

Ruter AS
Postboks 1030 Sentrum

0104 OSLO

Deres referanse

Vår referanse (bes oppgitt ved svar)
09/00163-3 /AAR

Dato
26. juni 2009

Varsel om vedtak og foreløpig kontrollrapport etter kontroll hos Ruter AS

Den 7. mai 2009 gjennomførte Datatilsynet en kontroll hos Ruter AS. Kontrollen skjedde med hjemmel i lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven) § 44, jf. § 42 tredje ledd nr. 3.

Foreløpig kontrollrapport

De avvik som ble avdekket i kontrollen er nærmere beskrevet i vedlagte kontrollrapport. Eventuelle feil eller mangler i de faktiske forhold som fremkommer i rapporten bes tatt opp med Datatilsynet i forbindelse med virksomhetens eventuelle tilsvarende til dette varselet, jf. siste avsnitt i dette brev. Det gjøres i den forbindelse oppmerksom på at rapporten skal gjenspeile de faktiske forhold på kontrolltidspunktet, slik at eventuelle senere endringer ikke får betydning for rapportens innhold. Dersom Datatilsynet ikke mottar merknader til kontrollrapporten blir denne å anse som endelig.

Varsel om vedtak

Dette er et varsel om at Datatilsynet, med hjemmel i personopplysningsloven § 46, vil fatte vedtak om følgende pålegg:

1. Virksomheten må gi informasjon til den registrerte om de forhold som er omtalt i personopplysningsloven § 19. Det vises til rapportens punkt 5.2.
2. Virksomheten må godtgjøre at det foreligger gyldig rettslig grunnlag for behandling av fødselsnummer som identifikasjonsmiddel for tildeling av skolebilletter, jf. personopplysningsloven § 12. Det vises til rapportens punkt 5.4.
3. Virksomheten må treffe de egnede tiltak i samsvar med personopplysningsloven § 13, jf. personopplysningsforskriften § 2-11, for å hindre uautorisert innsyn i personopplysninger. Det vises til rapportens punkt 5.5.
4. Tilgangen til kundenes personopplysninger for egne ansatte og de aktuelle databehandlers ansatte, må begrenses til det som er nødvendig for å utføre de pålagte oppgaver, jf. personopplysningsloven § 13, jf. personopplysningsforskriften § 2-11. Det vises til rapportens 5.6.

5. Virksomheten må inngå databehandleravtale med de databehandlere som virksomheten benytter, jf. personopplysningsloven § 15. Det vises til rapportens 5.7.
6. Opplysninger om den *initierende validering* må slettes senest tretti dager etter at billettens gyldighetsperiode har løpt ut, jf. personopplysningsloven § 28. Det vises til rapportens punkt 5.8.2.
7. Opplysninger om de reisendes *etterfølgende valideringer*, som allerede er registrert og lagret på bakgrunn av utilstrekkelig rettslig grunnlag, må slettes, jf. personopplysningsloven § 27, jf. § 11. Det vises til rapportens punkt 5.8.3.

Frist for tilsva

Eventuelle merknader til foreliggende varsel eller kontrollrapport bes sendt Datatilsynet snarest, og senest **innen 6. august 2009**.

Det anbefales at virksomheten oversender Datatilsynet et forslag til fremdriftsplan for lukking av de avvik som er beskrevet i kontrollrapporten. Datatilsynet vil se hen til denne fremdriftsplanen når det skal vedtas en frist for virksomhetens gjennomføring av påleggene.

Datatilsynet vil ikke fatte vedtak som her nevnt dersom virksomheten innen samme frist dokumenterer at de avvikene som er beskrevet i kontrollrapporten er lukket.

Med hilsen

Leif T. Aanensen
avdelingsdirektør

Atle Årnes
senioringeniør

Vedlegg: Foreløpig kontrollrapport
Kopi: Eva I.E. Jarbekk, advokat, Brækhus Dege Advokatfirma ANS
Postboks 1369 Vika, 0114 Oslo

Foreløpig kontrollrapport		
Saksnummer: 09/00163-3	Kontrollobjekt:	Utarbeidet av:
Dato for kontroll: 07. mai 2009	Ruter AS	Jørgen Skorstad og
Rapportdato: 26. juni 2009	Sted:	Atle Årnes
	Dronningensgate 40, Oslo	

1 Innledning

Datatilsynet gjennomførte kontroll hos Ruter AS ('Ruter' eller 'virksomheten') den 7. mai 2009. Kontrollen ble gjennomført i medhold av personopplysningsloven § 44, jf. § 42 tredje ledd.

Temaet for kontrollen var virksomhetens behandling av personopplysninger i forbindelse med elektronisk billettering. Kontrollen ble gjennomført i virksomhetens faste forretningsadresse.

I det følgende vil Datatilsynet beskrive de faktiske forhold som ble avdekket under kontrollen. Kontrollrapporten danner grunnlag for Datatilsynets vurderinger og eventuelle pålegg.

2 Tilstede under kontrollen

2.1 Fra virksomheten:

- Runar Hannevold, viseadm. direktør
- Svend Erik Wandaas, leder for faggruppe IKT, sikkerhet og personvern
- Einar Bjørkevold, teknisk leder
- Ellen Rogde, salgs- og markedsdirektør
- Marit Nilsen, prosjektleder
- Irene Vabe, medlem faggruppen
- Eva I.E. Jarbekk, advokat, Brækhus Dege Ans

2.2 Fra Datatilsynet:

- Jørgen Skorstad, juridisk rådgiver
- Hågen Ljøgodt, juridisk rådgiver
- Atle Årnes, senioringeniør

3 Generelt

Ruter tilbyr reisekort som kan utstyres med elektroniske billetter (e-billetter) til alle som benytter kollektivtransporttilbudene i Oslo og Akershus. Reisekortet, som har fått navnet *Flexus*, er utviklet av Ruter i samarbeid med NSB.

Flexuskortet er et personlig plastkort som utstedes til den enkelte kollektivreisende. Kortets eier kan i neste omgang kjøpe de billettprodukter som tilbys, enten av NSB eller av Ruter. På

kontrolltidspunktet besto Ruters tilbud av elektroniske billetter utelukkende av periodebilletter med en gyldighetsperiode på 30 dager. Det er også denne billettypen som har stått i fokus ved Datatilsynets kontroll.

I løpet av sommeren 2009 er det, slik Datatilsynet har forstått det, planlagt en utvidelse i utbudet av billettprodukter, i form av periodebilletter med kortere gyldighet.

På kontrolltidspunktet hadde Ruter registrert 24000 aktive reisekort. 12000 av disse kortene var skolekort for elever ved videregående skoler i Akershus, mens de en andel på om lag 7000 av de resterende kort var utstedt til ordinære kunder, og resten var frikort.

Ordningen med Ruters bruk av reisekort med e-billett har vært i drift i to og et halvt år. Ordningen så langt omfatter kun personlige reisekort med personlig e-billett, mens upersonlige Flexus-kort og elektroniske billetter er planlagt innført i fremtiden. Det er for øvrig fremdeles mulig å kjøpe ulike varianter av papirbilletter.

4 Kort om bruk av personopplysninger samt formålet med behandlingene

Dersom den reisende ønsker å benytte seg av tilbudet om personlig reisekort med e-billett, må han eller hun først oppgi kontaktopplysninger om seg selv. Disse personopplysningene blir knyttet til nummeret på reisekortet i en sentral kundedatabase. Informasjon om bruken av kortet, herunder de opplysninger som genereres ved en *validering* (se rapportens punkt 5.1.1.2), lagres sentralt i flere databaser.

Ruter ønsker å benytte disse opplysningene til forskjellige formål:

- for å administrere kundemassen
- for å kontrollere bruken av kortet
- for å etablere statistikk til bruk ved planlegging av rutetilbud.

Ruter registrerer og lagrer kundeopplysninger om alle kunder som kjøper kort hos Ruter. Tilsvarende lagrer NSB kundedata på de kunder som kjøper kort hos NSB. Kunden kan kjøpe e-billetter av begge operatører, men e-billetten blir levert av den virksomheten hvor kunden er registrert med reisekort. NSB har ikke tilgang til kundedata på Ruters kunder, og Ruter har ikke tilgang til kundedata på NSBs kunder. I fremtiden er det planer om at e-billetter fra forskjellige operatører kan legges på reisekort fra en annen operatør.

NSB lagrer reisedata som genereres av Ruters kunder på NSBs utstyr. NSB har ikke tilgang til de reisedata som genereres på Ruters utstyr av Ruters kunder. Tilsvarende vil Ruter lagre de reisedata som genereres av NSBs kunder på Ruters utstyr, men ikke ha tilgang til de reisedata som genereres på NSBs utstyr av NSBs kunder.

Under kontrollen fremkom det at avregning mellom selskapene ikke er et formål med lagringen av opplysninger i dag. Dette vil imidlertid være aktuelt i fremtiden.

5 Funn og avvik fra lovbestemte krav til behandling av personopplysninger

5.1 Generelle krav i forhold til behandling av personopplysninger

5.1.1 Oversikt over behandlinger, og hvilke personopplysninger som behandles

5.1.1.1 Kundeopplysninger

Virksomheten behandler personopplysninger for å administrere kundemassen og for å gjennomføre kontraktsforpliktelser overfor kundene. De opplysninger som registreres omfatter følgende:

- fornavn
- etternavn
- fødselsdato
- e-postadresse
- mobiltelefonnummer
- fasttelefonnummer
- adresse, postnummer, poststed
- kjønn

De foran nevnte opplysningene vil heretter blir referert til som *kundeopplysninger* eller *kundedata*.

Datatilsynet legger til grunn at virksomheten har rettslig anledning til å behandle disse opplysningene i medhold av personopplysningsloven § 11 første ledd bokstav a, jf § 8 bokstav a.

5.1.1.2 Reiseopplysninger

Hver gang kunden benytter reisekortet ved bruk av et transportmiddel, det vil si hver gang kunden foretar en validering, sendes informasjon om hendelsen til sentralsystemet.

Registreringene omfatter følgende personopplysninger:¹

- Transaksjons type
- Business date.
- Status på transaksjonen
- Utførende PTO (KTP, NSB eller Ruter)
- Stasjons id eller utstyrs id
- Kort eier
- Kort type
- Slutt dato for kortet
- Status for applikasjonen på kortet
- Transaksjons teller (telles opp hver gang det skrives til kortet)
- Slutt dato for applikasjonen
- Produkt eier

¹ Opplysningskategoriene er gjengitt ordrett, slik de er angitt i oversendt informasjon fra virksomheten, ved e-post av 11. mai 2009.

- Produkt template id
- Produkt kode
- Produkt sekvens nr
- Salgs dato fro produktet
- Selgende PTO (KTP, NSB eller Ruter)
- Sone fra, via og til dersom sone produkt
- Utløpsdato for produktet (ved valideringer)
- Om produktet er solgt via AutoRenew eller ikke
- Slutt dato for AutoRenew
- Gjenværende verdi på Flexus-konto
- Transaksjons verdi (0 ved valideringer)
- Betalingsmåte
- Linje (buss/ trikk)
- Avgangstid (buss, trikk avgangstid fra startholdeplass)
- Transaksjonstidspunkt
- Utførende transportør
- Sjøfører og id (pga salgsrapporter)

Disse opplysningene vil heretter omtales som *reiseopplysninger* eller *reisedata*.

Ruter har ikke direkte overfor Datatilsynet gitt uttrykk for hvilket rettslig grunnlag som det anser at behandlingen av disse opplysningene baserer seg på. Se imidlertid nedenfor, under 5.3 for indikasjoner på at behandlingene anses som samtykkebaserte.

5.2 Informasjon, innsyn, retting og sletting

5.2.1 Personopplysningslovens krav

I henhold til personopplysningsloven § 19 skal den behandlingsansvarlige av eget tiltak informere den registrerte om forhold som gjør vedkommende i stand til å bruke sine rettigheter etter personopplysningsloven. Blant annet skal det gis informasjon om formålet med behandlingen, jf. § 19 første ledd bokstav b. Ifølge lovbestemmelsen skal det dessuten gis informasjon om følgende forhold:

- navn og adresse på den behandlingsansvarlige og dennes eventuelle representant,
- hvorvidt opplysningene vil bli utlevert, og eventuelt hvem som er mottaker,
- at det er frivillig å gi fra seg opplysningene, og annet som gjør den registrerte i stand til å bruke sine rettigheter etter loven her på best mulig måte, som f.eks. informasjon om retten til å kreve innsyn, jf. § 18, og retten til å kreve retting, jf. § 27 og § 28.

5.2.2 Faktagrunnlag

Informasjon til de registrerte, det vil si virksomhetens kunder, er gitt på Ruters nettsted *ruter.no*. Denne rapport tar utgangspunkt i de opplysninger som var presentert på nettstedet på kontrolltidspunktet.

5.2.3 Datatilsynets vurdering

Datatilsynet vil understreke at virksomhetens rettslige forpliktelse til å informere de registrerte om forhold som nevnt over, jf. personopplysningsloven § 19, ikke nødvendigvis må oppfylles ved hjelp av internettbasert kommunikasjon, selv om dette i mange tilfelle kan være hensiktsmessig. Ettersom Datatilsynet ikke er kjent med at Ruter har formidlet de nødvendige opplysninger til virksomhetens (fremtidige) kunder på annen måte, vil imidlertid de vurderinger som følger nedenfor relatere seg til den informasjon som er kommunisert via nettstedet ruter.no.

Datatilsynet kan ikke se at det er gitt noen opplysninger på nettstedet om hva som er formålet, eller formålene, med behandlingen av de aktuelle personopplysningene. Den manglende informasjonen om dette forholdet, vil dermed være i strid med personopplysningslovens regler om innformasjonsplikt, jf. lovens § 19 første ledd bokstav b.

Det fremgår ikke hva slags personopplysninger som blir registrert om kunden ved validering av reisekort, eller hvorvidt disse opplysningene lagres i en sentral database eller lokalt på kortet. Slik Datatilsynet ser det, kan informasjonen på nettstedet skape et inntrykk av at det ikke lagres informasjon om de valideringer som gjøres i tidsrommet mellom første gangs validering og tidspunktet for utløpet av e-billettens gyldighetsperiode.

På Ruters nettsted kan kunden få tilgang til de personopplysninger som er registrert om ham eller henne, på ”MinRuter”. På kontrolltidspunktet var det ikke mulig å få tilgang til valideringsinformasjon via dette nettstedet. På bakgrunn av dette, er det nærliggende å trekke den slutning at informasjonsplikten vanskelig lar seg oppfylle via MinRuter.

5.3 Grunnleggende vilkår for å behandle personopplysninger

5.3.1 Personopplysningslovens krav

I personopplysningsloven § 11 oppstilles en rekke kumulative grunnkrav til behandling av personopplysninger. Ifølge bestemmelsens første ledd bokstav a, jf. § 8, plikter den behandlingsansvarlige – det vil i dette tilfellet si Ruter – å påse at det foreligger et gyldig rettslig grunnlag for en hver behandling av personopplysninger som faller innenfor dens ansvarsområde.

Etter personopplysningsloven § 8 kan en behandling av personopplysninger baseres på hjemmel i lov, samtykke, eller en av de nødvendighetsgrunner som er angitt i bokstavene a til f. Spørsmålet om det foreligger gyldig behandlingsgrunnlag, må i utgangspunktet stilles i relasjon til samtlige personopplysninger som behandles. Videre vil det formålet som ligger til grunn for den enkelte behandling kunne være avgjørende, jf. § 8 bokstavene a til f.

Behandlingsformålet har også betydning når det gjelder hvilke personopplysninger som kan anses som relevante, og som det dermed er adgang til å behandle, jf. § 11 første ledd bokstav d. Bestemmelsen fastslår: _

”Den behandlingsansvarlige skal sørge for at personopplysningene som behandles [...] er tilstrekkelige og relevante for formålet med behandlingen”.

Bestemmelsens relevanskriterium markerer en ytre grense for hvilke personopplysninger som kan trekkes inn i den aktuelle behandlingen; eller uttrykt på en annen måte: Behandlingen må ikke omfatte andre personopplysninger enn hva som er nødvendig for å nå det berettigede behandlingsformål.²

Begrensningen kommer også klart til uttrykk i personverndirektivet, som personopplysningsloven bygger på, gjennom presiseringen av at ”*personal data must be [...] adequate, relevant and not excessive*” i relasjon til behandlingsformålet.³

5.3.2 Faktagrunnlag

På bakgrunn av de faktiske opplysninger som er kommet frem så langt, kan de aktuelle behandlinger av personopplysninger som Ruter er ansvarlig for inndeles i følgende kategorier:

- Behandling (innsamling, registrering og lagring) av *kundeopplysninger*
- Behandling av *reiseopplysninger*

Det er utelukkende spørsmål om reiseopplysninger i tilknytning til de valideringer som gjøres i tidsrommet mellom den *initierende validering* og e-billettens utløpstidspunkt som berøres under dette avsnittet (*etterfølgende valideringer*).

Det bestrides ikke at det foreligger gyldige rettsgrunnlag for behandling av *kundeopplysninger* og opplysninger om den *initierende validering* av en elektronisk billett. Av samme årsak vil begrepet ”reiseopplysninger”, eller varianter av dette, i det følgende referere seg til de opplysninger som genereres, innsamles, registreres og lagres i kjølvannet av de *etterfølgende valideringer* – med mindre noe annet skulle være presisert.

Etter at kontrollen fant sted har Datatilsynet mottatt en kopi av et brev som Ruter har sendt til alle brukere av Flexuskortet i Akershus og til testbrukere i Oslo. Det fremgår altså at brevet, som er datert 6. mai 2009, er sendt ut til eksisterende Flexus-kunder etter at disse har inngått avtaler med Ruter. Brevet har overskriften ”Viktig informasjon om samtykke til behandling av personopplysninger”, og inneholder blant annet følgende passasjer:

”Personopplysningsloven krever at du gir oss ditt samtykke til behandling av personopplysninger for at vi skal kunne lagre data om deg på denne måten. Vi har derfor lagt ved et skjema som du må fylle ut og returnere til oss. På baksiden av skjemaet finner du mer informasjon.

Dersom du signerer og returnerer skjemaet innen 22. mai, kan du fortsette å reise med Flexus som før. Ønsker du ikke å signere og returnere skjemaet, må vi dessverre sperre kortet ditt den 15. juni.”

² Jf. Ot.prp. nr. 92 (1998-1999), i kapittel 16 ”Merknader til de enkelte paragraferne”.

³ Direktiv 95/46/EF artikkel 6 (1) litra c.

I informasjonsbrevet opplyses det også om at det lagres ”informasjon om deg og ditt kundeforhold til oss, blant annet hvilken billett du reiser med og når den utløper.” I selve samtykkeformularet er dessuten følgende oppgitt: ”Når du reiser med et registrert Flexuskort, vil Ruter lagre og behandle personopplysninger om deg, herunder dine reisedata.”

5.3.3 Datatilsynets vurdering

5.3.3.1 Kravet om behandlingsgrunnlag

Som det fremgår av sitatet over, har Ruter lagt til grunn at det kreves samtykke for behandling av personopplysninger om kunden. Datatilsynet har i prinsippet ingen innvendinger mot dette synspunktet. Imidlertid er tilsynet ikke enig i at samtykket som forsøkes innhentet er gyldig, jf. personopplysningsloven § 2 nr. 7 – først og fremst siktes det her til kravet om at et gyldig samtykke må være *informert*.

Hva som ligger i de begreper som er benyttet i Ruters informasjonsskriv er etter Datatilsynets oppfatning ikke klart. Utsagnet om at det lagres *kundeopplysninger* gir, slik Datatilsynet ser det, anvisning på at det foregår en innsamling, registrering og lagring grunnopplysninger om den enkelte reisende person, samt hvilke avtaler denne har inngått med Ruter og på hvilket tidspunkt, jf. det i sitatet nevnte eksempel (på kontrolltidspunktet var dette ensbetydende med periodebillett med en måneds gyldighet/varighet). Innhenting og registrering av denne typen opplysninger anses sjelden som kontroversielt, all den tid disse behandlingene relaterer seg til inngåelse av en eller annen form for kundeavtale.

Når det gjelder begrepet ”reisedata”, anser Datatilsynet dette som nokså uklart. Selve uttrykket sier lite annet enn at det dreier seg om ”data”, eller informasjon, om en eller flere *reiser*. Det kan ikke utledes av begrepet hvorvidt Ruter her har hatt identifiserbare eller pseudonymiserte opplysninger i tankene, eller om det siktes til opplysninger som ikke kan knyttes til den reisendes identitet, det vil si anonyme opplysninger.

Tilsynet er av den oppfatning at det i det minste må informeres om at det finner sted en innsamling og registrering av reisemønstre som kan knyttes til den enkelte kundes identitet, dersom man velger det elektroniske billettalternativet. Datatilsynet anser informasjon om dette forholdet som en grunnleggende forutsetning for at enkeltindividet skal kunne ta et kvalifisert valg mellom det elektroniske og sporbare alternativ på den ene siden, eller det anonyme alternativ, i form av papirbilletter, på den andre.

I forarbeidene til personopplysningsloven er det for øvrig uttalt at en av årsakene til at det stilles krav om at det gis informasjon i forbindelse med innhenting av samtykke, er at ”den registrerte må forstå hva erklæringen gjelder, og hvilke konsekvenser denne får eller kan få.”⁴ Slik tilsynet ser det, er de anvendte begreper i Ruters informasjonsskriv ikke entydige nok til at de registrerte kan forventes å se rekkeviddene av den databehandling som samtykkene ønskes innhentet for. At det heller ikke går klart frem hva formålet med behandlingen av disse opplysningene er, vil også være en medvirkende faktor til at det blir vanskelig for den enkelte å trekke slutninger om de konsekvenser behandlingen av opplysningene ”får eller kan få”.

⁴ Ot.prp. nr. 92 (1998-99), s. 119.

Det må være et minstekrav at de "reisedata" som lagres og behandles blir definert eller nærmere forklart, alternativt at det opplyses om hvilke konsekvenser behandlingen av reisedata medfører eller kan medføre for den enkelte reisende – altså at den reisendes bevegelser vil kunne være sporbare i ettertid. Slik informasjon må karakteriseres som helt essensiell for alle som ønsker å ta et kvalifisert valg mellom et anonymt eller sporbart alternativ.

Ei heller er det sagt noe om hvor ofte disse "reisedata" skal innhentes og registreres, om dette skal skje regelmessig eller kun unntaksvis, eller hvor lenge disse opplysningene oppbevares. Slik Datatilsynet ser det, er det en vesentlig forskjell mellom de tenkelige ytterpunkter i denne sammenheng: Hvorvidt det dreier seg om opplysninger om enhver påstigning til et transportmiddel, eller bare den initierende validering, må følgelig presiseres.

Informasjonskriteriet i personopplysningsloven § 2 nr. 7 kan etter dette ikke anses oppfylt. Et samtykke gitt med utgangspunkt i det omtalte informasjonsskriv tilfredsstillers således ikke de nødvendige krav til et gyldig samtykke som personopplysningsloven oppstiller.

Det skal tilføyes at personopplysningsloven legger opp til at samtykket må innhentes *før* den aktuelle behandlingen av personopplysninger tar til, jf. uttrykket "har samtykket" i lovens § 8. Det er med andre ord i strid med personopplysningsloven å innhente et samtykke etter at de aktuelle personopplysningene allerede er samlet inn og registrert.

5.3.3.2 Kravet om relevans

Datatilsynet bestrider ikke at Ruter har et saklig behov for å kartlegge reisemønstre, slik at kollektivtilbudet kan planlegges på en rasjonell måte. Dette formålet må imidlertid kunne nås uten at det samles inn og registreres opplysninger som kan knyttes til den enkelte reisendes identitet. Dersom de personidentifiserende parametrene som er angitt i rapportens punkt 5.1.1.2. utelates ved kommunikasjon mellom valideringsutstyr og Ruters sentrale system, vil den reisende forbli anonym i Ruters registre, samtidig som virksomheten får samlet inn relevant statistisk materiale som grunnlag for sin ruteplanlegging.

Etter det Datatilsynet har forstått, er det teknisk mulig å lagre opplysninger om en passasjers foregående validering lokalt i reisekortet. Et eventuelt behov for å kartlegge en passasjers overgang fra ett transportmiddel til et annet kan dermed imøtekommes: Opplysninger om at et bestemt individ har foretatt en overgang innenfor et gitt tidsrom kan lagres lokalt i kortet, for deretter å kommuniseres til sentralsystemet, uten at opplysningene kobles til passasjerens identitet.

Det ovennevnte relevanskriterium kan etter dette ikke anses som oppfylt, ettersom det ikke vil være nødvendig å behandle *personopplysninger*, i den forstand som definert i personopplysningsloven § 2 nr. 4, for å nå de uttalte planleggingsformål. Konklusjonen blir at grunnkravet i personopplysningsloven § 11 første ledd bokstav d ikke er oppfylt.

5.4 Bruk av fødselsnummer

5.4.1 Personopplysningslovens krav

I henhold til personopplysningsloven § 12 kan fødselsnummer og andre entydige identifikasjonsmidler bare nyttes i behandlingen når det er saklig behov for sikker identifisering og metoden er nødvendig for å oppnå slik identifisering.

5.4.2 Faktagrunnlag

Omlag halvparten av Ruters 24000 brukere av elektroniske billetter er skoleelever, som har fått utstedt et særskilt *skolekort*. Disse skolekortene er distribuert til elever ved videregående skoler i Akershus, som oppfyller vilkårene for å motta kortet. Ifølge den databehandleravtalen som Ruter har inngått med Safir Data, benyttes et sett med personopplysninger for å avgjøre om den enkelte eleven har rett til skoleskyss, og til produksjonen av selve kortene. De aktuelle opplysninger om elevene som innhentes og registreres i denne sammenheng er:

- fødselsnummer
- navn
- gateadresse, postnummer og poststed
- inntaksskole
- telefonnummer

5.4.3 Datatilsynets vurdering

For at en behandling av fødselsnummer skal være lovmessig, må begge vilkårene i personopplysningsloven § 12 være oppfylt samtidig:

- For det første må det foreligge et *saklig behov* for sikker identifisering
- For det andre må det være *nødvendig* å benytte fødselsnummer for å oppnå en slik sikker identifisering

Datatilsynet er ikke kjent med bakgrunnen for at Ruter benytter elevenes fødselsnummer i denne sammenheng, og det blir dermed vanskelig å si om det foreligger et saklig behov for slik identifisering som nevnt. Datatilsynet ser imidlertid ikke bort fra at saklighetskriteriet kan være oppfylt i denne saken, da terskelen for oppfyllelse av kravet, på generelt grunnlag, ikke nødvendigvis er spesielt høy. I praksis er det da også det foran nevnte nødvendighetskriteriet som utgjør hindringen for bruk av fødselsnummer. I dette vilkåret ligger det altså et krav om at andre alternative parametere for personidentifikasjon ikke kan anses tilstrekkelige for å oppnå entydig identifisering. Dersom faren for at to eller flere individer forveksles med hverandre kan elimineres ved hjelp av navn, fødselsdato og folkeregistrert adresse, vil det normalt ikke anses som nødvendig å bruke fødselsnummer.

Datatilsynet kan ikke se at nødvendighetskriteriet i personopplysningsloven § 12 er oppfylt, og konkluderer således med at Ruters bruk av fødselsnummer utgjør et brudd på nevnte lovbestemmelse.

5.5 Krav om informasjonssikkerhet – forholdsmessig sikring av personopplysninger

5.5.1 Personopplysningslovens krav

I henhold til personopplysningsloven § 13 skal den behandlingsansvarlige gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

5.5.2 Faktagrunnlag

Blant de omlag 24000 brukerne av Ruters elektroniske billettløsninger, var det på kontrolltidspunktet kun et fåtall som hadde opprettet personlig profil på MinRuter. For å etablere en profil eller brukerkonto på dette nettstedet, må kunden oppgi kundenummer, Flexus-kortnummer, e-postadresse og egenvalgt passord.

5.5.3 Datatilsynets vurdering

Først når passordet er satt, vil profilen være utstyrt med et passord som i det minste gir en viss grad av beskyttelse. Dette betyr at de som ikke aktiverer ”MinRuter” har en ubeskyttet profil ute på Internett som inneholder personopplysninger. Kun kjennskap til ubeskyttet informasjon er tilstrekkelig for å ”skaffe seg kontroll over” en kundes profil.

Dersom kunden glemmer passordet sitt, kan han eller hun få tilsendt et nytt passord ved å oppgi sin registrerte e-postadresse. Denne e-postadressen vil – etter det tilsynet har forstått – alltid være identisk med kundens brukernavn. E-posten som kunden mottar inneholder dermed alle de opplysninger som er nødvendige for å få tilgang til kundens reisekonto. Passordet sendes ubeskyttet.

Datatilsynet anser at det strider mot personopplysningsloven § 13 og personopplysningsforskriftens § 2-11 å gjøre tilgjengelig og sende personopplysninger hvor konfidensialitet er nødvendig, ubeskyttet på Internett.

5.6 Krav om informasjonssikkerhet – tilgangskontroll

5.6.1 Personopplysningslovens krav

I henhold til personopplysningsloven § 13 skal den behandlingsansvarlige gjennom planlagte og systematiske tiltak sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Ifølge personopplysningsforskriften § 2-8 skal medarbeiderne hos den behandlingsansvarlige bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk. Det fremgår videre av personopplysningsforskriften § 2-11 at det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig.

5.6.2 Faktagrunnlag

En rekke personer har tilgang til personopplysninger og valideringsdata som lagres i Ruters datasystemer. Det dreier seg om kundebehandlere ved kundesentre og bussterminaler, systemutviklere, med flere. Databehandlere som for eksempel Trafikanten har også tilgang til slike data.

5.6.3 Datatilsynets vurdering

Datatilsynet anser at beskyttelsen av kundenes personopplysninger ikke oppfyller kravene i personopplysningsloven § 13 og personopplysningsforskriften § 2-11. Datatilsynet anser at det ikke er nødvendig at ansatte, for eksempel kundeservice, skal ha tilgang til historiske valideringsdata på kunden. Faren for urettmessig overvåkning av kunder og deres reisemønster er til stede.

5.7 Krav om databehandleravtale

5.7.1 Personopplysningslovens krav

I henhold til personopplysningsloven § 15 kan en databehandler ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke uten slik avtale overlates til noen andre for lagring eller bearbeidelse. I avtalen med den behandlingsansvarlige skal det også gå frem at databehandleren plikter å gjennomføre slike sikringstiltak som følger av personopplysningsloven § 13.

Begrepet *databehandler* er i personopplysningsloven § 2 nr. 5 definert som ”den som behandler personopplysninger på vegne av den behandlingsansvarlige”.

5.7.2 Faktagrunnlag

Datatilsynet ba under kontrollen om informasjon om de databehandlere som Ruter benytter i forbindelse med elektronisk billettering. Følgende ble opplistet:

- Trafikanten
- Safir Data
- Kollektivtransportproduksjon (KTP)
- PayEx
- NSB
- PL4
- IOS (Felles løsning)
- ERG

Nedenfor følger Datatilsynets gjengivelse av dets forståelse av de ovennevnte selskaperes roller i forbindelse med de behandlinger av personopplysninger som finner sted. I tillegg omtales enkelte av de datasystemer som er i bruk.

Trafikanten har tilgang til kundeopplysninger lagret hos PayEx og valideringsdata lagret i PL4 (IOS).

Safir Data håndterer de elektroniske billettene som benyttes av videregående skoler i Akershus. Dette omfatter kundeopplysninger om omtrent 12000 elever. Safir Data AS skal avgjøre om den enkelte eleven har rett til skolekyss ut fra geografiske kriterier. I tillegg besørger selskapet produksjonen av Flexus skolebilletter. Lagrede data gir også grunnlag for uttak av statistikk og ligger til grunn for utarbeidelse av økonomiske oppgjør. Safir Data

håndterer elevopplysninger (fødselsnummer, navn, adresse, postnummer, poststed, inntaksskole og telefonnummer).

I **KTPs** database *Thales* innsamles og lagres de valideringsdata som genereres via valideringsautomatene i det enkelte transportmiddel. Opplysningene lagres i systemet i to måneder.

PayEx utfører faktureringsoppdrag på vegne av Ruter. Det er følgelig nærliggende å anta at PayEx' databaser inneholder en rekke opplysninger om Ruters kunder. Disse opplysningene oppbevares og lagres i PayEx' systemer inntil kunden eventuelt ber om at de slettes. Ruter opplyste for øvrig under kontrollen at NSB ikke har tilgang til Ruters kunder i PayEx' database.

NSB – Lagrer reisedata for de av Ruters kunder som validerer på NSBs utstyr, se egen kommentar nedenfor.

PL4 – Felles kortholderdatabase. Foretar konsolidering og langtidslagring av transaksjonsopplysninger og kundedata. Støtte for felles kundehåndtering, felles funksjoner for rekonstruksjon, private aksjonslister og datafangst for statistikkformål. Alle opplysninger lagres i er to og et halvt år.

IOS – Interoperabelt system. Transaksjoner sendes via IOS til korteier og produkteiers system. Foretar transaksjonsinnsamling og distribusjon og avregning. Håndterer avregning, oppgjør, validering, informasjonsutveksling og registrar-støtte. Det fremsto som uklart hvor lenge opplysningene blir lagret i denne databasen.

ERG – Lagrer data om alle valideringer som gjøres på Ruters valideringsutstyr. Opplysningene lagres i to og et halvt år.

Under kontrollen etterspurte Datatilsynet kopier av de avtaler som Ruter har inngått med sine databehandlere, det vil si de aktuelle *databehandleravtaler*. Ruter ga uttrykk for at disse ville kunne ettersendes den 11. mai. Ved utløpet av 11. mai hadde Datatilsynet imidlertid bare mottatt en kopi av databehandleravtalen mellom Ruter og Safir Data AS. Denne databehandleravtalen er generelt utformet. Databehandleravtalen inneholder dermed ikke spesifikk informasjon om hvordan Safir Data skal håndtere personopplysninger. Avtalen lister kun opp de samme krav som fremkommer i personopplysningsloven og personopplysningsforskriften.

Slik Datatilsynet ser det, forelå det på kontrolltidspunktet flere databehandlerrelasjoner, uten at de nødvendige avtaler var inngått. Imidlertid er det ettersendt flere databehandleravtaler ved Ruters e-post av 20. mai 2009. Dette gjelder for følgende relasjoner:

- Trafikanten - Ruter
- KTP - Ruter
- OKB - Ruter

I tillegg er det oversendt ulike avtaler mellom Ruter på den ene siden, og henholdsvis PayEx, eSolutions Group (ESG) og NSB på den andre, men Datatilsynet kan ikke se at det dreier seg om *databehandleravtaler* i disse tilfellene.

Når det gjelder forholdet mellom NSB og Ruter, har Ruter gitt uttrykk for at det er i tvil om det her foreligger en databehandlerrelasjon, eller hvorvidt det dreier seg om en situasjon hvor personopplysninger utleveres fra en behandlingsansvarlig til en annen. I sistnevnte tilfelle vil i så fall personopplysningslovens grunnkrav måtte være oppfylt, i likhet med de øvrige pliktbestemmelsene i lovens kapittel II og III, med unntak av § 15.

5.7.3 Datatilsynets vurdering

Datatilsynet har funnet det lite hensiktsmessig å varsle om at det vil bli fattet vedtak om at databehandleravtaler må utarbeides i de relasjoner som eksisterer mellom Ruter og de selskaper som er angitt over, til tross for at enkelte avtaler ikke kunne fremskaffes på kontrolltidspunktet. Hovedårsaken til dette er at de aktuelle databehandleravtaler er ettersendt.

Tilsynet anser det likevel som kritikkverdig at et bredt spekter av personopplysninger om så vidt beskyttelsesverdige forhold som enkeltindividers reisemønstre, er overlatt til eksterne aktører uten den nødvendige avtaleregulering, som skal beskytte de registrertes interesser, jf. personopplysningsloven § 15.

Når det gjelder de personopplysningsrettslige spørsmål som oppstår om forholdet mellom Ruter og NSB, anser Datatilsynet at det vil gå utover rammene for denne tilsynsrapporten å drøfte disse. Det vil være nødvendig med en ytterligere klargjøring av personopplysningsflyten mellom de nevnte aktører, før det kan trekkes konklusjoner i den ene eller den andre retning. Tilsynet stiller seg til disposisjon for et fremtidig avklaringsmøte i den henseende.

Datatilsynet ønsker å henvise til at det er utarbeidet en veileder som er myntet på virksomheter som skal utarbeide og inngå slike avtaler med en eller flere databehandlere. Veilederen, med tilhørende eksempler på slike avtaler, er å finne på www.datatilsynet.no.

I ett tilfelle har Datatilsynet lagt til grunn at det foreligger en databehandlerrelasjon, uten at noen tilsvarende avtale er oversendt. Det dreier seg om forholdet Ruter – PayEx. Tilsynet konkluderer av samme årsak med at det her foreligger et brudd på lovens § 15.

5.8 Sletting av personopplysninger

I henhold til personopplysningsloven § 28 skal den behandlingsansvarlige ikke lagre personopplysninger lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Hvis ikke personopplysningene deretter skal oppbevares i henhold til annen lovgivning, skal de slettes.

Av personopplysningsloven § 27 følger det at den behandlingsansvarlige skal ”rette” personopplysninger ”som det ikke er anledning til å behandle”. Det er på det rene at retting kan skje ved at opplysningene slettes, jf. forutsetningen i § 27 tredje ledd.

5.8.1 Sletting av personopplysninger generert ved bruk av periodekort

I avsnittene nedenfor skal det sondres mellom:

- Behandling av reiseopplysninger som er generert ved initierende validering
- Behandling av reiseopplysninger generert ved de etterfølgende valideringer innenfor billettens gyldighetsperiode

5.8.2 Opplysninger generert ved initierende validering

5.8.2.1 Faktagrunnlag

Et periodekort aktiviseres ved første validering, det vil normalt si idet ihendehaveren av kortet stiger på transportmiddelet, og holder kortet opp for elektronisk avlesning. Ved den første valideringen begynner billettens gyldighetsperiode å løpe. Lengden på denne perioden kan i prinsippet tenkes å være varierende, men på kontrolltidspunktet besto Ruters billetttilbud utelukkende av billetter med en sammenhengende gyldighetsperiode på tretti dager. Billetten vil med andre ord ikke lenger være gyldig når tretti dager har gått siden den *initierende* validering fant sted.⁵

Valideringstidspunktet registreres og lagres sentralt, sammen med de øvrige opplysninger som er angitt i rapportens punkt 5.1.1.2. Det fremstår imidlertid som uklart hvor lenge disse opplysningene lagres i Ruters sentralsystem; Ruter har for eksempel ingen skriftlige rutiner for sletting av disse personopplysningene, etter det Datatilsynet kjenner til, jf. personopplysningsloven § 14. Det er dermed nærliggende å legge til grunn at disse opplysningene heller ikke er gjort til gjenstand for slik sletting på noen regelmessig eller systematisk basis.

5.8.2.2 Datatilsynets vurdering

Datatilsynet bestrider ikke at Ruter har anledning til å behandle opplysninger om denne valideringen, jf. personopplysningsloven § 11 første ledd bokstav a, jf. § 8. Det følger av sakens omstendigheter at innsamling, registrering og lagring av opplysninger om denne handlingen, på et eller annet vis, vil være nødvendige behandlinger for å beregne reisekortets gyldighetsperiode. De sentrale spørsmålene er hvor lenge det er nødvendig å lagre denne opplysningen, for å oppnå det nevnte formålet.

Slik Datatilsynet ser det, må svaret på dette spørsmålet være nært forbundet nettopp med reisekortets gyldighetsperiode. Dersom beregning av gyldighetsperioden er det eneste legitime formålet som kan berettige lagring av reiseopplysningene, taler det for at opplysningene ikke bør lagres utover denne 30-dagersperioden.

Imidlertid kan den enkelte kunde ha et behov for å kontrollere at de relevante økonomiske transaksjoner har gått rett for seg. Den enkelte reisende kan tenkes å komme i en situasjon hvor det oppstår et behov for å etterkontrollere det første valideringstidspunktet, for eksempel

⁵ Den reisende kan selvsagt kjøpe en *ny* billett av samme type, hvis gyldighetsperiode utløses ved neste validering.

fordi gyldighetsperioden på billetten, mot den reisendes formodning, viser seg å være utløpt. For at kunden skal ha en mulighet til å områ seg, og komme med innsigelser overfor selskapet, har Datatilsynet kommet til at opplysningene omkring den første valideringen må kunne oppbevares en tid utover billettens gyldighetsperiode, som på kontrolltidspunktet var på 30 dager. Det samme hensynet kan for øvrig anføres på vegne av Ruter – selskapet må gis en reell mulighet til å imøtekomme kundenes eventuelle påstander om feilaktig valideringstidspunkt.

På bakgrunn av det ovennevnte, anser Datatilsynet at opplysninger om den initierende valideringen kan lagres i 30 dager etter billettens utløpstidspunkt er passert, og at opplysningene må slettes etter dette tidspunktet.

5.8.3 Opplysninger generert ved etterfølgende validering

5.8.3.1 Faktagrunnlag

Etter at den initierende validering av periodebillett er utført, oppfordres kunden til å validere billetten hver gang han eller hun stiger på et nytt transportmiddel. Disse valideringene, og den registrering og lagring av transaksjonsdata som følger, er her kalt ”etterfølgende validering(er)”.

Datatilsynet har for øvrig mottatt tips fra publikum om at enkelte reisende – til tross for at disse er i besittelse av gyldige reisekort/e-billetter – nektes adgang til det aktuelle transportmiddelet, med mindre vedkommende validerer ved påstigning.

Ruter har gitt uttrykk for at de etterfølgende valideringer av periodekort er begrunnet i følgende forhold:

- Det er nødvendig å validere for å få bekreftelse på at kunden har gyldig billett
- Ruter ønsker å tilegne seg statistiske opplysninger om bruk av transportmidlene

Det er de samme reiseopplysninger som genereres, registreres og lagres, både i forbindelse med den første valideringen av et periodekort og de etterfølgende valideringer, se listen i rapportens punkt 5.1.1.2.

5.8.3.2 Datatilsynets vurdering

Datatilsynet kan, som nevnt over, ikke se at det er nødvendig å formidle opplysninger om den reisendes identitet til sentralsystemet for å oppfylle noen av de anførte formålene. En bekreftelse av at den reisende er i besittelse av gyldig billett kan angis gjennom kommunikasjon mellom valideringsutstyret i transportmiddelet og reisekortet, som inneholder informasjon om utløpstidspunktet for billettens gyldighet. Datatilsynet anser altså at det mangler rettslig anledning til å samle inn og registrere personopplysninger i forbindelse med de etterfølgende valideringer – se over i rapportens punkt 5.3.

Spørsmålet om hvor lenge opplysningene om de etterfølgende valideringer kan oppbevares, blir dermed subsidiært, og tas følgelig ikke opp til vurdering.

I stedet er Datatilsynet av den oppfatning – ettersom det ikke er rettslig adgang til å behandle disse opplysningene i utgangspunktet – at Ruter dermed har en plikt til å slette de opplysningene som er registrert og lagret, jf. personopplysningsloven § 27 første ledd, jf. også § 28.