Datatilsynet

Altinn Sentralforvaltning
v/fung. Avdelingsdirektør H. Andersson
8900 BRØNNØYSUND

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
200800660-6	08/00291-10 /FUE	14. november 2008

Kontroll hos Altinn sentralforvaltning og Altinn-portalen 14052008 - Brønnøysundregistrene - Vedtak

Den 14. mai 2008 gjennomførte Datatilsynet kontroll hos Altinn Sentralforvaltning og Altinn-portalen, med hjemmel i lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven) § 42 tredje ledd nr. 3.

Vurdering av virksomhetens tilsvar
Datatilsynet viser til tilsvar fra virksomheten av 5. september 2008. Tilsynet har vurdert og knyttet kommentarer til virksomhetens anførsler. Innledningsvis presiseres at en tilsynsrapport skal gi en beskrivelse av situasjonen på kontrolltidspunktet. Det innebærer at eventuelle endringer i ettertid ikke vil påvirke rapportens innhold, men kan likevel påvirke hvilke vedtak tilsynsmyndigheten fatter. Datatilsynet noterer seg planer for fremtidig utvikling av ny Altinn-løsning, men finner det ikke riktig å drøfte forholdene i foreliggende sak. Datatilsynet er imidlertid godt tilfreds med at Altinn Sentralforvaltning ønsker å ha en aktiv dialog med tilsynet for den nye løsningen, Altinn II.

Ad. Punkt 1
Datatilsynet noterer seg at virksomheten har lagt til rette for gjennomgang av behandlingsansvar. Formuleringene tolkes dit hen at avviket ikke er lukket, men at det skisseres planer for hvordan det kan gjøres. Tilsynet opprettholder med det konstatert avvik og fatter vedtak i samsvar med varsel.

Ad. Punkt 2
Datatilsynet merker seg virksomhetens synspunkter vedrørende de såkalte latente kontoer. Altinn oppgir å ha fått tilgang til opplysninger som Skattedirektoratet forvalter i folkeregisteret i medhold av folkeregisterforskriften § 9-3 nr 1, jf. lov om folkeregistrering § 14. Etter hva Datatilsynet forstår, gir dette tilgang til å *hente ut* opplysninger fra folkeregisteret basert på en avtale inngått mellom partene for utveksling og kontinuerlig oppdatering av nevnte opplysninger.

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

Etter tilsynet vurdering gir imidlertid ovennevnte hjemmel ikke anledning til å opprette latente konto. Datatilsynet anfører med det at det foreligger tilstrekklig hjemmel for utlevering av relevant informasjon, men at bruk av informasjonen til å opprette omtalte elektroniske konto krever et behandlingsgrunnlag.

Datatilsynet oppfatter at det er frivillig å benytte Altinn sine tjenester. Av det følger, etter tilsynets vurdering, at borgeren bør innrømmes rett til å kunne velge samhandlingsform. I og med at det etter tilsynets vurdering finnes alternativer, kan Datatilsynet vanskelig se at Altinn Sentralforvaltning kan påberope seg allmenn interesse som behandlingsgrunnlag for sin tjeneste, jf. personopplysningslovens § 8, litra d.

Tilsynet har falt ned på den oppfatning at Altinn Sentralforvaltning må basere seg på samtykke fra brukerne for opprettelse av kontoer i portalen. Dersom frivilligheten skal tilsidesettes, må det foreligge et gyldig lovgrunnlag som tilsier at det kan opprettes latente kontoer på borgeren. I svaret fra Skattedirektoratet, påvises det at ligningsopplysninger etter ligningslov kan publiseres elektronisk. Datatilsynet mener at det uansett være nødvendig å ha et gyldig behandlingsgrunnlag, selv om ligningsloven åpner for elektronisk publisering. Skattedirektoratet kan da bare opprette elektroniske selvangivelser til personer som aktivt har samtykket til bruk av Altinn-portalen. Utsendelse av selvangivelse til latente kontoer mangler behandlingsgrunnlag og vil dermed etter tilsynets oppfatning være en ulovlig behandling av personopplysninger og i strid med personopplysningslovens § 8.

Når ovennevnte er anført, vil Datatilsynet presisere sin interesse i å bidra til i å finne gode alternativer til usikret utsendelse av papirbaserte selvangivelser i mottakers postkasse. Selvangivelsen innholder så betydelige mengder økonomisk informasjon til at den vil kunne betraktes som et verdipapir for kriminelle aktører. Dokumentet inneholder som kjent en samlet oversikt over fødselsnummer, inntekt, formue, finansielle forbindelser, eiendom, bankkontonumre, sikkerhetskoder m.v. Erkjennelsen underbygger behovet både for å vurdere dagens praksis med usikret utsendelse av selvangivelser, og behovet for sikring av elektroniske konto.

Det presiseres at tilsynet intensjon ikke er å avvikle bruk av Altinn-portalen, men få på plass tilstrekkelig behandlingsgrunnlag for de personopplysninger som er nødvendig for å benytte tjenestene som tilbys. Dersom aktørene faller ned på at hovedprinsippet i personvernet skal fravikes, nemlig frivillighet gjennom borgerens samtykke, må dette forelegges lovgiver. Datatilsynet er klar over at utformingen av et lovgrunnlag vil ta noe tid.

Datatilsynet vil derfor fatte vedtak om i tråd med tidligere varsel om vedtak.

Ad. Punkt 3
Datatilsynet noterer seg virksomhetens synspunkter vedrørende bruk av fødselsnummer ved pålogging til nettjenester. Datatilsynet tar videre til etterretning at Buypass ikke benytter seg av fødselsnummer i sin autentiseringsløsning. Endelig kontrollrapport under punkt 5.1.2.1 er korrigert i tråd med dette.

Datatilsynet anser fødselsnummer som en beskyttelsesverdig opplysning, det er imidlertid ikke begrunnet ut fra at identifikatoren skal ha noen verdi i forbindelse med autentisering. Tilsynets vurdering bygger primært på det faktum at fødselsnummer er en statsautorisert, varig og entydig identifikator. Slike unike identifikatorer har vist seg attraktive blant kriminelle som samler inn personopplysninger med det formål å foreta identitetstyveri. Datatilsynet er kjent med at skattemyndighetene har et annet syn på foreliggende trussel. Skattedirektoratet har blant annet publisert formelen for oppbygning av fødselsnummer på sine hjemmesider. Fødselsnummer er heller ikke underlagt taushetsplikt. Datatilsynet vil dog trekke frem personopplysningsforeskriftens § 9-2 som omhandler postforsendelse inneholdende fødselsnummer. Bestemmelsen gir prinsipielle føringer i retning av et foreliggende behov for å beskytte slike data. Av samme bestemmelse følger, etter Datatilsynets vurdering, et behov for å beskytte tilsvarende informasjon ved elektronisk samhandling.

Likevel, gitt den foreliggende realitet: Fødselsnummer er ikke en særlig beskyttet opplysning. Flere tidligere hendelser har medført at uvedkommende sannsynligvis sitter på større mengder fødselsnummer, koblet til navn, adresse og andre karakteristika. Blant annet bidro masseinnhøstningen i 2007, hvor blant annet portalen www.altinn.no skal ha vært kompromittert, til foreliggende status. Uvedkommende kan med det i praksis benytte seg av andres fødselsnummer på Internett. Altinn vet følgelig ikke hvem det kommuniserer med, med mindre det foreligger en adekvat autentisering.

Etter Datatilsynets vurdering er foreliggende løsning for autentisering en svak form for autentisering. Tilsynet er langt fra overbevist at dette gir tilfredstillende autentisering av bruker, i forhold til informasjonen som skal beskyttes.

Det at Skattedirektoratet gir tilgang til folkeregisteropplysninger medfører ikke automatisk at kravene i personopplysningslovens § 12 er oppfylt for enhver bruk av fødselsnummer. Datatilsynet erkjenner at portalen må kunne skille på hvem de samhandler med for å skille de konkrete innsende skjema fra hverandre. Tilsynet er imidlertid av den oppfatning at dette kan gjøres senere, internt i informasjonssystemet, om nødvendig basert på fødselsnummer. Bruk av fødselsnummer i en innloggingsprosess anses etter tilsynets oppfatning som uheldig og sterkt uønsket. Datatilsynet ser imidlertid at tidligere forvaltningspraksis svekker tilsynets muligheter til å fatte det varslede vedtaket. Datatilsynet velger derfor å frafalle vedtaket, men vil gi en sterk tilrådning om å endre praksisen. Tilsynet vil også orientere om at det er tatt konkrete initiativ for å skjerpe regelverket på dette området. Hva utfallet av en slik prosess blir er det for tidlig å fastslå.

Datatilsynet vil derfor ikke fatte vedtak om i tråd med tidligere varsel om vedtak.

Ad. Punk 4
I tilsvaret kommenterer virksomheten logging av brukers fødselsnummer og tilhørende benyttet IP-adresse. Virksomheten kommenterer det slik:

"*Vi ønsker å presisere at det kun er den offentlige IP-adressen, som viser hvilket domene brukeren tilhører, som blir logget. IP-adressen som identifiserer den spesifikke brukeren innenfor et domene fremkommer ikke for Altinn*"

Datatilsynet ønsker i denne sammenheng å påpeke at denne offentlige adressen i mange tilfeller faktisk forteller hvem som har besøkt deres nettsider. Rundt 40% av norske husholdninger oppgis av Statistisk Sentralbyrå å bestå av en person. For disse vil en slik adresse direkte kunne knyttes relativt entydig til en enkelt person. For IP-adresser som er tilknyttet en organisasjon, er entydigheten vesentlig lavere. De aller fleste IP-adresser er faktisk tilknyttet, eller nært knyttet til enkeltindivider men koblingen vil ikke være tilgjengelig for enhver. En IP-adresse er dermed sett på som en indirekte identifiserbar personopplysning. Slike indirekte identifiserbare personopplysninger omfattes av personopplysningsloven jf. personopplysningslovens § 2 nr. 1, og behandlingen trenger et gyldig behandlingsgrunnlag.

Videre hevder virksomheten at ordningen med logging av fødselsnummer og IP-adresse hindrer uautorisert bruk av Altinn. Tilsynet har vanskelig for å se hvilken preventiv effekt et slikt tiltak vil ha. I beste fall vil loggene kunne anvendes til oppklaring av sikkerhetsbrudd, men neppe håndtering av et pågående sikkerhetsbrudd. Datatilsynet mener videre at praksisen er nok et eksempel på misbruk av fødselsnummer.

På bakgrunn av det ovennevnte anser Datatilsynet at denne type logging ikke oppfyller personopplysningslovens grunnkrav til behandling av personopplysninger, jf. personopplysningslovens § 11. Datatilsynet vil i tillegg peke på at en eventuell sammenstilling av IP-adresse og fødselsnummer krever et eget behandlingsgrunnlag

Det vil bli fattet vedtak om at logging som nevnt må opphøre da det ikke foreligger gyldig behandlingsgrunnlag og kravene til saklig grunnlag ikke anses oppfylt.

Ad. Punkt 5
Datatilsynet viser til virksomhetens tilbakemelding vedrørende logger. Datatilsynet anser virksomhetens tilbakemelding bekreftelse på lukking av avvik. Varslet vedtak frafalles.

Ad. Punkt 6
Altinn Sentralforvaltning opplyser at samtykke er behandlingsgrunnlag for arbeidsarkivet. Datatilsynet vil i denne sammenheng peke på kravene til et gyldig samtykke som fremgår i personopplysningslovens § 2 nr. 7. Dersom samtykke skal være gyldig må det være frivillig, utrykkelig og informert. Dette kan løses ved at man innfører en løsning hvor den registrerte haker av for at samtykke gis.

Datatilsynet gjør oppmerksom på at et samtykke kan trekkes tilbake på ethvert tidspunkt. Det må derfor foreligge løsninger som ivaretar dette, for eksempel et sted der den registrerte kan

hake av for at samtykket nå trekkes tilbake. Det må i tilknytning til dette opprettes løsninger for sletting av arbeidsarkivet dersom samtykket trekkes tilbake.

Datatilsynet kan ikke se at disse vilkårene er ivaretatt i dagens løsning, og anser derfor at samtykke ikke kan anføres som behandlingsgrunnlag på det nåværende tidspunkt.

Datatilsynet fatter derfor vedtak som varslet. Datatilsynet legger imidlertid til grunn at en løsning som bygger på et reelt frivillig samtykke vil kunne opprettes gjennom den nye AltinnII løsningen..

Ad. Punkt 7.
Datatilsynet viser til virksomhetens tilsvar vedrørende servicearkivet. Tilsynet tar tilbakemeldingen på dette punkt til etterretning. Slik servicearkivet er organisert, innebærer det en akkumulering av enorme mengder informasjon. Forholdet synes bare å ville tilta over tid, både i forhold til akkumulert mengde og utvidelse av omfang. Stadig flere tjenesteeiere vil ifølge virksomheten bruke servicearkivet som en form for elektronisk arkiv. Det tegnes et bilde der Altinn Sentralforvaltning blir en databehandler for et stort antall offentlige aktører. Praksisen som har vært ført så langt, hvor mangel på segmentering av informasjon til de ulike behandlingsansvarlige er avdekket, gir dårlige rammevilkår for forsvarlig håndtering av informasjonen dersom utviklingen blir som beskrevet. Datatilsynet fatter på denne bakgrunn vedtak i tråd med tidligere varsel.

Ad. Punkt 8.
Det vises til kommentarer vedrørende internkontroll. Datatilsynet tar tilbakemeldingen på dette punkt til etterretning. Vedtak fattes i tråd med tidligere varsel.

Ad. Punkt 9.
Datatilsynet er inneforstått med at det er vanskelig å innføre segmentering i dagens løsning, noe tilsynet også kommenterte i kontrollrapporten. Vedtak fattes i tråd med tidligere varsel, men frist for vedtaket knyttes opp mot innføringen av den nye Altinn II løsningen.

Vedtak
Datatilsynet fatter med hjemmel i personopplysningslovens § 46 følgende vedtak:

1. Altinn Sentralforvaltning må foreta en gjennomgang av hvilke behandlinger som skjer i virksomheten og avklare behandlingsansvaret i forhold til disse, jf personopplysningslovens § 8. Se rapportens 5.1.1. ***Frist for gjennomføring av vedtaket er 31.12.2008.***
2. Altinn Sentralforvaltning må fremskaffe lovlig grunnlag for opprettelse av latente konto for alle landets innbyggere jf. personopplysningslovens § 8 jf. § 11. Se rapportens pkt. 5.1.2.1. ***Frist for gjennomføring av vedtaket er 01.06.2009.***
3. Altinn Sentralforvaltning må avslutte logging av fødselsnummer og tilhørende IP-adresse. Se rapportens pkt. 5.1.2.2. ***Frist for gjennomføring av vedtaket er 31.12.2008.***

4. Altinn sentralforvaltning må godtgjøre at det foreligger et gyldig behandlingsgrunnlag iht. personopplysningslovens § 8 jf. § 11, for lagringen i arbeidsarkivet. ***Frist for gjennomføring av vedtaket er 31.12.2009***.
5. Altinn Sentralforvaltning må slette informasjonen i det såkalte "servicearkivet" med mindre det kan dokumenteres lovlig grunnlag for arkivet jf. personopplysningslovens §§ 8, 11. I sistnevnte tilfelle må "servicearkivet" uansett sikres og segmenteres på en tilfredsstillende måte jf. personopplysningslovens §§ 13 og 15. Se rapportens 5.1.2. ***Frist for gjennomføring av vedtaket er 31.12.2009.***
6. Altinn Sentralforvaltning må utarbeide et system som ivaretar kravene i personopplysningslovens § 14 for egen behandling, samt gjøre seg kjent med relevante rutiner som er stadfestet av behandlingsansvarlig for databehandler, jf § 15. Se rapportens 5.1.3. ***Frist for gjennomføring av vedtaket er 31.12.2008.***
7. Altinn Sentralforvaltning må implementere en tilfredstillende logisk eller fysisk segmentering av informasjonssystemet slik at krav til tilfredstillende informasjonssikkerhet og ulike behov mht. sletting mellom ulike behandlingsansvarlige, kan ivaretas, jf. personopplysningslovens §§ 13 og 15. Se rapportens 5.2.1. ***Frist for gjennomføring av vedtaket er 31.12.2009.***

Det skal dokumenteres at justerte løsninger er tilfredstillende gjennom en risikovurdering, jf. personopplysningsforskriftens § 2-4. Risikovurderingen skal oversendes Datatilsynet som dokumentasjon på lukking av avvik.

Klageadgang
Det gjøres oppmerksom på at vedtak fattet av et forvaltningsorgan kan påklages. En eventuell klage rettes til det organ som har fattet vedtaket. I den grad forvaltningsorganet opprettholder vedtaket oversendes saken til klageinstans. For vedtak fattet med hjemmel i personopplysningsloven er klageorganet Personvernnemnda.

Med hilsen

Leif T. Aanensen
avdelingsdirektør

Frank U. Eriksen
overingeniør

Vedlegg: Endelig kontrollrapport
Kopi: Skattedirektoratet

Datatilsynet

Endelig kontrollrapport		
Saksnummer: 08/00291 Dato for kontroll: 14.05.2008 og 15.05.2008 Rapportdato: 14.11.2008	Kontrollobjekt: Altinn Sentralforvaltning Sted: Brønnøysund	Utarbeidet av: Christine Lie Ulrichsen Astrid Flesland Frank Ulfsby Eriksen

1 Innledning

Datatilsynet viser til kontroll av Skattedirektoratet og Altinn Sentralforvaltning 14. og 15. mai 2008. Kontrollen ble utført i lokalene til Altinn Sentralforvaltning, med begge etater tilstede. Kontrollen begrenset seg til skjemaer for innrapportering for Skattedirektoratet samt informasjonssystemet og sikkerhetsløsningen til Altinn Sentralforvaltning.

Sikkerhet er vurdert i lys av og avgrenset til Skattedirektoratet bruk. Det vil si for behandling der personopplysningene kun unntaksvis vil være sensitive. Et eventuelt utbud av tilsvarende konsept til andre statlige eller kommunale aktører som formidler sensitive personopplysninger, vil fordre en vesentlig heving av den konseptuelle og reelle sikkerhet i løsningen. Datatilsynet gjør spesielt oppmerksom på at både behandlingsansvarlig og databehandler pekes ut som pliktsubjekter i forhold til personopplysningslovens § 13 om informasjonssikkerhet.
Kontrollen skjedde med hjemmel i lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven) § 42 tredje ledd nr. 3.

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

Datatilsynet har laget en separat rapport for Skattedirektoratet ettersom det er viktig å skille merknadene, med bakgrunn i databehandler og behandlingsansvarlige sine plikter. Kopi av rapportene vil forlegges alle parter.

1.1 Oppsummering av sentrale forhold i tilsynets anførsler

Datatilsynet har en rekke vesentlige anførsler til måten www.altinn.no er organisert. Tilsynet er spesielt kritisk til at:

- løsningen i praksis fungere som et sentralarkiv som lagrer kopi av all kommunikasjon mellom borger og ulike behandlingsansvarlig,
- det opprettes en latent konto på enhver innbygger, med tilhørende personopplysninger, uten at vedkommende har bedt om dette,
- det benyttes fødselsnummer som et ledd i innloggingsprosedyren, og
- personopplysninger tilhørende ulike behandlingsansvarlige, med ulike behov til sikring, lagres i en samlet database uten segmentering.

2 Tilstede under kontrollen

2.1 Fra Altinn Sentralforvaltning:

- Ann-Christine Nybacka – avd.dir AEI
- Henning Andersen – seksjonssjef AEI
- Håkon Olderbakk, avd.dir Plan og Utvikling
- Harald Thomassen, seniorrådgiver
- Olav Melteig, sikkerhetsansvarlig
- Roger Skoglund, Dataess, innleid konsulent
- Roy Horn, superbruker

2.2 Fra Skattedirektoratet

- Svein Mobakken, sikkerhetssjef
- Lars Nilsen, avd.dir Rettsavdelingen
- Erling Solberg, systemjurist
- Jan Erik Norheim, tjenestedir I/J

2.3 Fra Datatilsynet:

- Christine Lie Ulrichsen, seniorrådgiver
- Astrid Flesland, seniorrådgiver
- Frank U Eriksen, overingeniør

3 Generelt

Datatilsynet gjennomførte våren 2008 kontroller mot offentlige virksomheter hvor temaet er behandling av personopplysninger ved elektronisk kommunikasjon og saksbehandling (e-forvaltning). Formålet med kontrollene var å sikre at brukernes personvern blir ivaretatt på en adekvat måte. Altinn Sentralforvaltning administrerer og drifter portalløsningen www.altinn.no hvor det kan leveres og rapporteres til statlige organer, herunder eksempelvis selvangivelsen til Skatteetaten.

For mer informasjon om formålet med kontrollen, vises det til varsel om kontroll av 18. februar 2008. Datatilsynet noterte seg at Altinn Sentralforvaltning anser seg som databehandler for alle personopplysninger som behandles i den omtalte løsningen, med unntak av personopplysninger som benyttes for sikkerhetsformål. I forhold til sistnevnte anser Altinn Sentralforvaltning seg som behandlingsansvarlig.

Kontrollen ble det avgrenset til følgende tjenester/skjemaer:

- Selvangivelse for lønnstakere og pensjonister
- Opplysninger om arbeidstakere
- Lønns- og trekkoppgave
- Innrapportering fra veldedige organisasjoner

4 Kort om bruk av personopplysninger samt formålet med behandlingene

Altinn Sentralforvaltning behandler i hovedsak personopplysninger på vegne av sine kunder (tjenestetilbyder/oppdragsgiver). Dette innebærer at virksomheten må støtte seg på en databehandleravtale for å kunne foreta en lovlig behandling av de

personopplysninger dette gjelder. Det er opprettet en felles portal der de ulike oppdragsgiveres logo fremgår ovenfor publikum. Via denne portalen kan publikum logge seg på for bruk av egen konto i Altinn. Informasjonen som brukeren legger inn, videreformidles til den aktuelle tjenesteeier (oppdragsgiver) i elektronisk form. Skjemaene er knyttet til et varierende innhold, fra selvangivelse til søknad om byggetillatelse. Ingen skjema som blir kommunisert gjennom løsningen innholdt, ifølge virksomhetene, sensitive personopplysninger på tidspunktet for kontrollen.

Før endelig utfylt skjema sendes inn til behandlingsansvarlig, etableres et foreløpig skjema som lagres i en temporær og ufullstendig utførelse. Det vil si at skjemaet blir mellomlagret i et slags "arbeidsarkiv" inntil det er sendt inn som ferdigutfylt til rette rapporteringsinstans, eksempelvis skattemyndighetene.

Alle ferdigutfylte, og innsendte skjema sendt inn via Altinn.no, lagres i tillegg i et "servicearkiv", heretter kalt arkiv, for oppslag eller nedlasting ved en senere anledning. Arkivet er basert på en database hvor opplysningene ligger sammenblandet (sekvensielt). I databasen kunne tilsynet konstatere at det finnes lagrede opplysninger tilbake til opprettelsen av arkivet. Det er ifølge Altinn Sentralforvaltning ikke foretatt slettinger i dette sentrale arkivet.

Altinn Sentralforvaltning tilbyr selve innrapporteringskonseptet foretatt gjennom et webgrensesnitt, inkludert loggfunksjoner. De forskjellige tjenesteeiere kan selv beslutte hvilket sikkerhetsnivå de ønsker for innlogging blant de nivåene/løsningene Altinn Sentralforvaltning tilbyr.

5 Funn og avvik fra lovbestemte krav til behandling av personopplysninger

Datatilsynet vil under dette avsnittet vurdere de faktiske forhold som ble avdekket under kontrollen i forhold til personopplysningslovens krav. De aktuelle punkter er inndelt i seksjoner.

5.1 Generelle krav i forhold til behandling av personopplysninger

5.1.1 Ansvarsforhold – Behandlingsansvar/databehandler

En *behandlingsansvarlig* er definert i personopplysningsloven som den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jf § 2, nr 4.

En *databehandler* er den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf lovens § 2, nr 5.

Mellom databehandler og behandlingsansvarlige skal det inngås en *databehandleravtale*, jf personopplysningslovens § 15. Denne er styrende for databehandlers rådighet over personopplysninger. Dersom en databehandler bruker personopplysninger utover det som er avtalt, er vedkommende å anse som behandlingsansvarlig for behandlingen og hjemmel for denne må finnes i personopplysningslovens § 8, evt. § 9.

Under kontrollen ble ansvarforholdet vurdert for følgende funksjoner:

1. Autentiserings og autorisasjonsfunksjonen (opprettelse av brukerkontoer)
2. Andre fellestjenester som logger og arbeidsarkiv
3. Servicearkivet

Altinn Sentralforvaltning vurderer seg som behandlingsansvarlig for autentiseringsløsningen, autorisasjonsløsningen, logger og arbeidsarkivet. Dette er fellestjenester som tilbys ovenfor alle etater som benytter Altinn.no for innrapportering.

Altinn Sentralforvaltning vurderer tjenesteeier som ansvarlig for behandling av personopplysninger i "servicearkivet", både når det gjelder meldingsinnhold og opplysninger i brukerprofil. Det er de ulike tjenesteeierne som utvikler og tilbyr tjenesten ut ifra sitt formål.

Det er inngått en databehandleravtale mellom Altinn Sentralforvaltning og Skattedirektoratet (tjenesteeier), underskrevet av begge partene den 31.04.2008. Avtalen presiserer Altinn Sentralforvaltning sitt ansvar og oppgaver i punkt 3, mens oversikt over de tjenester Skatteetaten har i Altinn.no følger som vedlegg til avtalen. Denne oppdateres ved behov.

Når det gjelder hvilke behandlinger Altinn Sentralforvaltning er ansvarlig for sier avtalen: "*Altinn Sentralforvaltning er behandlingsansvarlig for de personopplysninger som er felles for alle tjenester i Altinn, herunder utdrag fra Det sentrale folkeregisteret, fullmakter og rettigheter som er tildelt og registrert og logger over aktiviteter i systemet*".

Videre presiseres det at "*Altinn Sentralforvaltning er databehandler for personopplysninger som behandles...i Altinn systemet for de tjenester som er lagt inn i systemet av Skattedirektoratet selv eller av sluttbruker.*"

Avtaleteksten korresponderer i hovedsak med Altinn Sentralforvaltning sin egen vurdering av ansvarsforholdene. Ordlyden er imidlertid vidt formulert, og det kan være uklart hvilke funksjoner som dekkes av denne. Blant annet gjelder dette for behandling av personopplysninger i arbeidsarkivet, hvor Altinn Sentralforvaltning legger til grunn at de er behandlingsansvarlige. I praksis er dette opplysninger som er lagt inn av sluttbrukerne, og i følge avtalen er Skattedirektoratet å anse som behandlingsansvarlig for disse.

Det å kartlegge hva man er ansvarlig for, er et grunnleggende krav i personopplysningsloven, og en forutsetning for at lovens øvrige krav kan etterleves. En slik oversikt skal finnes i den styrende delen av Altinn Sentralforvaltnings dokumenterte datasikkerhet og internkontroll, jf. personopplysningslovens § 14. Det er ikke nok at eventuelle databehandleravtaler presiserer hva man *ikke* er behandlingsansvarlig for, det må foretas en positiv avgrensning hva gjelder ansvarsforholdene.

Datatilsynet mener at kartlegging av behandlinger og stadfesting av behandlingsansvar er særdeles viktig i virksomheter som dels opererer som behandlingsansvarlige og dels som databehandlere. Her er det helt nødvendig å identifisere hva man gjør for eget formål og etter eget ansvar, i henhold til egne akseptkriterier og motsatt, hvor eksterne parter legger føringene.

Altinn Sentralforvaltning hadde ikke fullt ut avklart og dokumentert sin rolle som henholdsvis databehandler eller behandlingsansvarlig i forhold til de behandlinger og prosesser som skjer i virksomheten. Dette er en klar mangel i forhold til internkontrollkravet i personopplysningslovens § 14.

Underlag for pålegg: Altinn Sentralforvaltning må foreta en gjennomgang av hvilke behandlinger som skjer i virksomheten og avklare behandlingsansvaret i forhold til disse.

De følgende vurderinger er basert på en foreløpig vurdering av at Altinn Sentralforvaltning er behandlingsansvarlig for de ovennevnte tjenestene.

5.1.2 Behandlingsgrunnlag og formål

Personopplysninger kan bare behandles når det finnes et grunnlag i personopplysningslovens § 8. Ved behandling av sensitive personopplysninger må i tillegg ett av vilkårene i § 9 være oppfylt. Videre må krav blant annet til saklighet, og relevans jf. § 11 være oppfylt.

I forhold til tema for kontrollen vurderte Datatilsynet behandlingsgrunnlaget og formålet i forhold til de tjenester/funksjoner som er listet opp under punkt 5.1.1 ovenfor. Av disse ble det avdekket at Altinn Sentralforvaltning er ansvarlig for autentiseringsløsningen, autorisasjonsløsningen, logger og arbeidsarkivet.

5.1.2.1 Autentiserings- og autorisasjonsløsningen (opprettelse av brukerkontoer)
Brukerkonto blir opprettet på bakgrunn av at en person er registrert i Folkeregisteret. Bakgrunnsinformasjonen blir innhentet elektronisk fra nevnte register. Utleveringen gjøres i henholdt til en avtale mellom Altinn Sentralforvaltning og Folkeregisteret. Opprettelsen av en konto medfører behandling av en del personopplysninger, eksempelvis fødselsnummer (11 siffer) og adresse. .

Løsningen innebærer i praksis at alle landets borgere har en konto på Altinn.no, men at disse kun ligger latent inntil borgeren aktiv tar kontoen i bruk. Dette gjøres ved hjelp av en autentiseringsprosess som vil omtales senere. Kontoen kan "fylles" med supplerende personopplysninger fra for eksempel Skatteetaten, uavhengig av om kontoen er aktivert av brukeren eller kun foreligger inaktiv (latent) i systemet.

Altinn Sentralforvaltning kunne ikke redegjøre for noe rettslig grunnlag for opprettelse av latente brukerkonto på landets innbyggere, uten den enkeltes viten eller vilje. Samtykke er ikke et alternativ tatt i betraktning at de latente kontoene opprettes uten noen forutgående kontakt med den enkeltperson kontoen er knyttet til.

Underlag for pålegg: Altinn Sentralforvaltning må dokumentere behandlingsgrunnlag som gir rett til uoppfordret å opprette latente kontoer for alle landets innbyggere.

Tjenesteeieren kan velge mellom flere sikkerhetsnivåer for pålogging som Altinn Sentralforvaltning tilbyr. Samtlige av disse løsningene, unntatt Buypass, bygger på fødselsnummeret som brukerID. Datatilsynet er inneforstått med at fødselsnummeret ikke tjener som autentisering. Tilsynet er likevel kritisk til at en statsautorisert, varig og entydig identifikator brukes til slike formål. Selv om fødselsnummer er en naturlig del av de offentlige etaters behandling for øvrig, synes dette å være eksempel på misbruk. Det er flere aspekter som kan anføres. For det første kan anføres at nettsteder som krever oppgitt fødselsnummer, før sikker samhandling med rette vedkommende er etablert, kan bidra til vasking av eller innhøsting av fødselsnummer. Disse kan siden havne i illegale databaser og utnyttes for uønskede eller kriminelle formål.

Så vidt tilsynet har brakt på det rene, bidro portalen www.altinn.no til vasking av gyldige fødselsnummer i forbindelse med angrepene mot teleoperatørenes nettsider sommeren 2007, hvilket illustrerer tilsynets poeng. For det andre må saken ses i sammenheng med det som anføres vedrørende bestilling av nye koder i rapporten om skatteetaten. For det tredje kan anføres at staten gjennom egne løsninger "legitimerer" bruk av fødselsnummer i slik påloggingsportaler. Datatilsynet har ved flere anledninger erfart at næringslivets aktører viser til statens løsninger når tilsvarende spørsmål aktualiseres.

Lovgiver har i personopplysningslovens forarbeider vektlagt at slike entydige identifikatorer ikke skal anvendes i utrengsmål. Bruk av fødselsnummer må oppfylle kravene i personopplysningsloven §§ 8, 11 og 12 med mindre det foreligger særskilt lovhjemmel. Altinn Sentralforvaltning kunne ikke redegjøre for om kravene var oppfylt og hvilke alternativer som var vurdert. En slik redegjørelse skal foreligge i forkant av at fødselsnummer tas i bruk. Det vises for øvrig til rapport om skatteetaten, hvor det redegjøres for råd som ble gitt i tilknytning med kontrollen mot likende statlig side høsten 2007.

Underlag for pålegg: Altinn Sentralforvaltning må avslutte bruk av fødselsnummer som brukerID ved pålogging, med mindre det kan påvises gyldig behandlingsgrunnlag.

5.1.2.2 Logger

Personopplysningsforskriftens § 2-8 pålegger behandlingsansvarlige å registrere (logge) autorisert bruk av informasjonssystemet. Det samme gjelder for forsøk på uautorisert bruk, jf personopplysningsforskriftens § 2-14. Loggene skal lagres i minst 3 måneder, jf personopplysningsforskriftens § 2-16. Men sletting skal skje når opplysningene ikke lenger er nødvendig for å gjennomføre formålet med behandlingen jf. personopplysningslovens § 28.

Informasjonssystemet til Altinn.no har i dag logger som inneholder mer informasjon enn hva som er nødvendig for å oppfylle kravene i henhold til ovennevnte bestemmelser. Blant annet logges sluttbrukers IP-adresse og fødselsnummer. Ettersom

logging av denne typen informasjon ikke kan sies å ha hjemmel i personopplysningsforskriftens §§ 2-8, 2-14 og 2-16, må behandling av slike opplysninger ha eget grunnlag i personopplysningslovens § 8. Det må også vurderes hva som er formålet med disse loggene og om dette er saklig begrunnet i virksomheten, jf personopplysningslovens § 11, 1. ledd bokstav b. Logging av fødselsnummer må dessuten vurderes særskilt opp mot kravene i personopplysningslovens § 12 jf. ovenfor.

Underlag for pålegg: Altinn Sentralforvaltning må dokumentere at logging av fødselsnummer og IP-adresse har hjemmel i personopplysningslovens § 8 og oppfyller grunnkravene i personopplysningslovens § 11. For fødselsnummer må også § 12 oppfylles.

5.1.2.3 Sletting av logger

Etter personopplysningsforskriften §§ 2-8, 2-14 og 2-16 skal det registreres autorisert og forsøk på uautorisert tilgang til informasjonssystemet. Denne dokumentasjonen skal lagres i minst 3 måneder.

For loggene nevnt i ovennevnte avsnitt er det etter Datatilsynets oppfatning viktig at det settes en grense for hvor lenge de skal lagres og dermed hvilken slettetid som er aktuell. Det vises i denne sammenheng til kravet om saklig begrunnelse i virksomhetens forhold i personopplysningslovens § 11 b jf. § 28. Etter revisjon av logger er det normalt av disse slettes fordi det ikke lenger foreligger noe saklig behov for lagringen.

Underlag for pålegg: Altinn Sentralforvaltning må definere og dokumentere når logger skal revideres, lagres og slettes i forhold til behov og innhold.

5.1.2.4 Arbeidsarkivet

Når en person er logget på portalen, kan vedkommende lagre dokumenter før de er ferdig utfylt, for så å fullføre dem på senere tidspunkter. Dette er en tjeneste Altinn Sentralforvaltning tilbyr til brukeren av tjenesten uten at det følger klart av databehandleravtalen. Det var under kontrollen uklart om lagringen skjer på vegne av Skattedirektoratet eller for eget formål. Dette må klarlegges. Dersom lagringen skjer på vegne av Skattedirektoratet må databehandleravtalen justeres tilsvarende. Dersom lagringen skjer for eget formål må behandlingsgrunnlag jf. personopplysningslovens § 8 jf. § 11 defineres og dokumenteres. Dersom gyldig behandlingsgrunnlag ikke foreligger, må løsningen med "arbeidsarkiv" avsluttes.
Underlag for pålegg: *Altinn Sentralforvaltning må godtgjøre at det foreligger gyldig behandlingsgrunnlag i personopplysningslovens § 8 jf. § 11 for lagringen i "arbeidsarkivet" eller at lagringen skjer i tråd med gyldig databehandleravtale. Alternativt må "arbeidsarkivet" avsluttes.*

5.1.2.5 Servicearkivet

Personopplysningslovens §§ 8 jf. §11 og 15 stiller krav til behandlingsgrunnlag for behandling av personopplysninger. Videre legger personopplysningslovens § 28

retningslinjer for sletting av personopplysninger når de ikke lenger er nødvendig for å gjennomføre formålet med behandlingen.

Datatilsynet konstaterte at Altinn Sentralforvaltning har etablert et arkiv som i praksis oppbevarer kopi av all kommunikasjon sendt mellom borger og den aktuelle tjenestetilbyder. Etter det tilsynet erfarer, forelå det ikke støtte i databehandleravtalen med Skattedirektoratet for at det skulle foretas slik aktivitet. I den grad det hadde gjort det, ville tilsynet likevel stilt seg meget skeptisk til en slik praksis. Løsningen kan langt på vei sammenlignes med at Posten eventuelt skulle ta kopi av all korrespondanse som ble sendt gjennom deres infrastruktur.
Arkivloven har til hensikt å sørge for tilfredstillende arkivering av relevant informasjon hos virksomheten. Tilsvarende er det borgerens plikt å sørge for gjenpart av kommunikasjonen om det eventuelt er ønskelig. Videre bør det uten tvil være den behandlingsansvarlige som på en forsvarlig måte bør forvalte den arkivverdig informasjon og eventuelt gi elektronisk tilgang til denne på konkret forespørsel.

Datatilsynet reagerer videre på måten ovennevnte arkiv var organisert på. Kommunikasjon mellom den enkelte borger og ulike behandlingsansvarlig ble blandet sammen i en og samme database, uten tilfredstillende segmentering av informasjonen. Det kan videre anføres at løsningen muligens kan være i konflikt med arkivlovens bestemmelser. Den usystematiske lagringen i databehandlers system oppfyller trolig ikke arkivmyndighetenes krav. I forhold til sistnevnte spørsmål, henvises det til Riksarkivet for råd.

Etter tilsynet vurdering sitter Altinn Sentralforvaltning uten lovlig grunnlag på et utilfredstillende sikret og uorganisert arkiv.

Underlag for vedtak: Altinn Sentralforvaltning må slette informasjonen i det såkalte "servicearkivet" med mindre det kan dokumenteres lovlig grunnlag for arkivet jf. personopplysningslovens §§ 8, 11. I sistnevnte tilfelle må "servicearkivet" uansett sikres og segmenteres på en tilfredsstillende måte jf. personopplysningslovens §§ 13 og 15.

5.1.3 Internkontroll

Personopplysningslovens § 14 pålegger behandlingsansvarlig å iverksette systematiske tiltak som sikrer at personopplysninger behandles lovlig, sikkert og forsvarlig. Dette innebærer at virksomheten må ha rutiner for sin bruk av opplysningene og tilfredstillende beskyttelse av disse. Rutinene skal dokumenteres.

Under kontrollen fokuserte Datatilsynet på de styrende elementene i virksomhetens internkontrollsystem. Det ble avdekket mangler i forhold til stadfesting av behandlingsansvaret (jf ovenfor), kartlegging av hvilke behandlinger som skjer i virksomheten og identifisering av hvilke plikter disse behandlingene utløser.

Når det gjelder rutiner for gjennomførende aktiviteter, foretok ikke Datatilsynet noen systematisk gjennomgang av disse. Rutiner for innsyn og retting/sletting ble imidlertid diskutert i forhold til utvalgte tjenester. Også her ble det avdekket mangler i

forhold til personopplysningslovens krav. Altinn Sentralforvaltning kunne ikke fremlegge rutiner for innsyn i de personopplysninger de har behandlingsansvar for, og heller ikke rutiner for sletting av logger eller opplysninger i arbeidsarkivet.

Som databehandler må Altinn Sentralforvaltning også utarbeide rutiner som sørger for at de føringer som ligger i databehandleravtalen implementeres i praksis.

Datatilsynet vil presisere at det utelukkende ble fokusert på rutiner relatert til tema for kontrollen, men det er nærliggende å tro at mangler i den styrende delen også gjelder for andre behandlinger som skjer i virksomheten. Datatilsynet vil derfor anbefale at Altinn Sentralforvaltning foretar en revisjon av sitt internkontrollsystem for alle deler av virksomheten.

Underlag for pålegg: Altinn Sentralforvaltning må utarbeide et system som ivaretar kravene i personopplysningslovens § 14 for egen behandling, samt gjøre seg kjent med relevante rutiner som er stadfestet av behandlingsansvarlig for databehandler, jf § 15.

5.1.4 Informasjonsplikt

Altinn Sentralforvaltning er informasjonspliktig i forhold til eget behandlingsansvar. I tillegg kan Altinn Sentralforvaltning påta seg å sørge for informasjon på vegne av den behandlingsansvarlig gjennom databehandleravtalen. Altinn Sentralforvaltning må sørge for dokumenterte rutiner for gjennomføringen av informasjonsplikten i forhold til latente brukerkontoer, arbeidsarkiv og sikkerhetsløsningene som står i forhold til dokumentert behandlingsansvar jf. pkt. 5.1.1 over.

5.2 Krav om informasjonssikkerhet

5.2.1 Segmentering av informasjonssystemet

Forholdet som omhandles her, er også omtalt i punkt 5.1.2.5. I dette avsnittet er problemstillingen ytterlig utdypet. Personopplysningslovens § 15 omhandler databehandlers rådighet over behandlingsansvarliges personopplysninger regulert i en databehandleravtale.

Personopplysninger kan behandles på vegne av andre med grunnlag i en databehandleravtale. Dette betyr i praksis at man, dersom man behandler personopplysninger på vegne av flere behandlingsansvarlige, må behandle informasjon for hver enkelt behandlingsansvarlig separat.

Informasjonssystemet til Altinn.no var på kontrolltidspunktet konstruert slik at all informasjon, uavhengig av behandlingsansvarlig, lagres i en sentral database sekvensielt. Denne databasen er kalt "servicearkiv". Dette vil si en sammenblanding av informasjon tilhørende alle de forskjellige behandlingsansvarlige. Nivået for informasjonssikkerhet er felles for alle behandlingsansvarlige basert på retningslinjer satt av Altinn Sentralforvaltning. En slik praksis harmoniserer dårlig med at Altinn Sentralforvaltning er en databehandler ulike aktører, som kan ha ulike krav til sikkerhet.

Datatilsynet

Problem med slik sekvensiell lagring tydeliggjøres videre ved behov for å slette informasjon fra arkivet etter de retningslinjer som de forskjellige behandlingsansvarlige legger opp til. Dette viser seg enda tydeligere ved spørsmål om sletting i sikkerhetskopier hvor dette er enda vanskeligere, jf. personopplysningslovens § 28 om sletting i alle ledd. Ved en sekvensiell database vil man måtte gå igjennom hver eneste instans i databasen for å vurdere om den skal slettes. I motsetning til en segmentert database for hver enkelt databehandler sine data hvor man kan gå inn å slette instanser som ikke lenger er relevant. Ulike skjemaer må også skilles i ulike tabeller ettersom det med stor sannsynlighet vil være forskjellige krav til oppbevaring og sletting for de enkelte skjemaene.

Datatilsynet har tidligere anført at ovennevnte arkiv må opphøre, med mindre det kan dokumenteres gyldig behandlingsgrunnlag. I den grad slikt grunnlag kan dokumenteres kommer påfølgende tekst til anvendelse. En segmentering vil være nødvendig for all informasjon som forholder seg til en behandlingsansvarlig, det vil si at eventuell kopi av kommunisert innhold, logger og andre systemer også må segmenteres. Grunnen til dette er som nevnt over, forholdet mellom behandlingsansvarlige og at det ikke skal lagres informasjon på en måte som strider mot nødvendigheten av separat behandling av informasjonen.

Datatilsynet merker seg at en endring i dagens Altinn.no løsning, etter Altinn Sentralforvaltning sin vurdering, vil lage unødvendig dobbeltarbeid og økte kostnader sett i sammenheng med at Altinn 2 lanseres innen en tidsramme på 2 år. Tilsynet vil av den grunn ta hensyn til dette ved fastsettelse av frist for lukking av avviket.

Underlag for pålegg: Altinn Sentralforvaltning må implementere en tilfredstillende logisk eller fysisk segmentering av informasjonssystemet slik at krav til tilfredstillende informasjonssikkerhet og ulike behov mht. sletting mellom ulike behandlingsansvarlige, kan ivaretas, jf. personopplysningslovens §§ 13 og 15.

Datatilsynet

Skattedirektoratet
Postboks 6300 Etterstad

0603 OSLO

Deres referanse	Vår referanse (bes oppgitt ved svar)	Dato
	08/00297-5 /FUE	14. november 2008

Kontroll hos Skattedirektoratet 14052008 - Vedtak

Den 14. mai 2008 gjennomførte Datatilsynet kontroll hos Skattedirektoratet og Altinn-portalen, med hjemmel i lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven) § 42 tredje ledd nr. 3. I brev av 4. september 2008 gir direktoratet sitt tilsvar.

Vurdering av virksomhetens svar
Datatilsynet vil i det følgende kommentere direktoratets tilsvar, herunder opplyse om innvendingene er tatt til følge. Datatilsynet ønsker innledningsvis å presiserer at en kontrollrapport skal gjenspeile situasjonen på kontrolltidspunktet. Eventuelle senere endringer vil derfor ikke påvirke rapportens innhold, men kan likevel påvirke hvilke vedtak som fattes. Det faller heller ikke naturlig at tilsynsmyndigheten tar hensyn til mulige fremtidige løsninger. I den grad slike planer er anført vil de kun tas til etterretning uten videre drøftelse.

Datatilsynet har forståelse for Skattedirektoratets ønske om å utnytte gevinster ved en effektiv bruk av informasjonsteknologi. Direktoratet har fremfor alt skissert et behov for en effektiv, elektronisk samhandling med publikum. Tilsynet erfarer at rammebetingelsene for trygg elektronisk samhandling med borgeren har vært utilfredstillende. Det derfor forståelig at det er tatt initiativ for å finne kostnadseffektive løsninger som samtidig ikke er for komplisert for bruker.

Likevel, Datatilsynet ser konturene av en vedvarende situasjon hvor de store offentlige aktørene opprettholder infrastrukturer som etter tilsynets oppfatning bryter med viktige prinsipper for sikker elektronisk samhandling. Datatilsynet observerer hvilke, etter tilsynets vurdering, uønskede virkninger dette får:

- Det etableres påloggingsløsninger som gjennomgående er av lav kvalitet
- Distribusjonskanalene for formidling av autentiseringsinstrumenter er basert på usikret postforsendelse (A-post)
- Det brukes beskyttelsesverdig fødselsnummer i innloggingsløsninger

Postadresse:	Kontoradresse:	Telefon:	Telefaks:	Org.nr:	Hjemmeside:
Postboks 8177 Dep 0034 OSLO	Tollbugt 3	22 39 69 00	22 42 23 50	974 761 467	www.datatilsynet.no

- Det etableres unødvendig mellomlagring av beskyttelsesverdig informasjon hos databehandlere. I noen tilfeller er slik mellomlagring vedvarende.
- Det etableres ulike former for uformaliserte elektroniske arkiv hos databehandler, med varig lagring av informasjon.
- Det er utilfredstillende skille eller segmentering av beskyttelsesverdig informasjon tilhørende ulike behandlingsansvarlig.
- Beskyttelsesverdig kryptert informasjon termineres hos databehandler og lagres ukryptert der.

Listen over er ikke uttømmende, men illustrer den uheldige situasjonen man etter tilsynets vurdering er kommet opp i. Det vil ofte vil det være manglende bedriftsøkonomisk motivasjon for å bedre situasjonen. Gevinstene vil derimot, etter tilsynets vurdering, ligge på det samfunnsøkonomiske plan. Utover det følger også forventningene om en ansvarlig forvaltning av personopplysninger i offentlig regi, herunder opprettholdelse av tillit i befolkningen.

Som det fremgår av kontrollrapporten, er flere av de ovennevnte problemstillinger aktuelle også i forhold til Skattedirektoratet. Datatilsynet finner det naturlig å appellere til direktoratets samfunnsansvar og til rollen som storforbruker av instrumenter for elektronisk samhandling. I det ligger det et ansvar, etter tilsynets vurdering, til å fremme samhandlingsinstrumenter som dekker et bredere behov.

Datatilsynet er klar på at problemstillingene som berøres i denne sak, i like stor grad er relevant i forhold til kommunal sektor og delvis i privat næringsliv. Bredden i problemet illustrerer godt behovet for en samfunnsøkonomisk tilnærming.

I det følgende vil Datatilsynet kommentere direktoratets tilsvar. Det vil gis opplysninger om eventuelle anførsler er tatt til følge. Datatilsynet har valgt å avgrenset egne kommentarene og henviser i hovedsak til rapport for tilsynets begrunnelse.

Ad. Punkt 2.1
Det vises til direktoratets kommentarer vedrørende de elektroniske selvangivelser. I brevet drøftes behandlingsgrunnlag for å opprette latente konto for hele befolkning.

Slik Datatilsynet ser saken, oppretter Altinn Sentralforvaltning en latent elektronisk konto hvor ulike tjenesteeiere kan legge inn informasjon til den enkelte borger. Altinn Sentralforvaltning henviser i sitt tilsvar til en avtale inngått med Skattedirektoratet om tilgang til folkeregisteret som primært behandlingsgrunnlag for opprettelse av slike kontoer. Datatilsynet vurderer det slik at denne avtalen kun regulerer tilgang og utlevering av personopplysninger, ikke opprettelse av latente konto. Etter tilsynets vurdering må Altinn Sentralforvaltning som behandlingsansvarlig ha et eget behandlingsgrunnlag for disse kontoene. Dette også sett i lys av at andre tjenestetilbydere vil kunne benytte den samme samhandlingskanal ovenfor borgeren. Det er også anført allmenn interesse, jf. personopplysningslovens §8, litra d, som et alternativt behandlingsgrunnlag. Datatilsynet mener at dette grunnlaget ikke er anvendelig, da elektronisk innlevering er en frivillig opsjon. Det vises for øvrig til vedtaksbrevet til Altinn Sentralforvaltning for ytterlig utdyping.

Datatilsynet deler ikke Skattedirektoratets vurdering av hjemmel i ligningsloven med forskrift. Det er, slik Datatilsynet ser det, verken i loven eller forskriften noe som tyder på at alle selvangivelser må tilgjengeliggjøres over Internett. Datatilsynet forholder seg med det til at selvangivelsen kan, om det foreligger behandlingsgrunnlag, gjøres tilgjengelig på denne måten. Opprettelse av latente konto som ikke borgeren er kjent med, utgjør etter tilsynets vurdering en uoppfordret eksponering av risiko for spredning av personopplysninger om borgeren. Forholdet må også ses i lys av de svake autentiseringsmekanismene.
Det kan videre spørres om forskriftshjemmelen i Ligningslovens § 4-5 nr. 6 vil være tilstrekkelig dersom det ble spørsmål om å opprette en forskrift om slik tilgjengeliggjøring.

Datatilsynet vil peke på at forventingen til en klar lovhjemmel øker med antallet personopplysninger og opplysningenes karakter som følsomme eller sensitive. Dette medfører at det i dette tilfellet må foreligge en klar hjemmel for behandlingen.

Når ovennevnte er anført, vil Datatilsynet presisere sin interesse i å bidra til i å finne gode alternativer til usikret utsendelse av papirbaserte selvangivelser i mottakers postkasse. Selvangivelsen innholder så betydelige mengder økonomisk informasjon til at den vil kunne betraktes som et verdipapir for kriminelle aktører. Dokumentet inneholder som kjent en samlet oversikt over fødselsnummer, inntekt, formue, finansielle forbindelser, eiendom, bankkontonumre, sikkerhetskoder m.v. Erkjennelsen underbygger behovet både for å vurdere dagens praksis med usikret manuell utsendelse av selvangivelser, og behovet for sikring av den elektronisk tilgjengelige.

Det presiseres at tilsynet intensjon ikke er å avvikle bruk av Altinn-portalen, men få på plass tilstrekkelig behandlingsgrunnlag for de personopplysninger som er nødvendig for å benytte tjenestene som tilbys. Dersom aktørene faller ned på at hovedprinsippet i personvernet skal fravikes, nemlig frivillighet gjennom borgerens samtykke, må dette forelegges lovgiver. Datatilsynet er klar over at utformingen av et lovgrunnlag vil ta noe tid.

Datatilsynet vil derfor fatte vedtak om i tråd med tidligere varsel om vedtak.

Ad. Punkt 2.2
Det vises til kommentarer vedrørende Internkontroll. Skatteetatens tilbakemelding tas til etterretning. Vedtaket justeres i tråd med tilbakemeldingen, slik at Skatteetaten kun pålegges å oppdatere og supplere internkontrollsystemet.

Ad. Punkt 2.3
Det vises til direktoratets kommentarer vedrørende utsendelse av brukernavn og passord.

Datatilsynet varslet opprinnelig et vedtak ovenfor Altinn Sentralforvalting og Altinn-portalen som tilsier at løsningen ikke tilfredstiller personopplysningslovens § 12. Tilsynet pekte på at det finnes alternative løsninger for entydig identifisering.

Datatilsynet anser fødselsnummer som en beskyttelsesverdig opplysning, det er imidlertid ikke begrunnet ut fra at identifikatoren vil ha noen verdi i forbindelse med autentisering.

Tilsynets vurdering bygger primært på det faktum at fødselsnummer er en statsautorisert, varig og entydig identifikator. Slike unike identifikatorer har vist seg attraktive blant kriminelle som samler inn personopplysninger med det formål å foreta identitetstyveri. Datatilsynet er kjent med at skattemyndighetene har et annet syn på foreliggende trussel. Skattedirektoratet har blant annet publisert formelen for oppbygning av fødselsnummer på sine hjemmesider. Fødselsnummer er heller ikke underlagt taushetsplikt. Datatilsynet vil dog trekke frem personopplysningsforeskriftens § 9-2 som omhandler sikkerhetskrav ved elektronisk forsendelse inneholdende fødselsnummer. Bestemmelsen gir prinsipielle føringer i retning av et foreliggende behov for å beskytte slike data. Av samme bestemmelse følger, etter Datatilsynets vurdering, et behov for å beskytte tilsvarende informasjon ved elektronisk samhandling.

Likevel, gitt den foreliggende realitet: Fødselsnummer er ikke en særlig beskyttet opplysning. Flere tidligere hendelser har medført at uvedkommende sannsynligvis sitter på større mengder fødselsnummer, koblet til navn, adresse og andre karakteristika. Blant annet bidro masseinnhøstningen i 2007, hvor blant annet portalen www.altinn.no skal ha vært kompromittert, til foreliggende status. Uvedkommende kan med det i praksis benytte seg av andres fødselsnummer på Internett. Tjenestetilbyder vet følgelig ikke hvem det kommuniserer med, med mindre det foreligger en adekvat autentisering.

Etter Datatilsynets vurdering er foreliggende løsning for autentisering en svak form for autentisering. Et moment som styrker en slik oppfatning, er det faktum at autentiseringsinstrumentene sendes ut ved usikret postgang (A-post). Tilsynet er langt fra overbevist at dette gir tilfredstillende autentisering av bruker, i forhold til informasjonen som skal beskyttes.

Datatilsynet erkjenner at portalen må kunne skille på hvem de samhandler med for å skille de konkrete innsende skjema fra hverandre. Tilsynet er imidlertid av den oppfatning at dette kan gjøres senere, internt i informasjonssystemet, om nødvendig basert på fødselsnummer. Bruk av fødselsnummer i en innloggingsprosess anses etter tilsynets oppfatning som uheldig og sterkt uønsket. Datatilsynet ser imidlertid at tidligere forvaltningspraksis svekker tilsynets muligheter til å fatte det varslede vedtaket. Datatilsynet velger derfor å frafalle vedtaket, men vil gi en sterk tilrådning om å endre praksisen. Tilsynet vil også orientere om at det er tatt konkrete initiativ for å skjerpe regelverket på dette området. Hva utfallet av en slik prosess blir er det for tidlig å fastslå.

Datatilsynet erkjenner at direktoratet strengt tatt har rett når man hevder at det ikke eksisterer kvalifiserte elektroniske signaturer på det norske markedet. Prosessen frem til å få slike signaturer tilgjengelig i det norske markedet vil ta tid. I påvente av dette har man imidlertid såkalte signaturer basert på kvalifiserte sertifikater. Skattedirektoratet hevder i sin tilbakemelding:

"*Alternativet som omhandler bruk av kvalifisert elektronisk signatur er utelukket da det pr dags dato ikke finnes tilbydere på det norske markedet*"

Datatilsynet legger til grunn at ovennevnte kommentar er en følge av tilsynets noe upresise språkbruk.

Tilsynet vil uansett påpeke nødvendigheten om at det er nødvendig for direktoratet å forsikre seg om at riktig mottaker har mottatt forsendelsen med brukernavn og passord for tilgang til Altinn-portalen, og at tilstrekkelig konfidensialitet er etablert. Datatilsynet vil derfor fatte vedtak om i tråd med tidligere varsel om vedtak.

Ad. Punkt 2.4
Datatilsynet noterer seg direktoratets synspunkter vedrørende hvilken informasjon den enkelte ansatte bør gis tilgang til. Skattedirektoratet gjør et poeng ut av at bruk av portalløsningen er frivillig og at virksomhetene får leve med foreliggende løsning.

Det ovennevnte forhold er kun et anliggende for tilsynet i den grad løsningen medfører at uvedkommende får tilgang til personopplysninger uten at dette følger av tjenestelig behov. Etter tilsynets vurdering foreligger det en reell fare for dette ved den foreliggende løsning.

Datatilsynet kan ikke se at direktoratets anførsler gir grunnlag for å avstå fra varslet vedtak.

Ad. Punkt 2.5
Datatilsynet har notert seg direktoratets avklaringer vedrørende ansattes bruk av eget fødselsnummer ved tjenestelig innrapportering. Tilsvaret peker i retning av at direktoratet later til å ha misforstått tilsynets anmerkinger. Tilsynets kommentar i dette punkt knytter seg delvis også til tilsvar som er gitt i forbindelse med punkt 2.4.

Skattetatens tilbakemelding tas til etterretning. Datatilsynet slutter seg ikke til direktoratet forståelse av kommentarutgave (s. 125) til personopplysningsloven. Det fremgår klart av sammenhengen at fødselsnummer aksepteres brukt til identifikasjon av skattepliktige borgere. Det ligger dog ikke i dette at fødselsnummeret kan benyttes i tilknytning til identifisering ved innrapportering knyttet til virksomhet.

Datatilsynet noterer likevel at de to forskriftene som er nevnt i tilbakemeldingen, angir at fødselsnummer skal benyttes. Behandlingsgrunnlag anses etter dette å foreligge i forhold til innrapportering av merverdiavgiftsoppgaver samt ved innlevering av ligningsoppgaver for næringsdrivende. Datatilsynet vil bemerke at hjemmelen ikke anses å strekke seg til andre plikter eller innrapporteringer. Dersom fødselsnummer skal benyttes i andre sammenhenger må det tilsvarende fremlegges et gyldig behandlingsgrunnlag for dette.

Datatilsynet mener det er viktig å være bevisst hvilken rolle man utfører en handling i kraft av; som privatperson eller som arbeidstaker. Selv om det er samme fysiske person, er det ofte knyttet helt andre rettigheter og plikter til rollen som yrkesutøver kontra privatpersonen. En arbeidstaker er for eksempel ikke under arbeidsgivers styringsrett og kontrollregime i fritiden. Videre, de rutiner og krav som kan foreligge for vedkommendes utøvelse av stillingen kommer ikke til anvendelse. Til sist vises det til at de fullmakter som tilligger en stilling ikke kan påberopes av privatpersonen som innehar den. Datatilsynet vil med det peke på et behov for at elektroniske ID må kunne skille mellom de to ulike rollene.

Ved introduksjon av elektroniske signaturer basert på kvalifiserte sertifikat åpnes slike muligheter. Et sertifikat kan anvendes i kraft av privatpersonen med de rettigheter og plikter det gir, mens et annet anvendes i kraft av yrkesutøver med de plikter og fullmakter det gir. En sammenblanding av dette rollebildet er i beste fall uheldig. Datatilsynet har for øvrig også mottatt en rekke reaksjoner fra for eksempel regnskapsmedarbeidere som har reagert på praksisen.

Datatilsynet legger etter dette til grunn at Skattedirektoratet vil avvikle bruken av fødselsnummer i tilknytning til eventuelt andre innrapporteringer, med mindre det kan vises til en klar hjemmel for bruken. Det vil ikke bli fattet vedtak i tråd med tidligere varsel.

Ad. Punkt 2.6
Skattedirektoratets syn på saken tas til etterretning. Datatilsynet fastslår imidlertid at det ikke er dokumentert noe behandlingsgrunnlag for servicearkivet. Datatilsynet vil derfor fatte vedtak om sletting av servicearkivet i tråd med tidligere varsel om vedtak. I vedtaksbrevet til Altinn Sentralforvaltning, er foreliggende problemstilling drøftet mer inngående. Datatilsynet viser til dette dokument for videre redegjørelse.

Vedtak
Datatilsynet fatter med hjemmel i personopplysningslovens § 46 følgende vedtak:

1. Skattedirektoratet må godgjøre at det foreligger tilstrekkelig behandlingsgrunnlag i § 8 for uoppfordret tilgjengeliggjøring av elektronisk selvangivelse til samtlige skatteytere. Se rapportens pkt. 5.1.2.1. ***Frist for gjennomføring av vedtaket er 01.06.2009.***
2. Skattedirektoratet må oppdatere og supplere sitt internkontrollsystem slik at dette ivaretar kravene i personopplysningslovens § 14. Se rapportens 5.1.3. ***Frist for gjennomføring av vedtaket er 01.06.2009.***
3. Skattedirektoratet må etablere en løsning for utsendelse av brukernavn og passord som ivaretar kravene til konfidensialitet, jf personopplysningslovens § 13 og personopplysningsforskriftens § 2-11. Se rapportens 5.1.4. ***Frist for gjennomføring av vedtaket er 01.06.2009.***
4. Skattedirektoratet må sørge for tilgangstyring som kan harmoniseres med virksomhetenes behov for intern delegasjon og tilgang til informasjon basert på tjenstlig behov jf. personopplysningslovens § 13 og personopplysningsforskriftens § 2-11. Se rapportens pkt. 5.1.5. ***Frist for gjennomføring er ved innføringen av Altinn II, dog senest 01.06.2010.***
5. Skattedirektoratet må avslutte lagring i "servicearkiv" hos Altinn Sentralforvaltning, se rapportens pkt. 5.1.7. ***Frist for gjennomføring av vedtaket er 01.06.2009.***

Det skal dokumenteres at justerte løsninger er tilfredstillende gjennom en risikovurdering, jf. personopplysningsforskriftens § 2-4. Risikovurderingen skal oversendes Datatilsynet som dokumentasjon på lukking av avvik.

Klageadgang
Det gjøres oppmerksom på at vedtak fattet av et forvaltningsorgan kan påklages. En eventuell klage rettes til det organ som har fattet vedtaket. I den grad forvaltningsorganet opprettholder vedtaket oversendes saken til klageinstans. For vedtak fattet med hjemmel i personopplysningsloven er klageorganet Personvernnemnda.

Med hilsen

Leif T. Aanensen
avdelingsdirektør

Frank U. Eriksen
overingeniør

Vedlegg: Endelig kontrollrapport
Kopi Altinn Sentralforvaltning

Datatilsynet

Endelig kontrollrapport		
Saksnummer: 08/00297 Dato for kontroll: 14.05.2008 og 15.05.2008 Rapportdato: 14.11.2008	Kontrollobjekt: Skattedirektoratet Sted: Brønnøysund	Utarbeidet av: Christine Lie Ulrichsen Astrid Flesland Frank Ulfsby Eriksen

1 Innledning

Datatilsynet viser til kontroll mot Skattedirektoratet og databehandler Altinn Sentralforvaltning 14. og 15. mai 2008. Kontrollen ble utført i lokalene til Altinn Sentralforvaltning, med begge etater tilstede. Kontrollen begrenset seg til skjemaer for elektronisk innrapportering til Skattedirektoratet samt informasjonssystemet og sikkerhetsløsningen til Altinn Sentralforvaltning på Altinn.no. Kontrollen skjedde med hjemmel i lov om behandling av personopplysninger av 14. april 2000 nr. 31 (personopplysningsloven) § 42 tredje ledd nr. 3.

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

Datatilsynet har laget en separat rapport for Altinn Sentralforvaltning (Datatilsynets referanse 08/00291) ettersom det er viktig å skille merknadene, med bakgrunn i databehandler og behandlingsansvarlige sine plikter. Kopi av rapportene vil forlegges alle parter og bør ses i sammenheng.

2 Tilstede under kontrollen

2.1 Fra Altinn:

- Ann-Christine Nybacka – avd.dir AEI
- Henning Andersen – seksjonssjef AEI
- Håkon Olderbakk, avd.dir Plan og Utvikling
- Harald Thomassen, seniorrådgiver
- Olav Melteig, sikkerhetsansvarlig
- Roger Skoglund, Dataess, innleid konsulent
- Roy Horn, superbruker

2.2 Fra Skattedirektoratet

- Svein Mobakken, sikkerhetssjef
- Lars Nilsen, avd.dir Rettsavdelingen
- Erling Solberg, systemjurist
- Jan Erik Norheim, tjenestedir I/J

2.3 Fra Datatilsynet:

- Christine Lie Ulrichsen, seniorrådgiver
- Astrid Flesland, seniorrådgiver
- Frank U Eriksen, overingeniør

3 Generelt

Datatilsynet gjennomførte våren 2008 kontroller mot flere virksomheter hvor temaet er det offentliges behandling av personopplysninger ved elektronisk kommunikasjon og saksforvaltning (e-forvaltning). Formålet med kontrollene er å sikre at brukernes personvern er tilstrekkelig ivaretatt ved bruk av de tjenester som virksomheten tilbyr.

Det var Skattedirektoratet som opprinnelig utviklet Altinn portalen for innlevering av selvangivelsen. Tjenesten har i senere tid har blitt overført til Altinn Sentralforvaltning ved Brønnøysundregisterne. Direktoratet er den største brukeren av Altinn portalen, med selvangivelsen som en viktigste bidragsyter til dette. Datatilsynet noterte seg at Skattedirektoratet anser seg som behandlingsansvarlig for alle personopplysninger knyttet til skjemaene som er tilgjengelig fra dem. Altinn Sentralforvaltning vil da være databehandler for Skattedirektoratet.

Det var enighet mellom de to etatene at Altinn Sentralforvaltning var behandlingsansvarlig for sikkerhetsløsningen, det vil si den tekniske infrastrukturen rundt autentisering av bruker og datafangsten. En nærmere vurdering av ansvarsforholdene følger nedenfor.

Kontrollen ble det avgrenset til følgende av Skattedirektoratets tjenester/skjemaer:

- Selvangivelse for lønnstakere og pensjonister
- Opplysninger om arbeidstakere
- Lønns- og trekkoppgave
- Innrapportering fra veldedige organisasjoner

4 Kort om bruk av personopplysninger samt formålet med behandlingene

Skattedirektoratet behandler personopplysninger via Altinn portalen. Formålet er å gjøre rapportering til skattemyndighetene lettere og mer tilgjengelig for næringslivet og befolkningen generelt. Forholdet mellom Skattedirektoratet og Altinn Sentralforvaltning er regulert i en databehandleravtale.

Personopplysninger blir samlet inn hos Altinn Sentralforvaltning og lagret her i maksimalt 10 år. Lagringstid er avhengig av hvilke vurderinger behandlingsansvarlig har foretatt i forhold til gjeldene lovverk og behov. Opplysningene formidles videre elektronisk til Skattedirektoratet over sikre kommunikasjonslinjer og behandles videre i etatssystemet.

Det er opprettet et "servicearkiv", heretter kalt arkivet. Her lagres alle skjema eller annen informasjon som er sendt borgeren (for eksempel selvangivelsen) i påvente av godkjenning eller utfylling. Alle ferdigutfylte og innsendte skjema som "returneres", lagres i arkivet. Ifølge aktørene ble dette gjort for eventuell senere oppslag eller nedlasting hos Skattedirektoratet. Ved innsending av billag til eksempelvis selvangivelsen blir disse lagret i arkivet og ikke sendt direkte videre til Skatteetaten sitt informasjonssystem. Disse må hentes ned ved behov for saksbehandling. Det er

kun et fåtall personer med tilgang, som legger til aktuell dokumentasjon i saken som behandles. Bakgrunnen for det sistnevnte er informasjonen i billagene kun er for tjenstlig behov hos saksbehandler.

I tillegg kan borgeren lagre delvis utfylte skjemaer i et arbeidsarkiv før oversending til Skattedirektoratet. Se nærmere om dette i rapport til Altinn Sentralforvaltning pkt. 5.1.1.

5 Funn og avvik fra lovbestemte krav til behandling av personopplysninger

5.1 Generelle krav i forhold til behandling av personopplysninger

Datatilsynet vil under dette avsnittet vurdere de faktiske forhold som ble avdekket under kontrollen i forhold til personopplysningslovens krav.

5.1.1 Ansvarsforhold – Behandlingsansvar/databehandler

En *behandlingsansvarlig* er definert i personopplysningsloven som den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jf § 2, nr 4.

En *databehandler* er den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf lovens § 2, nr 5.

Mellom databehandler og behandlingsansvarlige skal det inngås en *databehandleravtale*, jf personopplysningslovens § 15. Denne er styrende for databehandlers rådighet over personopplysninger. Dersom en databehandler bruker personopplysninger utover det som er avtalt, er vedkommende å anse som behandlingsansvarlig for behandlingen og hjemmel for denne må finnes i personopplysningslovens § 8, evt. § 9.

Under kontrollen ble ansvarforholdet vurdert for følgende funksjoner:

1. Autentiserings og autorisasjonsfunksjonen (opprettelse av brukerkontoer)
2. Andre fellestjenester som logger og arbeidsarkiv
3. Arkivet (servicearkivet)

Skattedirektoratet vurderte seg som behandlingsansvarlig for behandling av personopplysninger i arkivet og Altinn Sentralforvaltning som ansvarlig for de øvrige funksjonene. Det vises til vurdering av ansvarsforholdene i rapport til Altinn Sentralforvaltning, punkt 5.1.1. Altinn Sentralforvaltning har påberopt seg behandlingsansvaret for opplysninger lagret i arbeidsarkivet. En slik konklusjon faller ikke intuitivt for tilsynet. Datatilsynet har derfor pålagt virksomheten å foreta en ny vurdering av ansvarsforholdene, hvilket kan få konsekvenser i forhold til Skattedirektoratet.

5.1.2 Behandlingsgrunnlag

Personopplysninger kan bare behandles når det finnes et grunnlag i personopplysningslovens § 8. Ved behandling av sensitive personopplysninger må i

tillegg ett av vilkårene i § 9 være oppfylt. Videre er det krav blant annet til saklighet, og relevans i lovens § 11.

Behandling av personopplysninger i forhold til de tjenestene som var i fokus under kontrollen, er i hovedsak hjemlet i lov. Datatilsynet etterlyste imidlertid en oversikt fra Skattedirektoratet hvor det rettslige grunnlaget er presisert i forhold til hver enkelt behandling. En slik oversikt er en nødvendig del av de styrende dokumentene i virksomhetens internkontrollsystem, jf nedenfor.

5.1.2.1 Tilgjengeliggjøring av selvangivelse på Internett
Altinn Sentralforvaltning administrerer brukerkonto i selve portalløsningen. Brukerkonto er opprettet på grunnlag av fødselsnummer hentet fra Folkeregisteret, og oppdateres ved jevne mellomrom. Det vil si at det er informasjon lagret hos Altinn sentralforvaltning om alle landets borgere, uavhengig av om elektronisk konto er forespurt eller ikke. Begrunnelsen synes å være at alle borgere skal ha mulighet til å benytte Altinn-portalen og at den derfor ligger latent. Med latent menes en uaktivisert konto. Kontoen blir først aktiv når borger selv ber om dette. Informasjonen som er nødvendig for å gjøre kontoen aktiv, følger med bla. skattekortet og selvangivelsen. Disse sendes ut til borgerens folkeregistrerte adresse, normalt i åpne postkasser.

Skattedirektoratet gjør tilgjengelig elektronisk selvangivelse til samtlige skatteytere, uavhengig av om disse har tatt i bruk eller ønsker å ta i bruk Altinn. Selvangivelsen blir, via fødselsnummer, koblet med vedkommendes konto hos Altinn.no, uavhengig av om konto er aktivert eller latent. Hvis borger kun har en latent konto hos Altinn.no, vil det etter det tilsynet erfarer, over tid, akkumulere seg opplysninger tilknyttet denne kontoen. Under tilsynet kunne Skattedirektoratet ikke redegjøre for noe behandlingsgrunnlag i forhold til slik lagring.

Kontrollen avdekket videre at Skattedirektoratet ikke kunne vise til hjemmel som lovfester en uoppfordret elektronisk tilgjengeliggjøring av selvangivelsen via Altinn portalen til enhver skatteyter. Etter tilsynets vurdering tilsidesetter staten med det borgerens autonomi i forhold til foretrukket samhandling. Som det fremgår senere i rapporten, har Datatilsynet enkelte kritiske merknader til hvordan sikkerheten er ivaretatt i løsningen. Tilsvarende kan enkelte borgere påberope tilsvarende anførsler. At slike konto opprettes uoppfordret, er etter tilsynets vurdering en uheldig tilsidesettelse av borgerens muligheter til å foreta egne valg.

Elektronisk tilgjengeliggjøring av selvangivelse må sees i sammenheng med kontrollrapporten mot Altinn Sentralforvaltning sitt punkt 5.1.2.1.

Underlag for pålegg: Skattedirektoratet må godtgjøre at det foreligger tilstrekkelig behandlingsgrunnlag i § 8 for uoppfordret tilgjengeliggjøring av elektronisk selvangivelse til samtlige skatteytere.

5.1.3 Internkontroll
Personopplysningslovens § 14 pålegger behandlingsansvarlig å iverksette systematiske tiltak som sikrer at personopplysninger behandles lovlig, sikkert og

forsvarlig. Dette innebærer at virksomheten må ha rutiner for sin bruk av opplysningene og tilfredstillende beskyttelse av disse. Rutinene skal dokumenteres.

Internkontroll består gjerne av styrende, gjennomførende og kontrollerende dokumentasjon. Styrende dokumentasjon gir en systembeskrivelse som innholder policy og målsetning, identifiserte krav og plikter, intern organisering, ansvar og myndighet. Dokumentasjonen er overordnet i sin form og spesielt ledelsesorientert.

I forkant av kontrollen ba Datatilsynet om å få oversendt styrende dokumenter for internkontroll samt databehandleravtale mellom Skattedirektoratet og Altinn Sentralforvaltning. Skattedirektoratet oversendte databehandleravtale med Altinn, men ingen fullgod oversikt over de styrende elementene i virksomhetens internkontrollsystem.

Under kontrollen ble internkontrollplikten diskutert ytterligere. Datatilsynet påpekte at plikten påhviler alle behandlingsansvarlige, herunder også de større statsetatene. Blant annet ble det konstatert at det mangler en oversikt over behandlingsgrunnlag og hjemmel for lagring av opplysninger i "servicearkivet" som er etablert hos Altinn. Det er avklart hvilken lagringstid som er aktuell, men ingen bakenforliggende begrunnelse eller vurdering i forhold til dette. Det ble også avdekket at det mangler rutiner for oppfyllelse av plikten til informasjon, jf personopplysningslovens §§ 19 og 20 og rutiner for innsyn og sletting, jf personopplysningslovens §§ 18 og 28.

Det ble også pekt på at behandlingsgrunnlag og saklig behov for dobbellagring i arkivet er mangelfullt dokumentert. Datatilsynet pekte særlig på vurderingen av lagring i arkivet etter at informasjonen som blir innsendt via Altinn er overført til skattemyndighetene for videre behandling.

Mangler ved dokumentert internkontroll er å anse som brudd på personopplysningsloven § 14.

Underlag for pålegg: Skattedirektoratet må oppdatere dagens internkontrollsystem slik at det ivaretar kravene i personopplysningslovens § 14.

5.1.4 Brukernavn og passord i samme forsendelse

Personopplysningsloven § 13 og personopplysningsforskriften kapittel to regulerer behovet for informasjonssikkerhet ved behandling av personopplysninger. Herunder spesielt forskriftens § 2-11 som omhandler konfidensialitet.

Skattedirektoratet sender i dag ut skattekort og selvangivelse som inneholder både brukernavn og passord. Brukernavn er fødselsnummer og passord er forskjellige pin-koder.

Utsendelse av bruknavn og passord i en og samme forsendelse er etter Datatilsynets oppfatning ikke tilfredstillende i forhold til de sikkerhetskrav som følger av behovet for konfidensialitet, jf. personopplysningsforskriften § 2-11. Datatilsynet er derfor av den oppfatning at dagens løsning med utsendelse av brukernavn og passord i samme

forsendelse må avvikles. Bruknavn og passord må minimum sendes i separate forendelser. Datatilsynet anbefaler at passord sendes i egen separat rekommandert sending eller på annen måte som sikrer at rette mottaker får forsendelsen. Dersom kvalifisert elektronisk signatur er et tilgjenglig alternativ, kan det også være egnet.

Hvis bruker mister sine koder, kan nye bestilles via skatteetatens hjemmeside. Det eneste som er påkrevd er at det tastes inn et fødselsnummer. Nye pin-koder blir sendt til folkeregistrert adresse. Etter Datatilsynets vurdering er løsningen med at brukeren kan bestille nye passord ved å legge inn et fødselsnummer uforsvarlig. Uvedkommende kan enkelt deaktivere koder den rettmessige bruker har i besittelse, for så å hente nye koder i vedkommendes postkasse etter få dager. Dette medfører fare for kompromittering av en sentral sikkerhetskomponent i løsningen. Tilsvarende problemstilling ble tatt opp i forbindelse med en kontroll mot www.minside.no i 2007.

Under et senere veiledningsmøte med ansvarlig etat for ovennevnte løsning, ble det presisert følgende alternativer:

- *Enten at etaten med rimelighet forvisser seg at det er rette vedkommende de samhandler med ved bestilling av nye koder, eller*
- *det sikres at det er rette vedkommende som er mottaker av kodene, for eksempel ved at det er legitimasjonskontroll ved utlevering, eller*
- *disse sendes på en trygg elektronisk måte ved bruk av kvalifiserte elektroniske signaturer*

Underlag for pålegg: Skattedirektoratet må etablere en løsning for utsendelse av brukernavn og passord som ivaretar kravene til konfidensialitet, jf personopplysningslovens § 13 og personopplysningsforskriftens § 2-11.

5.1.5 Tilgangsstyring ved rapportering fra virksomheter

Personopplysningsloven § 13 og personopplysningsforskriften kapittel to regulerer behovet for informasjonssikkerhet ved behandling av personopplysninger. Herunder spesielt forskriftens § 2-11 som omhandler konfidensialitet.

Rapportering av virksomhetsrelatert informasjon til skattemyndighetene skjer i økende grad via Altinn-portalen. Virksomhetene, representert ved daglig leder eller annen ansvarlig person, vil være autorisert for å rapportere på vegne av virksomheten. Ofte vil tilgangen for å rapportere bli delegert til økonomiansvarlig eller til ekstern part, typisk regnskapsfører. Det er virksomheten selv som vurderer hva som er en egnet intern fordeling av rapporteringsoppgaver.

Dersom muligheten til å rapportere elektronisk øker, vil også tilgangen til informasjon i Altinn-portalen øke vesentlig. Det er i denne sammenhengen viktig å sørge for at opplysninger som er rapportert inn ikke blir tilgjengelig for andre ansatte i rapporterende virksomhet med mindre det foreligger delegasjon og tjenestelig behov for dette.

Kriteriene for tilgang er i dag konfigurert ut fra at det kun er én ansvarlig person som skal rapportere. En slik ordning vil ikke være representativ for alle virksomheter med rapporteringsplikt, jf. det som er sagt over. Et godt eksempel vil være organisasjoner hvor det er delegert ansvar til flere ulike personer internt i virksomheten. Her kan en person rapporterer lønnsrelatert informasjon, mens andre for eksempel rapporterer frivillig skattefradrag for bidrag til veldedige formål som nødhjelp.

Delegasjon av ansvar internt i en virksomhet, som er mer regel enn unntak, vil dermed medføre at enhver som autoriseres for å rapportere får tilgang til all informasjon virksomheten rapporterer. Personen ansvarlig for rapportering av frivillig skattefradrag for bidrag vil dermed ha tilgang til lønns- og trekkoppgaver for alle ansatte i virksomheten, eventuell all annen informasjon virksomheten rapporterer. Dette er ikke i tråd med kravet til at tilgang til personopplysninger skal defineres etter delegasjon og tjenestelig behov.

Underlag for pålegg: Skattedirektoratet må sørge for tilgangsstyring som kan harmoniseres med rapporterende virksomhets behov for intern delegasjon og tilgang til informasjon basert på tjenstlig behov.

5.1.6 Bruk av fødselsnummer for intern delegering i Altinn

Personopplysningslovens §12 stiller krav om av bruk av fødselsnummer kun skal skje når det foreligger saklig grunn for sikker identifisering og at metoden er nødvendig for å oppnå sikker identifisering.

Intern delegasjon av rettigheter for tilgang i Altinn hos Skatteetaten gjøres på bakgrunn av fødselsnummer. Datatilsynet antar at grunnen til dette er at selve sikkerhetsløsningen til Altinn er basert på fødselsnummer. Det at fødselsnummer er tilgjengelig og at man har lovmessig rett til å benytte fødselsnummer i én sammenheng betyr imidlertid ikke automatisk at man kan benytte det i alle andre sammenhenger. Kan man benytte andre metoder for identifisering, skal disse foretrekkes. Eksempelvis ansattnummer, fødselsdato og lignende.

Den ansatte må i dagens løsning benytte sitt eget fødselsnummer for å gjennomføre tjenestelige plikter for arbeidsgiver ovenfor skattemyndighetene. Etter tilsynets vurdering er det nærliggende å hevde at ovennevnte praksis medfører et misbruk av en ansattes fødselsnummer. Datatilsynet mener det ikke foreligger gyldig grunnlag for å benytte fødselsnummer som identifikator for tilgangsstyring.

Underlag for pålegg: Skattedirektoratet må endre praksisen med å kreve at arbeidstaker benytter eget fødselsnummer ved innrapportering på vegne av arbeidsgiver. Alternativt må direktoratet dokumentere gyldig behandlingsgrunnlag for praksisen.

5.1.7 Servicearkiv

Personopplysningslovens §8 jf. §11 stiller krav til behandlingsgrunnlag for behandling av personopplysninger. Videre legger personopplysningslovens § 28

retningslinjer for sletting av personopplysninger når de ikke lenger er nødvendig for å gjennomføre formålet med behandlingen.

Innsendte skjemaer for rapportering til skattetaten blir mellomlagret i informasjonssystemet til Altinn.no. Lagringen skjer i et arkiv (servicearkiv), hvor også de eventuelle billagene sendt inn elektronisk blir lagret. Ved overførsel av informasjon blir all informasjon liggende igjen i arkivet. Billagene blir ikke overført elektronisk til skattemyndighetene, men må manuelt hentes ned ved behov. Også disse blir liggende igjen etter at de eventuelt er lastet ned.

Datatilsynet oppfatter Altinn-portalen primært som en formidlingssentral, som tilrettelegger for samhandling mellom publikum og de ulike behandlingsansvarlige. I dette ligger å sørge for autentisering av bruker, samt formidle ønsket kommunikasjon mellom partene. Arkivet er i realiteten en database som systematisk lagrer informasjonskomponentene som "flyter gjennom" Altinn sitt system. Det er altså ikke et arkiv i tradisjonell forstand. De ulike informasjonskomponentene knyttes til de ulike brukerne, og gjøres tilgjengelig for både bruker og skattedirektoratet. Datatilsynet er sterkt kritisk til denne form for "sentralarkiv" opprettet av en databehandler. Løsningen fremstår fremfor alt meningssløs i det informasjonen er formidlet til behandlingsansvarlige. Det er hos den behandlingsansvarlige at arkivplikten oppstår og forutsetningene for forsvarlig langsiktig håndtering av informasjonen kan ivaretas. Eventuelle behov som bruker måtte ha i forhold til å skaffe seg innsyn, kan løses på annen måte. Dette kan løses ved at innsendte skjema gjøres tilgjengelig (elektronisk) fra behandlingsansvarliges side når behovet foreligger.

Skattedirektoratet har antydet at det er viktig for de som benytter Altinn-portalen å kunne se sin egen historikk over innsendte opplysninger. Det er nevnt at løsningen foregriper forespørsler direkte ovenfor skattemyndighetene og derfor er praktisk og hensiktsmessig for alle parter. En historisk oversikt må etter Datatilsynets oppfatning forankres i et behandlingsgrunnlag og ikke bare ut fra en antagelse om at det er viktig for brukerne av Altinn.

Det kunne under tilsynet ikke godgjøres at enhver bruker av Altinn portalen ønsker å ha en historikk i løsningen. Datatilsynet har vanskelig for å se noen saklig begrunnelse for lagringen i "servicearkivet". Etter tilsynets oppfatning er det ene og alene et teknisk designspørsmål om hvordan slike forhold tilrettelegges. Den tekniske infrastruktur utgjør ikke i seg selv er argument for å opprettholde en løsning som ikke oppfyller lovens krav.

Datatilsynet reagerer også på måten opplysningene lagres og systematiseres i "servicearkivet". Se nærmere om dette i rapporten for Altinn Sentralforvaltning pkt. 5.1.2.5.

Underlag for pålegg: Skattedirektoratet må dokumentere gyldig behandlingsgrunnlag for sitt "servicearkiv" hos Altinn Sentralforvaltning. Alternativt må lagring i "servicearkivet" avsluttes.