

Datatilsynets årsmelding 2003

Utdrag av omtalen av Datatilsynets tilsynsvirksomhet

Tilsynsvirksomheten i 2003

Både personopplysningsloven og helseregisterloven vektlegger tilsynsarbeid som et viktig virkemiddel for å sikre et godt personvern i samfunnet. Datatilsynet bruker operative tilsyn i kombinasjon med andre virkemidler for på den måten å oppnå en mest mulig samlet effekt.

Grunnlaget for tilsynsarbeidet er nedfelt i dokumentet *Strategi og metodikk for operative tilsyn*. Strategien omtaler Datatilsynets forvaltningsområde som helhet og legger føringer for hvordan de operative tilsynene organiseres og gjennomføres. På basis av dette underlaget, og de føringer som følger av Datatilsynets virksomhetsplan, utarbeides halvårlige tilsynsplaner.

I tråd med de overordnede prioriteringene ble tilsynsarbeidet i 2003 konsentrert om behandling av personopplysninger i helsesektoren, kommunene og arbeidslivet.

Det ble gjennomført 79 tilsyn. Dette representerer en nedgang i forhold til året før på 25 prosent. En hovedårsak til reduksjonen er at Datatilsynet i meldingsåret hadde en redusert ressursramme, og dermed også begrenset handlefrihet.

Oversikt over gjennomførte tilsyn (se vedlegg 1 for detaljert oversikt):

Sektor	Delsektor	Antall tilsyn
Helsesektoren	Primærhelsetjeneste	9
	Større helseforetak	10
	Andre	2
Kommunesektoren	Primærkommuner	31
	Fylkeskommuner	0
Arbeidsliv	Kundesentre, butikk, taxi mv.	11
Annet	Markedsførere	3
	Kameraovervåking	10
	Schengen informasjonssystem	2
	Telekom	1
Sum		79

Tilsynsvirksomheten avdekket at et flertall av de besøkte virksomhetene hadde liten kunnskap om regelverket og de prinsippene dette er tuftet på. Kunnskap er en nødvendig betingelse for etterlevelse av de pliktene som personopplysningsloven og helseregisterloven setter opp. Kunnskap er imidlertid ikke tilstrekkelig. Det må også være en underliggende motivasjon og et ønske om å prioritere dette arbeidet i en ellers travel hverdag. Mange virksomheter ser ut til å oppfatte arbeidet med eksempelvis å etablere et internkontrollsystem som en tung prosess, der man ikke riktig vet hvor man skal starte. Det blir til at man skyver arbeidet foran seg.

Ser man alle tilsyn under ett, er følgende avvik typiske:

- uryddighet knyttet til ansvar og myndighet
- brudd på bestemmelser om internkontroll
- brudd på bestemmelser om informasjonssikkerhet

Til forskjell fra tidligere år er ikke lenger brudd på meldeplikten så fremtredende. Det kan skyldes at plikten til å melde behandling av personopplysninger inn til Datatilsynet er blitt bedre kjent som følge av en informasjonskampanje ved inngangen til 2003.

Uryddighet knyttet til ansvar og myndighet

Det ble avdekket flere tilfeller hvor virksomhetens ledelse ikke hadde sørget for å definere klare rammer for ansvars- og myndighetsforhold omkring behandlingen av personopplysninger. Det var også en manglende helhetsoversikt over hva slags personopplysninger som faktisk behandles.

Det at en virksomhet setter bort deler av sin behandling av personopplysninger til underleverandører betyr ikke at man samtidig setter bort *ansvaret* for oppfyllelse av personopplysningsloven eller helseregisterloven. Virksomheten beholder fortsatt ansvaret, ved den behandlingsansvarlige. Gjennom tilsynene har det imidlertid vist seg at ansvarsforholdene ofte ikke er tilstrekkelig avklart mellom behandlingsansvarlig og underleverandør, kalt databehandler. Dette skal gjøres gjennom en databehandleravtale.

Brudd på bestemmelser om internkontroll

Personopplysningsloven og helseregisterloven krever at virksomheter som behandler personopplysninger skal etablere et system for internkontroll. Dette innebærer at den behandlingsansvarlige skal sørge for å ha kjennskap til gjeldende regler for behandling av personopplysninger. Det skal også foreligge en tilstrekkelig og oppdatert dokumentasjon for de rutiner og tiltak som er satt i gang for å sikre etterlevelse av regelverket.

Å få etablert et system for internkontroll synes imidlertid å være et gjennomgående problem for virksomhetene. I overraskende grad er det også i flere av de store virksomhetene kun satt i gang fragmenterte arbeider med å dokumentere at virksomheten har kontroll over sin behandling av personopplysninger.

Vanlige avvik med hensyn til internkontroll er:

- at arbeidet med internkontroll ikke har tilstrekkelig forankring i toppledelsen
- at virksomheten ikke har identifisert krav og plikter etter personvernlovgivningen
- at internkontrollsystemet ikke er konsistent, og at det kun foreligger sporadiske rutiner med hensyn til å sikre et godt personvern
- at behandlingene av personopplysninger i virksomheten ikke er systematisk kartlagt
- at relevante rutiner ikke er kjent blant ansatte (manglende implementering)
- at rutiner for periodisk gjennomgang og for avvikssituasjoner mangler. Hvis rutinene finnes blir de i liten grad fulgt.

Fra flere tilsynsobjekters side ble det uttrykt at de har problemer med å få bygget opp et enhetlig internkontrollsystem. Man finner det vanskelig å etablere en struktur i systemet og å ta stilling til hva som faktisk skal inngå i dette.

Brudd på bestemmelser om informasjonssikkerhet

Den behandlingsansvarlige skal, gjennom planlagte og systematiske tiltak, sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Tiltakene skal vurderes ut fra hensynet til konfidensialitet, integritet og tilgjengelighet. Tiltakene skal også dokumenteres. Alle som behandler personopplysninger skal derfor gjøre en risikovurdering. I

denne risikovurderingen skal man ta utgangspunkt i de personopplysningene som behandles, holdt opp mot det trusselbildet som virksomheten ut fra sin egenart står overfor.

Vanligste avvik med hensyn til bestemmelsene om informasjonssikkerhet er:

- manglende sikkerhetsmål og sikkerhetsstrategi
- manglende risikovurdering
- manglende konfigurasjonskontroll
- uavklart ansvar og myndighet mht. informasjonssystemet
- manglende implementering av organisatoriske og tekniske sikkerhetstiltak
- driftsmessige forhold slik som autorisasjonsrutiner (tilgangskontroll) og bruk av sikkerhetslogger

Det ble observert noe bedring knyttet til etablering av sikkerhetsmål, sikkerhetsstrategi og konfigurasjonskontroll. I dette ligger at virksomhetene har fastsatt rammer for informasjonssikkerheten. Imidlertid varierer det mye i hvilken grad disse rammene faktisk er implementert. Det ble på tilsynene gitt uttrykk for at regelverket innen informasjonssikkerhet er noe vanskelig å forstå. Videre ble det, spesielt hos de mindre virksomhetene, hevdet at regelverket er for pretensiøst og omfattende i forhold til virksomhetens størrelse.

Mange virksomheter ser ut til å oppfatte personopplysningsloven til kun å gjelde informasjonssikkerhet. Dette fører til at regelverkets øvrige plikter lett blir neglisjert, for eksempel når det gjelder å ha rutiner for innsyn, retting og sletting av personopplysninger.

Oppfølgende tiltak

Datatilsynet ser klart behov for en fortsatt tett oppfølging av de tre sektorene som har vært i fokus i 2003. Tilsynet vil i tiden fremover satse på målrettede tiltak mot de aktuelle sektorene, for på den måten å bidra til en positiv utvikling. Dette innebærer blant annet:

- å spisse og målrette de operative tilsynene mot bestemte objekter og typer behandling av personopplysninger. Dette vil særlig gjelde innen helsesektor og arbeidsliv.
- å utarbeide veiledninger knyttet til informasjonssikkerhet og internkontroll
- å utarbeide retningslinjer som berører personvern innen arbeidslivet, og distribuere disse til partene i arbeidslivet
- å delta i ulike seminarer, samarbeidsfora og arbeidsgrupper hvor de mest relevante problemstillinger tas opp og behandles
- å utarbeide artikler til bransjetidsskrifter
- å bistå med råd og veiledning ovenfor sentrale aktører

Se vedlagt oversikt over tilsynsobjekter.

Nærmere om tilsyn i kommunesektoren

Kommunene kjennetegnes ved å være tilbyder av et vidt spekter av tjenester og oppgaver overfor sine innbyggere. Omfanget og bredden i kommunens tjenestespekter gjør at det i en rekke av fagetatene er behov for å behandle også sensitive personopplysninger.

Den teknologiske utviklingen og satsingen på service og tilgjengelighet, kombinert med krav til effektivisering, har gjort at det i mange kommuner foregår et betydelig utviklingsarbeide. Det legges opp til selvbetjeningsløsninger via Internett, samlokalisering av etater og etablering av offentlige servicekontorer. Flere kommuner satser også på regionale samarbeidsløsninger. Dette stiller store krav til avklaring av ansvarsforhold og en dokumentert informasjonssikkerhet.

Lite systematisk tilnærming i kommunene

Det ble i 2003 gjennomført operative tilsyn hos 31 kommuner spredt over hele landet. Ved tilsynene ble det i første rekke kartlagt i hvor stor grad kommunene etterlever de krav som personopplysningsloven stiller til at det skal være etablert et system for internkontroll. Gjennom internkontrollsystemet skal det foreligge dokumentasjon for at det er iverksatt rutiner og tiltak som sikrer at kommunen virkelig etterlever de formelle kravene som gjelder for behandling av personopplysninger.

I den gamle personregisterloven var kommunene underlagt konsesjonsplikt for sin behandling av personopplysninger. Kommunene er derfor stort sett godt kjent med de *prinsippene* som ligger til grunn også for dagens personvernlovgivning. Gjennomgående gjøres det derfor i praksis mye korrekt, idet saksbehandlere og mellomledere i kommunen ser ut til å være bevisste sitt ansvar når det gjelder å sikre at personopplysninger blir behandlet på en betryggende måte. For eksempel er taushetsplikten i medhold av forvaltningsloven og annen særlovgivning godt innarbeidet. Det mangler imidlertid en systematisk tilnærming og dokumentasjon når det gjelder hvordan personopplysninger blir behandlet. Det oppstår lett misforståelser og feil, for eksempel når det kommer nye medarbeidere som ikke har god nok kjennskap til de ikke-dokumenterte rutinene.

Manglende oversikt

Kommunene må forholde seg til regelverket som helhet og derigjennom iverksette de pliktene som kommer til anvendelse. For i det hele tatt å kunne ha mulighet til å identifisere og gjennomføre sine plikter, må kommunene ha definert klare ansvars- og myndighetsforhold. Videre må det eksistere en oversikt over hvilke behandlinger av personopplysninger kommunen faktisk utfører. Ved tilsynene ble det funnet mange avvik i forhold til disse helt elementære forutsetningene.

Ivaretagelse av et lovfestet personvern vil i slike tilfeller bero mer på tilfeldigheter og de enkelte medarbeideres holdninger til personvern. Dette er lite tilfredstillende.

Rådmannens ansvar

Rådmannen, dvs. kommunens øverste administrative leder, er vanligvis den funksjonen som ivaretar behandlingsansvaret i kommunen. Rådmannen vil naturlig nok måtte delegerer ansvar

og myndighet videre til respektive etatsledere når det gjelder å effektivere de enkelte pliktene. Det er imidlertid rådmannen som behandlingsansvarlig som skal fastsette rammene som de øvrige aktørene skal forholde seg til. Det kan ikke overlates til andre.

Hos kun et mindretall av tilsynsobjektene var det etablert en god formell struktur i forhold til ansvar og myndighet. I flere tilfeller synes rådmannen å ha svært liten medvirkning i forhold til implementering av regelverket. I andre tilfeller var det uklare rammer for ansvar og myndighet. Betydningen av orden og en ledelsesmessig struktur kan ikke understrekes nok.

Internkontroll ikke etablert

Det ble påvist mangler i forhold til etablering av internkontrollsystem hos et flertall av de kommunene som ble besøkt. Det var imidlertid store variasjoner med hensyn til hvor omfattende manglene var. Noen av kommunene hadde ikke i det hele tatt startet prosessen med å etablere et internkontrollsystem, mens noen få var nær ved å ha et fullt ut dokumentert internkontrollsystem på plass. Hos de fleste kommunene var situasjonen noe i mellom disse to ytterpunktene; det var etablert kun sporadiske rutiner for enkelte plikter i regelverket. Rutinene var ikke forankret i et helhetlig system.

Hvilke behandlinger foretas?

Behandlingsansvarlig må ha oversikt over hvilke behandlinger som foretas for å vite hvilke plikter den behandlingsansvarlige har, og hvilke rettigheter lovverket gir den registrerte. Plikter og rettigheter er knyttet til selve behandlingen og kan derfor variere fra virksomhet til virksomhet, avhengig av hvilke behandlinger som finner sted.

Gjennom tilsynsvirksomheten ble det avdekket at mange kommuner mangler en samlet oversikt over hvilke behandlinger som foretas i kommunens regi. Dette innebærer i praksis at rådmannen som behandlingsansvarlig har liten reell kontroll med hvilke behandlinger vedkommende står ansvarlig for. Dette avskjærer den behandlingsansvarlige fra å ivareta sine plikter på en tilstrekkelig måte. En rekke kommuner sitter følgelig nå i den situasjon at de behandler en rekke personopplysninger uten at behandlingsansvaret er ivaretatt slik regelverket krever.

Mangelfulle avtaler med databehandlere

Regelverket krever at databehandler kun kan behandle personopplysninger i samsvar med det som er fastsatt i avtale med behandlingsansvarlig. Det ble påvist mangler i forhold til avtale med databehandler hos en rekke kommuner. I noen tilfeller kunne ikke avtale eller kontrakt med databehandler fremlegges, mens i andre tilfeller inneholdt avtalen få eller ingen elementer som berørte databehandlers behandling av personopplysningene.

Meldeplikten overholdes ikke

I motsetning til den gamle personregisterloven, gir dagens personvernlovgivning i stor grad kommunene fritak for konsesjonsplikt når det gjelder behandling av personopplysninger. Vilkåret er imidlertid at behandlingen har hjemmel i lov. Det er fortsatt konsesjonsplikt når det gjelder elektronisk behandling av sensitive personopplysninger som ikke er hjemlet i lov. Selv om konsesjonsplikten stort sett er falt bort, er den erstattet av en meldeplikt. På Datatilsynets hjemmeside er det publisert en veileder som orienterer nærmere om konsesjons- og meldeplikten kommunene skal forholde seg til.

Naturlig nok er kommunene rimelig ensartede med hensyn til hva slags tjenester de yter, og hva slags type personopplysninger de behandler. Dette skulle tilsi at de behandlingene av

personopplysninger som er meldepliktige til Datatilsynet, også burde være tilsvarende ensartet. Kommunestørrelsen eller geografisk plassering bør i liten grad gi forskjeller med hensyn til hva som meldes inn til Datatilsynet. Gjennom tilsynsvirksomheten ble det imidlertid avdekket at antallet meldinger som kommunene hadde sendt inn til Datatilsynet, varierte fra null til over tretti. Gjennomgående var det sendt for få meldinger i forhold til hva regelverket forutsetter. Brudd på denne plikten henger tydelig sammen med en manglende oversikt over hvilke behandlinger som foretas i kommunen.

Samlokalisering av fagetater og offentlige servicekontorer

I en del kommuner er det samlokalisert ulike fagetater. Dette innebærer gjerne også felles arkiv, skrivere mv. Selv om dette ut fra hensynet til effektivisering og helhetlig betjening av den enkelte bruker kan synes fornuftig, reises imidlertid en rekke prinsipielle spørsmål knyttet til innbyggernes personvern. Taushetsplikten som følger av de enkelte særlover kan stå i fare ved denne typen organisering. Taushetsplikten gjelder også overfor egne kollegaer uten tjenstlig behov for tilgang til opplysningene, så vel som overfor andre uvedkommende. I små kommuner er denne problemstilling særlig relevant fordi mye og detaljert informasjon om den enkelte bruker lett blir tilgjengelig for hele personalet som holder til i de samlokaliserte tjenestene. Kommunene synes gjennomgående å være klar over denne problemstillingen. I den praktiske virkelighet er det imidlertid bare i varierende grad tatt hensyn til dette.

SATS

Det er også i enkelte kommuner planer om å samlokalisere etter den såkalte SATS-modellen (samordning trygd, sosial og arbeidsformidling).

Denne typen behandling av sensitive personopplysninger i servicekontorer, hjemlet i ulike særlover, kan skape særlige personvernmessige utfordringer. Datatilsynet vil derfor følge utviklingen nøye.

Interkommunalt samarbeid

I økende grad etablerer kommunene samarbeidsløsninger på tvers av kommunegrensene som innebærer felles bruk av informasjonsteknologi. For små kommuner kan det være vanskelig å etablere en IT-infrastruktur som ivaretar kommunens behov for fleksibilitet, samtidig som en tilfredsstillende informasjonssikkerhet opprettholdes. Datatilsynet ser derfor positivt på at kommunene etablerer samarbeidsløsninger. Imidlertid må den felles infrastrukturen som etableres ivareta at hver enkelt kommune fortsatt har et selvstendig ansvar i forhold til sin behandling av personopplysninger. Klargjøring av ansvar er derfor viktig forutsetning for å lykkes med slike interkommunale samarbeidsprosjekter.

Ikke rutiner for sletting

Gjennom tilsynene ble det avdekket at mange av kommunene hadde mangelfulle rutiner for sletting av personopplysninger. Det ble særlig gjort denne typen funn innen barnevernet. Bekymringsmeldinger ble ikke slettet, selv om det ikke lenger var grunnlag for å beholde dem. Datatilsynet påpekte avviket overfor de aktuelle kommunene, slik at forholdet er rettet. Det er likevel grunn til å tro at dette med manglende rutiner for sletting av personopplysninger er et gjennomgående problem i kommunesektoren.

Tilgangskontroll og sikkerhetslogger

Datatilsynet avdekket ingen alvorlig brudd på regelverket knyttet til tilgangskontroll. Imidlertid var det en del kommuner som opererte med *singel log-on*. Dette gir den ansatte tilgangsrettigheter som også omfatter fagapplikasjoner. Dette, kombinert med en noe svak

autentisering av bruker, og mangler i forhold til kontroll av sikkerhetslogger, kan sette personvernet i fare. Datatilsynet kunne ikke direkte påvise brudd hvor nevnte kombinasjoner var tilstede. Mange kommuner er også flinke til å seksjonere brukere til henholdsvis sikker og administrativ sone, hvilket kan begrense konsekvensene ved eventuelle brudd. Datatilsynet anbefaler likevel at kommunene setter fokus på denne problemstillingen.

Kommunene synes i varierende grad å forholde seg til kravene om at det skal foretas sikkerhetslogging. Dette var knyttet både til bruk av loggene og hvor lenge de skal oppbevares. Det ble også påvist problemer med å håndtere loggene for visse fagapplikasjoner. Struktur og anvendelse av sikkerhetslogger er derfor noe sikkerhetslederne i kommunene bør se nærmere på.

Hva gjør Datatilsynet?

Gjennom de 31 tilsynene hos kommunene i 2003 har Datatilsynet dannet seg et godt bilde av hvor skoen trykker i forhold til kommunenes behandling av personopplysninger. Datatilsynet vil derfor nå prioritere arbeidet med å få utarbeidet nytt veiledningsmateriell om internkontroll og informasjonssikkerhet. I tillegg vil tilsynet bidra med foredragsholdere på kurs- og seminarer rettet mot kommunene. Datatilsynet har i den forbindelse tatt initiativ til et samarbeid med Kommunenes sentralforbund om blant annet å arrangere et seminar om personvern i kommunesektoren.

Som en følge av den økte oppmerksomheten omkring kommunenes behandling av personopplysninger har flere kommuner gått sammen og etablert *Foreningen kommunal informasjonssikkerhet*, (www.kins.no). Datatilsynet deltok på stiftelsesmøtet våren 2003, og var også bidragsyter på foreningens første konferanse om kommunal informasjonssikkerhet. Datatilsynet ser svært positivt på at noen aktive kommuner på denne måten har skapt en felles arena for de utfordringene kommunene står overfor når det gjelder å ivareta en god informasjonssikkerhet.

Gjennomførte tilsyn 2003

Saksnummer	Tilsynsobjekt	Poststed	Kjerneområde	Bransje/sector
2003/0826	Taxisentralen i Bergen BA	Kokstad	Hordaland	Arbeidsliv
2003/0988	Norges Informasjonsteknologiske høgskole	Bekkestua	Akershus	Arbeidsliv
2003/1018	Komplett Data AS	Sandefjord	Vestfold	Arbeidsliv
2003/1021	Norsk Statistikk Markedsundersøkelser	Oslo	Oslo	Arbeidsliv
2003/1073	Oslo Taxi AS	Oslo	Oslo	Arbeidsliv
2003/1080	Computerland Norge AS	Kolbotn	Akershus	Arbeidsliv
2003/1126	Leatherman Drift AS	Oslo	Oslo	Arbeidsliv
2003/1415	Enter forsikring AS	Oslo	Oslo	Arbeidsliv
2003/1416	Elkjøp Norge AS - Callsenter	Lørenskog	Akershus	Arbeidsliv
2003/1417	Sparebank 1	Oslo	Oslo	Arbeidsliv
2003/1424	Hermelin Research AS	Halden	Østfold	Arbeidsliv
2003/1103	Vital Eiendomsforvaltning AS	Oslo	Oslo	Fjernsynsovervåking
2003/1104	Car Park - Oslo City	Oslo	Oslo	Fjernsynsovervåking
2003/1420	Sameiet Glasshuset AS	Bodø	Nordland	Fjernsynsovervåking
2003/1425	Radisson SAS Bodø	Bodø	Nordland	Fjernsynsovervåking
2003/1426	Cardinal AS	Bodø	Nordland	Fjernsynsovervåking
2003/1427	Coop Mega City Nord	Bodø	Nordland	Fjernsynsovervåking
2003/1855	Bergen Storsenter AS	Bergen	Hordaland	Fjernsynsovervåking
2003/1865	Finnegaarden AS	Bergen	Hordaland	Fjernsynsovervåking
2003/1987	Musikkbar Garman AS	Stavanger	Rogaland	Fjernsynsovervåking
2003/2004	Welhavensgate borettslag	Oslo	Oslo	Fjernsynsovervåking
2003/0827	Finansnæringens Hovedorganisasjon - sentralregister	Oslo	Oslo	Helsesektoren
2003/0909	Helse Finmark HF, Hammerfest sykehus	Hammerfest	Finnmark	Helsesektoren
2003/0975	Sykehuset Buskerud HF	Drammen	Buskerud	Helsesektoren
2003/0976	Aker universitetssykehus	Oslo	Oslo	Helsesektoren

2003/0977	Sykehuset innlandet HF	Hamar	Hedmark	Helsesektoren
2003/1022	Statens vegvesen - Vegdirektoratet - Statens biltilsyn	Oslo	Oslo	Helsesektoren
2003/1081	Asker og Bærum HF - Blakstad sykehus	Rud	Akershus	Helsesektoren
2003/0854	Os kommune	Os	Hordaland	Kommune
2003/0902	Sarpsborg kommune	Sarpsborg	Østfold	Kommune
2003/0907	Kristiansund kommune	Kristiansund	Møre og Romsdal	Kommune
2003/0908	Hammerfest kommune	Hammerfest	Finnmark	Kommune
2003/0916	Froland kommune	Froland	Aust-Agder	Kommune
2003/0917	Gjerstad kommune	Gjerstad	Aust-Agder	Kommune
2003/0947	Bergen kommune	Bergen	Hordaland	Kommune
2003/0948	Steinkjer kommune	Steinkjer	Nord-Trøndelag	Kommune
2003/0978	Nittedal kommune	Nittedal	Akershus	Kommune
2003/0987	Bodø kommune	Bodø	Nordland	Kommune
2003/0998	Halden kommune	Halden	Østfold	Kommune
2003/1072	Arendal kommune	Arendal	Aust-Agder	Kommune
2003/1394	Drammen kommune	Drammen	Buskerud	Kommune
2003/1395	Larvik kommune	Larvik	Vestfold	Kommune
2003/1397	Sande kommune	Sande	Vestfold	Kommune
2003/1398	Namsos kommune	Namsos	Nord-Trøndelag	Kommune
2003/1399	Overhalla kommune	Overhalla	Nord-Trøndelag	Kommune
2003/1400	Grong kommune	Grong	Nord-Trøndelag	Kommune
2003/1401	Vågen kommune	Svolvær	Nordland	Kommune
2003/1402	Nedre Eiker kommune	Mjøndalen	Buskerud	Kommune
2003/1403	Vestvågøy kommune	Leknes	Nordland	Kommune
2003/1405	Elverum kommune	Elverum	Hedmark	Kommune
2003/1406	Kongsvinger kommune	Kongsvinger	Akershus	Kommune
2003/1407	Stange kommune	Stange	Hedmark	Kommune

2003/1409	Fet kommune	Fetsund	Akershus	Kommune
2003/1410	Rælingen kommune	Fjerdingsby	Akershus	Kommune
2003/1411	Sandnes kommune	Sandnes	Rogaland	Kommune
2003/1412	Sola kommune	Sola	Rogaland	Kommune
2003/1413	Strand kommune	Jørpeland	Rogaland	Kommune
2003/1414	Klepp kommune	Klepp	Rogaland	Kommune
2003/1422	Sortland kommune	Sortland	Nordland	Kommune
2003/0900	Norges Astma- og allergiforbund	Oslo	Oslo	Markedsførere
2003/1442	Catosenteret/Stiftelsen Sofienlund	Son	Østfold	Markedsførere
2003/1444	TV2 AS	Oslo	Oslo	Markedsførere
2003/1428	Hudklinikken	Oslo	Oslo	Primærhelsetjenesten
2003/1429	Lillestrøm Legesenter	Kjeller	Akershus	Primærhelsetjenesten
2003/1430	Søndre Frydenlund Legesenter	Sortland	Nordland	Primærhelsetjenesten
2003/1431	Robrygga legekantor	Namsos	Nord-Trøndelag	Primærhelsetjenesten
2003/1432	Byåsen legesenter	Trondheim	Sør-Trøndelag	Primærhelsetjenesten
2003/1433	Din doktor	Trondheim	Sør-Trøndelag	Primærhelsetjenesten
2003/1434	Fagerborg-legene	Oslo	Oslo	Primærhelsetjenesten
2003/1436	Centrum fastlegegruppe	Oslo	Oslo	Primærhelsetjenesten
2003/1438	Lege Cato A. Guldborg	Stavanger	Rogaland	Primærhelsetjenesten
2003/0000	Central Schengen Information System	Strasbourg	Strasbourg	SIS kontroll
2003/1892	Vestfold Politidistrikt	Tønsberg	Vestfold	SIS kontroll
2003/1404	Stokmarknes Sykehus	Stokmarknes	Nordland	Større helseforetak
2003/1421	Akershus Universitetssykehus HF	Norbyhagen	Akershus	Større helseforetak
2003/1439	Haraldsplass Diakonale sykehus	Bergen	Hordaland	Større helseforetak
2003/1440	Betanien Hospitalet	Fyllingsdalen	Hordaland	Større helseforetak
2003/1441	Jæren Distriktpsikiatriske senter	Bryne	Rogaland	Større helseforetak
2003/1418	Chess Communication AS	Bergen	Hordaland	Telekom

