog ansvarlige for udvikling, drift og vedligeholdelse af det fælles Datawarehouse. Rejsekort A/S og Bus & Tog benytter IT Kompagniet som deres leverandør til drift af Datawarehouse-systemet.

8.3 Rejsekort Kundecenters sagssystem (RESS)

Rejsekorts kundecenter drives af trafikselskaberne med Bus & Tog som koordinator. Bus & Tog er ansvarlig for Rejsekort Kundecenters sagssystem (RESS). I RESS registreres henvendelser fra kunder, der henvender sig til Rejsekort Kundecenter, kontaktinformation, som kundens navn, adresse og kundetype, samt kundecentrets besvarelse af henvendelser.

Bus&Tog benytter KMD som deres leverandør af drift af RESS.

8.4 Øvrige forhold

Oplysninger om kundens brug af et rejsekort, dvs. transaktionsoplysninger, registreres – udover i Rejsekort A/S' databaser – også på chippen i rejsekortet, hvorpå de seneste 5 foretagne rejser er registreret.

For så vidt angår Rejsekort personligt er desuden kortindehavers navn og evt. foto påtrykt kortet. For Rejsekort flex fremgår kortindehavers navn påtrykt kortet.

Oplysninger om spærrede kort registreres endvidere i kortdatabasen for hvert enkelte kort.

Herudover kan oplysningerne om kunder, som ikke har betalt eller på anden måde har misbrugt adgangen til at benytte et rejsekort, registreres i kundedatabasen for hver enkelt kunde.

En person kan således registreres, hvis 1) personen skylder et trafikselskab mere end 1.000 kr., og vedkommende skriftligt har accepteret gælden, eller trafikselskabet har indledt retslige skridt mod skyldneren, eller 2) personen ikke har foretaget check ud mindst 3 gange inden for 12 måneder, og kunden ved hvert tilfælde er oplyst om, at vedkommende vil blive optaget i advarselsregistret tredje gang inden for et år, vedkommende glemmer at foretage check ud.

Formålet med registrering af kunder, som ikke har betalt eller på anden måde har misbrugt adgangen til at benytte et rejsekort, er at undgå, at Rejsekort eller trafikselskaberne indgår nye aftaler med de registrerede.

Der er i Rejsekort A/S' såkaldte "Compliance Manual" (version 1.4 af 1. januar 2014) (herefter "Compliance Manual") fastsat yderligere betingelser for registrering og behandling af oplysninger i kunderegistret. Compliance Manual er en intern vejledning til Rejsekort A/S medarbejdere.

9. HVOR LÆNGE OPBEVARES PERSONOPLYSNINGERNE?

Identitetsoplysninger, som er indhentet i forbindelse etablering af et kundeforhold, opbevares i 5 år efter, at kundeforholdet er ophørt. Dette omfatter også oplysninger om, hvilken legitimation der er forevist i forbindelse med kundeforholdets etablering, herunder nummer og udløbsdato.

Oplysninger, der registreres i forbindelse med rejser, altså såkaldte transaktionsoplysninger, gemmes i 5 år samt det løbende år fra transaktionsdatoen. Dette gælder også, selvom kundeforholdet måtte ophøre indenfor de 5 år.

Oplysninger om kort og tank-op-aftaler gemmes i fem år fra udgangen af det regnskabsår, som transaktionen vedrører.

I forhold til oplysninger om kunder, som ikke har betalt eller på anden måde har misbrugt adgangen til at benytte et rejsekort, i Rejsekorts kunderegister, gemmes disse oplysninger – hvis årsagen til registreringen er den pågældende kundes gæld – indtil den fordring, der ligger til grund for registreringen, er betalt. Oplysninger om en registreret kunde gemmes dog højst i 2 år, efter at registreringen er sket – også i de tilfælde, hvor kunden fortsat måtte have en gæld til et trafikselskab. Registrering på grund af manglende check-ud gemmes højest i 1 år efter den handling, der har medført registrering.

Oplysninger, der lagres i Rejsekortsystemet, hvor de er tilgængelige for kunden selv og de medarbejdere, der administrerer og betjener kunder, er alene tilgængelige her i 13 måneder. Herefter slettes oplysningerne i Rejsekortsystemet.

Oplysningerne lagres fortsat i det tilknyttede arkivsystem, hvor oplysningerne opbevares iht. lovgivningens krav. Arkivsystemet er en del af Rejsekortsystemet, men er adskilt fra den del af systemet, der er online, og hvor data for de sidste 13 måneder er tilgængelig for kunden og de relevante medarbejdere. Rejsekort A/S har oplyst, at kun enkelte medarbejdere har adgang til arkivsystemet.

Trafikselskaberne skal ifølge Compliance Manualen, s. 71, slette personoplysninger, som ikke længere anvendes, og data må således ikke ophobe sig på medier, der ikke længere anvendes, f.eks. pc'er, håndholdte enheder mv.

10. HVEM HAR ADGANG TIL DE REGISTREREDE PERSONOPLYSNINGER?

10.1 Brugeradgang til Rejsekort A/S' databaser

Medarbejdere i Rejsekort A/S og de medarbejdere hos de tilsluttede trafikselskaber, der arbejder med betjening og administration af Rejsekort-kunder, har mulighed for at få adgang til de oplysninger, der er registreret i Rejsekort A/S' databaser.

IT-leverandøren East-West, som har leveret og står for driften af Rejsekortsystemet, har desuden adgang hertil og de oplysninger, der er registreret heri, med det formål at overvåge driften og foretage korrektioner ved fejl. Retningslinjerne for tildeling af adgangsrettigheder til medarbejdere i East-West er nærmere beskrevet i bilag 1 til databehandleraftale mellem Rejsekort A/S og East-West, jf. nærmere nedenfor.

For at få adgang til Rejsekort A/S' databaser skal den enkelte medarbejder hos Rejsekort A/S, trafikselskaberne eller East-West tildeles en brugeradgang. Reglerne herfor er nærmere beskrevet i Compliance Manualen, s. 9-12, og gennemgås kort her.

Virksomhederne skal sørge for, at tildelingen af brugeradgange sker i overensstemmelse med det behov for adgang, som den enkeltes arbejde kræver. F.eks. skal medarbejdere, der er ansvarlige for trafik- og takstplanlægning, gives adgang til anonymiserede oplysninger om f.eks. rejsemønstre, men ikke personhenførbare oplysninger.

Det er desuden specificeret i Compliance Manualen, s. 17, at medarbejderen kun må behandle oplysninger, som er nødvendige for udførelsen af en konkret opgave, at der kun må behandles oplysninger om en kundes rejseoplysninger, betalinger mv. til brug for betjening og administration af kunden, og at søgningen skal foretages i overensstemmelse med de modtagne instrukser.

De medarbejdere, som har adgang til personoplysninger i Rejsekort A/S' databaser, skal underskrive en tro- og loveerklæring (en "tavshedserklæring"). Erklæringen indeholder både bestemmelser om tavshed med hensyn til oplysninger om kunder, samt krav om, at videregivelse til kolleger indenfor virksomheden alene må ske, hvis det anses for påkrævet for udførelsen af arbejdsopgaven, og den modtagende person har underskrevet en tilsvarende tavshedserklæring.

Databaserne indeholder en registrering af, hvilke medarbejdere der er tildelt de forskellige adgangsrettigheder.

Pr. april 2015 har 1.100 medarbejdere hos Rejsekort A/S, de tilsluttede trafikselskaber og East-West adgang til personoplysninger i Rejsekortsystemet – med undtagelse af CPR-numre, der kun kan tilgås af en begrænset kreds af medarbejdere. Rejsekort A/S har oplyst,

at hovedparten er medarbejdere hos trafikselskaberne, der arbejder med kundebetjening på betjente salgssteder og i trafikselskabernes kundecentre.

For så vidt angår adgangen til oplysninger i Datawarehouse, har Rejsekort A/S desuden oplyst, at 6 medarbejdere hos Rejsekort A/S, der arbejder med administrationen af Datawarehouse, har fuld adgang hertil. Medarbejdere hos trafikselskaberne har en begrænset adgang til at udtrække rapporter indeholdende en afgrænset mængde af de oplysninger, der ligger i Datawarehouse.

For så vidt angår adgangen til oplysninger i RESS har Rejsekort A/S oplyst, at 805 medarbejdere i Rejsekort A/S og de tilsluttede trafikselskaber, der arbejder med kundebetjening, har adgang til oplysninger, der ligger her.

Til at føre kontrol med tildeling af adgangsrettigheder, har Rejsekort A/S oprettet en "Brugeradministrationsgruppe", der overvåger adgangsrettigheder mv. I denne gruppe sidder brugeradministratorerne for henholdsvis Rejsekort A/S, trafikselskaberne og East-West. Det er disse brugeradministratorer, der kontrollerer, at det tildelte brugerniveau dækker det arbejdsmæssige behov i forhold til adgangsrettigheder til systemet, konfiguration af sikkerhedsstillinger mv. Der er defineret et autorisationskoncept, ud fra hvilket brugerrettighederne skal tildeles.

Hver 6. måned skal trafikselskaberne ifølge Compliance Manualen kontrollere, at kun de medarbejdere, der opfylder kravene til brugeradgang, har denne adgang, og at den tildelte adgang svarer til den adgang, der er nødvendig i forhold til medarbejderens arbejdsopgaver.

Trafikselskaberne er desuden forpligtet til at sørge for, at eventuelle underdatabehandlere foretager en lignende kontrol, jf. Compliance Manualen, s. 68.

Det fremgår imidlertid af ISAE 3402-erklæringen af 6. marts 2015, udarbejdet af revisionsfirmaet Ernst & Young s. 31, at Rejsekort Brugeradministration *kvartalsvis* skal lave et udtræk over alle brugere og tildelte rettigheder, og at denne liste sendes til trafikselskaberne, East-West og Rejsekort A/S. Disse skal herefter kvittere for, at deres brugerprofiler og tildelte rettigheder stadig er korrekte og modsvarer deres arbejdsmæssige behov og herefter svare tilbage med en gennemgået liste. Rejsekort A/S har hertil oplyst, at oplysningerne i erklæringen om, at der skal ske en kvartalsvis kontrol, skyldes, at der er indført strammere procedurer end påkrævet i Compliance Manualen.

10.2 Udveksling af oplysninger indenfor Rejsekort A/S' databaser

Visse medarbejdere hos de tilsluttede trafikselskaber, disses datterselskaber samt Metro Service A/S har adgang til den samme mængde personoplysninger om Rejsekort A/S' kunder – nemlig de oplysninger, som medarbejderne via deres brugeradgang kan tilgå i

Rejsekort A/S' databaser, og som er nødvendige for at de kan betjene og administrere kunder i rejsekortforhold, jf. Rejsekorts privatlivspolitik, pkt. 2.

Når en medarbejder registrerer eller behandler oplysninger om en kunde, skal dette derfor altid ske i Rejsekortsystemet, således at de øvrige trafikselskaber ligeledes får adgang til registreringer, ændringer, m.v. af oplysninger.

10.3 Videregivelse af oplysninger udenfor Rejsekort A/S' databaser

Rejsekort A/S videregiver oplysninger om navn og evt. foto til en kortproducent til brug for produktion af rejsekort personligt eller rejsekort flex. Oplysningerne bruges alene i forbindelse med fremstilling af kortet og gemmes ikke herefter hos kortproducenten.

Rejsekort A/S videregiver desuden oplysninger om kundernes navn, adresse og mailadresse til analyseinstitutter i forbindelse med udførelse af kundetilfredshedsundersøgelser for Rejsekort A/S. Analyseinstitutterne sletter de modtagne oplysninger, når opgaven er udført.

Endelig kan Rejsekort A/S under visse betingelser udlevere oplysninger til politiet i forbindelse med efterforskning, jf. Compliance Manualen, s. 19.

11. SIKKERHEDSFORANSTALTNINGER

11.1 Databehandlere og underdatabehandlere

11.1.1 Databehandleraftaler

I tilslutningsaftalen, der indgås mellem Rejsekort A/S og det enkelte trafikselskab, er der en række bestemmelser, der regulerer forholdet mellem Rejsekort A/S (som den dataansvarlige for de personoplysninger, der behandles i Rejsekort A/S' databaser) og trafikselskaberne (som databehandler), samt trafikselskabernes generelle forpligtelser i relation til opbevaring af personoplysninger, jf. Tilslutningsaftalen, pkt. 2.6.

Det fremgår bl.a., at trafikselskabet alene må handle efter instruks fra Rejsekort A/S, og at Rejsekort A/S afgør til hvilke formål og med hvilke hjælpemidler, der må foretages behandling af oplysningerne. Trafikselskabet skal herudover træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger, som sikrer, at oplysninger ikke hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt at de ikke kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med persondataloven. Trafikselskaberne skal som led heri iagttage og efterleve de instruktioner, som Rejsekort A/S har udstedt i tilslutningsaftalen og i Compliance Manualen.

De tilsluttede trafikselskaber er desuden ansvarlige for at indgå underdatabehandleraftaler med de datterselskaber og samarbejdspartnere, der som underdatabehandlere har adgang til Rejsekort A/S' databaser, på mindst samme vilkår som fastsat i Tilslutningsaftalen, jf. Tilslutningsaftalens, s. 7, og Compliance Manualen, s. 6.

Jeg har ikke kendskab til, at der eksisterer øvrige databehandleraftaler mellem Rejsekort A/S og trafikselskaberne, udover den databehandleraftale som indgår implicit i tilslutningsaftalen.

Rejsekort A/S har endvidere indgået en databehandleraftale med IT-leverandøren East-West Denmark ApS (herefter "East-West"), jf. databehandleraftale af 25. november 2014.

East-West er Rejsekorts primære leverandør. Det er således East-West, der driver it-systemet "Rejsekortsystemet" og varetager følgende opgaver gennem deres underleverandører IBM, IT Kompagniet og Gemalto CP, jf. ISAE 3402-erklæringen, s. 13-14: (1) levering af råkort og personalisering (herunder distribution) af personlige rejsekort gennem Gemalto CP, (2) drift og servicering af Datawarehouse gennem ITK, og (3) drift af datanetværket og understøttelse af BackOffice-systemet gennem IBM.

Det fremgår af databehandleraftalens pkt. 1.1, at formålet med aftalen er at sikre, at East-West som databehandler opfylder de krav for behandling af personoplysninger, der følger af persondataloven og sikkerhedsbekendtgørelsen, samt anden relevant lovgivning.

Aftalen regulerer bl.a. vilkårene for behandling af personoplysninger, herunder krav til tildeling af brugeradgang til Rejsekort A/S' systemer, interne kontrolprocedurer, krav til fysisk sikring af East-Wests lokaler mm., krav til logning etc., jf. pkt. 3. Det fremgår desuden af aftalen, at East-West er forpligtet til at overholde forbuddet mod dataophobning i persondatalovens § 5, jf. pkt. 3.13.

Endelig er East-West forpligtet til at indgå selvstændige databehandleraftaler med de underleverandører, der har adgang til data i "Rejsekortsystemet", og påse, at disse aftaler overholdes, jf. databehandleraftalens pkt. 3.14. Det fremgår desuden, at databehandleraftalerne skal sikre, at persondatalovens regler overholdes, ved at de pågældende underleverandørers behandling af Rejsekort A/S' data følger retningslinjerne i databehandleraftalen mellem Rejsekort A/S og East-West. East-West er forpligtet til at "snarest" at indgå disse databehandleraftaler og fremsende kopi heraf til Rejsekort.

11.1.2 Kontrol med data- og underdatabehandlere

Rejsekort A/S' kontrol med trafikselskaberne er reguleret i tilslutningsaftalen, hvoraf fremgår, at trafikselskaberne på Rejsekort A/S' anmodning uden unødigt ophold skal give Rejsekort A/S tilstrækkelige oplysninger til, at Rejsekort A/S kan påse, at de fastsatte sikkerhedsforanstaltninger er truffet, samt at Rejsekort A/S og dennes revision har adgang til al nødvendig information, der vedrører forhold reguleret i tilslutningsaftalen, samt adgang til, såvel varslet som uvarslet, at foretage sikkerhedsrevision, at få udleveret dokumentation, herunder logs, og stille spørgsmål, m.v., jf. Tilslutningsaftalens pkt. 2.6.

Trafikselskabet skal desuden på anmodning fra Rejsekort A/S afgive en erklæring fra trafikselskabets revisor, hvor det dokumenteres, at Brugeren lever op til de fastsatte krav.

Om Rejsekort A/S' kontrol med East-West fremgår af databehandleraftalen af 25. november 2014, at East-West på Rejsekorts anmodning skal give denne nødvendige oplysninger til at påse, at der er truffet tilstrækkelige og relevante sikkerhedsforanstaltninger, herunder at der findes procedurer for tildeling af medarbejderes adgang til rejsekortsystemet og at de i databehandleraftalen fastlagte krav overholdes, jf. aftalens pkt. 3.4.

Rejsekort A/S har oplyst, at der ikke hidtil er foretaget fysisk tilsyn med databehandlere og underdatabehandlere, idet Rejsekort A/S i denne periode har fokuseret på at udarbejde skriftlige instrukser og overføre viden til databehandlerne. Fysiske tilsyn planlægges ifølge Rejsekort A/S fremadrettet, f.eks. er der planlagt tilsyn hos Sydtrafik i 3. kvartal 2015.

Rejsekort A/S har desuden oplyst, at Rejsekort A/S har alle underdatabehandlere registreret og at kopi af underdatabehandlere fremsendes ved behov.

Der henvises i øvrigt til afsnit 11.11 nedenfor om egenkontrol og ekstern kontrol.

11.2 Fastsættelse og ajourføring af interne sikkerhedsretningslinjer

Som tidligere nævnt har Rejsekort A/S udarbejdet en Compliance Manual, der indeholder retningslinjer for behandling af personoplysninger, herunder en række sikkerhedsforanstaltninger.

Det skal hertil bemærkes, at Rejsekort A/S har oplyst, at Rejsekort A/S ikke er omfattet af sikkerhedsbekendtgørelsen, jf. afsnit 14.5 nedenfor, men har valgt at følge bekendtgørelsens principper.

Formålet med Compliance Manualen er at identificere og sikre, at de lovgivningsmæssige krav, herunder persondataloven, efterleves hos både Rejsekort A/S og de tilsluttede trafikvirksomheder og disses underleverandører, samt at sikre ensartethed i de processer, der implementeres og anvendes i Rejsekort A/S og hos trafikvirksomhederne i forbindelse med anvendelsen af rejsekortsystemet.

Rejsekort A/S har tillige nedsat et complianceudvalg med repræsentanter fra de tilsluttede trafikselskaber og Rejsekort A/S, der bl.a. har til opgave at afgøre tvivlsspørgsmål i forbindelse med tildeling af brugerrettigheder.

Ifølge manualens s. 7 vil Rejsekort A/S løbende ajourføre Compliance Manualen med henblik på, at denne stedse er i overensstemmelse med gældende lovgivning på området. Ifølge Rejsekort A/S foretages der årligt en kontrol af, at retningslinjerne ajourføres.

11.3 Instruktion af medarbejdere

Trafikselskaberne er forpligtet til at uddanne deres medarbejdere for at sikre, at de har en tilstrækkelig grad af uddannelse og instruktion bl.a. i forhold til de adgangsrettigheder og autorisationer, de er blevet tildelt i forbindelse med behandling af personoplysninger. I øvrigt skal alle medarbejdere, der har adgang til Rejsekort A/S' databaser, have en detaljeret beskrivelse af deres arbejdsfunktioner, samt hvilke specifikke compliancekrav, der gælder for disse arbejdsfunktioner, jf. Compliance Manualen, s. 63.

Det fremgår af Compliance Manualens s. 10, at de tilsluttede trafikselskaber skal sikre, at en række sikkerhedsforanstaltninger (omtalt "Standardvilkår for datasikkerhed og brugeradministration") overholdes. Disse foranstaltninger indebærer, at medarbejdere med adgang til personoplysninger skal være instrueret om, at denne kun må behandle personoplysninger i systemet, når det sker til relevante og saglige formål, at hver medarbejder skal have en funktions- og arbejdsgangsbeskrivelse, at databærende medier skal være sikret med adgangskode, og at manuelle fortrolige personoplysninger skal opbevares aflåst. Foranstaltningerne indebærer desuden en række regler om udarbejdelse, anvendelse og udskiftning af medarbejdernes adgangskoder til Rejsekort A/S' databaser.

Samtlige medarbejdere, der har adgang til personoplysninger fra rejsekortsystemet, anmodes desuden om at underskrive en tro- og loveerklæring (en "tavshedserklæring"), som beskrevet i afsnit 10.1 ovenfor.

11.4 Brug af it-udstyr på fremmede lokaliteter (hjemmearbejdspladser o.lign.)

Reglerne om brug af it-udstyr på fremmede lokaliteter fremgår af Compliance Manualen, s. 66-67, hvor der er fastsat regler om bl.a. transport af databærende medier og udstyr (f.eks. bærbar computer) og opbevaring udenfor virksomhedens lokaliteter.

Det fremgår desuden, at trafikselskaberne er ansvarlige for løbende at sikre deres IT-systemer og IT-infrastruktur på forsvarlig måde, således at forhold vedrørende "distancearbejdspladser" lever op til det aftalte sikkerhedsniveau og til de gældende revisionskrav omkring IT- og datasikkerhed. Trafikselskaberne skal endvidere sørge for at adgangen til rejsekortfunktioner og -data fra hjemmearbejdspladser og arbejdspladser udenfor trafikselskabernes infrastruktur er elimineret, medmindre specifikke procedurer og sikkerhedsforskrifter er vurderet og udarbejdet for disse, jf. Compliance Manualen s. 67.

11.5 Fysisk sikkerhed

Der er i Compliance Manualen, s. 66 ff., fastsat forholdsregler mod uvedkommendes adgang, som Rejsekort A/S og trafikvirksomhederne skal følge. Disse forholdsregler

vedrører bl.a. fysisk beskyttelse, herunder f.eks. aflåsning af lokaler, etablering af alarmsystemer, sikring af yderdøre, placering af skærme og printere, så uvedkommende ikke kan se dem mv.

11.6 Sikkerhed ved reparation og service samt ved salg og kassation af anvendte datamedier

Compliance Manualen, s. 69, indeholder retningslinjer for reparation af enheder med lagringsmedier, kassation af medier, herunder makulering af print med personoplysninger samt effektiv sletning af lagringsmedier ved kassation mv.

11.7 Autorisation og adgangskontrol mv.

I forhold til reglerne om autorisation og adgangskontrol henvises til afsnit 10 ovenfor.

11.8 Sikkerhed ved transmission af personoplysninger via internettet (eller andre åbne net)

Af Compliance Manualen, s. 68, fremgår følgende om sikkerhed ved transmission af personoplysninger via internettet:

"Der skal foretages kryptering, og så vidt muligt signering, af personfølsomme oplysninger samt CPR-nummer ved overførsel på internet og via e-mail, således at fortroligheden samt afsenders og modtagers og de transmitterede oplysningers ægthed sikres."

11.9 Kontrol med afviste adgangsforsøg samt blokering

Af Compliance Manualen, s. 69, fremgår følgende om logning af afviste adgangsforsøg samt blokering:

"Logningen i systemet skal endvidere omfatte alle afviste adgangsforsøg så vidt muligt, således at tidspunkt og sted (f.eks. PC), og såfremt det er muligt den benyttede bruger-identifikation, for afviste adgangsforsøg registreres.

Systemet skal lukke adgangen for en bruger-identifikation, for hvilken der inden for kort tid registreres gentagne afviste adgangsforsøg, f.eks. efter 3 afviste adgangsforsøg på samme PC."

11.10 Logning

Af Compliance Manualen, s. 68 ff., fremgår bl.a. følgende om logning og sporbarhed:

"Rejsekort og Trafikvirksomhederne er ansvarlige for, at der i rejsekortsystemet og i Trafikvirksomhedernes front-end IT-systemer, der giver adgang til rejsekortsystemet, foretages logning af adgangen til rejsekortsystemet, funktioner og data samt i muligt omfang af forsøg på tilgang til personoplysninger mv. i rejsekortsystemet.

Logningen skal omfatte både ændringer i data, som udføres, samt så vidt muligt læsning af persondata, så vidt muligt inkl. det anvendte søgekriterium, herunder skal logningen omfatte registrering af oplysninger om, hvem der har fået adgang til oplysninger i advarselsregisteret og oplysninger om spærrede kort.

Registreringen skal indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte.

[…]

Logs skal opbevares af Rejsekort og Trafikvirksomhederne, i 6 måneder, hvorefter de kan og skal slettes. Der skal løbende ske opfølgning på logningen, f.eks. stikprøvevis eller ved mistanke om forsøg på uautoriseret adgang eller misbrug af data.

Forsøg på misbrug af adgangen til persondata eller til systemets funktioner i øvrigt, skal følges op i den organisation, hvor dette er sket, samt rapporteres til Rejsekorts Sikkerheds-forum, som skal vurdere eventuel opfølgning af generel art mht. hvilke tiltag dette kan give anledning til."

Kravene til logning er nærmere beskrevet i bilag 5 til databehandleraftale mellem Rejsekort og East-West.

Det bemærkes, at der på s. 6 under overskriften "Vurdering af hvilke behandlinger, der skal anmeldes" står følgende:

"East-West har noteret sig, at rejsekort har anmeldt behandlingen af data i et advarselsregister og spærreliste til Datatilsynet, Rejsekorts advokat har derimod ikke vurderet, at der var grundlag for at anmelde oplysninger om rejsemønstre krydsrefereret med generelle kundeoplysninger (f.eks. navn og cpr.nr.). Oplysningerne i advarselsregistre og spærrelister er anset for fortrolige og personlige. Med henvisning til brev af 13. september 2006 har Rejsekorts advokat vurderet og konkluderet, at kun behandlingen af personlige og fortrolige oplysninger i advarselsregistret og spærrelisten er omfattet af anmeldelsespligten. Udfra disse oplysninger udleder East-West, at alle øvrige behandlinger af data i rejsekort systemet, som følge heraf ikke er omfattet af anmeldelsespligten." (understreget her).

På s. 7 under overskriften "Generelle krav til logning af personoplysninger" står herefter, at det er East-Wests vurdering, at*"[a]lene behandlingen af data, som skal anmeldes til Datatilsynet skal logges."*

Det fremstår altså som om det alene er behandling af oplysninger i advarselsregistret og i spærrelister, der logges, og ikke behandling af oplysninger om rejsemønstre krydsrefereret med generelle kundeoplysninger, dvs. selve transaktionerne.

Rejsekort har hertil oplyst, at ovenstående citater er udtryk for East-Wests opfattelse på et tidligere tidspunkt, men at logning – uanset ovenstående – efter aftale med East-West sker og er sket af alle tilgange til oplysninger.

Det fremgår af s. 9, afsnit 1.4.2 om "Konkret implementering af krav om logning", at der gælder følgende logningskrav for "personlige og fortrolige oplysninger": (1) System tidspunkt, (2) Login ID, (3) identifikation af den person oplysningerne vedrørte, (4) type af anvendelse (f.eks. læsning, skrivning og hvilken liste, der er anvendt), og (5) søgeord (f.eks. navn, fødselsdato eller cpr.nr.).

Logning foretages ikke i følgende tilfælde: (1) "spørgsmål vedr. overvågning af systemet og driften" (dette vedrører alene den tekniske drift) og (2) når der køres en "batch run", hvorved databaserne opdateres.

Om "Konkret implementering af kontrol med afviste forsøg", jf. afsnit 1.4.3, fremgår det bl.a., at der skal foretages en registrering af ethvert afvist forsøg på adgang til systemet, uanset om afvisningen er forårsaget af brug af forkert password, forkert brugeridentifikation eller manglende autorisation til en vis funktion eller andet. Systemet skal herefter udvise en reaktion, f.eks. lukning af pc'en o. lign., så yderligere forsøg på adgang forhindres, og hændelsen skal kommunikeres til den relevante systemadministrator.

Logs opbevares af Rejsekort, trafikselskaberne og East-West i 6 måneder, hvorefter de slettes.

Trafikselskaberne har en generel rapporteringspligt til Rejsekort vedrørende fejl og lignende i Rejsekort A/S' systemer.

11.11 Egenkontrol og ekstern kontrol

Det fremgår af Compliance Manualens s. 64-65, at Rejsekort A/S og trafikselskaberne skal udarbejde procedurer for kontrol af eget arbejde (egenkontrol), og at en ekstern kontrol årligt skal vurdere, om de interne kontroller er tilstrækkelige og gennemføres i fornødent omfang.

Ved ISAE 3402-erklæring af 6. marts 2015 har revisionsselskabet Ernst & Young vurderet de interne forretningsprocesser og kontroller hos Rejsekort A/S og East-West, der sikrer driften af Rejsekort A/S' databaser samt de ydelser i databaserne, som Rejsekort A/S leverer til de tilsluttede trafikselskaber.

I relation til kontrollen af brugeradministration og de tildelte brugeradgange, jf. afsnit 10.1 ovenfor, kommer erklæringen til følgende resultater:

I relation til proceduren for trafikselskabernes kvartalsvise gennemgang af de tildelte brugeradgange, konstateres det, at kontrollen kun er udført i andet kvartal 2014 i forbindelse med forberedelse til opgradering af rejsekort version 5.1, og at kontrollen ikke har været udført herudover.

I relation til proceduren for East-Wests kvartalsvise gennemgang af de tildelte brugeradgange, konstateres det, at kontrollen ikke har været udført i 2014, og at kontrollen ikke er effektiv.

Frem til og med februar 2014 oprettede Rejsekort A/S på vegne af visse trafikselskaber brugere i BackOffice, og det konstateres, at disse brugere er oprettet som kopi af andre brugere i samme medarbejderkategori, og at der i den forbindelse ikke er taget stilling til tildelte rettigheder.

I forhold til reglen om funktionsadskillelse og at adgang til de "globale brugeradministratorer" skal være begrænset, konstateres det, at der indtil september 2014 har været et større antal brugere hos East-West, som er tildelt rettigheder, som tillader, at de uden begrænsning og logning kan tildele sig selv og andre alle rettigheder, og at kontrollen vedrørende identifikation af privilegerede rettigheder samt gennemgang af brugere tildelt disse ikke har været udført frem til september 2014.

Rejsekort A/S har hertil bemærket, at årsagen til disse resultater er, at der i 2014 blev leveret en ny systemversion af Rejsekortsystemets software af East-West. I forbindelse med leverancen blev alle brugers adgang slettet og brugere med behov for adgang blev vurderet og tildelt adgang på ny.

Da leverancen imidlertid blev udskudt flere gange i tidsrummet fra 1. januar 2014 og frem til den faktiske leverance den 29. september 2014, blev gennemgangen af de tildelte adgange (sletning og ny oprettelse) udskudt tilsvarende, da det ved hver udskydelse var forventet, at den ny software version ville blive leveret efter kort tid.

Rejsekort A/S har videre oplyst, at gennemgang af de tildelte brugeradgange efter 29. september 2014 foretages i henhold til instrukserne.

Der er ikke i ISAE 3402-erklæring konstateret afvigelser i forhold til reglen om, at oprettelse af en bruger kræver besked fra en leder omkring tildeling af rettigheder, ligesom der heller ikke er konstateret afvigelser i relation til procedurerne for certifikatfornyelse.

Endelig er der – med en enkelt undtagelse i relation til ajourføring af forretningsgange inden for Fraud Management – ikke fundet nogen afvigelser med hensyn til kontrollen af, at ansatte i Rejsekort A/S og trafikselskaberne følger bestemmelserne i Compliance Manualen, jf. erklæringens s. 50.

12. TILLADELSER FRA DATATILSYNET

Rejsekort A/S har ved brev af 3. september 2009 fra Datatilsynet modtaget en tilladelse til behandling af personoplysninger med henblik på førelse af en spærreliste over spærrede rejsekort. Tilladelsen meddeles på baggrund af en række vilkår vedrørende bl.a. optagelse på spærrelisten, videregivelse og sletning af oplysninger, udsteders oplysningspligt, den registreredes indsigtsret, urigtige/vildledende oplysninger, sikkerhedsforanstaltninger og ændring og ophør af førelsen af spærrelisten. Rejsekort A/S' egne retningslinjer vedrørende spærring af kort fremgår af Compliance Manualens s. 45-47.

Rejsekort A/S har desuden ved breve af 9. og 26. september 2013 modtaget tilladelse fra Datatilsynet til behandlingen "Kunderegister for særlige rabatordninger i rejsekortsystemet". Tilladelsen indebærer, at Rejsekort kan behandle personoplysninger om kortindehavere hos Rejsekort A/S i forbindelse med ansøgning til rabatordningen på grund af særlige personlige forhold (handicap eller førtidspension), og er givet under forudsætning af, at Rejsekort A/S iagttager persondatalovens regler.

Endelig har Rejsekort A/S oplyst, at virksomheden har holdt flere møder med Datatilsynet, hvor Rejsekort A/S har forklaret Datatilsynet om virksomhedens håndtering af personoplysninger, bl.a. at rejse- og betalingstransaktioner opbevares i 5 år, og at Datatilsynet ikke har haft bemærkninger hertil.

13. DE REGISTREREDES RETTIGHEDER

13.1 Rejsekort A/S' underretningspligt

Rejsekort A/S underretter kunderne om de generelle vilkår for anvendelse af rejsekortet i kortbestemmelserne.

Rejsekort A/S skal derudover give skriftlig meddelelse om spærring af rejsekortet til kortindehaveren af rejsekort personligt eller rejsekort flex i de tilfælde, hvor Rejsekort A/S har spærret kortet, jf. Compliance Manualen, s. 46. Meddelelsen indeholder bl.a. oplysning om årsagen til spærringen, kundens ret til indsigt og ret til anmodning om sletning/berigtigelse af oplysninger om spærring, samt oplysning om evt. klageadgang til Datatilsynet og Ankenævnet for Bus, Tog og Metro. Trafikselskaberne sender ligeledes en spærremeddelelse med disse oplysninger, når kortindehaveren selv ønsker kortet spærret.

I Rejsekorts privatlivspolitik (dokumentet "Beskyttelse af persondata – Rejsekort A/S"), der ligger tilgængelig på Rejsekorts hjemmeside fremgår i øvrigt oplysninger om, hvilke oplysninger, der registreres, hvordan de behandles, hvem der har adgang til oplysningerne, mv.

13.2 Kundens indsigtsret

Det følger af Compliance Manualen, s. 55, at Rejsekort A/S' kunder har ret til at få indsigt i de oplysninger, som er registreret om den pågældende i Rejsekort A/S' databaser, og ret til at få oplyst, hvilke andre virksomheder der har adgang til disse informationer. Kunden har også ret til at få berigtiget eller rettet eventuelle forkerte eller vildledende oplysninger om den pågældende, eller alternativt at få slettet eller blokeret sådanne oplysninger.

Kunder med et rejsekort personligt eller rejsekort flex kan via Rejsekort Selvbetjening se de sidste 13 måneders rejsehistorik, samt hvilke personoplysninger, der er registreret i Rejsekortsystemet.

Herudover kan kunderne få indsigt i disse oplysninger ved at henvende sig skriftligt, telefonisk eller ved personligt fremmøde til et trafikselskab eller Rejsekort A/S. I disse tilfælde kan der kun udleveres oplysninger, når den, der ønsker indsigt, har legitimeret sig. Reglerne herom er nærmere beskrevet i Compliance Manualen, s. 56-58.

Såfremt kunden ønsker indsigt i samtlige registreringer eller behandlinger af dennes personoplysninger, eller i øvrigt ønsker indsigt i oplysninger, der ikke er tilgængelige for kundecentret, kan kunden rette henvendelse til Rejsekort A/S.

Rejsekort A/S vil herefter give kunden indsigt i følgende: En oversigt over indholdet af samtlige registrerede personoplysninger, en udskrift af alle registrerede oplysninger om den pågældende, oplysning om, hvorfra oplysningerne stammer og kopi af den generelle persondatapolitik.

Ifølge Compliance Manualens s. 9 omfatter retten til indsigt ikke følgende: oplysning om, hvilke specifikke oplysninger, der er videregivet hvornår, til hvem og på hvilke betingelser, oplysning om hvem, der har foretaget opslag i vedkommendes data, oplysning om de IP-adresser, der har logget på Rejsekorts selvbetjening, eller oplysning vedrørende indbetalinger (NETS-transaktioner).

Retten til indsigt omfatter ligeledes indsigt i oplysninger om optagelse på listen over spærrede kort eller optagelse i advarselsregistret. Hvilke oplysninger, der gives i denne henseende, er nærmere beskrevet i Compliance Manualens s. 60.

Ifølge Compliance Manualens s. 62 skal oplysninger, der viser sig urigtige eller vildledende, snarest muligt slettes eller rettes.

Det fremgår endvidere, at anmodninger om sletning af oplysninger, der ifølge Rejsekort A/S' regler skal registreres og opbevares i en længere periode, jf. afsnit 9, ikke kan imødekommes.

Indsigelser fra en registreret over for berettigelsen af en behandling af oplysninger skal snarest – og inden 4 uger – besvares skriftligt af Rejsekort eller trafikselskabet.

13.3 Berigtigelse og sletning af oplysninger

Det fremgår af Compliance Manualens s. 62, at oplysninger, der viser sig urigtige eller vildledende, snarest muligt skal slettes eller rettes. Det fremgår endvidere, at anmodninger om sletning af oplysninger, der efter lovgivningen er pligt til at registrere og opbevare i en længere periode, ikke kan imødekommes, og at den pågældende registrerede skal orienteres om årsagen til, at anmodningen ikke kan imødekommes.

Indsigelser fra en registreret over for berettigelsen af en behandling af oplysninger skal snarest – og inden 4 uger – besvares skriftligt af Rejsekort A/S eller den pågældende trafikvirksomhed.

DEL II – BESKRIVELSE AF RETSGRUNDLAGET FOR REJSEKORT A/S' BEHANDLING AF PERSONOPLYSNINGER

14. PERSONDATALOVEN

14.1 Anvendelsesområde, databehandler og dataansvarlig

Det relevante retsgrundlag for Rejsekort A/S' behandling af personoplysninger er lov nr. 429 af 31. maj 2000 om behandling af personoplysninger med senere ændringer (herefter "persondataloven"), der bl.a. gælder for behandling af personoplysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling, jf. § 1, stk. 1.

Begrebet personoplysninger defineres bredt og omfatter enhver form for information om en identificeret eller identificerbar fysisk person, jf. persondatalovens § 3, nr. 1.

Behandlingsbegrebet er tilsvarende bredt, idet det følger af lovens § 3, nr. 2, at loven finder anvendelse på enhver operation eller række af operationer med eller uden brug af elektronisk databehandling, som oplysninger gøres til genstand for. Behandling i form af f.eks. indsamling, videregivelse og opbevaring mv. er således omfattet.

I persondatalovens § 3, nr. 4, defineres den dataansvarlige som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der alene eller sammen med andre afgør, til hvilket formål og med hvilke hjælpemidler, der må foretages behandling af oplysninger.

Det er som udgangspunkt den dataansvarlige, som er ansvarlig for overholdelsen af persondataloven, og som har en række pligter i medfør af loven. Den dataansvarlige er således den fysiske eller juridiske person, offentlige myndighed etc., som over for den registrerede har det umiddelbare ansvar for behandlingen, og som i det daglige har dispositionsretten over de oplysninger, der indgår i behandlingen, jf. Henrik Waaben og Kristian Korfits Nielsen, Lov om behandling af personoplysninger med kommentarer, 2. udg., 2008, DJØF, s. 117.

I persondatalovens § 3, nr. 5, defineres en "databehandler", som den fysiske eller juridiske person, offentlige myndighed, institution eller ethvert andet organ, der behandler oplysninger på den dataansvarliges vegne. En databehandler kendetegnes altså ved kun at behandle personoplysninger på vegne af (efter instruks fra) en dataansvarlig. Databehandleren behandler således aldrig personoplysninger til egne formål eller bruger de overladte oplysninger til andet end udførelsen af opgaven for den dataansvarlige.

Databehandlerens behandling af oplysninger betragtes som en overladelse – og ikke en videregivelse – af de oplysninger, der stilles til rådighed af den dataansvarlige. Det betyder,

at den dataansvarlige kan overlade oplysninger til databehandleren, uden at det kræver en hjemmel (videregivelseshjemmel) i persondataloven.

14.2 Hjemmel for behandling af personoplysninger og kravene til samtykke

En betingelse for, at en dataansvarlig efter persondataloven lovligt kan behandle personoplysninger, er, at den dataansvarlige har hjemmel til det efter loven.

I persondatalovens § 6 fastsættes de generelle betingelser for, hvornår en dataansvarlig må foretage behandling af personoplysninger, som ikke er følsomme oplysninger, dvs. alle andre oplysninger end dem, der er omfattet af lovens §§ 7-8. Det gælder f.eks. stamoplysninger i form af kunders navn og adresse, e-mails og telefonnummer, men også oplysningerne om kundernes rejsehistorik, jf. herved forudsætningsvis Datatilsynets udtalelse af 12. februar 2009 om overdragelse af kundeoplysninger fra Sterling Airlines A/S under konkurs (j.nr. 2009-212-0145), som er nærmere omtalt nedenfor.

Det følger af lovens § 6, stk. 1, nr. 1, at behandling af personoplysninger kan finde sted, hvis den registrerede har givet sit udtrykkelige samtykke hertil. Der er endvidere hjemmel til at behandle ikke-følsomme personoplysninger, hvis behandlingen er nødvendig for, at den dataansvarlige eller den tredjemand, til hvem oplysningerne videregives, kan forfølge en berettiget interesse og hensynet til den registrerede ikke overstiger denne interesse, jf. lovens § 6, stk. 1, nr. 7.

Tilsvarende må den dataansvarlige behandle følsomme oplysninger om bl.a. helbredsmæssige forhold, hvis den registrerede har givet sit udtrykkelige samtykke til en sådan behandling, jf. lovens § 7, stk. 2, nr. 1.

Endelig må private dataansvarlige behandle oplysninger om personnumre, når den registrerede har givet sit udtrykkelige samtykke hertil, jf. lovens § 11, stk. 2, nr. 2.

Det reguleres i persondatalovens § 3, nr. 8, hvilke krav der skal være opfyldt, for at den registrerede kan siges at have givet et udtrykkeligt samtykke i lovens forstand. Det fremgår heraf, at der ved den registreredes samtykke forstås enhver frivillig, specifik og informeret viljestilkendegivelse, hvorved den registrerede indvilger i, at oplysninger, der vedrører den pågældende selv, gøres til genstand for behandling.

Efter forarbejderne til persondataloven betyder kravet om, at der skal være tale om et specifikt samtykke, at et samtykke skal være konkretiseret i den forstand, at det klart og utvetydigt fremgår, hvad det er, der meddeles samtykke til. Det skal således af et meddelt samtykke fremgå, hvilke typer af oplysninger der må behandles, hvem der kan foretage behandling af oplysninger om den samtykkende, og til hvilke formål behandlingen kan ske.

Heraf følger bl.a., at det skal fremgå af et meddelt samtykke, hvorledes oplysningerne må anvendes af tredjemænd, hvortil oplysningerne ønskes videregivet, jf. Waaben og Korfits Nielsen, ovf.a.st., s. 126.

Den dataansvarlige må sikre sig, at der gives den registrerede tilstrækkelig information til, at den pågældende kan vurdere, hvorvidt samtykke bør meddeles.

Det antages, at dette krav nærmere betyder, at den dataansvarlige skal oplyse sin identitet, formålet med behandlingen og hvilke former for behandlinger der påtænkes, herunder i hvilken udstrækning videregivelse vil ske.

I en udtalelse af 4. juli 2006 om anmeldelse af personoplysninger i forbindelse med sæddonation (j.nr. 2004-42-0711) fandt Datatilsynet således, at kravene om et tilstrækkeligt samtykke bl.a. indebar, at doneren skulle have oplyst, hvor længe sæden og andre oplysninger blev opbevaret.

Den registrerede kan tilbagekalde et samtykke, jf. lovens § 38. Tilbagekaldelsen kan ske på et hvilket som helst tidspunkt, dog ikke med tilbagevirkende kraft.

14.3 Grundlæggende principper for behandling af personoplysninger

Enhver behandling af personoplysninger skal leve op til de grundlæggende principper i persondatalovens § 5.

Det følger således af lovens § 5, stk. 1, at oplysninger skal behandles i overensstemmelse med god databehandlingsskik. Derudover skal indsamling af oplysninger ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål, jf. lovens § 5, stk. 2, 1. pkt.

Efter lovens § 5, stk. 3, skal oplysningerne endvidere være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles og senere behandles. Behandling af oplysninger skal tilrettelægges således, at der foretages fornøden ajourføring mv. af oplysningerne, jf. § 5, stk. 4.

De indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til formålet med behandlingerne, jf. § 5, stk. 5.

Personoplysninger må således ikke opbevares i identificerbar form i længere tid end, hvad der er nødvendigt at hensyn til de formål, hvortil oplysningerne indsamles eller senere behandles. Det er ikke muligt generelt at beskrive, for hvilke tidsrum opbevaring af

identificerbare oplysninger vil kunne ske. Dette må afgøres efter en konkret vurdering i den enkelte situation.

Vejledende for vurderingen er f.eks. Datatilsynets udtalelse af 26. november 2004 om Parkering-Københavns opbevaring af oplysninger om betalte parkeringsafgifter (j.nr. 2203-313-0180). Det var oplyst i sagen, at oplysningerne om parkeringsafgifter blev slettet senest 5 år efter sagens afslutning. Datatilsynet udtalte, at Parkering-Københavns opbevaring af oplysningerne ikke var i strid med persondatalovens § 5, stk. 5. Tilsynet lagde vægt på, at Parkering-København som en del af den offentlige forvaltning er underlagt forpligtelser med hensyn til opbevaring af sagsakter og registre, ligesom arkivlovgivningen stiller krav til myndighedens opretholdelse af registreringer. Tilsynet henviste endvidere til, at Parkering-København kunne have brug for de i sagen omhandlede oplysninger til behandlingen af eventuelle klagesager eller til genoptagelse af parkeringssager. Det ville i disse tilfælde være nødvendigt at kunne identificere parten i sagen.

Datatilsynet har i en række tilfælde forholdt sig til spørgsmål vedrørende oplysninger om passagerers rejsemønstre.

Der kan f.eks. henvises til ovennævnte udtalelse af 12. februar 2009 om overdragelse af kundeoplysninger fra Sterling Airlines A/S under konkurs (j.nr. 2009-212-0145). Sagen vedrørte en overdragelse af kundedatabasen i det konkursramte luftfartsselskab til et nyt luftfartsselskab. Det var oplyst i sagen, at kundedatabasen indeholdt en række personoplysninger vedrørende ca. 15 mio. rejser, herunder bl.a. navn, adresse og kontaktoplysninger samt fløjen rute (afrejse- og destinationslufthavn).

Datatilsynet fandt, at oplysninger om bl.a. navn, adresse, kontaktoplysninger, samt oplysning om, at vedkommende havde købt en flyrejse med det konkursramte luftfartsselskab udgjorde generelle kundeoplysninger som nævnt i persondatalovens § 6, stk. 3, hvorfor oplysningerne som udgangspunkt kunne videregives til det nye luftfartsselskab uden samtykke fra de registrerede. Derimod krævedes samtykke for videregivelse af oplysningerne om fløjen rute. Datatilsynet forholdt sig dog ikke til spørgsmålet om opbevaringsperioden for kundedatabasen i det nye luftfartsselskab.

Der kan endvidere henvises til, at luftfartslovens § 148 a blev indført med anti-terrorpakke II (lov nr. 542 af 8. juni 2006) med henblik på at give PET en hurtigere og mere effektiv adgang til oplysninger om passagerer og besætningsmedlemmer (herunder rejsemønster), der ankommer til eller afgår fra Danmark. Efter bestemmelsen skal luftfartsselskaber foretage registrering og opbevaring i 1 år af oplysninger om passagerer og besætningsmedlemmer, der ankommer til eller afgår fra Danmark. Sigtet med luftfartsloven er at danne grundlag for etablering af et dansk PNR-system (”Passenger Name Record”). Bestemmelsen er endnu ikke sat i kraft.

Datatilsynet har i et høringssvar af 23. marts 2006 forholdt sig til lovforslaget til loven (L 217, FT 2005-2006) (j.nr. 2006-111-0029). Datatilsynet udtalte bl.a., at persondatalovens § 5, stk. 2 og 3, fører til, at luftfartsselskaber kun må behandle, herunder indsamle og registrere, oplysninger, som de selv har et aktuelt behov for af hensyn til varetagelse af deres egne formål (og ikke alene med henblik på politiets retshåndhævelse). Selskaberne må også kun opbevare oplysningerne, så længe de selv har behov for dem af hensyn til varetagelse af deres egne formål, jf. lovens § 5, stk. 5.

Det er karakteristisk for sagen, at den angår et kontrol- eller overvågningselement i forhold til de registrerede, herunder videregivelse af oplysninger til myndighederne i kontroløjemed, og derfor ikke umiddelbart lader sig overføre på nærværende problemstilling, der vedrører en privat virksomheds opbevaring af bl.a. rejsemønstre på passagerer.

14.4 Reglerne om de registreredes rettigheder

Persondataloven indeholder en række rettigheder for de registrerede personer.

Efter persondatalovens § 28, stk. 1, skal den dataansvarlige eller dennes repræsentant som udgangspunkt skal underrette den registrerede om en række oplysninger, når personoplysningerne er indhentet hos den registrerede selv. Det følger af bestemmelsen, at den dataansvarlige eller dennes repræsentant ved indsamling af oplysninger hos den registrerede skal give den registrerede meddelelse om følgende:

1) Den dataansvarliges og dennes repræsentants identitet.
2) Formålene med den behandling, hvortil oplysningerne er bestemt.
3) Alle yderligere oplysninger, der under hensyn til de særlige omstændigheder, hvorunder oplysningerne er indsamlet, er nødvendige for, at den registrerede kan varetage sine interesser, som f eks:
    a) Kategorierne af modtagere.
    b) Om det er obligatorisk eller frivilligt at besvare stillede spørgsmål samt mulige følger af ikke at svare.
    c) Om reglerne om indsigt i og om berigtigelse af de oplysninger, der vedrører den registrerede.

Efter stk. 2 gælder bestemmelsen i stk. 1 ikke, hvis den registrerede allerede er bekendt med de i nr. 1-3 nævnte oplysninger.

Persondataloven giver endvidere den registrerede ret til hos den dataansvarlige at få indsigt i de oplysninger, der behandles om den registrerede, hvis vedkommende ønsker det, jf. lovens § 31.

Den registrerede kan også til enhver tid over for den dataansvarlige gøre indsigelse mod, at oplysninger om vedkommende gøres til genstand for behandling, jf. lovens § 35.

Derudover har den dataansvarlige pligt til at rette eller slette oplysninger, der er urigtige eller vildledende, samt i den forbindelse at orientere andre, der har modtaget oplysningerne, om rettelserne, jf. lovens § 37.

14.5 Regler om sikkerhedsforanstaltninger

Når personoplysningerne er indsamlet, skal de behandles sikkerhedsmæssigt forsvarligt. Efter lovens § 41, stk. 3, skal den dataansvarlige (og databehandlere) træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

For offentlige myndigheder er persondatalovens sikkerhedskrav nærmere udmøntet i sikkerhedsbekendtgørelsen (nr. 528 af 15. juni 2000) og sikkerhedsvejledningen (nr. 37 af 2. april 2001).

Der findes ikke en tilsvarende sikkerhedsbekendtgørelse for den private sektor, men Datatilsynet anbefaler generelt, at private dataansvarlige i videst muligt omfang tilrettelægger sikkerhedsforanstaltningerne i overensstemmelse med sikkerhedsbekendtgørelsen, jf. f.eks.
Datatilsynets udtalelse af 6. juni 2012 om behandling af personoplysninger i cloud-løsningen Office 365 (j.nr. 2011-082-0216).

Persondatalovens sikkerhedskrav omfatter – afhængigt af den konkrete behandling af personoplysninger – navnlig følgende:

1. Forpligtelsen til at fastsætte nærmere retningslinjer, der beskriver, hvordan de fornødne sikkerhedsforanstaltninger konkret er etableret i organisationen, samt gennemgang af retningslinjerne mindst én gang årligt, jf. sikkerhedsbekendtgørelsens § 5,

2. kravet om instruktion af medarbejderne, herunder at de gøres bekendt med retningslinjerne, jf. bekendtgørelsens § 6,

3. kravet om særlige retningslinjer ved adgang til personoplysninger ved brug af it-udstyr uden for den dataansvarliges lokaliteter (hjemmearbejdspladser o.l.), jf. bekendtgørelsens § 7, stk. 2,

4. kravet om fysisk sikkerhed, jf. bekendtgørelsens § 8,

5. kravet om iagttagelse af de fornødne sikkerhedsforanstaltninger i forbindelse med reparation og service samt ved salg og kassation af anvendte datamedier, jf. bekendtgørelsens § 9,

6. kravet om autorisation og adgangskontrol, der sikrer, at kun personer, som autoriseres hertil, har adgang til personoplysninger, og at der kun autoriseres personer, for hvem adgangen er nødvendig som led i deres jobfunktion, at disse tildeles et individuelt personligt login, samt at den udstedte autorisation ændres eller lukkes ved medarbejderens fratræden eller flytning inden for organisationen, jf. bekendtgørelsens §§ 11-12 (se også afsnit 20 nedenfor),

7. kravene om, at der ved transmission via internettet (eller andre åbne net) foretages en risikovurdering omfattende alle elementer i løsningen, at der implementeres de fornødne sikkerhedsforanstaltninger til imødegåelse af de foreliggende risici, herunder brug af kryptering, hvis fortrolige eller følsomme personoplysninger overføres via internettet (eller andre åbne net), og om sikring af sikkerhed for autenticitet (afsenders og modtagers identitet) og integritet (de transmitterede oplysningers ægthed) i fornødent omfang ved anvendelse af passende sikkerhedsforanstaltninger, jf. bekendtgørelsens § 14,

8. kravet om kontrol med afviste adgangsforsøg, herunder blokering for yderligere forsøg efter et antal afviste adgangsforsøg, jf. bekendtgørelsens § 18 samt

9. kravet om registrering (logning) af alle anvendelser af personoplysninger, jf. bekendtgørelsens § 19.

14.6 Adgangen til personoplysninger

Sikkerhedsbekendtgørelsens regler, som skitseret umiddelbart ovenfor, indeholder som nævnt regler i §§ 11-12 om autorisation og adgangskontrol.

Hensynet bag bestemmelserne findes i persondatalovens § 41, stk. 3, hvoraf fremgår, at der skal træffes de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod bl.a., at oplysningerne kommer til uvedkommendes kendskab.

Det fremgår derfor af sikkerhedsbekendtgørelsens § 11, stk. 1, at kun de personer, som autoriseres hertil, må have adgang til de personoplysninger, der behandles, jf. stk. 1. Dette forudsætter, at der fastlægges en formel autorisationsordning og -arbejdsgang.

Ifølge bekendtgørelsens § 11, stk. 2, må der endvidere kun autoriseres personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles. De enkelte brugere må ikke autoriseres til anvendelser, som de ikke har behov for. Også personer, for hvem adgang til oplysninger er nødvendig med henblik på revision eller drifts- og systemtekniske opgaver, må autoriseres, jf. stk. 3.

Der ligger heri, at alle andre personer, også øvrige medarbejdere hos den dataansvarlige myndighed, i forbindelse med den omhandlede behandling er uvedkommende og ikke må have adgang til oplysningerne. Tilsvarende betragtninger ligger bag begrænsningen i autorisationen til kun at omfatte anvendelser, som de enkelte brugere har behov for. Det forudsættes, at der i den formelle autorisationsprocedure vil indgå en forudgående vurdering af, hvad den enkelte bruger har behov for at være autoriseret til, jf. sikkerhedsvejledningen.

Sikkerhedsbekendtgørelsens § 12 indeholder et krav om adgangskontrol, idet databehandleren skal træffes foranstaltninger for at sikre, at kun autoriserede brugere kan få adgang, og at disse kun kan få adgang til de personoplysninger og anvendelser, som de er autoriserede til. Denne bestemmelse indebærer, at der udover den ovenfor omtalte formelle autorisation af brugere, også skal etableres en teknisk adgangskontrol i systemerne (typisk en brugeridentifikation med tilhørende password), jf. sikkerhedsvejledningen.

14.7 Pligten til at indgå (under)databehandleraftaler og foretage kontrol

Når en dataansvarlig overlader en behandling af oplysninger til en databehandler, skal den dataansvarlige sikre sig, at databehandleren kan træffe de i § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og påse, at dette sker, jf. lovens § 42, stk. 1.

Det følger endvidere af lovens § 41, stk. 1, at personer, virksomheder mv., der udfører arbejde under den dataansvarlige, og som får adgang til oplysninger, kun må behandle disse efter instruks fra den dataansvarlige, medmindre andet følger af lov eller bestemmelser fastsat i henhold til lov.

Når den dataansvarlige gør brug af en databehandler, skal den dataansvarlige indgå en såkaldt databehandleraftale, der skal være skriftlig, i medfør af lovens § 42, stk. 2. Hertil kommer, at det følger af sikkerhedsvejledningens § 7, stk. 1, at hvis behandling af personoplysninger foretages af en databehandler på den dataansvarliges vegne, skal det fremgå af den skriftlige databehandleraftale, at reglerne i sikkerhedsbekendtgørelsen ligeledes gælder for behandlingen ved databehandleren. Endvidere bør det fremgå, om behandlingen af personoplysninger hos databehandleren sker helt eller delvist ved anvendelse af hjemmearbejdspladser.

Der skal endvidere indgås databehandleraftaler af ovennævnte indhold mellem den dataansvarlige og eventuelle underdatabehandlere.

Det følger af sikkerhedsvejledningen, at den dataansvarlige aktivt skal sikre, at de krævede sikkerhedsforanstaltninger også overholdes hos underdatabehandlere, og det kan i den sammenhæng være relevant at indhente en årlig revisionserklæring fra en uafhængig tredjepart. Den skriftlige aftale parterne imellem som nævnt ovenfor kunne bl.a. indeholde denne revisionserklæring som en betingelse for at lade behandlingen foretage hos databehandleren.

Hvis databehandleren gør brug af en underdatabehandler, skal den dataansvarlige modtage kopi af sådanne underdatabehandleraftaler, når de indgås.

14.8 Anmeldelse til Datatilsynet

Det følger af persondatalovens § 48, stk. 1, at den dataansvarlige eller dennes repræsentant – forinden iværksættelse af en behandling, som foretages for en privat dataansvarlig – skal foretage anmeldelse til Datatilsynet. Det gælder dog ikke, hvis der er tale om, at behandlingen omfatter oplysninger om kunder, leverandører eller andre forretningsforbindelser, i det omfang behandlingen ikke omfatter følsomme personoplysninger som nævnt i lovens § 7, stk. 1, og § 8, stk. 4, jf. lovens § 49, stk. 1, nr. 4.

15. SÆRLIGE REGLER OM OPBEVARINGSPLIGT AF PERSONOPLYSNINGER I SÆRLOVGIVNINGEN

Persondataloven indeholder en generel regulering af behandling, herunder opbevaring, af personoplysninger. I tillæg hertil er der i særlovgivningen fastsat regler af betydning for fastsættelsen af, hvor længe oplysninger kan opbevares i personhenførbar form. Det gælder f.eks. betalingstjenesteloven, hvidvaskningsloven og bogføringsloven.

Der er ikke tvivl om, at hvis der er pligt til at opbevare oplysninger, herunder personoplysninger, efter særlovgivningen, er opbevaringen tillige nødvendig i persondatalovens forstand, og opbevaringen er dermed lovlig, smh. Waaben og Korfits Nielsen, ovf.a.st., s. 156.

Jeg henviser f.eks. til Datatilsynets udtalelse af 18. maj 2005 (j.nr. 2004-311-0406), der bl.a. vedrørte en bank og to teleselskabers opbevaring af personoplysninger om kunder. Det var oplyst i sagen, at det ene teleselskab ikke slettede oplysninger om kunderne straks efter kundeophør. Teleselskabet henviste til, at virksomheden principielt kunne blive mødt med regningsklager i op til 5 år. Datatilsynet udtalte under henvisning til opbevaringspligten i bogføringslovens § 10, stk. 1, at teleselskabet bl.a. med hjemmel i denne bestemmelse kunne opbevare oplysninger om kunder i op til 5 år.

Rejsekort A/S har henvist til bestemmelser i henholdsvis betalingstjenesteloven, hvidvaskningsloven og bogføringsloven til støtte for, at Rejsekort A/S efter selskabets

opfattelse er forpligtet til at opbevare personoplysninger, herunder kundernes rejsemønstre og betalingstransaktioner i personhenførbar form i 5 år.

15.1 Betalingstjenesteloven

Rejsekortet er efter Finanstilsynets vurdering e-penge og omfattet af reglerne i lovbekendtgørelse nr. 613 af 24. april 2015 om betalingstjenester og elektroniske penge (betalingstjenesteloven), herunder lovens § 39 p, stk. 1, nr. 1, om tilladelse til at udstede elektroniske penge med begrænset anvendelse, jf. Finanstilsynets begrænsede tilladelse til Rejsekort A/S af 16. december 2011 til at udstede elektroniske penge her i landet.

Rejsekort A/S mener, at selskabet er forpligtet til at opbevare alle oplysninger, der kan være relevante for Finanstilsynets vurdering af Rejsekort A/S' forhold i relation til den meddelte begrænsede tilladelse til at udstede e-penge i mindst 5 år, jf. betalingstjenestelovens § 10.

Efter betalingstjenestelovens § 10 er betalingsinstitutter forpligtet til at opbevare alle oplysninger, der kan være relevante for Finanstilsynets vurdering af betalingsinstituttets forhold i relation til den meddelte tilladelse, i mindst 5 år.

Det er Rejsekort A/S' opfattelse, at Rejsekort A/S i medfør af denne regel er forpligtet til at gemme alle kunders rejsemønstre og betalingstransaktioner i personhenførbar form i 5 år.

15.2 Hvidvaskningsloven

Det følger af lovbekendtgørelse nr. 1022 af 13. august 2013 om forebyggende foranstaltninger mod hvidvask af udbytte og finansiering af terrorisme (hvidvaskningsloven) § 23, stk. 1, at de af loven omfattede virksomheder og personer skal opbevare identitets- og kontroloplysninger, i mindst 5 år efter at kundeforholdet er ophørt.

Det fremgår desuden af lovens § 23, stk. 2, at dokumenter og registreringer vedrørende transaktioner skal opbevares, så de kan fremfindes samlet i mindst 5 år efter transaktionernes gennemførelse.

Det er Rejsekort A/S' opfattelse, at selskabet er forpligtet til at opbevare kunders navn, adresse og CPR-nr. i 5 år efter et kundeforholds ophør, jf. hvidvaskningslovens § 23, stk. 1.

15.3 Bogføringsloven

Efter lovbekendtgørelse nr. 648 af 15. juni 2006 (bogføringsloven), § 10 skal den bogføringspligtige opbevare regnskabsmaterialet på betryggende vis i 5 år fra udgangen af det regnskabsår, materialet vedrører. Opbevaringen skal ske på en måde, som i hele opbevaringsperioden gør det muligt selvstændigt og entydigt at fremfinde det pågældende regnskabsmateriale.

Efter lovens § 3, nr. 1 og 5, defineres regnskabsmateriale som bl.a. registreringer, herunder transaktionssporet efter lovens § 4, stk. 1, og oplysninger i øvrigt, som er nødvendige for kontrolsporet, jf. § 4, stk. 2.

Efter lovens § 4, stk. 1, forstås ved transaktionssporet den sammenhæng, der er mellem de enkelte registreringer og den bogføringspligtiges årsregnskab, skatte- eller afgiftsopgørelse, tilskudsregnskab eller tilsvarende regnskabsopstilling, der skal udarbejdes i henhold til lovgivning. Efter lovens § 4, stk. 2, forstås der ved kontrolsporet de oplysninger, der dokumenterer registreringernes rigtighed.

Af forarbejderne til loven (lovforslag nr. 63, FT 1998-99) fremgår bl.a. følgende om bestemmelsen i § 4:

> *"Transaktionssporet er et samleudtryk for de oplysninger, der efter § 4, stk. 1, skal sikre, at det altid er muligt at kontrollere, om alle registreringer er medtaget i regnskabet og hvilke registreringer regnskabets poster er sammensat af. Det er derfor bestemt i forslagets § 8, stk. 1, at det skal være muligt ud fra f.eks. årsregnskabets eller skatteopgørelsens enkeltposter at kunne fremfinde alle de registreringer, som danner grundlag for den pågældende enkeltpost.*
> *Ligeledes skal det være muligt fra en registrering at følge denne til årsregnskabet eller skatteopgørelsen.*
>
> *[…]*
>
> *Kontrolsporet er et samleudtryk for de oplysninger, der efter § 4, stk. 2, skal sikre, at det altid er muligt at verificere grundlaget for registreringerne. Forslagets § 9 kræver i den forbindelse, at alle registreringer skal dokumenteres ved et bilag. […]*
>
> *Tilstedeværelsen af transaktionssporet og kontrolsporet efter forslagets § 4 indebærer, at alle regnskabets poster kan følges fra regnskabet over bogføringen og ned til enkeltbilag. Indretningen af bogføringen vil ofte indebære, at bilag kan følges over bogføringen og helt frem til regnskabet. Transaktions- og kontrolsporet er en del af regnskabsmaterialet, jf. forslagets § 3, og skal være til stede i hele opbevaringsperioden på 5 år, jf. forslagets § 10."*

Derudover definerer lovens § 5, 1. pkt., et bilag som enhver nødvendig dokumentation for transaktioner, der registreres i bogføringen, uanset dokumentationen er på elektronisk medie, mikrofilm, papir eller andet medie.

Lovens §§ 7-9 indeholder en række krav til registreringer og dokumentation. Således skal alle transaktioner registreres nøjagtigt under hensyn til virksomhedens art og omfang, jf. § 7, stk. 1, 1. pkt.

Efter forarbejderne (ovf.a.st.) skal ordet "transaktion" forstås bredt, og begrebet omfatter såvel en handling som et forhold af økonomisk betydning for virksomheden, herunder f.eks. køb og salg, likvide bevægelser, men også f.eks. rent regnskabsmæssige dispositioner. Det anføres, at bestemmelsen må ses i lyset af kravet om transaktionsspor i lovens § 8, stk. 1, jf. nærmere nedenfor.

Efter lovens § 7, stk. 2, skal registreringerne så vidt muligt foretages i den rækkefølge, som transaktionerne er foretaget i. Registreringerne skal henvise til de tilhørende bilag og indeholde oplysninger, der gør det muligt at bestemme den enkelte registrerings tidsmæssige placering i bogføringen.

Efter forarbejderne (ovf.a.st.) skal registreringsmetoden sikre den tidsmæssigt kronologiske rækkefølge i registreringerne. Disse skal henvise til de tilhørende bilag og indeholde oplysninger om f.eks. registreringsdatoen, der i mange situationer – typisk ved varesalg – vil svare til transaktionsdatoen. Denne skal altid fremgå af bilaget, jf. lovens § 9 og nedenfor.

Efter § 8 skal alle registreringer kunne følges til det i § 4, stk. 1, omhandlede regnskab, opgørelse eller opstilling. Tallene heri skal kunne opløses i de registreringer, hvoraf de er sammensat.

Endelig fremgår det af lovens § 9, stk. 1, at enhver registrering skal dokumenteres ved bilag. Er der udstedt eksternt bilag, skal dette så vidt muligt benyttes. Bilag skal oplyse, hvad der er nødvendigt for at identificere kontrolsporet, herunder tydeligt angive transaktionsdato og beløb.

I Bogføringsvejledningens punkt 4.6.2.2 er anført følgende konkrete eksempel til belysning af registrerings- og opbevaringspligterne efter bogføringsloven (eksempel 1, s. 41):

> *"Et eksempel kan være et teleselskab, som gemmer oplysninger om hvert telefonopkald, en kunde foretager. Dvs. oplysninger om, hvornår en kunde ringer, hvilket nummer der ringes til og hvor lang tid, der ringes, osv. Teleselskabet har i princippet på tidspunktet for hvert telefonopkald foretaget et salg til kunden og er nødt til at registrere oplysningerne med henblik på (en senere) fakturering.*
>
> *Er disse oplysninger en del af transaktionssporet eller kontrolsporet?*

Her er det nødvendigt at vurdere, om det er nødvendigt dokumentationsmateriale, og om det senere bliver erstattet af et andet materiale, der er tilstrækkelig dokumentation i sig selv.

Teleselskabet udskriver på et tidspunkt en faktura med specifikation opgjort på grundlag af de akkumulerede oplysninger. Denne faktura kan kunden tage stilling til og betale. På et tidspunkt efter betaling har kunden fortabt sin reklamationsret over opgørelsen.

Efter dette tidspunkt kan teleselskabet dokumentere sin salgsregistrering ved den udstedte faktura, herunder dokumentation for, at den er betalt. Tidligere oplysninger om de enkelte telefonopkald er nu ikke længere nødvendig dokumentation, fordi der nu foreligger en betalt faktura mellem to uafhængige parter. Fakturaen skal dog indeholde et vist minimum af oplysninger, så den kan medføre en korrekt registrering i bogføringen og dermed i regnskab eller anden opgørelse."

DEL III – MIN VURDERING AF REJSEKORT A/S' BEHANDLING AF PERSONOPLYSNINGER

16. REJSEKORT A/S INDSAMLING OG BEHANDLING AF OPLYSNINGER

Persondataloven finder anvendelse i forhold til Rejsekort A/S' behandling af de indsamlede oplysninger om kunderne til rejsekortet, da der foretages elektronisk behandling af personoplysninger i personhenførbar form. Rejsekort A/S er dataansvarlig i forhold til de behandlede oplysninger, jf. nærmere nedenfor.

Rejsekort A/S' indsamling og øvrige behandling af personoplysninger, som et led i driften af rejsekortet, er ganske omfattende. Rejsekort A/S behandler primært almindelige personoplysninger, men også i begrænset omfang følsomme personoplysninger. Der er – foruden kundernes CPR-nummer og de følsomme oplysninger om visse kunders handicap og førtidspension – tale om almindelige og ikke-fortrolige personoplysninger, som er omfattet af persondatalovens § 6.

16.1 Hjemmel for behandling af personoplysninger og kravene til samtykke

Rejsekort A/S har efter min opfattelse i almindelighed tilstrækkelig behandlingshjemmel til at indsamle og behandle både de almindelige og ikke-fortrolige personoplysninger samt de følsomme personoplysninger, fordi Rejsekort A/S får samtykke til behandlingen fra de registrerede kunder, jf. henholdsvis persondatalovens § 6, stk. 1, nr. 1, og § 7, stk. 2, nr. 1, og § 8, stk. 4. Tilsvarende gælder i forhold til Rejsekort A/S' behandling af oplysninger om kundernes CPR-numre, jf. lovens § 11, stk. 2, nr. 2.

Det kræver dog, at samtykkeerklæringerne er fyldestgørende udformet, således at der foreligger et informeret samtykke fra den, som oplysningerne vedrører. Det er ikke på alle punkter tilfældet.

Samtykketeksten, hvor de registrerede samtykker til behandling af de ikke-følsomme oplysninger om bl.a. CPR-nummer og rejsehistorik, indeholder således ikke nogen beskrivelse af, at de foretagne transaktioner på rejsekortet (dvs. rejsemønsteret) overvåges med det formål at opdage og forhindre overtrædelse af regler, vilkår m.v.

På denne baggrund er det min opfattelse, at samtykketeksten på dette punkt er for upræcis.

Det er min vurdering, at det er bedst stemmende med kravet om et informeret samtykke i persondatalovens § 3, nr. 8, at den registrerede tillige oplyses om dette formål.

Det er endvidere min opfattelse, at samtykkeerklæringen bør indeholde oplysning om opbevaringsperioden for oplysningerne om kundernes rejsemønster (transaktionsoplysningerne). Jeg har herved lagt vægt på, at der foretages en omfattende og

systematisk registrering af de pågældende kunders rejsemønstre, der på individniveau giver mulighed for en detaljeret kortlægning af deres rejsemønstre i en flerårig periode, hvilket kan føles indgribende for de pågældende.

Jeg anbefaler derfor følgende:

Anbefaling 1: Det bør fremgå af samtykkeerklæringen, at de foretagne transaktioner på rejsekortet (dvs. rejsemønsteret) overvåges med det formål at opdage og forhindre overtrædelse af regler, vilkår m.v. Samtykkeerklæringen bør endvidere indeholde oplysning om opbevaringsperioden for oplysningerne om kundernes rejsemønster (transaktionsoplysningerne)

Endelig har jeg overvejet, om samtykket kan anses for frivilligt_under hensyn til om der reelt eksisterer andre alternative rejsehjemler end rejsekortet. Det er for så vidt korrekt, at der ikke eksisterer en alternativ rejsehjemmel med samme opbygning og funktion som rejsekortet. Dog er der et udvalg af andre rejsehjemler, kunderne kan benytte sig af, hvis de ikke ønsker at anvende et rejsekort. Der er således mulighed for – afhængig af hvilken landsdel, man befinder sig i – at købe enkeltbilletter, klippekort samt at benytte et periodekort eventuel via en applikation (app) til smartphone. Derudover er det muligt at købe et rejsekort anonymt, jf. afsnit 3 nedenfor, hvis man som kunde ikke ønsker at give samtykke til registrering og opbevaring af personoplysninger, omend der ikke gives de samme rabatter på rejser foretaget med rejsekort anonymt som på rejser foretaget med rejsekort personligt

Jeg mener på den baggrund ikke, at samtykke fra kunderne til, at Rejsekort A/S kan behandle personoplysninger, kan anses for ufrivilligt på grund af mangel på alternative rejsehjemler. Hvis der derimod vil opstå en situation, hvor rejsekortet reelt er eneste mulighed for at købe rejsehjemmel til kollektiv transport (busser, tog, metro) kan der imidlertid rejses spørgsmål om, hvorvidt et samtykke er frivilligt.

Til ovenstående anbefaling har Rejsekort A/S oplyst, at Rejsekort A/S har udarbejdet den nuværende samtykketekst med henblik på at undgå en tekst, der var for lang og derved fremstår uklar for kunderne. Rejsekort A/S mener desuden, at Rejsekort A/S lovligt – uden at indhente samtykke hertil – kan overvåge rejsemønstre og gemme oplysninger om rejse- og betalingsmønstre i 5 år, fordi der kan findes alternativ behandlingshjemmel hertil i persondatalovens § 6, stk. 1, nr. 3 og 7. Rejsekort A/S har dog oplyst, at Rejsekort A/S under alle omstændigheder vil følge min anbefaling til samtykkeerklæringen.

Til Rejsekort A/S opfattelse bemærker jeg, at Rejsekort A/S i almindelighed har valgt at indhente samtykke til behandling af personoplysninger efter persondatalovens § 6, stk. 1, nr. 1. Behandlingshjemlen er på denne baggrund kundens samtykke. Jeg finder det bedst

stemmende med dette samtykke, at Rejsekort A/S udtømmende oplyser, til hvilke formål behandlingen kan ske. På den baggrund, og da Rejsekort A/S vil ændre samtykkeerklæringen, finder jeg ikke anledning til at gå ind i, om Rejsekort A/S kan anvende en anden behandlingshjemmel.

16.2 Grundlæggende principper for behandling af personoplysninger

Efter persondatalovens § 5, stk. 1, skal oplysninger behandles i overensstemmelse med god databehandlingsskik. Efter § 5, stk. 2, 1. pkt., må indsamling af oplysninger alene ske til udtrykkeligt angivne og saglige formål, og senere behandling må ikke være uforenelig med disse formål.

Efter min opfattelse lever Rejsekort A/S' behandling af personoplysninger op til kravet i persondatalovens § 5, stk. 2, om, at behandlingen af de registrerede personoplysninger skal ske til udtrykkeligt angivne og saglige formål, og at senere behandling ikke må være uforenelig med disse formål. Formålene med Rejsekort A/S' behandling af personoplysningerne er således udtrykkeligt opregnet som formålet om at administrere og betjene kunderne, at overholde gældende lovgivning, at kunne dokumentere rejsernes pris overfor kunderne i tilfælde af uenighed herom, samt at opdage og forhindre overtrædelse af regler, vilkår m.v. (såkaldt "Rejsekort A/S Fraud Management"), hvilket må anses for saglige formål. Der er endvidere ikke grundlag for at antage, at Rejsekort A/S foretager en senere behandling af personoplysningerne, der er uforenelig med disse formål.

Det følger af § 5, stk. 3, at behandling af oplysninger skal være relevante og tilstrækkelige og ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.

Rejsekort A/S indsamler og behandler efter min opfattelse i almindelighed kun de relevante og nødvendige oplysninger, som er et led i driften af rejsekortet som rejsehjemmel. Jeg har således ikke efter min gennemgang grundlag for at antage, at Rejsekort A/S systematisk indsamler og behandler personoplysninger i videre omfang, end Rejsekort A/S' behov tilsiger, jf. dog nedenfor om opbevaringsperioden. Rejsekort A/S har endvidere efter min opfattelse etableret en række adækvate procedurer, der sikrer at oplysningerne er ajourførte og korrekte.

17. OPBEVARING OG SLETNING AF PERSONOPLYSNINGERNE

17.1 Indledning

Rejsekort A/S' behandling af personoplysninger rejser imidlertid spørgsmål om, hvorvidt opbevaringsperioden for oplysningerne om kundernes rejsehistorik er for lang, med den konsekvens at der unødigt ophobes sådanne data i systemet.

Det fremgår af lovens § 5, stk. 5, at indsamlede oplysninger ikke må opbevares på en måde, der giver mulighed for at identificere den registrerede i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil oplysningerne behandles.

Rejsekort A/S opbevarer oplysninger om kundernes rejsemønstre i 5 år og har som begrundelse for opbevaringsperioden henvist til, at oplysningerne bevares for at kunne administrere og betjene kunderne samt for at overholde gældende lovgivning, herunder reglerne om opbevaringspligt af visse oplysninger efter bogføringsloven, betalingstjenesteloven og hvidvaskningsloven.

Det skal herefter vurderes, om betalingstjenestelovens § 10, hvidvasklovens § 23, stk. 2, og bogføringslovens § 10 hjemler en 5-årig pligt for Rejsekort A/S til opbevaring af rejse- og betalingstransaktioner i personhenførbar form.

17.2 Betalingstjenesteloven

Det er min vurdering, at betalingstjenestelovens § 10 ikke hjemler en pligt for Rejsekort A/S til at opbevare kunders rejsemønstre og betalingstransaktioner.

Jeg har lagt vægt på, at Rejsekort A/S som en *virksomhed med en begrænset tilladelse til udstedelse af elektroniske penge*, jf. betalingstjenestelovens § 39 p, stk. 1, nr. 1, ikke er omfattet af anvendelsesområdet for samme lovs § 10. Det fremgår således af bestemmelsens ordlyd, at alene *betalingsinstitutter* er forpligtet til at opbevare alle oplysninger, der kan være relevante for Finanstilsynets vurdering af betalingsinstituttets forhold i relation til den meddelte tilladelse, i mindst 5 år.

Af § 39 a fremgår det, at § 10 om opbevaring af oplysninger ligeledes finder anvendelse på *e-penge-institutter*. Det fremgår imidlertid af lovens systematik, at der er en klar sondring mellem *e-penge-institutter* og *virksomheder med en begrænset tilladelse til udstedelse af elektroniske penge*, jf. eksempelvis § 39 t, hvor det fremgår, at *"§ 84 om god skik finder tilsvarende anvendelse på e-penge-institutter og virksomheder med en begrænset tilladelse til udstedelse af elektroniske penge.*"

Da Rejsekort A/S ikke er et e-penge-institut, men en virksomhed med en begrænset tilladelse til udstedelse af elektroniske penge, er det min vurdering, at opbevaringspligten i betalingstjenestelovens § 10 således ikke finder anvendelse på Rejsekort A/S.

17.3 Hvidvaskningsloven

For så vidt angår opbevaringspligten efter hvidvaskningslovens § 23, stk. 2, er det min vurdering, at Rejsekort A/S ikke i medfør af bestemmelsen er forpligtet til at opbevare oplysninger om transaktioner i forbindelse med enkelte rejser, dvs. oplysninger om tidspunkt og sted for check ind, check ud og kontrol undervejs på rejsen, valgt kundetype, rejsepris og kortsaldo. Derimod er det min opfattelse, at Rejsekort A/S efter bestemmelsen

skal opbevare oplysninger i personhenførbar form om optankning og udbetalinger af penge på rejsekortet (kortsaldooplysninger).

Jeg har ved min vurdering lagt vægt på, at den nærmere fastlæggelse af opbevaringsforpligtelsen indenfor bestemmelsens rammer må antages at bero på en konkret vurdering. Jeg har herved lagt vægt på, dels at risikoen for at hvidvaske penge gennem brug af rejsekortet synes begrænset (lavrisikoscenarie), dels at kontrol- og dokumentationshensynet bag bestemmelsen efter min opfattelse må anses for at være tilstrækkeligt varetaget ved opbevaring af kortsaldooplysningerne.

For så vidt angår opbevaringspligten efter hvidvaskningslovens § 23, stk. 1, er det i øvrigt min vurdering, at Rejsekort A/S efter bestemmelsens ordlyd er forpligtet til at opbevare kunders navn, adresse og CPR-nr. i 5 år efter et kundeforholds ophør. Rejsekort A/S foretager da også efter det oplyste en sådan opbevaring.

17.4 Bogføringsloven

Det er min vurdering, at bogføringslovens § 10 ikke hjemler en pligt for Rejsekort A/S til i 5 år at opbevare oplysninger om kundernes rejsetransaktioner (rejsedata), der specificerer lokaliteterne for de enkelte kunders check ud og ind med rejsekortet.

Det er derimod min opfattelse, at bogføringslovens § 10, sammenholdt § 3, forpligter Rejsekort A/S til at opbevare oplysninger om kundernes betalingstransaktioner (tidspunkt for betaling, valgt kundetype, rejsepris og kortsaldo) i 5 år. Det er endvidere min opfattelse, at disse oplysninger skal opbevares på en sådan måde, at det er muligt at koble disse betalinstransaktioner til de pågældende kunders identitet.

Jeg har ved min vurdering lagt vægt på, at den nærmere fastlæggelse af opbevaringsforpligtelsen indenfor bestemmelsens rammer må antages at bero på en konkret vurdering af opbevaringens nødvendighed, og at kontrol- og dokumentationshensynet bag bestemmelsen efter min opfattelse må anses for at være tilstrækkeligt varetaget ved opbevaring af kundernes betalingstransaktioner (i personhenførbar form), og ikke de nævnte rejsetransaktioner (rejsedata).

Hertil kommer, at situationen i nærværende sag efter min opfattelse er at sammenligne med situationen i bogføringseksemplet i bogføringsvejledningens punkt 4.6.2.2, hvor et teleselskab efter et stykke tid ikke (længere) behøver at opbevare oplysninger om kundernes telefonopkald (hvem ringes til, hvornår, hvor lang tid osv.), da selskabets salgsregistreringer på dette tidspunkt kan dokumenteres i tilstrækkeligt omfang ved udstedte fakturaer.

Jeg henviser ved min vurdering til min beskrivelse af retsgrundlaget, jf. afsnit 15.3 ovenfor.

17.5 Konklusion

Det kan på ovenstående baggrund konkluderes, at Rejsekort A/S hverken i medfør af betalingstjenesteloven, hvidvaskningsloven eller bogføringsloven er forpligtet til at opbevare oplysningerne om kundernes rejsemønstre (transaktionerne) i personhenførbar form i 5 år.

Herefter skal spørgsmålet om opbevaringsperiodens længde afgøres efter persondatalovens § 5, stk. 5. Det er min vurdering, at Rejsekort A/S' opbevaring af oplysningerne om kundernes rejsemønstre i 5 år ikke er nødvendig med henblik på at varetage de formål, hvortil oplysningerne behandles.

Efter min vurdering må en 3-årig opbevaringsperiode på det foreliggende grundlag i almindelighed anses for tilstrækkeligt til at varetage de pågældende formål.

Jeg lægger herved vægt på, at kundernes mulighed for at gøre indsigelse mod rejserne som udgangspunkt bortfalder efter 3 år efter den almindelige, formueretlige forældelsesfrist, jf. forældelseslovens § 3, jf. lovbekendtgørelse nr. 1063 af 28. august 2013 om forældelse af fordringer. En 3-årig opbevaringsperiode må derfor anses for i almindelighed i tilstrækkeligt omfang at kunne varetage hensynet til, at Rejsekort A/S kan have brug for oplysningerne til behandlingen af eventuelle klagesager eller ved civile søgsmål.

Såfremt der indføres en 3-årig opbevaringsperiode, bør oplysningerne om kundernes rejsetransaktioner (rejsedata), der specificerer lokaliteterne for de enkelte kunders check ud og ind med rejsekortet, slettes efter 3 år.

Det er dog min opfattelse, at oplysninger om kundernes betalingstransaktioner (tidspunkt for betaling, valgt kundetype, rejsepris og kortsaldo) fortsat må opbevares i 5 år, jf. bogføringslovens § 10, smh. § 3 (se afsnit 15.3).

Endvidere bør der indføres en mulighed for, at samtlige oplysninger om en bestemt kundes rejse(r), dvs. oplysninger om tidspunkt og sted for check ind og ud, valgt kundetype, rejsepris og kortsaldo, i specifikke situationer skal kunne opbevares i længere tid end anbefalet ovenfor. Såfremt der verserer en klagesag ved Ankenævnet for Bus, Tog og Metro eller en efterfølgende retssag ved domstolene om kundens brug af rejsekort, skal Rejsekort A/S således have mulighed for at opbevare oplysninger om den eller de rejser, som sagen omhandler, med henblik på at kunne fremlægge den fornødne dokumentation i sagen.

Persondataloven er ikke til hinder for, at Rejsekort A/S § 10 opbevarer oplysninger om kundernes rejsemønstre i anonymiseret form (dvs. ikke personhenførbar form). Disse oplysninger udgør en nødvendig del af transaktionssporet i forbindelse med indtægtsfordelingen henholdsvis indtægtsregistreringen i de enkelte rejseselskaber.

Indtægtsfordelingen baserer sig således på, i hvilke geografiske områder de enkelte rejser er foretaget.

Jeg anbefaler derfor følgende:

Anbefaling nr. 2: Rejsekort A/S skal i udgangspunktet slette alle personhenførbare rejseoplysninger, senest når kunderne ikke længere kan gøre indsigelse mod de pågældende rejser. Da Rejsekort A/S hverken efter betalingstjenesteloven, hvidvaskningsloven eller bogføringsloven har pligt til at opbevare oplysninger om kundernes rejser i 5 år, anbefales det, at Rejsekort A/S indfører en kortere opbevaringsperiode – f.eks. 3 år. I særlige tilfælde, hvor der f.eks. på grund af en klage- eller retssag er konkret behov herfor, kan oplysningerne forblive registreret i længere tid. Oplysninger om kundernes betalingstransaktioner (tidspunkt for betaling, valgt kundetype, rejsepris og kortsaldo) må dog af hensyn til bogføringsloven fortsat opbevares i 5 år

18. ADGANGEN TIL PERSONOPLYSNINGERNE

Det skal herefter vurderes, om Rejsekort A/S lever op til kravene om autorisation og adgangskontrol i § 11-12 i sikkerhedsbekendtgørelsen. Overordnet set, er det min vurdering, at Rejsekort A/S opfylder de formelle krav i §§ 11, stk. 1, idet Rejsekort A/S har fastlagt en autorisationsordning og -arbejdsgang, både for så vidt angår medarbejdere hos Rejsekort A/S, de tilsluttede trafikselskaber og IT-leverandøren East-West, jf. gennemgangen af de af Rejsekort A/S fastsatte instrukser i afsnit 10.1 ovenfor.

Det er dog tydeligt ud fra ISAE 3402-erklæringen af 6. marts 2015, udarbejdet af revisionsfirmaet Ernst & Young, at den praktiske implementering og overholdelse af reglerne, navnlig udførelsen af effektive kontroller af de tildelte brugeradgange, på visse punkter har været mangelfuld i 2014. Der henvises for en nærmere beskrivelse heraf til afsnit 11.11 ovenfor.

Det skal dog bemærkes, at Rejsekort A/S har oplyst, at gennemgang af de tildelte brugeradgange efter 29. september 2014 foretages i henhold til de fastsatte instrukser. I forhold til kravet i § 11, stk. 2 om, at kun personer, der er beskæftiget med de formål, hvortil personoplysningerne behandles, må autoriseres, er der ikke på baggrund af en gennemgang af instrukserne anledning til at tro, at Rejsekort A/S ikke skulle leve op til dette krav.

Det fremgår således af instrukserne, at der i den formelle autorisationsprocedure indgår en forudgående vurdering af, hvad den enkelte bruger har behov for at være autoriseret til, jf. også kravet herom i sikkerhedsvejledningen.

Rejsekort A/S har imidlertid oplyst, at ca. 1.100 medarbejdere hos Rejsekort A/S, de tilsluttede trafikselskaber og East-West per april 2015 har adgang til alle personoplysninger i Rejsekortsystemet, dvs. oplysninger om kunder (dvs. navn, adresse samt oplysning om kundetype) og samtlige rejse- og betalingstransaktioner i 13 måneder fra transaktionsdatoen. Disse medarbejdere har herunder adgang til følsomme personoplysninger omfattet af § 7 (handicap).

Uanset, at jeg er bekendt med, at der er en driftsøkonomisk begrundelse for, at alle medarbejdere i kundeservicecentrene har adgang til alle data i Rejsekortsystemet, er det høje antal personer med adgang til kundernes data efter min opfattelse betænkeligt og kan give anledning til kritik af Rejsekortet A/S.

Det forhold, at det kan føre til overkapacitet i kundeservicecentre at nedsætte antallet af personer med adgang til data, hvis den samme service skal opretholdes, kan efter min opfattelse ikke i tilstrækkelig grad opveje den omfattende adgang til rejse- og transaktionsoplysninger i 13 måneder, der eksisterer p.t.. Ud fra et hensyn om at minimere adgang til personoplysninger, herunder følsomme oplysninger, mest muligt, anbefaler jeg derfor, at Rejsekortet A/S tager skridt til at sikre, at et færre antal personer har adgang til rejsekortsoplysninger.

En måde at begrænse antallet af medarbejdere, der har adgang til de omhandlede data, er at sikre, at der alene gives adgang til de medarbejdere, der arbejder med servicering af Rejsekort-kunder, samt andre medarbejdere, der varetager funktioner, som nødvendiggør, at de har adgang til oplysningerne, og at sikre, at de pågældende medarbejdere alene har adgang til de specifikke oplysninger, de anvender i deres arbejde. Grundlæggende handler dette altså om at sikre, at medarbejdere alene har adgang til oplysningerne, når det er nødvendigt – og at øvrige adgange skæres væk.

Alternativt kunne kundeservice omorganiseres med henblik på at nedbringe antallet af medarbejdere med adgang til data, eksempelvis ved at rejsende i f.eks. hovedstadsområdet alene serviceres af de trafikselskaber, der opererer her, eller ved at trafikselskaberne udpeger specifikke medarbejdere i deres kundeservicecentre, der kan servicere Rejsekort-kunder.

Jeg anbefaler derfor følgende:

Anbefaling 3: Rejsekort A/S bør tage initiativ til at få reduceret antallet af personer, der har adgang til personoplysninger gennem rejsekortet, herunder bl.a. i forhold til personer i kundeservice og salgsrettede funktioner. Rejsekort A/S bør således overveje, hvordan understøttelsen og organiseringen af kundeservice og salg kan omlægges, så færre samlet set har adgang til oplysningerne om kunder og deres rejse- og betalingstransaktioner.

19. VURDERING AF SIKKERHEDSFORANSTALTNINGER

Det skal vurderes, om Rejsekort A/S som dataansvarlig overholder reglerne om sikkerhedsforanstaltninger i persondataloven og i sikkerhedsbekendtgørelsen, som er nærmere beskrevet i sikkerhedsvejledningen.

19.1 (Under)databehandleraftaler og kontrol med (under)databehandlere

Rejsekort A/S har indgået en databehandleraftale med East-West, jf. databehandleraftale af 25. november 2014. Databehandleraftalen er standardmæssigt udformet. Det er min vurdering, at aftalen indeholder de bestemmelser, som en sådan aftale skal have, herunder bestemmelser, som forpligter databehandlerne til at overholde persondataloven og sikkerhedsbekendtgørelsen.

I tilslutningsaftalen, der indgås mellem Rejsekort A/S og det enkelte trafikselskab, er der en række bestemmelser, der regulerer forholdet mellem Rejsekort A/S (som dataansvarlig) og trafikselskaberne (som databehandler), samt trafikselskabernes generelle forpligtelser i relation til opbevaring af personoplysninger, jf. Tilslutningsaftalen, pkt. 2.6. Også i forhold til tilslutningsaftalen er det vurderingen, at aftalen indeholder de bestemmelser, som en sådan aftale skal have, for at overholde kravene til en databehandleraftale.

I både databehandleraftalen med East-West og tilslutningsaftalen det enkelte trafikselskab er det anført, at databehandleren kan indgå underdatabehandleraftaler med underleverandører.

Rejsekort har oplyst, at man modtager kopi af disse underdatabehandleraftaler efter behov. Persondatareglerne pålægger den dataansvarlige at føre kontrol med databehandleres og underdatabehandleres overholdelse af reglerne. Dette indebærer bl.a., at den dataansvarlige skal modtage kopi af de underdatabehandleraftaler, som måtte blive indgået, så den dataansvarlige bliver bekendt med underdatabehandlerens identitet og kan kontrollere denne.

Jeg anbefaler derfor følgende:

Anbefaling 4: Rejsekort A/S skal sikre sig, at man modtager kopi af underdatabehandleraftaler, så snart East-West eller de enkelte trafikselskaber måtte indgå sådanne aftale.

Den dataansvarliges kontrol med databehandlere og underdatabehandlere skal desuden have realitet. Det er ikke nok, at det i databehandleraftalen eller et andet dokument er anført, at databehandleren vil føre kontrol, hvis denne kontrol ikke rent faktisk finder sted.

Det er hensigtsmæssigt, at kontrollen tilrettelægges sådan, at kontrolforanstaltningerne efterfølgende kan dokumenteres. En ofte anvendt kontrolmodel for dataansvarlige er brug af ekstern bistand i form af indhentelse af en revisionserklæring, som dokumenterer, at databehandleren overholder persondatareglerne, herunder har etableret de fornødne sikkerhedsforanstaltninger.

Jeg anbefaler derfor følgende:

Anbefaling 5: Rejsekort A/S bør udarbejde og implementere et bedre tilsyn med trafikselskaberne gennem en konkret handlingsplan herfor. I handlingsplanen bør mulighederne for anvendelse af tilsynsmidler såsom kontrolbesøg eller stikprøvekontroller mv. inddrages. Det anbefales, at tilsynet navnlig fokuserer på at styre tildeling af medarbejderadgang til personoplysninger, jf. ligeledes anbefaling nr. 3

19.2 Fastsættelse og ajourføring af interne sikkerhedsretningslinjer

Det er min vurdering, at Rejsekort A/S opfylder forpligtelsen i sikkerhedsbekendtgørelsens § 5 til at fastsætte nærmere retningslinjer, der beskriver, hvordan de fornødne sikkerhedsforanstaltninger konkret er etableret i organisationen, idet Rejsekort A/S har udarbejdet en Compliance Manual, der indeholder retningslinjer for behandling af personoplysninger, herunder en række sikkerhedsforanstaltninger.

Jeg vurderer ligeledes, at Rejsekort A/S opfylder kravet i § 5 om at foretage en ajourføring af retningslinjerne og til årligt at føre kontrol hermed. Det fremgår nemlig af Compliance Manualen, at Rejsekort A/S løbende ajourfører denne med henblik på at sikre, at manualen er i overensstemmelse med gældende lovgivning på området, og Rejsekort A/S har oplyst, at der foretages en årlig kontrol af ajourføringen.

19.3 Kravet om instruktion og uddannelse af medarbejderne

På baggrund af oplysningerne i afsnit 11.3 er det min umiddelbare vurdering, at medarbejdere hos Rejsekort A/S, de tilsluttede trafikselskaber og øvrige data og

underdatabehandlere, som udfører behandlingen, bibringes den nødvendige viden, herunder at medarbejderne har kendskab til de gældende sikkerhedsregler, jf. sikkerhedsbekendtgørelsens § 6. Jeg har dog i sagens natur ikke haft adgang til at efterprøve den faktiske efterlevelse af reglerne om instruktion og uddannelse af medarbejderne.

19.4 Særlige retningslinjer ved brug af hjemmearbejdspladser o.lign.

Rejsekort A/S har i Compliance Manualen fastsat regler, der sikrer, at der udarbejdes særlige retningslinjer ved adgang til personoplysninger ved brug af IT-udstyr uden for den dataansvarliges eller databehandlerens lokaliteter, f.eks. hjemmearbejdspladser o. lign., med henblik på at oprette det fornødne sikkerhedsniveau, og opfylder på denne baggrund kravet i sikkerhedsbekendtgørelsens § 7, stk. 2.

De pågældende regler er nærmere beskrevet i afsnit 11.4 ovenfor.

19.5 Kravet om kontrol med afviste adgangsforsøg mv.

Compliance Manualen og databehandleraftalen mellem Rejsekort A/S og East-West indeholder – i overensstemmelse med sikkerhedsbekendtgørelsens § 18 – krav om logning af alle afviste adgangsforsøg, og om at systemet skal lukke adgangen for en brugeridentifikation, for hvilken der inden for kort tid registreres gentagne afviste adgangsforsøg, jf. afsnit 11.9 ovenfor. Der skal ifølge manualen ligeledes ske rapportering til den relevante systemadministrator af forsøg på misbrug af adgangen til personoplysninger.

19.6 Kravet om logning

Det skal endelig vurderes, om Rejsekort A/S lever op til kravet i sikkerhedsbekendtgørelsens § 19, om der skal foretages logning af alle anvendelser af personoplysninger, og om at registreringen mindst skal indeholde oplysning om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte, eller det anvendte søgekriterium.

Ifølge Compliance Manualen er Rejsekort A/S og trafikselskaberne ansvarlige for, at der i Rejsekortsystemet og i trafikselskabernes front-end-IT-systemer, der giver adgang Rejsekortsystemet, foretages logning af adgangen til Rejsekortsystemet, funktioner og data samt i muligt omfang af forsøg på tilgang til personoplysninger mv. i Rejsekortsystemet.

Logningen skal omfatte både ændringer i data, som udføres, samt så vidt muligt læsning af persondata, så vidt muligt inkl. det anvendte søgekriterium, herunder oplysninger om, hvem der har fået adgang til oplysninger i advarselsregisteret og oplysninger om spærrede kort, og registreringen skal indeholde oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte.

Jeg mener på denne baggrund, at sikkerhedsbekendtgørelsens krav om logning er opfyldt for så vidt angår Rejsekort A/S' og trafikselskabernes logning af adgang til Rejsekortsystemet.

Det er dog ikke helt klart for mig, om der ligeledes sker logning af anvendelser af personoplysninger i Rejsekort A/S' øvrige databaser, dvs. Datawarehouse og RESS, idet der alene står i Compliance Manualen, at der skal foretages logning i "rejsekortsystemet".

Det fremgår dog af Compliance Manualen, s. 8, hvor de forskellige databaser – hhv. Rejsekortsystemet, RESS og Datawarehouse – gennemgås, at "*nærværende compliancemanual er i relevant omfang gældende for disse tre systemer, og hvor der i teksten er anført "rejsekortsystemet", skal det derfor forstås som gældende uanset fra hvilket af disse systemer data tilgås*". Jeg lægger derfor til grund, at reglerne om logning i Compliance Manualen gælder samtlige Rejsekort A/S' databaser, hvori der foretages anvendelse af personoplysninger.

For så vidt angår kravene til logning hos East-West, er disse nærmere beskrevet i bilag 5 til databehandleraftale mellem Rejsekort og East-West. Som beskrevet i afsnit 11.10 ovenfor fremgår det af bilag 5 til databehandleraftalen, at det alene er behandling af oplysninger i advarselsregistret og i spærrelister, der logges, og ikke behandling af oplysninger om rejsemønstre krydsrefereret med generelle kundeoplysninger, dvs. selve transaktionerne.

Rejsekort har hertil oplyst, at ovenstående citater er udtryk for East-Wests opfattelse på et tidligere tidspunkt, men at logning – uanset ovenstående – efter aftale med East-West sker og er sket af alle tilgange til oplysninger.

Det fremgår endvidere, at logningskravene for personlige oplysninger omfatter de krævede oplysninger om tidspunkt, bruger, type af anvendelse og angivelse af den person, de anvendte oplysninger vedrørte.

Jeg vurderer på denne baggrund, at den logning af anvendelse af personoplysninger, der foretages hos East-West, ligeledes lever op til sikkerhedsbekendtgørelsens krav, idet jeg lægger til grund, at der, som oplyst af Rejsekort A/S, er foretaget logning af alle tilgange til oplysninger, uanset det af East-West anførte.

Jeg bemærker i øvrigt, at logs efter de fastsatte regler opbevares af Rejsekort A/S, trafikselskaberne og East-West i de påkrævede 6 måneder, hvorefter de slettes.

20. DE REGISTREREDES RETTIGHEDER

Jeg vurderer i det følgende, om Rejsekort A/S i nødvendigt omfang sikrer de registreredes rettigheder, herunder om Rejsekort A/S lever op til kravene om underretning

(persondatalovens § 28), om Rejsekort A/S sikrer den registreredes indsigtsret (persondatalovens § 31) og om Rejsekort A/S overholder den registreredes indsigelsesret og pligten til at slette og berigtige oplysninger, der er urigtige eller vildledende (persondatalovens §§ 35 og 37)

20.1 Rejsekort A/S' underretningspligt

For så vidt angår Rejsekort A/S' pligt til at underrette de registrerede, fremgår det af afsnit 7, at kunden ved bestilling af rejsekortet meddeler samtykke til behandling af personoplysninger om den pågældende. Når der er tale om personer, der er omfattet af en særlig rabatordning (handicappede og førtidspensionister), meddeler den pågældende ligeledes samtykke. De to samtykketekster er dog ikke enslydende.

Det følger af persondatalovens § 28, at kunden som udgangspunkt skal have meddelelse om, at Rejsekort A/S og dets repræsentanters identitet, formålet med behandlingen og alle yderligere oplysninger, der er nødvendige for, at kunden kan varetage sine interesser. Sådanne oplysninger kan være om kategorien af modtagere af oplysninger om den pågældende og om reglerne om indsigt. Der gælder ingen formkrav til meddelelsen, men det påhviler Rejsekort A/S at kunne dokumentere, at oplysningspligten er opfyldt. Det samtykke, som kunden giver i forbindelse med køb af rejsekortet, vil derfor kunne være tilstrækkelig til at opfylde underretningspligten efter persondatalovens § 28, hvis samtykketeksten indeholder de nødvendige oplysninger efter § 28.

Begge samtykketekster indeholder oplysninger om, at det er Rejsekort A/S og de tilsluttede trafikvirksomheder, der behandler kundens personoplysninger samt formålet med indsamlingen. Endvidere erklærer kunden i den almindelige samtykketekst at have læst Rejsekort A/S' persondatapolitik, der indeholder yderligere oplysninger bl.a. om hvem, der har adgang til oplysningerne og kundens ret til indsigt og berigtigelse efter persondataloven. Samtykketeksten for personer, der er omfattet af en særlig rabatordning indeholder ikke en sådan erklæring eller henvisning.

Det er min vurdering, at samtykketeksten indeholder tilstrækkelige oplysninger til at opfylde underretningspligten i persondatalovens § 28, stk. 1, nr. 1 - 2.

20.2 Kundens indsigtsret

Det fremgår af afsnit 13.2, der henviser til Compliance Manualen afsnit 9.4., at Rejsekort A/S' kunder kan få indsigt i de oplysninger, som Rejsekort A/S har registreret om den pågældende i sine databaser for at imødekomme den registreredes indsigtsret. Kundens ret til indsigt i de oplysninger, der behandles om den pågældende, følger af persondatalovens § 31. Efter bestemmelsen er Rejsekort A/S forpligtet til på begæring fra kunden, at meddele den pågældende visse oplysninger, der er oplistet i bestemmelsens stk. 1, nr. 1-4.

Det er min vurdering, at de oplysninger, som Rejsekort A/S udleverer ved besvarelse af en indsigtsanmodning, opfylder kravene i persondatalovens § 31, stk. 1, nr. 1-4. Jeg har i den forbindelse lagt vægt på, at kunden får udleveret et udskrift af alle registrerede oplysninger om den pågældende, oplysninger om den pågældende, oplysning om, hvorfra oplysningerne stammer, og en kopi af persondatapolitikken. Jeg bemærker i den forbindelse, at persondatapolitikken indeholder oplysninger om behandlingens formål og hvem oplysningerne videregives til, jf. persondatapolitikken afsnit 1 og 2, hvilket er påkrævet efter persondatalovens § 31, stk. 1, nr. 2 og 3.

Jeg har desuden noteret mig, at Rejsekort A/S ikke stiller formkrav til indsigtsbegæringen. Rejsekort A/S stiller dog krav om legitimation, hvis begæringen sker ved personlig henvendelse eller telefonisk. Endvidere har jeg noteret mig, at svar meddeles snarest og senest inden for 4 uger. En sådan fremgangsmåde ved behandling af indsigtsanmodninger er ligeledes i overensstemmelse med persondatalovens §§ 31 og 41, stk. 3, der bl.a. angiver, at personoplysninger ikke må komme til uvedkommendes kundskab.

20.3 Kundens indsigelsesret og retten til at få berigtiget og slettet oplysninger

Det fremgår af afsnit 13.2, at indsigelser fra en kunde over for berettigelsen af en behandling af oplysninger snarest – og inden 4 uger – besvares skriftligt af Rejsekort A/S eller trafikvirksomheden.

Endvidere fremgår det af Compliance Manualen afsnit 7.4. (om spærring af kort), 8.6. (om advarselsregisteret), og 9.6. (særligt om berigtigelse eller sletning af oplysninger), at kunden har ret til at få berigtiget eller rettet eventuelle forkerte eller vildledende oplysninger om den pågældende, eller alternativt at få slettet eller blokeret sådanne oplysninger. Denne adgang til berigtigelse omfatter dog ikke oplysninger, som Rejsekort A/S er forpligtet til at opbevare i medfør af anden lovgivning.

Det følger af persondatalovens § 35, at kunden har ret til at gøre indsigelse mod de oplysninger, der behandles om den pågældende. Endvidere følger det af persondatalovens § 37, at den dataansvarlige har pligt til at rette eller slette oplysninger, der er urigtige eller vildledende. Det følger bestemmelsens stk. 2, at på anmodning fra kunden skal Rejsekort A/S underrette andre, der har modtaget oplysningerne, der skal rettes/slettes om, at oplysningerne er blevet berigtiget.

I Compliance Manualen er der både taget højde for kunders indsigelsesret, ligesom adgangen for kunder til at få korrigeret urigtig eller vildledende oplysninger er beskrevet. Som Rejsekort A/S' behandling af indsigelser fra kunder er beskrevet, har jeg ikke grundlag for at mene, at behandlingen skulle være i strid med de krav, der stilles til behandlingen af indsigelser fra kunder, jf. persondatalovens § 35, eller kundernes adgang til at få rettet eller slettet oplysninger efter lovens § 37.

Jeg bemærker dog, at det fremgår af Compliance Manualen afsnit 7.4, at der skal gives meddelelse til personer, der har modtaget oplysninger, der skal rettes eller slettes. Noget tilsvarende fremgår ikke af hverken manualens afsnit 8.6. eller 9.6. Jeg skal for god ordens skyld bemærke, at underretningspligten gælder generelt, og det kan overvejes at præcisere dette med en henvisning i de to afsnit.

Bilag 1

Kammeradvokaten har til brug for udarbejdelsen af dette notat, modtaget flere dokumenter fra Rejsekort A/S vedrørende virksomhedens behandling af personoplysninger. Disse dokumenter omfatter følgende:

- Rejsekort A/S' privatlivspolitikker, herunder pjecen "Rejsekort passer godt på dine oplysninger" og dokumentet "Beskyttelse af persondata – Rejsekort A/S", version 2.1 af 13. oktober 2014
- Compliance Manual, version 1.4 af 1. januar 2014
- Kortbestemmelser for private brugere, gældende fra 11. april 2014
- Tilslutningsaftale mellem Rejsekort A/S og de tilsluttede trafikselskab, version 6.2 af 8. december 2014
- ISAE 3402-erklæring af 6. marts 2015, udarbejdet af revisionsfirmaet Ernst & Young)
- Dokumenter fra databehandleren East-West ("system/subsystem specification for the Rejsekort System" Vol. 1.50: Archiving og Vol. 1.52: Logging Framework, databehandler aftale af 25. november 2014 mellem Rejsekort og East-West med bilag (bilag 1, 3, 4a, 4b og 5)
- Dele af Rejsekort A/S' korrespondance med Datatilsynet, Finanstilsynet og Forbrugerombudsmanden