

Personvernemnda
Postboks 4594 Nydalen

0404 OSLO

Deres referanse
02/60-82

Vår referanse (bes oppgitt ved svar)
06/01019-20 /SVE

Dato
22. juni 2007

Klage på vedtak - Elektronisk billettering i Rogaland

Innledning

Sommeren 2006 mottok Datatilsynet flere henvendelser (klager) fra innbyggere i Rogaland som uoppfordret hadde fått et "plastkort" påført navn og fødselsdata, i posten. Kortet var utstedt av Rogaland Kollektivtrafikk FKF (RKT), og var et såkalt reisekort, med betegnelsen "Kolumbuskortet".

Saksgang

I brev av 4. juli 2006 (vedlegg 1) ber Datatilsynet RKT redegjøre for Kolumbuskortet. Brevet ble besvart av virksomheten den 18. juli 2006 (vedlegg 2). Datatilsynet vurderte besvarelsen som mangelfull, og rettet derfor et nytt brev til RKT den 15. august 2006 (vedlegg 3). Samme dag ble det sendt brev til Skattedirektoratet med spørsmål om bruk av folkeregisteropplysninger (vedlegg 4). RKT besvarte Datatilsynets henvendelse ved brev av 12. september 2006 (vedlegg 5). Skattedirektoratet svarte ved brev av 13. oktober 2006 (vedlegg 6), hvor det redegjøres for bakgrunnen, og vilkårene for, utlevering av folkeregisteropplysninger. Den 6. november 2006 sendte Datatilsynet varsel om vedtak (vedlegg 7). Tilsvaret på varselet er datert 28. november 2006 (vedlegg 8).

I brev av 18. januar 2007 (vedlegg 9) fattet Datatilsynet, med hjemmel i personopplysningsloven § 46 følgende vedtak:

1. Rogaland Kollektivtrafikk FKF må endre "Min reisekonto" og løsningen for etablering av reisekonto slik at tilstrekkelig informasjonssikkerhet oppnås, jf. personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.
2. Risikovurderinger for løsningen **må**¹ oversendes Datatilsynet, jf. personopplysningsforskriften § 2-4.
3. Rogaland Kollektivtrafikk FKF må slette reisemønster koblet til den enkelte reisende dersom det ikke kan påvises å foreligge samtykke eller annen hjemmel for lagring, jf. personopplysningsloven § 8.

¹ Skrivefeil i det opprinnelige vedtaket rettet

RKT påklaget Datatilsynets vedtak i brev av 12. februar 2007 (vedlegg 10). Punkt 1 og 3 ovenfor ble påklaget. Klagen gjaldt imidlertid også Datatilsynets ”oppfatning” av at Kolumbuskortet er utsendt i strid med personopplysningslovens §§ 11 og 20, samt standpunktet om at RKT ikke utøver offentlig myndighet. Da det sistnevnte primært må oppfattes som en ytring, og ikke er omfattet av eller har relevans for Datatilsynets vedtak, er det i begrenset utstrekning behandlet i det følgende.

Virksomheten oversendte en risikovurdering for løsningen i brev av 26. mars 2007 (vedlegg 11).

Faktum

Kolumbuskortet er et såkalt reisekort / elektronisk billett, påført innehaverens navn og fødselsdata. Tilbudet innebærer opprettelse av en reisekonto, hvor innehaveren overfører et nærmere bestemt pengebeløp til kortets ”konto” i forkant av reisen(e).

Kolumbuskortet ble sendt alle innbyggere i Rogaland fylke, fra og med fylte 16 år. Totalt utgjorde dette 309 000 kort. Kortet er utstedt av RKT. RKT er et fylkeskommunalt foretak, ledet av et styre som er utpekt av Rogaland fylkesting. Utsendelsen ble gjennomført uoppfordret, hvilket innebærer at både aktive brukere og potensielle brukere av offentlig kollektivtilbud var mottakere av kortet. For nærmere informasjon se: kolumbus.no

Klagers anførsler

RKT påklaget Datatilsynets vedtak i brev av 12. februar 2007 (vedlegg 10). Når det gjelder vedtaket punkt 1 om informasjonssikkerhet anføres at *”RKT etterstreber en tilstrekkelig kryptert Reisekontoløsning. En del av dette er å ha et sikkerhetsdomene med https-løsning som innebærer ssl kryptering. Personopplysninger samt reiseinformasjon vil da være beskyttet både ved etablering og senere pålogging til tjenesten. Utover dette sendes det kun passord på E-post dersom kunden selv, ved å skrive inn sitt brukernavn og passord i selvbetjeningsløsningen, bestiller nytt passord. Passordet blir automatisk generert og sendes kun til den adressen som kunden har registrert i systemet. Ingen personer er involvert i denne prosessen. Alle systemer, selv sikker e-post, er basert på at brukeren kan holde på en hemmelighet, som passord, sikkerhetsnøkkel osv. Det finnes en lang rekke måter å stjele både nøkler og e-post på dersom kundens lokale dataressurser ikke er tilstrekkelig sikret. Vi mener det er nødvendig å kunne yte service overfor våre kunder hvor de har mulighet til å endre sitt passord og vi mener at sikkerheten her er godt nok ivarettatt fra vår side.”*

Nærmere oversikt og dokumentasjon av informasjonssystemet og sikkerhetstiltakene, fremgår ifølge virksomheten av risikovurderingen som ble oversendt separat til Datatilsynet (vedlegg 10).

For den del som gjelder vedtakets punkt 3, om sletting av reisemønster, anføres at bedrifter og organisasjoner i løpet av kort tid vil kunne registrere seg med en Reisekonto. *”Vi mener det er mer nærliggende å sammenlikne tjeneste med banktjenester enn teletjenester og ønsker å opprettholde at sletting av reisemønster først skjer automatisk etter 12 måneder. Dette mener vi at våre kunder vil forvente av tjenesten. Videre mener vi at det vil ivareta både privat- og bedriftskunders ”behov” for dokumentasjon til bruk i forhold til arbeidsgiver og*

forretningsreiser, samt selvangivelse. Kundens mulighet til å holde oversikt over, samt kontrollere sin bruk av Reisekonto er en viktig del av tjenesten og den servicen vi ønsker å yte.”

Videre er det anført som moment at Rogaland Revisjon IKS, blant annet har påpekt at det reiser seg et problem m.h.t. bokføring og bruk av Kolumbuskort for privatpersoner. *”Rogaland Revisjon anser dette som forskuddsfakturerings og kravet om ”sporbarhet” må oppfylles for bokføring eller inntektsføring av bruk fra reisekonto. Det er krav om reskontroføring ved forskuddsfakturerings. Rogaland Revisjon peker videre på at [det] ikke er noen mulighet for å endre bokføringsopplysninger og dermed imøtekomme datatilsynets krav om sletting av reisemønsteret etter 3 - 5 måneder. Det oppstår derfor en konflikt mellom datatilsynets krav og bokføringsloven.”*

Klagen omfattet også Datatilsynets vurdering, som var inntatt i varsel om vedtak av 6. november (vedlegg 7), av at Kolumbuskortet er utsendt i strid med personopplysningslovens §§ 11 og 20, samt standpunktet om at RKT ikke utøver offentlig myndighet. Dette var imidlertid ikke en del av det endelige vedtaket.

Datatilsynets vurdering

Den foreliggende sak reiser spørsmål av viktig prinsipiell art. For det første reiser saken spørsmål om enhver offentlig eid virksomhet har anledning til, på eget initiativ, å legge til grunn at alle innbyggerne ønsker et kundeforhold. I dette tilfelle har virksomheten tatt det for gitt at et kort som kan benyttes som elektronisk billett for kollektivreiser, er ønsket av mottaker. Dette spørsmål er imidlertid ikke omhandlet i klagen.

For det andre reiser saken spørsmål om virksomheters anledning til å lagre detaljert informasjon om kundenes bruk av offentlig kommunikasjon, hvilket også medfører lagring av innehavers bevegelsesmønster. For det tredje reiser saken spørsmålet om hvordan virksomheten skal sikre opplysningene de behandler, herunder hvor godt beskyttet tilgangen på kundesidene bør være. Saken ventes å få presedensvirkning, da reisekortløsninger er under utvikling og til dels lansert i en rekke andre fylker. Dette vil spesielt gjelde omfang av informasjon det er anledning til å lagre og for hvor lang tid. Spørsmålet om krav til sikkerhet vil også kunne ha presedensvirkning utover nevnte sektorområde.

Personopplysningsloven § 13 krever forholdsmessig sikring av personopplysninger. Kravene suppleres i personopplysningsforskriftens kapittel 2. Hovedregelen er at behandlingsansvarlig selv skal ta stilling til, og underbygge, om forholdsmessig sikring er oppnådd. Regelverket er utformet generelt, og gir ikke direkte føringer for hvordan slik sikring skal oppnås. Det sentrale begrep i bestemmelsen er ”forholdsmessig” som innebærer en stadfesting av behandlingsansvarliges forhold til risiko, herunder hvilke akseptkriterier som skal legges til grunn. Behandlingsansvarlig forutsettes videre å gjennomføre en risikovurdering som underbygger at forholdsmessig sikkerhet er oppnådd. Datatilsynet har laget egen veiledning om hvordan risikovurderinger kan gjennomføres. Denne er tilgjengelig på etatens nettside.

I foreliggende sak er det tale om behandling av personopplysninger for rundt 309.000 personer i et geografisk avgrenset område. I tillegg til grunndata om kunde, ønsker

virksomheten også å lagre opplysninger om innehavers bruk av kortet (reisemønster). Virksomhetens utgangspunkt var opprinnelig at denne informasjonen burde kunne oppbevares så lenge ”kundeforholdet” bestod. I senere korrespondanse oppgir virksomheten at den er villig til å justere oppbevaringstid til maksimalt et år. Virksomheten påberoper blant annet konflikt mellom bokføringsloven og personopplysningsloven.

Krav til sikring av informasjonen vil påvirkes av hvilke personopplysninger som inngår i behandlingen, samt omfanget av opplysningene som lagres. I dette tilfelle vil det, i den grad virksomhetens ønsker skal legges til grunn, lagres opplysninger om grunndata og reisemønster for alle brukere av offentlig kommunikasjon i Rogaland. I den grad en slik praksis skal legges til grunn krever det betydelig sikring av informasjonen.

Datatilsynet krever i vedtakets første punkt en bedre sikring av kundesidene ”min reisekonto”. I dette ligger det primært tre forhold:

- Sikring av database mot uvedkommende
- Sikring av at innsyn gis til rette vedkommende
- Sikring av selve kommunikasjonen

Sikring av database mot uvedkommende er spesielt viktig der behandlingsansvarlig eksponerer interne databaser på for eksempel nettbaserte kundesider. I slike situasjoner øker risiko for at personopplysninger kan komme på avveie. Behandlingsansvarlig må derfor utrede og iverksette tiltak som gjør at opplysningene er tilstrekkelig sikret. Dokumentasjon av dette må fremgå i risikovurdering.

Sikring av at rette vedkommende gis innsyn i personopplysninger forutsetter at det etableres gode mekanismer for autentisering av brukeren. Blant annet må spørsmålet om antall faktorer som skal benyttes og kvaliteten på disse drøftes i en risikovurdering. I foreliggende sak har behandlingsansvarlig, tilsynelatende uten særlige vurderinger, trukket den slutning at brukernavn og passord er tilstrekkelig. Rutiner rundt utstedelse og fornyelse er, etter tilsynets vurdering, ikke tilstrekkelig vurdert.

Virksomheten har begrenset seg til å etablere såkalt SSL kryptering av produktet ”Min reisekonto”. Dette innebærer i praksis at virksomheten kun sikrer selve kommunikasjonen av opplysninger over fremmed nettverk. Imidlertid er dette, som det fremgår over, kun en del av den sikring som er nødvendig. Datatilsynet har ikke mottatt risikovurderinger som i tilstrekkelig grad oppfyller de forventninger som følger av regelverkets krav. I brev av 26. mars 2007 fra RKT (vedlegg 11) er det i hovedsak kun redegjort meget kort for informasjonssikkerheten mellom kort og kortavleser. Datatilsynet mener, som det fremgår ovenfor, det er en alvorlig mangel at det ikke er utarbeidet risikovurderinger for selvbetjeningsløsningen ”Min Reisekonto”, lagringen av reisedata for selvbetjeningsløsningen, samt for selskapets generelle lagring av reisedata. Det er spesielt konfidensialiteten som er utsatt for risiko. Datatilsynet har etterspurt disse risikovurderingene flere ganger både muntlig og skriftlig, senest i vedtaket av 18. januar 2007 (vedlegg 9). Risikovurderinger i henhold til personopplysningsforskriften § 2-4 og generelt informasjonssikkerheten i henhold til personopplysningsloven § 13 er avgjørende

forutsetninger for om løsningen kan benyttes. Når tilstrekkelig informasjonssikkerhet i henhold til personopplysningsloven § 13 ennå ikke foreligger, eventuelt ikke er dokumentert i henhold til personopplysningsforskriften kapittel 2, er dette etter Datatilsynets mening en vesentlig mangel som får den følge at løsningen ikke kan benyttes.

Når det gjelder vedtakets punkt 3 om lagringstid, er Datatilsynets utgangspunkt at det ikke skal lagres personopplysninger lenger enn det som er nødvendig, jf. personopplysningslovens § 28, og at behandlingen må ha et grunnlag i § 8, jf. § 11.

Etter konkrete spørsmål fra Datatilsynet ble det i brev, mottatt hos Datatilsynet 12. september 2006 (vedlegg 5), uttalt at reisemønsteret til en navngitt reisende lagres så lenge den reisende ønsker å ha et forretningsforhold til RKT. Når den reisende ønsker å avslutte kundeforholdet, så slettes koblingene mellom kundenummeret og kundens reiser. Navn, personlige opplysninger og eventuell negativ sluttsaldo blir liggende igjen i dataregisteret.

Virksomheten opplyste i brev av 28. november 2006 (vedlegg 8) at det vil gå ned til 12 måneders lagringstid. Det er, etter Datatilsynets oppfatning, ikke oppgitt hjemmel eller formål som tilsier lagring av reisemønster for annet enn faktureringsformål. For en rekke andre norske tjenester tilsynet mener det er naturlig å sammenlikne med (for eksempel teletjenester), er lagringsbehov ansett å være begrenset til 3 måneder, maksimalt 5 måneder, for å ivareta fakturering etter at reisen er utført. Da virksomheten ikke har kunnet vise til hjemler som tilsier lengre lagringstid enn andre sammenliknbare tjenester, vil 3 måneder og maksimalt 5 måneder være aktuell lagringstid etter at reise er gjennomført ved etterskuddsfakturering. Ved forhåndsbetaling vil det ikke være grunnlag for å lagre opplysningene lenger enn til klagefristen er utløpt.

Eventuelt kan den reisende selv, aktivt ta initiativ og samtykke til lengre lagringstid.

Når det gjelder forholdet til bokføringsloven, er tilsynet kjent med krav om oppbevaring av tid og sted for ytelsen. Tilsynet kan vanskelig se at det ved overgang fra manuell betaling til bruk av kort, følger et krav om at enhver reiseopplysning skal oppbevares knyttet til den reisendes identitet. Prinsipielt er det ingen forskjell mellom et ordinært klippekort, eller flerreisekort, og elektroniske billetter som, ut fra lovens formål, tilsier at det er nødvendig å registrere og lagre reiseopplysninger knyttet til identitet. Ved kjøp av klippekort og/eller flerreisekort må det kunne forutsettes at kravet om angivelse av tid og sted for ytelsen referer seg til selve kjøpet eller påfyllingen av kortet.

Fra innstilling til Stortingets kommunal- og forvaltningskomité om Datatilsynet og Personvernemndas årsmeldinger for 2005, pkt. 2.2 hitsettes: *”Komiteen registrerer at økt adgang til personidentifisering er et viktig trekk ved utviklingen og at en vesentlig drivkraft bak dette er muligheten for å ta betalt for tjenester og kravet til å identifisere betaleren. Komiteen viser til at identitetstyveri synes å være et økende problem og at dette kan henge sammen med at det blir stadig mer vanlig å måtte oppgi personopplysninger ved blant annet kjøp av tjenester. Komiteen viser til at kravet til å oppgi personopplysninger i stadig flere tilfeller fører til at anonyme alternativer forsvinner. Komiteen har i den sammenheng særlig merket seg Datatilsynets innvendinger mot helautomatiske bomstasjoner der det ikke*

eksisterer anonyme alternativer. Komiteen kan ikke se at det eksisterer velbegrunnede og påtrengende hensyn som taler for å gjøre unntak fra retten til anonym ferdsel i forbindelse med bomstasjoner.” Etter det Datatilsynet kan forstå fremstår behovet for reell anonymitet som minst like fremtredende i denne sammenheng.

Det gjøres for øvrig oppmerksom på at temaet har vært gjenstand for diskusjoner i øvrige europeiske land, og etter det Datatilsynet har forstått, samsvarer tilsynets standpunkt i all hovedsak med praksis i de andre landene.

Med hilsen

Georg Apenes
direktør

Sverre Engelschiøn
seniorrådgiver

Kopi: Kolumbus Rogaland Kollektivtrafikk FKF, Postboks 270, 4002 STAVANGER

Vedlegg:

1. Datatilsynets brev av 4. juli til RKT
2. Brev fra RKT av 18. juli
3. Datatilsynets brev til RKT av 15. august
4. Datatilsynets brev til Skattedirektoratet av 15. august
5. RKTs brev til Datatilsynet av 12. september
6. Skattedirektoratets brev til Datatilsynet av 13. oktober
7. Datatilsynet varsel om vedtak av 6. november
8. Tilsvare på varselet, datert 28. november
9. Datatilsynets vedtak av 18. januar 2007
10. Klage på vedtak fra RKT av 12. februar 2007
11. Risikovurdering fra RKT av 26. mars 2007