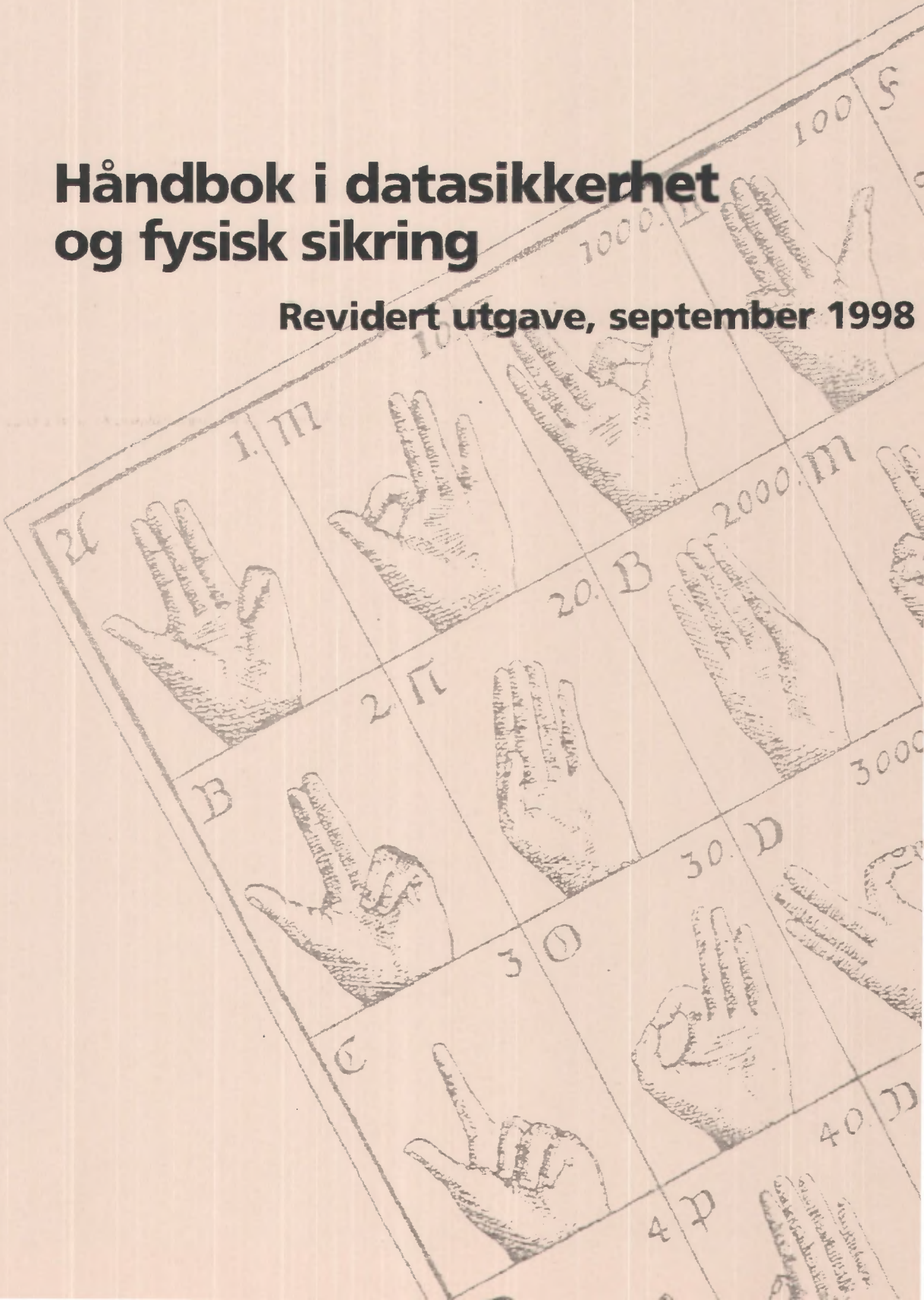
Statistics Norway

Statistisk sentralbyrå

Håndbok i datasikkerhet og fysisk sikring

Revidert utgave, september 1998



Håndbok i datasikkerhet og fysisk sikring

Revidert utgave, september 1998

Statistisk sentralbyrå • Statistics Norway
Oslo–Kongsvinger 1998

Forord

En av de viktigste forutsetningene for at datasikkerheten og den fysiske sikringen i Statistisk sentralbyrå er god, er at alle ansatte kjenner de viktigste regler og rutiner som gjelder og respekterer disse.

«Sikkerhetshåndbok for Statistisk sentralbyrå» inneholder de regler og interne retningslinjer som styrer sikkerheten i Statistisk sentralbyrå og som er av allmenn interesse for alle ansatte. Den inneholder også beskrivelser av hvordan sikkerhetsarbeidet er organisert, hvordan sikkerhetsoppgaver og ansvar er fordelt samt at den sier litt om de viktigste rutinene som skal følges for ivaretagelse av sikkerheten for hele Statistisk sentralbyrå. I tillegg er det tatt med stoff som er av mer informativ karakter.

Sikkerhetshåndboka deles ut til alle ansatte i Statistisk sentralbyrå, men jeg forutsetter ikke at alle skal måtte lese alt. Det viktigste er at den enkelte gjør seg kjent med boka og at de deler av den som har interesse og betydning i den enkeltes daglige arbeid blir lest mer nøye.

Stoffet i denne 3. utgaven av Sikkerhetshåndboka er disponert slik at det er lagt større vekt på behandling av person- og foretaksopplysninger enn tidligere. Dette betyr imidlertid ikke at Statistisk sentralbyrå anser fysiske og IT-messige sikringstiltak som mindre viktige.

Har du spørsmål til håndboka eller andre forhold rundt sikkerheten i Statistisk sentralbyrå som du ikke får svar på ved din enhet, kan du henvende deg til et av Sikkerhetsutvalgets medlemmer.

Statistisk sentralbyrå,
Oslo, september 1998

Svein Longva

Innhold

A
1. Innledning

Sikkerhet deles inn i tre forhold som skal dekke den totale sikkerheten:

Konfidensialitet	(Begrenset innsyn)
Kvalitet	(Data er til å stole på)
Tilgjengelighet	(Data er tilgjengelig)

1.1. Mål for sikkerheten i Statistisk sentralbyrå

En god sikkerhet skal medvirke til at Statistisk sentralbyrå oppfyller målsetningen om å fremme effektiv produksjon av tjenlig statistikk uten å bryte statistikkloven, andre lovbestemmelser eller pålegg fra Datatilsynet.

Dette innebærer at den totale informasjonsmengde Statistisk sentralbyrå til enhver tid sitter inne med blir godt ivaretatt gjennom en tilfredsstillende datasikkerhet og fysisk sikring av bygninger og materiell.

Dette skal forhindre at informasjonen blir:
Brukt til andre formål enn forutsatt
Ødelagt/slettet tidligere enn nødvendig
Endret/forfalsket/feiltolket
Brukt av ikke autorisert personale
Oppbevart lenger enn nødvendig

Sikkerhetstiltakene må være rettet mot de hovedformer for trusler som finnes. De må være rettet mot misbruk hos Statistisk sentralbyrås medarbeidere og andre som kommer i lovlig kontakt med våre data og dataanlegg, da disse representerer alle former for trusler.

Det er særlig viktig at all utlevering av individuelle opplysninger/mikrodata fra statistiske grunndata blir nøye vurdert i forhold til de lover og retningslinjer som gjelder for slik utlevering.

Videre må tiltakene være rettet mot innbrudd i Statistisk sentralbyrås lokaler, tapping av linjer og alle former for ulovlig adgang til data fra fremmede terminaler, mot tekniske feil og ulykker som brann, strømbrudd, vannskader, innbrudd o.l. som kan forårsake ødeleggelse av data og utstyr.

Det er dessuten viktig å ha et datavern som kan forsvares økonomisk og som ikke sinker statistikkproduksjonen unødig. Det er derfor også viktig å redusere sikkerhetsrisikoen og dermed sikkerhetstiltakene så langt som mulig.

Sikkerhetsrisikoen kan bl.a. reduseres ved å slette data som det ikke lenger er bruk for, kryptere identifikasjonsnumre eller avidentifisere data der dette er mulig, og ikke lagre data med en detaljrikdom Statistisk sentralbyrå ikke har bruk for.

Sikringstiltakene bør ikke være av en slik art at de skaper unødige tunge arbeidsrutiner og redusert trivsel for den enkelte. På den annen side må medarbeiderne sette seg inn i og respektere de sikkerhetsregler og tiltak som gjelder til enhver tid.

En god sikkerhet har også som mål å ivareta den enkelte ansattes sikkerhet og eiendom ved å redusere risikoen mest mulig for at uvedkommende tar seg inn i Statistisk sentralbyrås bygninger.

Arbeidet med å sikre den enkeltes arbeidsplass, arbeidsmiljø, helse o.l. vil ellers ikke bli behandlet i denne håndboka da dette er saksområder som reguleres av arbeidsmiljøloven samt annet regelverk. Disse forhold er det blant annet egne utvalg i Statistisk sentralbyrå som har ansvar for.

1.2. Lovgrunnlag for SSBs virksomhet

Statistikkloven

Statistisk sentralbyrås virksomhet reguleres av statistikkloven. Statistikklovens formål er å fremme effektiv produksjon av tjenlig statistikk gjennom regler for innsamling og bruk av opplysninger til statistiske formål (statistikkloven § 1-1).

Statistisk sentralbyrå er det sentrale organ for utarbeiding og spredning av offisiell statistikk, men skal også gi opplysninger til statistisk bruk for forskningsformål og for offentlig planlegging innenfor de rammer loven gir.

Både innhenting, bruk og utlevering av opplysninger reguleres i statistikkloven. Både opplysninger innhentet på frivillig grunnlag og opplysninger innhentet etter fastsatt opplysningsplikt reguleres av loven.
.
Statistisk sentralbyrå kan med hjemmel i statistikkloven § 2-2 benytte oppgaveplikt dersom opplysningene er nødvendig for utarbeidelse av offisiell statistikk. Bare lovbestemt taushetsplikt kan stå i veien for oppgaveplikten. Oppgaveplikten kan pålegges «enhver», dvs. både fysiske og juridiske personer, private som offentlige.

I tillegg har Statistisk sentralbyrå rett til å utnytte allerede eksisterende administrative registre i statsforvaltningen og i landsomfattende kommunale organisasjoner. Dette følger av statistikkloven § 3-2.

Statistikklovens regler om taushetsplikt (statistikkloven § 2-4), bruk av opplysninger (statistikklovens § 2-5) og offentliggjøring av opplysninger (statistikklovens § 2-6) angir rammene for hvordan vi kan behandle de opplysninger som er innhentet med sikte på å utarbeide offisiell statistikk.

Datatilsynets rammekonsesjon
Selv om Statistisk sentralbyrås virksomhet, inkludert innhenting og bruk av opplysninger, reguleres av statistikkloven, vil det oppstå konsesjonsplikt ved opprettelse av personregistre, se punkt 3.7.

Dette følger av personregisterloven. Lovgiver har m.a.o. overlatt til Datatilsynet å sette vilkår for etablering av personregistre i Statistisk sentralbyrå utover det som følger av statistikkloven mht. innhold og bruk.

Dessuten er Datatilsynet gitt myndighet til å bestemme at opplysninger gitt frivillig eller innhentet etter fastsatt opplysningsplikt kan brukes til annet enn utarbeidelse av offisiell statistikk (statistikklovens § 2-5).

Det følger av forarbeidene til loven at man her snakker om enkelte, lite følsomme opplysninger. Eksempel på slik godkjennelse av «annen bruk» er den tillatelse som er gitt i rammekonsesjonen til utlevering av særskilte næringsopplysninger til bruk for opprettelse og oppdatering av andre offentlige og private registre.

Den tillatelse som er gitt i rammekonsesjonen til statistisk bruk av opplysninger til forsknings- og offentlige planleggingsformål, er også eksempler på at Datatilsynet har godkjent «annen bruk».

Da Statistisk sentralbyrå er innehaver av et stort antall personregistre som ville gjøre det upraktisk å ha en egen konsesjon for hvert enkelt register, har Datatilsynet regulert våre registre gjennom en egen rammekonsesjon.

Her er det gitt rammebetingelser for registrene og det skal innenfor rammekonsesjonen sendes melding for hvert nytt register som opprettes og/eller for eventuelle endringer i forhold til tidligere meldinger. Slik meldeplikt gjelder imidlertid kun for registre som inneholder sensitive personopplysninger og for registre der opplysningene er innhentet på frivillig grunnlag. For andre registre gjelder det en halvårlig rapporteringsplikt. Se mer om dette under kapittel C, pkt. 3.

Det er et grunnleggende og viktig krav at medarbeiderne i Statistisk sentralbyrå må kjenne til og overholde bestemmelsene i statistikkloven og vilkår satt i Datatilsynets rammekonsesjon. Statistikkloven og rammekonsesjonen følger som vedlegg til denne håndboka.

Forvaltningslov og offentlighetslov
Statistisk sentralbyrå som forvaltningsorgan er underlagt forvaltningsloven og offentlighetslovens bestemmelser om saksbehandling, journalføring, tilgang til opplysninger, offentlighet/unntak fra offentlighet mv.

En del av disse bestemmelsene som omhandler tilgang til og beskyttelse av opplysninger, vil være av betydning for ivaretakelse av sikkerheten i Statistisk sentralbyrå og vil derfor bli gjennomgått i det følgende.

Personregisterloven
En god del av våre registre vil være opprettet til andre formål enn til utarbeidelse av offisiell statistikk. Slike registre vil ikke høre inn under rammekonsesjonen, men i utgangspunktet være konsesjonspliktige.

I forskriftene til personregisterloven er det gjort unntak fra konsesjonsplikten for en del typiske registre, som lønns- og personalregistre, journal/brevarkiv, adresseregistre og kunderegistre.

Forskriftene angir hvilke opplysninger disse registrene kan inneholde, hva de kan brukes til og hvem/hva det kan utleveres opplysninger til. Holder man seg innenfor vilkår satt i forskriftene trenger man ikke søke konsesjon.

Ved opprettelse av personregistre som faller utenfor rammekonsesjonen (opprettet til andre formål enn statistikk) og opprettelse av personregistre som ikke er unntatt fra konsesjon, jf. personregisterlovens forskrifter, vil det måtte søkes særskilt konsesjon. Eksempel på register som krever særskilt konsesjon er bedriftshelsetjenestens IT-register.

EØS
Enkelte EØS-relevante forordninger og direktiver er med å danne grunnlag og sette rammebetingelser for Statistisk sentralbyrås virksomhet. Både EUs personverndirektiv, rådsforordning om overføring av konfidensielle data til Eurostat og EUs statistikklov bør nevnes i denne sammenheng.

Implementeringsarbeidet som gjelder for all EØS-relevant EU-lovgivning er imidlertid ikke sluttført. Det foreligger utkast til ny lov om behandling av personopplysninger. Loven forventes vedtatt i løpet av 1998 og vil erstatte dagens personregisterlov.

EUs statistikklov forutsettes også implementert i norsk lovgivning. Loven antas ikke å medføre behov for særlige endringer i statistikkloven, men arbeidet her er ennå ikke sluttført fra Finansdepartementets side.

1.3. Opplegg for sikkerhetshåndboka

Sikkerhetshåndboka er delt inn i 4 hovedkapitler. Til forskjell fra tidligere utgaver av sikkerhetshåndboka er nå temaer som mer naturlig hører sammen, samlet innenfor hvert av disse hovedkapitlene. Man håper med dette å gjøre det enklere for leserne å bruke håndboka.

Kapittel A er en innledende redegjørelse for utgangspunktet for sikkerhetsarbeidet i SSB samt for rammene for virksomheten.

Kapittel B beskriver hvordan sikkerhetsarbeidet i SSB er organisert og plasserer ansvar for de forskjellige deler av sikkerhetsarbeidet.

Kapittel C omhandler reglene for behandling av personopplysninger som gjelder for SSB og tar for seg de bestemmelser og vilkår for behandling som følger av statistikkloven, personregisterloven og rammekonsesjonen fra Datatilsynet.

Kapittel D omhandler fysiske, IT-messige og prosedyremessige sikringstiltak som må gjelde for å sikre tilgjengelighet til opplysningene og den nødvendige konfidensialitet.

B
2. Sikkerhetsorgansisasjon, ansvar/oppgavefordeling

2.1. Instrukser for sikkerhetsansvarlige

Statistisk sentralbyrå samler inn og lagrer store mengder data om personer, foretak, organisasjoner og myndigheter. Det er etter statistikkloven og personregisterloven vårt ansvar at disse dataene blir effektivt utnyttet til statistikk og forskning og samtidig blir beskyttet slik at den enkelte oppgavegiver ikke blir skadelidende. Statistisk sentralbyrå har også et ansvar for at data som skal brukes i fremtiden blir arkivert på en forsvarlig måte.

Alle tilsatte i Statistisk sentralbyrå skal følge de regler og instrukser de blir pålagt av sine overordnede. Hver tilsatt har et eget ansvar for at taushetsbelagte opplysninger ikke blir gjort tilgjengelig for uvedkommende. Den som oppdager brudd på sikkerhetsregler eller mangelfull sikring av data skal melde dette til nærmeste overordnede eller til Sikkerhetsutvalget.

Administrerende direktør har det øverste ansvaret for sikkerheten i Statistisk sentralbyrå.

Sikkerhetsutvalget skal sørge for at Statistisk sentralbyrå holder en høy sikkerhetsstandard ved å utarbeide regler, retningslinjer og instrukser.

Avdelingslederne skal sørge for at seksjons- og gruppeledere kjenner og etterlever det regelverk som gjelder og at dette regelverket blir supplert etter behov med spesielle tiltak og instrukser i forståelse med Sikkerhetsutvalget.

Seksjonsledere og kontorsjefer skal sørge for at alle ved seksjonen/gruppa kjenner og etterlever det regelverket som gjelder for den enkeltes arbeidsområde og foreslå spesielle tiltak og instrukser for områder som er spesielle for seksjonen/gruppa.

Avdelingsleder

1. Avdelingslederen skal sette seg inn i alle lover, regler og instrukser for innsamling, lagring, behandling og utlevering av data som gjelder i Statistisk sentralbyrå, og som er aktuelle for egen avdeling.

   Dersom avdelingslederen mener det er behov for andre instrukser i tillegg til disse ved avdelingen, skal vedkommende ta initiativ til at slike blir utarbeidet og godkjent av Sikkerhetsutvalget.

2. Avdelingslederen skal gjøre alle ved avdelingen kjent med de lover, regler og instrukser som skal gjelde for den enkelte seksjon eller gruppe og påse at disse blir etterlevd.

3. Avdelingslederen er ansvarlig for at saker forelegges Sikkerhetsutvalget der hvor dette følger av gjeldende regelverk og instrukser.

4. Avdelingslederen skal sørge for klarering og autorisasjon av sitt personale.

5. Avdelingslederen skal i januar hvert år sende en melding til Sikkerhetsutvalget om sikkerhetsarbeidet ved avdelingen.

   Sikkerhetsrapporten skal dekke de områder avdelingsleder har ansvaret for. Ut fra dette skal rapporten minst gi opplysninger om følgende:
   - Hvem som har ansvaret for sikkerheten (inkl. gitte fullmakter) ved avdelingen.
   - Hvilke sikkerhetstiltak som er gjennomført i løpet av året, opplæring, nye instrukser mv.
   - Antall meldinger sendt til Datatilsynet.
   - Praksis ved utlevering av data i året som gikk.
   - Informasjon til nye medarbeidere - hva som blir gitt.
   - Kryptering av fødselsnummer - bruk av dette innen avdelingen.
   - Problemer som det arbeides med, opprydding i dataarkiv, nye instrukser mv.
   - Spesielle problemer som avdelingen trenger hjelp til.

6. Avdelingslederen er innenfor gjeldende regelverk ansvarlig for:

6.1. De registre avdelingen eier eller låner. Dette omfatter:
   - Gradering av egne registre.
   - Nødvendige konsesjoner fra Datatilsynet.
   - Melding til Datatilsynet i henhold til gitte konsesjoner.
   - Lagring av data.
   - Utlevering til interne og eksterne brukere av egne registre.
   - Kobling med andre registre.
   - Kryptering.
   - Sletting/makulering.
   - Eventuelle andre spesielle pålegg.
   - Behandle lånte registre etter eierens instruks.

6.2. Bruk og vedlikehold av eget frittstående teknisk utstyr og IT-utstyr (utstyr som ikke er koblet til lokalnett eller sentral stormaskin).

6.3. Fysisk sikkerhet i avdelingens lokaler og adgangskontroll til disse, se imidlertid punkt 9 nedenfor.

Ansvaret for dette kan avdelingslederen delegere til avdelingens seksjons- og kontorsjefer.

7. Avdelingslederen skal påse at avdelingen følger forsvarlige regler for publisering innenfor hvert statistikkområde ved avdelingen og at oppgavegiverne blir gjort kjent med at de kan kreve tall i Statistisk sentralbyrås tabeller undertrykket dersom det etter en nærmere vurdering viser seg at publisering er i strid med statistikkloven.

8. Avdelingsleder ved Administrasjonsavdelingen er hovedansvarlig for den fysiske sikkerheten i Statistisk sentralbyrås lokaler, kontroll av adgang til bygningene og for at retningslinjer og rutiner for makulering av sensitiv informasjon etterleves. Avdelingsleder ved administrasjonsavdelingen er videre ansvarlig for utlevering av nøkkelkort og adgangstegn.

9. Den avdelingsleder som administrerende direktør peker ut er ansvarlig for sikring av den sentrale databehandling og beskyttelse av det sentrale arkiv.

Juridisk rådgiver tilknyttet Sikkerhetsutvalget

- skal være SSBs rådgiver innen de fleste områder av sikkerhetsarbeidet
- skal forelegges alle vesentlige saker av sikkerhetsmessig art og skal kunne uttale seg om disse
- skal kunne møte i de fora der sikkerhetsspørsmål drøftes
- skal kunne veilede og orientere linjelederne i sikkerhetsspørsmål.

Seksjonssjef for Seksjon for IT-drift har det overordnete ansvaret for den daglige datasikkerheten i Statistisk sentralbyrå. Dette inkluderer bl.a. ansvar for systemprogrammering og driftsansvar for felles programvare og datamaskiner. Seksjonssjefen for IT-drift har også det overordnede ansvar for å holde à jour lese- og skrivetillatelser i sikkerhetsprogrammet og for at de er i samsvar med skriftlig ordre fra registeransvarlig.

Dataadministratoren, ved Seksjon for IT-drift, skal tildele registernummer og føre en journal over alle registre. Journalen skal vise hvem som eier registeret og hvilke restriksjoner som er lagt på registeret.

Dataadministrator skal sørge for at rutiner for kryptering av identifikasjonsnummer blir holdt ajour, tilfredsstillende beskrevet, og at informasjonen om bruken av rutinen er tilfredsstillende. Dataadministrator er videre ansvarlig for oppfølging av halvårlige rapporteringer til Datatilsynet i tråd med rammekonsesjonen.

Kontorsjefene ved IT-kontorene i avdelingene vil ha ansvar for datasikkerheten i avdelingen og for de edbrutiner som utvikles ved avdelingene og for tildeling av brukerprofiler for ansatte i IT-gruppa.

Sikkerhetsutvalget

1. Utvalget har en rapporterings- og orienteringsplikt overfor administrerende direktør i alle sikkerhetssaker. Utvalget skal hvert år utarbeide en rapport om sikkerhetsarbeidet i Statistisk sentralbyrå.

2. Utvalget er ansvarlig for at Statistisk sentralbyrå til enhver tid både har en tilfredsstillende edbsikkerhet og organisatorisk sikkerhet ved å utarbeide regler, retningslinjer og instrukser som:
   - Sikrer at datainnsamling, datalagring og datautlevering skjer i samsvar med de lover og forskrifter som gjelder slik at Statistisk sentralbyrås interesser ivaretas.
   - Regulerer sikkerheten og pålegger de ansatte og andre som befinner seg i Statistisk sentralbyrås lokaler ansvar og plikter.
   - Sørger for at arbeidet innen hver avdeling blir organisert på en slik måte at de sikkerhetsmessige hensyn blir ivaretatt.

3. Sikkerhetsutvalget møter i Statistisk sentralbyrås direktørmøter 2 ganger i året for å ta opp aktuelle sikkerhetsspørsmål. De aktuelle spørsmålene forutsettes behandlet i avdelingene på forhånd.

4. Sikkerhetsspørsmål skal settes opp som sak på minst ett Alledermøte i året etter forslag fra Sikkerhetsutvalget.

5. Sikkerhetsutvalget velger tilfeldig ut minst en seksjon i året til sikkerhetskontroll. Kontrollen gjennomføres av Sikkerhetsutvalget i samarbeid med IT-utvalget og dataadministrator. Etter kontrollen lages det en rapport som behandles i Direktørmøte.

6. Utvalget har ansvar for å holde à jour Statistisk sentralbyrås beredskapsplan.

7. Utvalget kan sette i gang sikkerhetstiltak etter godkjenning av administrerende direktør.

8. Statistisk sentralbyrås kontakt med Datatilsynet skal skje gjennom Sikkerhetsutvalget, unntatt rutinemessige meldinger om opprettelse av personregistre hvor Sikkerhetsutvalget har et tilsynsansvar.

Sikkerhetsutvalget oppnevnes av administrerende direktør og består av den i ledelsen som er tillagt politikk- og tilsynsansvaret for området, for tiden Johan-Kristian Tønder, lederen for IT-drift, for tiden Rune Gløersen, en av Administrasjonsavdelingens jurister, for tiden Mette Bredengen, og Sikkerhetsutvalgets sekretær, for tiden Britt Laberg.

C Behandling av personopplysninger/foretaks-opplysninger i statistikkproduksjon

3. Datainnsamling

3.1. Generelt

Selv om de regler og rutiner som er nevnt nedenfor relaterer seg til behandling av informasjon til statistikkproduksjonen, er det viktig å huske at Statistisk sentralbyrå også behandler mye informasjon også til andre formål.

Som eksempel nevnes lønns- og personalopplysninger om tilsatte i Statistisk sentralbyrå, økonomi- og budsjettopplysninger og korrespondanse med andre offentlige etater, bedrifter og enkeltpersoner.

For behandling av denne type informasjon vil mange av de samme retningslinjer og rutiner som nevnes nedenfor, i stor grad gjelde tilsvarende.

I Statistisk sentralbyrå er det nødvendig å gjøre mange unntak fra allmennhetens rett til innsyn i dokumenter mv. Primærdata og administrative data innhentet med hjemmel i statistikkloven og opplysninger innhentet på frivillig grunnlag, er i medhold av loven undergitt taushetsplikt.

Oppgavegiverne har ifølge loven krav på at opplysningene bare nyttes til utarbeiding av offisiell statistikk eller annen bruk godkjent av Datatilsynet, og at opplysningene ikke offentliggjøres slik at de kan spores tilbake til oppgavegiver eller annen identifiserbar enkeltperson til skade for denne (eller til *urimelig* skade for denne dersom oppgavegiveren er et foretak eller offentlig organ).

Opplysningene som blir gitt frivillig eller som blir samlet inn med hjemmel i andre lover, skal i denne sammenheng behandles som om de var samlet inn med hjemmel i statistikkloven.

Det er et generelt prinsipp for behandling av all informasjon som skal brukes i statistikkproduksjon at:

1. Det bare skal samles inn den informasjon det er behov for i statistikkproduksjonen.
2. Oppgavegiverne skal ikke identifiseres mer enn det er behov for på hvert trinn i produksjonen.
3. Sikkerhetsgradert informasjon som det ikke er behov for i statistikkproduksjonen skal fjernes så tidlig som mulig.
4. Informasjon som skal brukes, må sikres. Informasjon som ikke brukes, skal slettes.
5. Informasjonene skal ordnes i registre, og hvert register skal ha en ansvarlig eier.
6. Rutiner og informasjon skal dokumenteres på en fullstendig og oversiktlig måte.

For øvrig viser vi til publiseringshåndboka og SLo 18.12.96, Etablering av ny statistikk (se vedlegg H).

3.2. Hjemmel for datainnsamling mv.

Lov om personregistre m.m. av 9.6.78 nr. 48 og forskrifter fastsatt med hjemmel i denne samt SSBs rammekonsesjon for føring av personregistre av 11.11.97, inneholder bestemmelser som er av betydning for hvordan Statistisk sentralbyrå kan bruke den informasjonen som befinner seg i SSBs lokaler.

Personregisterloven pålegger enhver som ønsker å opprette et register for lagring av identifiserbare personopplysninger å innhente tillatelse (konsesjon) fra Datatilsynet.

Loven gir videre anvisning på generelle retningslinjer for enhver som er i befatning med personopplysninger, bl.a. presiseres den regel at identifiserbare personopplysninger bare skal lagres dersom det er en saklig begrunnelse for det og at sensitive personopplysninger, som helseopplysninger, opplysninger om seksuelle forhold, straffbare forhold m.m., bare skal registreres i den grad det er *nødvendig*. Personregisterloven stiller m.a.o. et sterkere behovskrav når det er snakk om sensitiv informasjon.

Disse krav vil stort sett være tilfredsstilt dersom opplysningene anses nødvendige for utarbeidelse av offisiell statistikk.

En strengere vurdering av sensitive opplysninger bør uansett, slik personregisterloven legger opp til, også være retningsgivende for Statistisk sentralbyrå i vurderingen av hva som er nødvendig å registrere/lagre i det enkelte tilfellet.

Slike sensitive opplysninger vil ofte være underlagt taushetsplikt i særlov. Det er da viktig å merke seg at det ved innhenting av slik informasjon vil være nødvendig med dispensasjon fra taushetsplikten fra det aktuelle fagdepartement.

For øvrig vil det alltid bli stilt strengere vilkår med hensyn til sikkerhet, oppbevaring og bruk av slik sensitiv informasjon.

Personopplysninger er opplysinger og vurderinger som direkte eller indirekte kan knyttes til identifiserbare enkeltpersoner, sammenslutninger eller stiftelser. Definisjonen omfatter således både fysiske personer (enkeltpersoner) og juridiske personer (foretak, selskap, AS, o.l.). For øvrig viser vi til Interne dokumenter 97/1 Hjemmel for datainnsamling.

3.3. Vedtak om bruk av lovhjemmel ved datainnsamling og ved bruk av tvangsmulkt

For alle data som SSB mottar, skal hjemmelsgrunnlaget gjøres klart for dataleverandør.

Datamottaket i SSB bygger på:
1. Hjemmel i statistikkloven § 2-2
2. Hjemmel i statistikkloven § 2-2 jf. § 3-2
3. Hjemmel i andre lover som gir SSB rett til å kreve opplysningene
4. Frivillig innsamling.

Det vises for øvrig til «Lovhjemmel ved datainnsamling». (Interne dokumenter 97/1.)

Oppgavegiverne skal ikke gis vederlag for å kunne oppfylle oppgaveplikten. Dette gjelder også for administrative data, jf. brev fra Finansdepartementet av 18.03.96 (saksnr. 96/309). Lovgiverne har imidlertid erkjent at det finnes en grense for hvor stor økonomisk belastning en oppgavegiver må tåle i denne sammenheng.

Vurderingen av hvor store kostnader en oppgavegiver kan påføres må foretas før beslutningen om bruk av oppgaveplikt tas. Som vurderingskriterier sies det i forarbeidene til statistikkloven (Innst. O nr. 97 1988/89 s. 3) at:
- Det skal tas hensyn til nødvendigheten av at opplysningene gis til SSB, men også til de omkostningene oppgavegiver pådrar seg i forbindelse med oppfyllelse av oppgaveplikten. Den samlede tidsbruk for oppgavegiverne skal anslås.
- Vurderingen skal foretas konkret i det enkelte tilfellet.
- Det skal i vurderingen også tas hensyn til «hva slags statistikk som er tilgjengelig for bedriftene og hvilken kvalitet statistikken har». Dette innebærer at selv om det vil være kostnadskrevende for en oppgavegiver å oppfylle oppgaveplikten, vil disse kostnadene tillegges redusert vekt dersom oppgavegiveren selv er bruker av statistikken og derved avhengig av at statistikken holder et høyt kvalitetsnivå.

Dersom omkostningene likevel blir for store, må alternativet til oppgaveplikt bli frivillig innlevering eller at undersøkelsen ikke gjennomføres.

Dette vil også til en viss grad kunne åpne for finansiering som skal kompensere for noe av oppgavegivernes kostnader ved å delta i en statistisk undersøkelse. En slik kompensasjon skal alltid godkjennes av administrerende direktør.

SSB har, med unntak av omfattende og ressurskrevende undersøkelser som krever særskilt budsjettbehandling i Stortinget, fått delegert myndigheten til selv å bestemme hva som skal lages av offisiell statistikk og hvilket grunnlag denne statistikken skal bygges på.

SSB må derfor konkret vurdere om de opplysninger den enkelte oppgavegiver blir bedt om å gi er nødvendige i forhold til formålet med undersøkelsen.

Oppgaveplikten er som omtalt i pkt. 3.2 begrenset av lovbestemt taushetsplikt. Statistikkloven eller forarbeidene til denne sier ellers lite om begrensninger i retten til å pålegge oppgaveplikt.

Det finnes imidlertid grenser for hva det kan spørres om, først og fremst av hensynet til diskresjon og urimelig inntrengen i den enkelte oppgavegivers private sfære. I praksis bør vi særskilt vurdere undersøkelser eller spørsmål som inneholder:
1. Vurderinger eller hypotetiske spørsmål (f.eks. konjunkturbarometeret).
2. Sensitive spørsmål (f.eks. politiske valg, seksualvaner, tidsbruk, helse, levekår mv.).
3. Undersøkelser/spørsmål som er særskilt tidkrevende og vanskelige.

Grensene mellom disse gruppene er ikke klare. Forbruksundersøkelsen i sin nåværende form er f.eks. særlig belastende og kan være sensitiv. For undersøkelser som faller inn under de to første gruppene, vil vi ikke bruke oppgaveplikt.

Vi bør også være noe tilbakeholdne med å pålegge oppgaveplikt for opplysninger om fremtidige planer. Men en vurdering av samfunnsnytten av f.eks. en statistikk over næringslivets investeringsplaner har resultert i innføring av oppgaveplikt for foretak til den kvartalsvise investeringsstatistikken.

I noen få tilfeller har vi i undersøkelser med oppgaveplikt tatt inn spørsmål som faller innen gruppe 1) eller 2), men markert at det er frivillig å svare på disse spørsmålene.

Vi bør unngå å ta med slike spørsmål i oppgavepliktige undersøkelser, men dersom det likevel gjøres må det tydelig oppgis hvilke spørsmål det ikke er oppgaveplikt for.

Innhenting av administrative data skal alltid baseres på oppgaveplikt med hjemmel i statistikkloven hvis ikke datainnhentingen er hjemlet i annen lov, (jf. begrensninger i særlov).

Statistikklovens §3-2 gir statistisk sentralbyrå rett til å utnytte administrative datasystemer i statsforvaltningen og landsomfattende kommunale organisasjoner som grunnlag for offisiell statistikk.

Med hjemmel i statistikkloven har derfor Statistisk sentralbyrå inngått avtale med de fleste aktuelle statlige forvaltningsorganer om utlevering av slike data, (jf. Rapport om bestemmelsene i statistikkloven om administrative data og samordning av statistikk. Status 31.12.1994 Planer og meldinger 9/95).

Disse avtalene med hjemmel i statistikklovens § 2-2, jf. §3-2 gir det formelle grunnlag for å be om overføring av slike data (jf. Forskrift om gjennomføring og utfylling av Statistikkloven, §1-2, fastsatt av Finansdepartementet 13.2.1990).

Det er ikke nødvendig med ytterligere godkjenning av administrerende direktør i forbindelse med overføring av data som er omfattet av en inngått avtale.

Dersom det ikke er inngått slik avtale mellom et statlig forvaltningsorgan og SSB, er det ikke tillatt å overføre data uten at det fattes særskilt vedtak av administrerende direktør. (For statlige forvaltningsorganer kan vi ikke pålegge tvangsmulkt, jf. delegeringsbrevet fra Finansdepartementet av 13.2.1990.)

Rutinene for vedtak om oppgaveplikt er beskrevet i Håndbok nr. 49 s. 9; «Oppgaveplikt og tvangsmulkt». Disse retningslinjene suppleres noe her.

For all statistikkproduksjon som skal baseres på ny direkte datainnsamling skal de respektive avdelinger vurdere om oppgaveplikt, med eller uten bruk av tvangsmulkt, skal benyttes. Statistikkloven hjemler altså grunnlag for å pålegge oppgaveplikt (§2-2).

SSB kan også med hjemmel i statistikkloven § 2-3 om nødvendig ilegge tvangsmulkt ved overskridelse av frist til å gi opplysninger. Oppgaveplikt kan altså vedtas både med og uten bruk av tvangsmulkt.

Avdelingens vurdering av bruk av oppgaveplikt skal dokumenteres skriftlig. Det samme gjelder ved større endringer i datainnsamling og når det er spørsmål om å innføre bruk av tvangsmulkt i tilfeller der det tidligere er fattet vedtak om oppgaveplikt uten bruk av tvangsmulkt.

Administrerende direktør fatter vedtak i Direktørmøte. Den skriftlige dokumentasjonen skal inneholde opplysninger om:

- Oppgavegivere.
- Hvilke data som skal samles inn (eventuelt med vedlegg for utfyllende informasjon).
- Bruk av dataene (med referanse til produkter i produktregisteret pluss eventuelle andre prosjekter).
- Begrunnelse for hvorfor det er ønskelig med oppgaveplikt, eventuelt bruk av tvangsmulkt.
- Finansiering av prosjektene dataene skal brukes til.
- Andre opplysninger som kan være av betydning for eventuelt vedtak (alternative datakilder jf. f.eks. oppgavepliktregisteret, bruk av andre data i tillegg til de som skal samles inn mv.).
- Forslag til vedtak av administrerende direktør.

Vedtak i saken tas inn i referat fra Direktørmøte sammen med eventuelle korrigeringer i saksdokumentene. Saksdokumentene og referatet fra Direktørmøtet oppbevares hos administrerende direktør.

Kopier av disse dokumentene skal også oppbevares av de seksjonene som foretar datainnsamlingen. Dokumentene med vedtak er ikke unntatt offentlighet. Vedtaket skal også registreres i produktregisteret. For øvrig henviser vi til SSH 49.

Kopi av vedtak om bruk av oppgaveplikt skal følge med den melding som sendes Datatilsynet.

3.4. Frivillige undersøkelser

Statistikkloven forutsetter at SSB kan innhente opplysninger på frivillig grunnlag. Det er således i rammekonsesjon fra Datatilsynet gitt tillatelse til å registrere opplysninger innhentet på frivillig grunnlag.

Når opplysninger innhentes på denne måten, gjelder det spesielle vilkår både med hensyn til den informasjon som gis til den enkelte og med hensyn til hvordan SSB kan bruke opplysningene.

Når intervjuundersøkelser eller oppgaveinnhenting er basert på samtykke fra den enkelte, er utgangspunktet at den bruk som i ettertid gjøres av opplysningene styres av det samtykket som er gitt, det vil si at SSBs rett til utnyttelse av opplysningene ikke går lenger enn hva den enkelte har gitt sitt samtykke til.

Det blir derfor avgjørende at den informasjon som gis så konkret som mulig beskriver hva SSB skal bruke opplysningene til. Dette innebærer også at det må informeres om hvorvidt opplysningene skal

kobles mot opplysninger i andre registre. (Se nærmere om dette i punkt 4.3.)

Når opplysninger innhentes på frivillig grunnlag, skal det alltid gjøres uttrykkelig oppmerksom på at den enkelte kan nekte å delta i vedkommende undersøkelse e.l. (rammekonsesjonens punkt 2.2).

SSBs praksis med å registrere opplysninger om personer som *ikke* samtykker til å delta, har vært kritisert av Datatilsynet. Grensene for hva som er tillatt er nå fastsatt i rammekonsesjonens pkt. 2.2 hvor hovedregelen er at registrering av frafallsårsak kun er tillatt der respondenten samtykker til slik registrering.

Frafallsårsak kan registreres i en av følgende grupper: intervjuobjektet indisponert, kommunikasjonsproblemer eller nekting. Dersom intervjuobjektet ikke treffes, kan dette registreres som «ingen kontakt med intervjuobjektet» eller «intervjuobjektet utilgjengelig».

3.5. Databehandling i Statistisk sentralbyrå som databehandlingsforetak

Dersom SSB bearbeider opplysninger på oppdrag fra andre offentlige etater eller private foretak, vil SSB etter personregisterloven kunne defineres som et databehandlingsforetak.

Databehandlingsvirksomhet er konsesjonspliktig virksomhet som reguleres av personregisterloven.

I den grad SSB mottar personregistre fra andre for å bearbeide personopplysninger etter oppdrag, vil slik virksomhet kunne være konsesjonspliktig databehandling. Personregisteret kan i så fall bare brukes til de formål og på den måte som oppdragsgiver bestemmer.

Det er usikkert i hvilken grad det er aktuelt for SSB å drive slik virksomhet. I forbindelse med ordinær oppdragsvirksomhet vil SSB alltid forbeholde seg retten til å publisere materialet som offisiell statistikk.

I de tilfellene der innhenting av opplysninger skjer med hjemmel i statistikkloven eller er basert på frivillighet fra den enkelte oppgavegiver, vil det være i strid med statistikkloven at oppdragsgiver avskjærer denne muligheten.

Dersom SSB mottar personregistre som et databehandlingsforetak, vil det ikke være nødvendig å bruke statistikkloven som hjemmel for innhentingen fordi en registereier lovlig kan utlevere et register til et foretak som har databehandlingskonsesjon.

3.6. Taushetsplikten

Statistikklovens § 2-4 pålegger taushetsplikt for ansatte i SSB når disse forbereder eller utarbeider offisiell statistikk. Dette gjelder opplysninger om personlige forhold, drifts- og forretningsforhold eller tekniske innretninger og fremgangsmåter.

I tillegg kan ansatte i SSB komme bort i informasjon som ikke har noe med statistikkproduksjon å gjøre, f.eks. personal- og budsjettopplysninger. I henhold til annen lovgivning (f.eks. forvaltningslovens § 13) vil det gjelde taushetsplikt også for denne type opplysninger.

Alt personale tilknyttet SSB skal derfor undertegne en egen taushetserklæring og gjøres kjent med det straffeansvar som følger av brudd på taushetsplikten, jf. statistikklovens § 5-1.

Når det gjelder innhenting av informasjon fra administrative registre i organ for stat og kommune, vil oppgavegiverens taushetsplikt som hovedregel ikke være til hinder for utlevering til SSB, jf. forvaltningslovens § 13b nr 4 ("opplysningene kan brukes for statistisk bearbeiding").

Unntak gjelder der taushetsplikt er fastsatt i særlov (f.eks. legelovens eller tannlegelovens § 31).

Det er også utarbeidet en taushetserklæring som må underskrives av personer med annen tilknytning til SSB enn ansettelseskontrakt, som i deres arbeid kan komme bort i taushetsbelagt informasjon.

Eksempler på ulike tilknytningsforbindelser i denne sammenheng kan være at en person:

- Er medlem av et utvalg tilknyttet SSB.
- Er deltaker i et internt prosjekt.
- Har konkret tilgang til opplysninger i forbindelse med eksterne prosjekter.
- Har tilgang til utstyr som kan inneholde taushetsbelagt informasjon (reparasjons- og servicepersonale).

Taushetserklæringen pålegger alle ansatte i SSB og andre med tilknytning til SSB, å vise aktsomhet i behandlingen av alle opplysninger som SSB henter inn.

Taushetsplikten gjelder overfor uvedkommende; det vil si også overfor andre personer i SSB som ikke har behov for å kjenne til en bestemt type informasjon i sitt arbeide. Personopplysninger skal ikke spres unødig. Det gjelder et "need to know"-prinsipp internt i SSB.

Opplysninger som av hensyn til offentlige, enkeltpersoners, institusjoners eller bedrifters interesser er å anse som fortrolige må ikke gjøres kjent for andre.

Alle blir også pålagt ikke å gi opplysninger om resultater av statistiske undersøkelser før SSB har frigitt dem til offentliggjøring.

Taushetsplikten gjelder også etter at man har sluttet i SSB eller oppdraget for SSB er ferdig utført. For opplysninger til bruk for statistikk gjelder taushetsplikten i 100 år for opplysninger om personlige forhold, og i 60 år for opplysninger om drifts- eller forretningsforhold.

3.7. Personregister

Personregistre er registre, fortegnelser m.m. der personopplysninger, dvs. opplysninger både om fysiske og juridiske personer, er lagret systematisk slik at opplysninger om den enkelte kan finnes igjen.

Det vil således alltid være et personregister dersom opplysningene er knyttet til fødselsnummer eller andre direkte identifiserende kjennetegn. Hva som er identifiserende må vurderes i forbindelse med det enkelte register.

Desto flere opplysninger om den enkelte et register inneholder, jo større er muligheten for identifikasjon. Summen av en rekke opplysninger vil kunne gjøre det mulig å identifisere en person selv om hverken fødselsnummer, fødselsdato eller navn er registrert.

I et avidentifisert register er navn, fødselsnummer eller andre direkte kjennetegn fjernet.

Et avidentifisert register vil kunne være et personregister dersom det til tross for avidentifiseringen kan «bakveisidentifiseres», dvs. at det er mulig å identifisere den enkelte på bakgrunn av de opplysninger som er gitt. Først når slik indirekte identifikasjon ikke er mulig (i hvert fall uforholdsmessig vanskelig), vil man kunne definere registeret som anonymt. Et anonymt register er pr. definisjon ikke et *person*register.

Det er derfor viktig å skille mellom avidentifiserte og anonymiserte registre (se også pkt. 7.3). Et avidentifisert register som ikke er tilstrekkelig anonymisert, er underlagt personregisterlovens bestemmelser.

Et tilstrekkelig anonymisert register faller utenfor disse bestemmelsene da det ikke regnes som et personregister.

Et kryptert register vil imidlertid alltid regnes for et personregister dersom registereier (se pkt. 3.8) sitter med krypteringsnøkkelen.

Det som er sagt om avidentifiserte registre vil også gjelde for krypterte registre med hensyn til hvorvidt det er tilstrekkelig anonymisert.

Det kreves som hovedregel samtykke (konsesjon) for å opprette personregister som skal gjøre bruk av elektroniske hjelpemidler.

Samtykke kreves også for å opprette manuelle personregistre dersom de skal inneholde opplysninger om rase, politisk eller religiøs oppfatning, helseforhold, misbruk av rusmidler, seksuelle forhold eller andre opplysninger om familieforhold enn slike som gjelder slektskap og familiestatus, formuesordningen mellom ektefeller og forsørgelsesbyrde.

For opplysninger samlet inn til bruk i statistikkproduksjon og annen nærmere angitt bruk godkjent av Datatilsynet med hjemmel i statistikkloven § 2-5 (spesifisert i SSBs rammekonsesjon, se vedlegg 1), behøves det imidlertid ikke å søke om konsesjon. Det skal i stedet sendes en melding om opprettelse av nytt/endring i allerede meldt register. Se pkt. 5.3 nedenfor for nærmere veiledning.

Hva er et register i Statistisk sentralbyrå?
Presisering av hva som er **ett** personregister har størst betydning for informasjon som skal brukes i statistikkproduksjonen. Dette fordi de fleste administrative registre til bruk internt i Statistisk sentralbyrå stort sett er unntatt fra konsesjonsplikten, se også nedenfor under punkt. 5.7.

Det er nødvendig å ha et godt register over alle oppgavegivere, dvs alle enheter som statistikken skal omfatte. Disse enhetene er personer og foretak. Offentlige myndigheter, foreninger osv. oppfattes her som foretak.

Det følger av definisjonen av et personregister at det kan bli vanskelig å avgrense registrene i Statistisk sentralbyrå. Det må derfor stilles tilleggsvilkår slik at registerbegrepet og konsesjonssystemet gir mening.

En samling opplysninger hvor den enkelte person/foretak/bedrift m.m. kan gjenfinnes må tilfredsstille følgende vilkår (alle må være oppfylt) for å kunne regnes som **ett** personregister:

1. Enhetene opplysningene gjelder er definert på samme måte.
2. Enhetene er identifiserbare ved samme identifikasjonssystem, f.eks. ved bruk av fødselsnummer/organisasjonsnummer.
3. Personopplysningene er standardiserte, dvs. at de enkelte kjennemerker som inngår i materialet må være definert og klassifisert på en ensartet måte.

Enkeltkjennemerker som refererer til ulike tidspunkter eller perioder, vil i denne sammenheng oppfattes som forskjellige kjennemerker.
4. Det faglige ansvar for lagring, oppdatering og bruk av data kan legges til en og samme administrative enhet.

Dersom ett eller flere punkter ikke er oppfylt, må samlingen av opplysninger deles i flere registre.

En rekke typer personregistre til ulike formål er unntatt konsesjonsplikt. Personregisterlovens forskrifter, kapittel 2, konkretiserer hvilke registre dette er.

Det er viktig å merke seg at forskriftene er uttømmende, dvs. registrene kan bare inneholde de nevnte opplysninger og kan bare brukes til de nevnte formål for å kunne være unntatt konsesjonsplikt.

Viktige unntak for SSB er registre over nåværende eller tidligere ansatte, bibliotekets låneregister og kunde-, abonnent- og leverandørregistre.

3.8. Plikter pålagt den registeransvarlige i Statistisk sentralbyrå

SSB defineres som registereier. Leder i sikkerhetsutvalget er i rammekonsesjonen oppnevnt som registeransvarlig generelt for alle SSBs registre. Dette ansvaret vil i praksis kunne delegeres til den enkelte avdeling/seksjon som oppretter registeret. Den som har fått delegert registeransvar må påse følgende:

- At melding om opprettelse og endring av personregister blir utarbeidet i tråd med rammekonsesjon fra Datatilsynet, behandlet i SSBs ledelse og sendt Datatilsynet.
- Ha ansvaret for de datasettene/opplysningene som et register til enhver tid består av.
- Avgjøre hvem som skal gis tilgang til datasett/opplysninger. Tilsatte ved den enkelte enhet skal bare gis tilgang til de datasett/opplysninger vedkommende har et tjenestemessig behov for.
- Ved ansettelse av nye personer orientere om hvilke data/opplysninger som er undergitt taushetsplikt, og betydningen av at taushetsplikten overholdes.
- Være ansvarlig for at det ved den enkelte avdeling/seksjon/gruppe etableres regler og rutiner for behandling av data gradert høyere enn FORTROLIG og BEGRENSET, jf. nedenfor under pkt. 9.5.

3.9. Rutiner ved søknad/melding om konsesjon

Hvordan melde registre?

SSBs rammekonsesjon har fastsatt rammen for hva slags type registre SSB kan ha, hvordan informasjon skal samles inn, oppbevares og brukes. Datatilsynet har imidlertid innenfor rammekonsesjonen et system hvor nye registre/endringer i tidligere etablerte registre skal *meldes* før opplysninger kan samles inn og lagres.

Disse meldingene skal skje på et fastsatt skjema, jf. vedlegg B. Praksis har vist at disse meldingene har blitt behandlet som ordinære søknader om konsesjon, noe som bl.a. innebærer at innholdet av disse meldingsskjemaene blir viktige.

Etter revisjonen av rammekonsesjonen (konsesjon av 11.11.97) har omfanget av meldeplikten blitt redusert. Det er nå kun to kategorier registre som skal meldes fortløpende:
1. Opprettelse/endring av personregistre som inneholder sensitive personopplysninger.
2. Opprettelse/endring av personregistre der opplysningene er innhentet på frivillig grunnlag. Slike registre er meldepliktige selv om de ikke inneholder sensitive personopplysninger.

Meldingen skal inneholde kopi av eventuelt vedtak om bruk av oppgaveplikt.

Disse to ovennevnte registertyper er skilt ut for at Datatilsynet skal kunne kontrollere at innhentingen av opplysningene er lovlig før konsesjon kan gis. Ved innhenting av sensitive opplysninger vil Datatilsynet kontrollere hvorvidt det foreligger lovbestemt taushetsplikt som kan være til hinder for innhenting av opplysningene.

Ved innhenting av opplysninger gitt på frivillig grunnlag, reguleres innhentingen av respondentens samtykke. Datatilsynet ønsker i den forbindelse å kontrollere at det avgitte samtykket er reelt. Dette vil gjøres ved at Datatilsynet gjennomgår den informasjon som gis respondenten i forbindelse med gjennomføring av undersøkelsen.

I tillegg til meldeplikt for de ovennevnte registre er det fastsatt at det hvert halvår skal sendes en oversikt til Datatilsynet med en kortfattet melding for *alle* registre som er opprettet i SSB de siste seks måneder. Dette vil da også gjelde de registre som hverken inneholder sensitive personopplysninger eller er innhentet på frivillig grunnlag. Også de registre som allerede er meldt skal omfattes av disse halvårlige meldingene.

Innenfor de regler rammekonsesjonen setter og utfra det som her er sagt om hva som er et personregister i SSB, er det fortsatt stor frihet i forhold til hva som skal meldes som *ett* register til Datatilsynet. Følgende regler kan imidlertid legges til grunn for de meldinger som skal sendes:

- Det skal ikke meldes unødig mange registre, dvs. en melding skal alltid dekke minst det omfang og

det datainnhold registret skal ha.

- Når det meldes et nytt register og det regnes som sikkert at det nye registeret vil bli koblet med et eksisterende eller fremtidig register, skal det sendes *en* melding som dekker de registrene som vil bli koblet. Meldingen om registre som inngikk i koblingen skal da tilbakekalles.
- En database som inneholder data fra to eller flere registre, skal meldes som et nytt register. Denne meldingen bør være så omfattende at den dekker de tidligere meldingene.
- Dersom datainnsamlingen utvides, må den registeransvarlige sørge for at det sendes en endringsmelding eller melding om nytt register til Datatilsynet. Dersom to eller flere tidligere meldte registre blir koblet til et register, og disse ikke skal oppbevares med kryptert identifikasjon, skal det nye registeret alltid meldes til Datatilsynet som nytt register. Meldingen om de registre som inngikk i koblingen skal da tilbakekalles.

4. Databearbeiding

4.1. Generelt

Statistikkloven hjemler SSBs adgang til å samle inn opplysninger som er nødvendige for å utarbeide offisiell statistikk. De personregistre som opprettes som en følge av oppgave-/datainnhenting er i hovedsak konsesjonspliktige, hvilket innebærer at enhver bruk av registrene må reguleres i konsesjon.

Således vil også den kobling som foretas mellom to eller flere registre måtte meldes til Datatilsynet dersom koblingen resulterer i et nytt register eller det blir tilført nye typer opplysninger i personregister som kobles. Dette kan gjøres ved at det ved innmeldingen av et nyopprettet register kan oppgis hvilke andre registre/opplysninger det ev. skal kobles med, eller det må meldes fra dersom det er aktuelt å koble to eller flere registre som det hver for seg er sendt melding om tidligere.

Meldeplikten ved kobling gjelder kun dersom det i utgangspunktet dreier som om registre som er meldepliktige. Koblinger som resulterer i statistikk og/eller koblinger med anonymt resultat, er ikke meldepliktige koblinger etter konsesjonen

4.2. Koblinger av data som er samlet inn med hjemmel i statistikkloven

Slike koblinger må meldes, slik det er beskrevet i punkt 4.1, dersom koblingen medfører at det oppstår et nytt register (at et register blir tilført nye opplysningstyper), og dersom det nye registeret inneholder sensitive personopplysninger. Dersom det ikke inneholder sensitive personopplysninger, skal registeret kun oppgis i de halvårlige meldingene.

Ifølge rammekonsesjonens punkt 2.6.1 kan opplysninger som er innhentet etter pålagt oppgaveplikt (inkludert administrative registre i det offentlige), kobles med SSBs egne eller andres registre.

Rammekonsesjonen setter som vilkår at slik kobling må være nødvendig for å gjennomføre de oppgaver SSB er pålagt etter statistikkloven.

4.3. Koblinger av frivillige undersøkelser med andre data

Det følger av frivillighetsprinsippet (som omtales under punkt 3.6) at det for opplysninger innhentet på frivillig grunnlag må kreves samtykke fra den enkelte registrerte før kobling kan finne sted.

Datatilsynet setter vilkår i rammekonsesjonens punkt 2.6.2 om at registre inneholdende opplysninger innhentet på frivillig grunnlag krever særskilt samtykke fra den registrerte.

Datatilsynet har gitt uttrykk for at det ikke vil være tilstrekkelig å informere generelt om at opplysningene som innhentes vil kunne bli koblet med *andre opplysninger*. Det kreves en mer konkret angivelse av hvilke registre eller hvilke typer registre det vil bli koblet mot. Også kobling av krypterte registre krever respondentens særskilte samtykke.

Hvorvidt det skal angis type register, navn på register, hvor opplysningene er hentet fra eller navn på registereier (f.eks. i de tilfellene det skal kobles mot administrative registre som er innhentet med hjemmel i statistikkloven), vil måtte vurderes i forbindelse med den enkelte undersøkelse og vil bl.a. avhenge av hva som er mest informativt. Ved tvil skal spørsmålet forelegges Sikkerhetsutvalget.

4.4. Kryptering av fødselsnummer, rutiner

Om kryptering av fødselsnummer og begrunnelse for dette

Krypteringen bidrar til avidentifisering av dataene og styrker derved vårt datavern. Kryptering kan være et alternativ til anonymisering (total fjerning av alle kjennetegn, S-nr. og K-nr.) som vil kunne avskjære SSBs mulighet til fremtidig kobling. Der fremtidig kobling helt klart ikke er aktuelt, bør imidlertid registeret anonymiseres.

Kryptering av personregistre i Statistisk sentralbyrå innebærer at fødselsnummeret blir erstattet av et informasjonsfritt og permanent nummer (K-nummer) som fremkommer ved å bruke spesielle krypteringsnøkler.

Før dette kan skje, må imidlertid fødselsnummeret gjøres om til et nummer (S-nummer) som er permanent knyttet til en person selv om fødselsnummeret skifter.

Formålet med kryptering er å:

- bygge opp beredskap for statistikkproduksjonen fordi det ofte vil være behov for å ta vare på muligheten for kobling av data fra ulike tidsperioder. Dersom fødselsnummer er koblingsnøkkelen, vil kobling være vanskelig, og ved å kryptere vil Statistisk sentralbyrå dessuten kunne bygge opp en høyere beredskap for tilfeldige oppdrag der det er behov for det.

Det er nedenfor gitt utfyllende informasjon om de mer tekniske sider av krypteringsrutinene.

Interne rutiner
Informasjon om kryptering fås hos Statistisk sentralbyrås dataadministrator. For øvrig gjelder følgende rutiner:

- Den registeransvarlige fyller ut krypteringsblanketten med blant annet forslag til hvilken krypteringsserie som skal nyttes, registernummer, filidentifikasjon på input og output, størrelsen på fila og startposisjoner for Snr./Knr.
- Krypteringsblanketten sendes Statistisk sentralbyrås dataadministrator som fastlegger krypteringsserien.
- Dataadministrator kaller inn de to krypteringsoperatørene, som er ansvarlige for hver sin del av krypteringsnøkkelen, og kjører krypteringen.
- Krypteringsblanketten signeres av Dataadministrator og krypteringsoperatørene og returneres den registeransvarlige sammen med utskrift fra krypteringskjøringen.
- Den registeransvarlige sørger for at en medarbeider som kjenner registeret kontrollerer innholdet i det krypterte registeret og bekrefter at bare det datainnholdet som skal være med har kommet med, og at det ikke inneholder noen form for identifikasjon.
- Den registeransvarlige kontrollerer at det krypterte registeret inneholder riktig antall records, at det er katalogisert på riktig fil-ident, bekrefter at register med fødselsnummer er slettet, signerer krypteringsblanketten og sender kopi av blanketten til dataadministrator.

Dekryptering av K-nr. til S-nr.
Den nøkkelen, og bare den, som ble brukt ved krypteringen kan brukes til å komme tilbake til S-nr. ved å bruke programmet for dekryptering. Det skal egentlig ikke være noe behov for å bruke dette programmet. Det kan betraktes som en beredskap i tilfelle et uforutsett behov skulle dukke opp. Dekryptering skal godkjennes av administrerende direktør.

Omkryptering
Ved kryptering fra S-nr. til K-nr. skal registre som det ikke er behov for å koble gis forskjellig krypteringsserie. Dersom det senere skulle vise seg nødvendig å koble registre fra forskjellige serier, kan programmet for omkryptering brukes for å flytte et register fra en serie til en annen uten å gå veien om S-nr. ved en dekryptering. Begge sett med nøkler må brukes ved en omkryptering.

Omkryptering vil også være aktuelt dersom krypteringsnøkkelen er blitt kjent eller K-nr. for deler av registeret er avdekket ved bakveisidentifisering. Etter en slik omkryptering skal de første nøklene slettes. Omkryptering skal godkjennes av administrerende direktør.

Hvor anonymt er et kryptert register?
Risikoen for at krypteringen blir brutt ved analyse av tilgjengelige K-nr. må regnes som liten da det er en rent tilfeldig sammenheng mellom S-nr. og K.nr. Krypteringsnøkkelen er delt i to deler som oppbevares av to personer på forskjellige steder. Dette gir stor sikkerhet mot at nøkkelen kommer på avveie. Men kryptering er aldri sikrere enn en avidentifisering, dvs. fjerning av fødselsnummer.

Det vil kunne være mulig med bakveisidentifikasjon, dvs. identifisering av personer gjennom andre data i registeret.

Statistisk sentralbyrå har oversikt over hvilke registre hver bruker har adgang til. Registereier har ansvar for å påse at registre som ikke er kryptert brukes sammen med krypterte registre på en slik måte at bakveisidentifikasjon ikke kan finne sted.

5. Datalagring

5.1. Lagring med identifikasjon

Det er et generelt personvernprinsipp at innhenting og registrering av personopplysninger bare skal skje i den grad man har saklig behov for det, eller i den grad det er nødvendig forsåvidt gjelder sensitive opplysninger. Datatilsynet har i rammekonsesjonen (punkt 2.5) derfor inntatt et vilkår om at opplysninger som ikke lenger har betydning for formålet skal slettes eller anonymiseres. Anonymisering likestilles her med sletting.

Som hovedregel bør personopplysninger kun oppbevares med full identitet i den grad det er absolutt nødvendig for utarbeidelse av statistikk. Dersom personopplysningene ikke lenger er aktuelle for utarbeiding av offisiell statistikk og opplysningene ikke slettes, skal det vurderes hvorvidt personopplysningene bør anonymiseres.

Det ble i ny rammekonsesjon av 11.11.97 satt vilkår om at registrene skal anonymiseres snarest mulig og senest innen ett år dersom ikke navn, fødselsnummer eller annen personidentifikasjon blir erstattet med kryptert nummer. Datatilsynet kan fastsette lengre oppbevaringstid i forbindelse med den enkelte melding.

Selv om det skulle være på det rene at et register vil kunne slettes utfra en behovsvurdering i SSB, vil det imidlertid være nødvendig først å avklare hvorvidt det eksisterer plikt eller anledning til å overføre registeret til Riksarkivet (jf. punkt 5.3).

5.2. Lagring med kryptert identifikasjon

Dersom det ikke er absolutt nødvendig å lagre personopplysninger med full identitet, skal opplysningene krypteres. (Se punkt 4.4; kryptering, rutiner.) Innen ett år skal registrene som hovedregel anonymiseres eller slettes dersom de ikke krypteres.

Hvorvidt personopplysninger er lagret med full identitet eller er kryptert, vil kunne ha betydning for hvilke sikringstiltak som anses nødvendige. Det vil også kunne være avgjørende for hvorvidt SSB får godkjent løsninger for ekstern kommunikasjon hvor godt "beskyttet" personopplysninger lagres.

Det er for øvrig som hovedregel et krav at elektronisk overføring av personopplysninger skal skje kryptert, hvilket f.eks. vil gjelde for overføring mellom Oslo og Kongsvinger.

5.3. Overlevering til Riksarkivet

Spørsmålet om avlevering av personopplysninger til Riksarkivet har lenge vært og er fortsatt pr. i dag uavklart, idet det er vedtatt ny arkivlov som foreløpig ikke har trådt i kraft på grunn av manglende forskrifter.

I henhold til Datatilsynets rammekonsesjon punkt 2.5 vil derfor krav til sletting/anonymisering måtte utstå inntil forholdet til Riksarkivet er avklart.

Det er etter dagens arkivlov anledning til å *deponere* registre hos Riksarkivet, hvilket innebærer en slag fjernarkivering hvor den som avleverer materialet fortsatt har råderetten over det. Slik avlevering vil kunne være et midlertidig alternativ for SSB i de tilfellene man ønsker å slette/anonymisere et register.

Det vil også kunne være et alternativ til "intern fjernlagring". Dersom registre overføres til Riksarkivet, vil det fortsatt gjelde taushetsplikt etter statistikkloven, samtidig som de vilkår som er satt i rammekonsesjonen når det gjelder utlevering til forskning og planlegging, vil gjelde.

Denne fremgangsmåten bør imidlertid bare benyttes unntaksvis idet man ved fysisk å skille seg med materialet nødvendigvis også i praksis gir fra seg kontrollen med sikringstiltak.

6. Offentliggjøring av statistikk

6.1. Offentliggjøring av statistikk

Statistikklovens § 2-6 omhandler offentliggjøring av statistikk. Opplysninger skal ikke i noe tilfelle offentliggjøres slik at de kan føres tilbake til oppgavegiver eller annen identifiserbar enkeltperson til skade for denne, eller til urimelig skade for denne dersom oppgavegiveren eller enkeltpersonen er et foretak som nevnt i § 5-1 tredje ledd (selskap med begrenset ansvar, et kommandittselskap eller annen sammenslutning eller en stiftelse) eller en offentlig virksomhet.

Loven skiller altså mellom fysisk person og juridisk person/offentlig virksomhet når det gjelder krav til anonymisering.

Statistikk blir gjort tilgjengelig i form av aggregerte størrelser, slik at de opplysninger som gis karakteriserer massen av oppgavegivere, og ikke de enkelte i den forstand at de kan identifiseres. Det kan likevel tenkes tilfeller hvor det, f.eks. av hensyn til en hensiktsmessig oppbygging av statistikken, vil være vanskelig å unngå at enkelte opplysninger indirekte kan føres tilbake til den enkelte oppgavegiver.

Det vil imidlertid ikke være adgang til å offentliggjøre offisiell statistikk slik at opplysninger kan føres tilbake til oppgavegiver eller annen identifiserbar enkeltperson (fysisk person) dersom dette er til skade for denne.

Dersom oppgavene gjelder juridiske personer eller offentlig virksomhet, sier loven imidlertid at opplysningene ikke må gjøre urimelig skade. Det er her tenkt på tilfeller hvor offentliggjøring er lite betenkelig, opplysningene kan være offentlig tilgjengelig, f.eks. regnskapsopplysningene i et aksjeselskap.

Det kan dessuten være tilfeller der en avveining mellom motstridende interesser faller slik ut at offentliggjøring bør skje, til tross for at dette kan være ubehagelig for oppgavegiver. Er interessene og hensynene som taler for offentliggjøring overveiende, kan oppgavegiverens interesse måtte vike. Det er likevel forutsatt at dette bare skjer dersom det ikke er til urimelig skade.

Loven pålegger oss å være særlig påpasselig med offentliggjøring av opplysninger om fysiske personer. Her må vi forvisse oss om at opplysningene ikke er til skade for den enkelte dersom indirekte informasjon er mulig. For juridiske personer/offentlig virksomhet gir loven adgang til å vurdere samfunnsnytten av offentliggjøring av opplysninger mot graden av skade publiseringen forårsaker.

Hva denne rettslige standard innebærer vil avhenge av opplysningenes karakter. Det vil være av særlig betydning, men ikke avgjørende, om oppgavegiver (og den opplysningene gjelder, dersom dette er en annen) samtykker i offentliggjøring av opplysningene.

Ovennevnte lovregel fører til at SSB vanligvis ikke publiserer tabeller med mindre enn tre enheter i en gruppe (tabellcelle). En befolkningstabell for en kommune må f.eks. kunne vise folketallet fordelt på geografisk område og kjønn selv om antall enheter skulle komme ned under tre i få områder.

Tilsvarende må vi kunne offentliggjøre at det er 0-2 bedrifter i en næring i en kommune, men i utgangspunktet ikke ytterligere spesifikasjoner for disse cellene med så få antall bedrifter.

Det er viktig å passe på at opplysninger for grupper med mindre enn tre enheter ikke kan avleses indirekte av aggregater i tabellverket. Det er f.eks. ikke noen hensikt å prikke ut tallet bare i en celle dersom det kan avleses ved å beregne det ut fra et aggregat i tabellen.

Innen de forskjellige statistikkområder har det i samråd med brukerne utviklet seg prioriteringer ved undertrykkinger i tabellverkene. I næringsstatistikken kan en f.eks. velge å beholde hovedtall for en næringsgruppe, men gi avkall på detaljert gruppering etter størrelse, geografi m.v.

I næringsstatistikken finnes det avvik fra hovedregelen om tre enheter i en gruppe. I en bedriftstabell vil en tabellcelle måtte inneholde bedrifter i minst tre foretak for å opprettholde ovennevnte sikkerhet med tre enheter.

Det samme gjøres f.eks. i tabell over vareproduksjonen i industrien. Produksjonsopplysninger om en vare kan ikke offentliggjøres uten at denne er produsert i minst tre foretak.

I utenrikshandelstatistikken praktiseres ikke uten videre denne regel med publisering uten at det minst er tre importører/eksportører. Her undertrykkes tallene bare i de tilfeller en næringsdrivende har hevdet at offentliggjøring av opplysninger vil være til urimelig skade for vedkommende. SSB har hittil akseptert den enkeltes egen vurdering.

For å vanskeliggjøre gjenkjenning kreves at summen av kjennemerker (f.eks. lønnssum) i bedriftene i et foretak ikke utgjør 90 prosent eller mer av

totalsummen for gruppen. Har f.eks. et foretak 90 prosent av lønnssummen i en næring i et fylke, skal tall for denne gruppen i utgangspunktet ikke offentliggjøres.

Videre praktiserer vi den regelen at vi ikke offentliggjør tall dersom de to største enhetene (foretakene) til sammen har minst 95 prosent av totalsummen.

I noen tilfeller har SSB innhentet samtykke fra enheter om å offentliggjøre statistikk som støter an mot disse reglene. Mange av disse tilfeller gjelder opplysninger for store foretak. Selv om lovreglene gir hjemmel for publisering så fremt det ikke kan påvises urimelig skade, bør eventuell publisering som vedkommende setter seg i mot, vurderes meget nøye.

7. Utlevering av individualopplysninger/mikrodata

7.1. Den enkeltes innsynsrett i SSBs personregistre

Den enkeltes innsynsrett, dvs. retten til å få vite hva som er registrert om en selv i et register, er en sentral rettighet i personvernsammenheng. Denne rettigheten er hjemlet i personregisterlovens § 7.

Av bestemmelsens første ledd fremgår at «alle har rett til å få vite hvilke opplysninger om dem selv som lagres eller bearbeides ved elektroniske hjelpemidler».

For SSBs virksomhet er det her særlig viktig å merke seg den begrensning som er gjort i innsynsretten forsåvidt gjelder registre som kun benyttes til *statistikk*, forskning eller planleggingsformål.

Begrunnelsen for dette er at slike registre ikke blir brukt til å fatte enkeltvedtak og at det også vil kunne være vanskelig å trekke ut opplysninger som gjelder den enkelte.

Statistisk sentralbyrå har imidlertid plikt til på forespørsel å informere om hvilke personregistre vi har. På grunnlag av denne informasjonen kan publikum få kunnskap om i hvilke registre de kan være registrert, men de vil ikke få informasjon om hva som står om dem i registrene.

Hvordan innsyn etter personregisterloven skal gis

I forskrift til personregisterloven av 21. des. 1979 nr 22 er det gitt en del bestemmelser om hvordan innsyn skal gis. Det gjelder ikke generell innsynsrett for SSBs registre, men det vil gjelde innsynsrett for SSBs egne ansatte i f.eks. lønns- og personalregisteret.

Ut fra rent praktiske grunner oppstilles et krav om skriftlighet. Forsåvidt gjelder identifikasjon av det register det ønskes innsyn i er det tilstrekkelig å rette en henvendelse til det organ som er registereier, uten at noen nærmere spesifisering anses for påkrevet.

Når det gjelder identifikasjon av den registrerte selv, er det her opp til den enkelte registereier å utforme interne retningslinjer, herunder påse at taushetsplikten og andre regler overholdes slik at opplysninger ikke utleveres til uvedkommende.

Svar på henvendelse skal ifølge forskriftens § 1-1 som hovedregel gis skriftlig, snarest mulig og senest innen en måned.

Formen må også være slik at den er forståelig for mottaker ut i fra dennes forutsetninger. Forsåvidt gjelder de manuelle registrene bestemmer her registeransvarlig, ut i fra hensynet til forsvarlig saksbehandling, hvordan opplysningene skal gjøres tilgjengelige. På anmodning skal svar gis skriftlig i form av utskrift eller avskrift.

Forsåvidt gjelder forespørsel om typer av opplysninger skal disse besvares umiddelbart. Dette følger av forskriftens § 1-3. Rent praktisk bør man her ha lister over dette liggende klart.

Avslutningsvis nevnes at avgjørelse som går på om innsynsrett skal gis eller ikke er et enkeltvedtak som kan påklages etter forvaltningslovens regler.

7.2. Offentlighetens rett til innsyn

Av § 2 i lov 19.6.70 nr 69 om offentlighet i forvaltningen fremgår at *forvaltningens saksdokumenter* er offentlige så langt det ikke er gjort unntak i lov eller medhold av lov og at enhver hos vedkommende forvaltningsorgan kan kreve å få gjøre seg kjent med det offentlige innholdet i en bestemt sak.

Innsynsretten gjelder sakens dokumenter og i den forbindelse må ikke begrepet dokument tolkes snevert. Som dokument regnes brev, uttalelser, journaler, registre, utskrifter, kart, skisser, fotografier og ellers alt som er relevant for den saken man ber om innsyn i. Forsåvidt gjelder dokumentbegrepets anvendelse på elektronisk lagret materiell vises til det som er sagt ovenfor under pkt. 7.1.

Man bør merke seg at begrensningene i offentlighetens innsynsrett til dels er vesentlige som følge av de mange lovfestede unntak som er gjort, ikke minst i **offentlighetsloven** selv. En annen begrensning kan følge av det faktum at man for å få innsyn må kunne identifisere den aktuelle sak man ønsker innsyn i; innsynsretten gjelder i en bestemt sak.

Nærmere om unntakene fra offentlighetsloven

Offentlighetslovens §§ 5, 5a og 6 har bestemmelser som sier hva som kan unntas fra offentlighet. Det er i den forbindelse viktig og merke seg skillet mellom dokumenter og opplysninger.

I noen tilfeller kan det derfor være slik at det er visse typer av opplysninger som kan unntas, mens dokumentet for øvrig er offentlig, med mindre disse deler alene vil gi et åpenbart misvisende bilde av innholdet eller de unntatte opplysninger utgjør den vesentligste del av dokumentets innhold, jf. § 5a annet

ledd. Jf. også § 6 siste ledd hvor det samme prinsipp er lagt til grunn forsåvidt gjelder unntak for dokumenter.

Det er også viktig å være oppmerksom på det forhold at bestemmelsene er formulert slik at opplysninger *kan* unntas. Dette betyr at det således er hjemmel for å unnta, men at det ikke foreligger noen plikt til å gjøre dette. En skjønnsmessig avveining på bakgrunn av prinsippet om meroffentlighet i forvaltningen vurdert opp mot de hensyn som taler for å unnta, blir derfor å legge til grunn.

Interne dokumenter
Offentlighetslovens § 5 hjemler unntak for interne dokumenter, dvs dokumenter som er utarbeidet for intern saksforberedelse. Dette kan f. eks. være interne notater, forslag, utkast, møtereferater, arbeidsdokumenter, korrespondanse med anmodning om faglig/teknisk rådgivning mv. Dokument som er utarbeidet av underordnede organ for den interne saksforberedelse kan også unntas.

Opplysninger undergitt lovbestemt taushetsplikt
Offentlighetsloven § 5a hjemler unntak for opplysninger som er undergitt taushetsplikt i lov eller i medhold av lov (forskrift). Bestemmelsen gjelder kun opplysninger, og det foreligger her en plikt til å unnta disse.

Generelle bestemmelser om taushetsplikten finnes i forvaltningslovens §§ 13 - 13 f, men det finnes også mange andre bestemmelser om dette spredt rundt om i lovverket.

Statistikklovens § 2-4 vil således være sentral for ansatte i SSB. Taushetsplikten etter § 2-4 gjelder imidlertid kun for opplysninger innhentet med sikte på utarbeidelse av offisiell statistikk. Utover dette gjelder forvaltningslovens taushetspliktbestemmelser.

Statistikklovens § 2-4 omfatter således opplysninger i alt statistisk grunnmateriale (skjemaer, revisjonsskriv, navnekort mv.) arbeidstabeller og manuskripter. Dette gjelder også opplysninger som er innhentet på frivillig grunnlag og data som andre organer stiller til rådighet. Videre omfattes opplysninger i statistiske registre, både sentrale og delregistre, som nyttes i samband med oppgaveinnhenting.

Unntak på grunn av dokumentets innhold
Offentlighetslovens § 6 hjemler unntak for visse typer av nærmere angitte dokumenter.

Dokumenter det kan være aktuelt å unnta med hjemmel i § 6 kan være saksdokumenter i forbindelse med personal- og lønnssaker (nr 2 a og nr 4), dokumenter i saker vedrørende oppgaveplikt, tvangsmulkt og politianmeldelser (nr 2 c og nr 5), dokumenter i saker som gjelder byråskolen/intern opplæring (nr 6), dokumenter i saker vedrørende budsjett og regnskap (nr 2 a og nr 7), graderte dokumenter (nr 1).

Saksbehandling
Det er viktig at dokumenter som skal unntas fra offentlighet eller som inneholder opplysninger som kan unntas, så snart som mulig (senest ved avsendelse av brev) påføres nøyaktig og fullstendig hjemmel for dette. F. eks. skal det ved bruk av § 5a også vises til den særlov/paragraf som inneholder den aktuelle taushetspliktbestemmelse.

Ansvaret for å unnta påhviler i utgangspunktet den ansvarlige saksbehandler.

Når det gjelder saksbehandlingsregler ved innsynshenvendelser, vises til bestemmelsene i offentlighetslovens §§ 8 og 9.

7.3. Generelt om utlevering av individualopplysninger/mikrodata fra statistiske grunndata

Adgangen til å utlevere opplysninger fra SSBs statistiske registre følger av statistikklovens § 2-5 og SSBs rammekonsesjon fra Datatilsynet (se vedlegg A). Det vises også til punkt 3 ovenfor, som må sees i sammenheng med reglene om utlevering.

Rammekonsesjonens system innebærer at det er nødvendig å skille mellom tre typer av opplysninger i denne sammenheng:

- *Identifiserbare opplysninger*, dvs. opplysninger hvor det er mulig å identifisere enkeltpersoner, bedrifter o.l. ved at den enkelte fil inneholder fødselsnummer/bedriftsnummer og/eller navn.
- *Avidentifiserte opplysninger,* dvs. opplysninger hvor de data som brukes som identifikasjonsnøkkel ved registeret er fjernet. Dette vil vanligvis være navn, adresser og fødselsnummer/bedriftsnummer.
- *Anonymiserte opplysninger,* dvs. opplysninger hvor så mange kjennemerker/kategorier er fjernet at det med rimelige midler ikke er mulig (er uforholdsmessig vanskelig) å knytte opplysningene hverken direkte eller indirekte til identifiserbare enkeltpersoner, sammenslutninger eller stiftelser. (Se også nærmere pkt. 3.7.)

Selv om registrering av anonymiserte opplysninger ikke krever konsesjon, bør det ved utlevering av denne type data, på samme måte som man må ved utlevering av avidentifiserte data, kreves undertegnet en erklæring som pålegger vedkommende

taushetsplikt i henhold til statistikklovens § 2-4 samt at dataene bør slettes etter at prosjektet e.l. er avsluttet, se standardavtale nr. 4 i vedlegg D.

Det er viktig å merke seg at reglene åpner for en adgang til utlevering av opplysninger ("kan utleveres"). Det er en forutsetning for utlevering av opplysninger at det "finnes rimelig og ikke medfører uforholdsmessig ulempe for andre interesser".

Et moment i denne vurderingen er de vilkår og begrensninger SSB kan sette for utleveringen som innebærer vurdering av både mottakers formål med bruk av opplysningene og eventuelle skadevirkninger for andre basert på opplysningenes følsomhet og faren for lekkasje og misbruk.

Det er viktig å merke seg at utlevering også kan være betinget av at det dispenseres fra lovbestemt taushetsplikt. Dette vil gjelde opplysninger som er taushetsbelagt i henhold til særlovgivning, som f.eks. legeloven, og hvor eksempelvis Sosialdepartementet må dispensere fra taushetsplikten før SSB kan utlevere opplysningene.

Hvem kan utlevere opplysningene?
Bare den som har ansvaret for et register og fullmakt til å utlevere opplysninger fra det, kan godkjenne slik utlevering. Vedkommende må kjenne bestemmelsene i Statistikkloven, rammekonsesjonen og eventuelle spesielle restriksjoner som er gitt for det aktuelle registeret. Slike restriksjoner er registrert på registernivå i datadokumentasjonen.

Sammendrag av reglene om utlevering:
Statistikklovens § 2-5 gir Datatilsynet fullmakt til å bestemme at opplysningene i SSBs registre kan brukes til annet enn å utarbeide offisiell statistikk. I SSBs rammekonsesjon har Datatilsynet gitt regler om slik "annen bruk". Konsesjonen gir også regler om:

- Formål for bruk av opplysningene.
- Hva som kan utleveres.
- Betingelser som SSB skal eller kan stille.

Etter konsesjonens bestemmelser kan utlevering av informasjon i annen form enn som offisiell statistikk, foretas i de tilfeller som er nevnt under punktene 7.4, 7.5 og 7.6.

7.4. Utlevering av individualopplysninger til forskningsformål og offentlig planlegging

Slik utleveringsadgang følger av Datatilsynets rammekonsesjon punkt 2.4.2. Utlevering til forskningsformål kan skje til etablerte forskningsinstitutter, forskere med forskerkompetanse og hovedfagsstudenter, forutsatt at disse er under veiledning av en med forskerkompetanse ved undervisningsstedet.

Utlevering til offentlig planlegging kan skje til organer som stat eller kommune. Utlevering kan også foretas til et organ som skal utarbeide slik statistikk på oppdrag for stat eller kommune.

For begge typer utlevering gjelder at opplysningene skal avidentifiseres i den grad formålet tillater det.

Det aktuelle fagdepartement må alltid dispensere fra taushetsplikt før utlevering finner sted dersom det dreier seg om opplysninger som er underlagt taushetsplikt etter særlovgivning.

Videre er det viktig å merke seg at data fra frivillige undersøkelser ikke kan utleveres uten samtykke fra informantene, hverken i identifiserbar eller avidentifiserbar form.

Søkeren må bekrefte at de data det søkes om er nødvendige for prosjektet. Dette gjelder spesielt hvor det er fremsatt ønske om at dataene må være identifiserbare.

Ved utlevering av personopplysninger må det alltid stilles som betingelse at søkeren har konsesjon fra Datatilsynet for å opprette det personregister som eventuelt følger av utleveringen.

Når opplysningene er hentet fra andre offentlige organer (administrative registre) og det er tvil om utlevering bør finne sted, skal SSB forelegge utleveringsspørsmålet for det avgivende organ.

Utlevering skjer etter skriftlig søknad, og øvrige vilkår følger av standardavtale nr. 1 i vedlegg D.

7.5. Utlevering av næringsopplysninger for etablering og ajourhold av registre

Med hjemmel i statistikklovens § 2-5 kan Datatilsynet gjøre unntak fra taushetsplikten i statistikklovens § 2-4 slik at visse næringslivsopplysninger kan brukes til annet enn å utarbeide offisiell statistikk.

I Statistisk sentralbyrås rammekonsesjon har Datatilsynet med hjemmel i statistikkloven gitt tillatelse til utlevering av enkelte næringslivsopplysninger til bruk for opprettelse og oppdatering av offentlige og private registre. Slike utleveringer er det bare Seksjon for bedriftsregister som kan foreta.

I konsesjonens pkt. 2.4.3 er det spesifisert hvilke opplysninger som kan gis. Dette er:

- Eierform (enhetstype) for juridiske personer og andre som driver næringsvirksomhet.
- Adresseopplysninger.
- Bransje (næringsgruppekode), sektorkode.
- Sysselsetting (i grupper etter antall sysselsatte/årsverk).

- Statuskode (om virksomheten er i vanlig drift/ute av drift/opphørt mv.
- Foretaks-/enhets-/organisasjonsnummer.
- Datoer for stiftelse/registrering og endring av ovennevnte opplysninger.

Datatilsynet setter visse vilkår for utlevering:
- Mottaker må ha nødvendig konsesjon fra Datatilsynet til å innhente opplysningene fra SSB, eventuelt være fritatt fra konsesjonsplikt, jf. personregisterlovens § 41 eller forskrifter til personregisterloven. Hjemmelen må omfatte innhenting av opplysninger fra SSB.
- Mottaker skal bruke registeret bare til de formål som er spesifisert i Datatilsynets konsesjon.
- Statistisk sentralbyrå skal påse at opplysningene oppdateres jevnlig og at tidligere versjoner slettes ved mottak av nye opplysninger.
- Statistisk sentralbyrå skal gjøre mottaker oppmerksom på at opplysningene ikke kan legges til grunn ved avgjørelser i enkeltsaker.
- Når oppdatering skal skje ved kobling av registre, skal koblingen skje i Statistisk sentralbyrå.

Utleveringen skal skje etter skriftlig søknad, og øvrige vilkår følger av Standardavtale for innvilget utlevering av registerdata som registeransvarlig og søker skal undertegne.

Seksjonen må kontrollere nøye at dataspesifikasjonene i mottakers konsesjon samsvarer med opplysningene som utleveres.

Kjennemerker utover de som er spesifisert i Datatilsynets konsesjon til Statistisk sentralbyrå kan ikke utleveres. Dette gjelder selv om mottaker har konsesjon for å opprette register, oppbevare det og ajourføre det og har fått Datatilsynets godkjennelse til å motta dataene fra Statistisk sentralbyrå.

Det er en rekke forutsetninger som må oppfylles og vedtak som må gjøres før Statistisk sentralbyrå skal kunne utlevere data utover de dataene som er spesifisert i vår konsesjon fra Datatilsynet. SSB må bl.a. søke Datatilsynet om konsesjon til å levere ut opplysninger for dette formål.

En slik søknad fra Statistisk sentralbyrå må i hvert enkelt tilfelle godkjennes av administrerende direktør. Grunnen til dette er bl.a. at Statistisk sentralbyrå ønsker å praktisere strenge restriksjoner for utlevering av identifiserbare opplysninger som er samlet inn av Statistisk sentralbyrå for utarbeiding av offisiell statistikk.

Dersom administrerende direktør vedtar å søke konsesjon for slik utlevering, skal seksjonen utarbeide vilkårene for utlevering i samråd med Sikkerhetsutvalget.

Datatilsynet har ved siste revisjon av rammekonsesjonen (11.11.97) vurdert etter søknad fra SSB hvorvidt det bør være samme adgang til utlevering av andre grunndata som inngår i Enhetsregisteret. Datatilsynet har ikke gitt tillatelse til dette fordi de ikke finner grunn til å sette likhetstegn mellom SSB og Enhetsregisteret med hensyn til adgangen til utlevering av opplysninger om de som er registrert i Enhetsregisteret. Dette hovedsakelig fordi det gjelder særskilte bestemmelser i Enhetsregisterloven om utlevering av opplysninger fra Enhetsregisteret. Disse bestemmelsene gjelder ikke for utlevering av opplysninger fra de tilknyttede registrene.

7.6. Overføring av personregistre til utlandet

Overføring av person*registre* til utlandet skal meldes til Datatilsynet på SSBs meldingsskjema (se vedlegg 2), jf. personregisterlovens § 36 og personregisterlovens forskrifter § 8-1.

Meldeplikt gjelder også for overføring av person*opplysninger* dersom formålet er å innføre opplysningene i et register som ville vært konsesjonspliktig her i landet.

Det foreligger ikke meldeplikt til Datatilsynet for overføringen dersom Norge har plikt til å foreta overføring etter folkerettslig overenskomst, f.eks. EØS-avtalen, eller som følge av medlemskap i internasjonal organisasjon.

Overføring av avidentifiserte personopplysninger (personopplysninger som ikke er fullstendig anonymisert) skal også meldes. (Om avidentifisering/anonymisering se pkt 3.7.)

Datatilsynet kan nekte overføring til utlandet eller sette vilkår for overføringen. I sin vurdering legger Datatilsynet bl.a. vekt på hvorvidt det er etablert tilstrekkelig personvernlovgivning i det land overføringen skal skje til, og det kan legges vekt på hvem som er mottaker av opplysningene og hva opplysningene skal brukes til.

7.7. Utlevering av data innenfor EØS-området

I artikkel 76 i EØS-avtalen sies det at avtalepartene skal påse at det utarbeides og spres statistikk med sikte på å beskrive og overvåke ulike sider av EØS-området samt "utvikle og benytte" harmoniserte metoder, felles programmer og fremgangsmåter for å organisere samarbeidet.

Videre henvises det til protokoll 30 i avtalen mht. særlige bestemmelser om organiseringen av samarbeidet. Hverken artikkel 76 eller protokoll 30 utpeker hvem som skal ha hovedansvar for produksjon av statistikk for EØS-området, eller gir klare og generelle regler om utleveringsplikt.

Disse spørsmålene avklares imidlertid gjennom konkrete rettsakter innenfor de områder hvor det skal utarbeides statistikk i henhold til EØS-avtalen og senere endringer i den. Se for øvrig også pkt. 1.2 om lovgrunnlag for SSBs virksomhet og implementeringsarbeidet for EØS-relevant EU-lovgivning.

Rådsforordning/EØF) nr. 1588/90 om oversendelse av fortrolige statistiske opplysninger til Det europeiske fellesskaps statistikkbyrå (Eurostat), har som hovedformål "to remove the legal obstacles which may have hindered Member States in transferring statistical information due to national confidentiality rules" (pkt. 2.2 i Eurostats utkast til Manual on protection of confidential data av 12.11.1993).

Forordningen gir ikke i seg selv Eurostat hjemmel til å pålegge de enkelte nasjonale statistikkbyråer utlevering, jf. også forordningens Art 3 nr. 2, men om slik plikt foreligger i en spesifikk EØS-rettsakt, skal personvern/taushetspliktsregler i de enkelte land ikke være til hinder for slik utlevering.

For å kunne fastslå om SSB har plikt til å utlevere data og eventuelt på hvilket detaljeringsnivå mv. er det derfor først og fremst de enkelte rettsakter (lovbestemmelser) innenfor de enkelte statistikkområder som fastlegger pliktens omfang.

Overføring av personopplysninger som følger direkte av en EØS-rettsakt vil ikke være meldepliktig til Datatilsynet. Overføring av personopplysninger uten hjemmel i en EØS-rettsakt vil imidlertid være meldepliktig. Det vises i denne forbindelse til det som er sagt under pkt. 7.6.

7.8. Saksbehandling ved utleveringssaker

Det skal alltid foreligge en skriftlig søknad om datautlevering med beskrivelse av formålet med datautleveringen og dokumentasjon av behovet for enkeltkjennemerker, med særlig vekt på behovet for identifiserende opplysninger.

Ved muntlige forespørsler kan det redegjøres for retningslinjene for utlevering, men saksbehandlingen og vedtakene skal alltid gjøres på grunnlag av en skriftlig søknad.

Alle skriftlige søknader skal journalføres. Dette skal gjøres uansett utfallet av søknaden. Dersom det under saksbehandlingen blir hentet inn tilleggsinformasjon fra søkeren, må det passes på at også denne blir journalført.

Søknaden skal behandles av den seksjon som «eier» dataene det er forespørsel om. Dersom søknaden gjelder data som tilhører flere seksjoner, må den seksjon som først får tilsendt søknaden straks ta kontakt med de andre aktuelle seksjonene og bli enige om hvilke seksjon som skal samordne saksbehandlingen. Blant annet for fremdriften av prosjektet og kontakten med søkeren er det viktig at en seksjon får oppgaven med å samordne arbeidet.

Det må vurderes/undersøkes om de formelle krav til datautlevering er til stede og hvilke krav som må være oppfylt før utlevering finner sted. Vær sikker på at alle kravene er oppfylt.

Blant kravene nevnes:

1. Krav til mottaker av dataene. Se f.eks. kravene som stilles til mottakere av data for forskningsformål. Er det spesielle grunner til at vi tviler på at mottakeren av data ikke er i stand til å oppfylle våre krav til fortrolig behandling av dataene?

2. Kravene til formålet med databruken. For utlevering til forskningsformål, må det f.eks. foreligge et seriøst forskningsprosjekt. Det kan være en rettesnor at et prosjekt er vurdert og finansiert av etater som forvalter offentlige forskningsmidler. Uansett må det vurderes om prosjektet på noen måte kan være til skade for SSB eller oppgavegiverne.

3. Har mottaker fått den nødvendige konsesjon fra Datatilsynet? SSB skal ha kopi av konsesjonen, og vi må vurdere nøye om dataene det er aktuelt å utlevere er innen konsesjonens rammer.

   For utlevering av særskilte næringsopplysninger skal datamottaker også ha konsesjon fra Datatilsynet til å motta data fra SSB. Bare dersom mottaker skal oppbevare dataene *manuelt* og dataene ikke er av sensitiv art, vil mottaker ikke trenge konsesjon fra Datatilsynet.

   Dersom dataleveransene går utover de rammer som er gitt i Datatilsynets rammekonsesjon til SSB, skal også SSB søke særskilt konsesjon for utlevering. Dette gjelder selv om datamottaker har konsesjon til å motta data fra SSB. Søknad om slik konsesjon skal godkjennes av administrerende direktør. Vilkår for utlevering i SSBs rammekonsesjon gjelder uavhengig av om mottaker skal lagre dataene manuelt eller elektronisk.

4. For administrative data samlet inn ved hjemmel i statistikkloven, skal det innhentes samtykke fra dataeier (den etat vi har fått dataene fra). Dette skal innhentes ved alle utleveringer så sant det ikke har blitt gitt generelt samtykke til utlevering, f.eks. til en viss type anvendelse. Søknad til en etat om utlevering av data skal gå fra den seksjonen i SSB som er ansvarlig for etatskontakten, eller sendes i samråd med denne seksjonen.

   Dersom data er underlagt taushetsplikt etter særlov, må det alltid søkes om dispensasjon fra det aktuelle fagdepartement. Det er viktig at dette vilkåret er oppfylt.

5. For utlevering av data innhentet på frivillig grunnlag gjelder spesielle regler. Det skal foreligge samtykke fra oppgavegiver for at dataene skal kunne utleveres i avidentifisert form. Dette gjelder for alle typer av data som klassifiseres som personregister i personregisterlovens forstand (avidentifiserte data, både for personer/husholdninger og bedrifter). Se omtale av frivillige undersøkelser i punkt 3.4.

   Det er viktig å forsikre seg om at en utlevering er i tråd med de retningslinjer vi har på dette området. Vær også oppmerksom på at kobling av frivillig avgitte data med andre data ikke kan gjøres uten etter samtykke fra den som frivillig har gitt oss opplysningene. Disse reglene er absolutte og er en nødvendig forutsetning for utlevering.

6. Dersom seksjonen/avdelingen er i tvil om det formelle grunnlaget, skal saken forelegges Sikkerhetsutvalget.

Under saksbehandlingen bør det vurderes om det finnes andre alternative datakilder enn utlevering av identifiserbare opplysninger. I noen tilfeller kan det f.eks. være tilstrekkelig med et utvalg i stedet for opplysninger om hele datamassen. I så tilfelle bør dette foreslås.

I visse tilfeller kan søkeren være fornøyd med å få tilsendt tabeller eller aggregerte utkjøringer. Dersom forholdene ellers ligger til rette for det, bør vi tilby oss å utarbeide slike tabeller/aggregater.

Vurder kritisk avidentifiseringen av dataene. Både ved utlevering til forskning og offentlig planlegging, skal dataene avidentifiseres så langt det ikke skaper problemer for den videre bruk av dataene. Vi må sørge for å sløyfe kjennemerker som ikke er nødvendige, og mulige aggregeringer foretas for identifiserende kjennemerker/kjennemerkealternativer.

Data skal tilbakeleveres snarest mulig etter endt bruk eller senest innen en oppgitt dato. Mottaker kan eventuelt selv slette dataene snarest mulig etter endt bruk og senest innen en oppgitt dato. Slettingen skal bekreftes skriftlig. Samme regler gjelder for koblinger. Disse skal oppløses etter bruk og senest innen en gitt dato.

Før utlevering skal mottaker få tilsendt skriftlig orientering om betingelsene for utlevering, bl.a. taushetsregler og tilbakelevering/sletting, og undertegne godkjenning av disse. Se vedlegg D. Dersom ikke malbrevene nyttes, må det alltid kontrolleres at alle betingelsene kommer med i brevet.

Utlevering av avidentifiserte data skal godkjennes av avdelingsleder eller den han/hun bemyndiger. Dersom leveransen omfatter koblinger mellom flere datakilder, skal utlevering godkjennes av administrerende direktør eller den han/hun bemyndiger.

Ved utlevering av anonymiserte mikrodata, skal anonymiseringen godkjennes av avdelingsleder eller den han/hun bemyndiger. Også i slike tilfeller skal datamottaker levere tilbake/slette opplysningene etter samme regler som for utlevering av avidentifiserte opplysninger. Vi stiller også ved utlevering av anonymiserte data krav om bruken av dataene og publisering av resultater, se vedlegg D.

Når vi stiller slike krav også til anonymiserte data, skyldes det at vi aldri kan se helt bort fra at personer med stor forhåndskunnskap om de individer dataene dekker, kan identifisere enkelte personer/foretak i det utleverte materialet.

Avslag på søknad om tilgang til opplysninger er et enkeltvedtak etter forvaltningslovens § 2 bokstav b, og kan påklages etter reglene i forvaltningslovens kapittel VI, jf. vedlegg D. Vedtak om avslag skal godkjennes av avdelingsleder.

Både brev med vedlegg om utlevering av mikrodata, avidentifisert eller anonymisert (også koblinger) og brev om avslag, skal alltid journalføres. Interne utredninger og vedtak i forbindelse med utleveringssakene skal også registreres i postekspedisjonen. Grunnen til at vi gjør dette er at en del av utleveringssakene er vanskelige og krever utredninger og uttalelser/godkjenninger før endelig beslutning om utlevering eller eventuelt nekting blir fattet.

Ved registrering i postekspedisjonen kan vi lett gå tilbake og sette oss inn i saksgangen og vurderingene i den enkelte sak. Saksbehandleren må passe på at denne registreringen blir gjort.

Postekspedisjonen skal også registrere den tilbakeleveringsdatoen (eventuelt bekreftelse på sletting) som er oppgitt i vårt brev til datamottakeren (se vedlegg E).

Postekspedisjonen skal, når vi kommer til denne datoen, varsle ansvarlig seksjon om at betingelsene i utleveringsbrevet ikke er oppfylt. Det er videre seksjonens oppgave å forfølge saken. For at denne ordningen skal fungere tilfredsstillende, må seksjonen sørge for at eventuell tilbakelevering før «siste frist datoen» blir registrert i postekspedisjonen.

D Sikringstiltak

Generelt
Sikringstiltakene deles inn i tre hovedområder, fysiske sikringstiltak, IT-messige sikringstiltak og prosedyremessige sikringstiltak.

De fysiske sikringstiltakene omfatter bygningsmessige forhold, branntekniske forhold og lignende. Altså forhold omkring fysiske objekter.

De IT-messige sikringstiltakene omfatter forhold omkring programvare og data benyttet på IT-utstyr.

De prosedyremessige sikringstiltakene er rettet mot å ha rutiner og tiltak som sørger for at de to andre sikringstiltakene får sin tiltenkte effekt.

Sikkerhet kan deles inn i tre sikkehetsaspekter:
- Konfidensialitet (Begrenset innsyn)
- Kvalitet (Data er til å stole på)
- Tilgjengelighet (Data er tilgjengelig)

8. Fysiske sikringstiltak

8.1. Behandling av makulatur

1. Innledning
Denne instruksen er retningsgivende for hvordan makulering av papir skal skje og for hvordan det praktiske arbeidet ved innlevering blir organisert.

2. Ansvarsfordeling
Den enkelte medarbeider har ansvaret for at papir for makulering (farlig makulatur) blir oppbevart på en betryggende måte før det blir levert til sentralt oppbevaringssted.

Den enkelte medarbeider må selv sørge for at makulatur blir brakt til sentrale oppbevaringssteder. Avdelingene v/avdelingslederne har det formelle ansvaret for at instruksen blir fulgt. Administrasjonsavdelingen har ansvaret for sentralt oppbevaringssted og for å avhende materiell.

3. Sikkerhetsgradert materiale
Det gjelder særskilte regler med hensyn til makulering/tilintetgjøring av materiale som er gradert etter Sikkerhetsinstruksen som STRENGT HEMMELIG, HEMMELIG, KONFIDENSIELT eller BEGRENSET, og etter Beskyttelsesinstruksen som STRENGT FORTROLIG eller FORTROLIG. Det vises for øvrig til pkt. 9.5 om gradering, beskyttelse og bruk av informasjonsmateriale i henhold til Sikkerhets- og Beskyttelsesinstruksen.

Ved tilintetgjøring av gradert materiale må fremgangsmåten i Sikkerhetsinstruksen eller Beskyttelsesinstruksen følges.

Bare administrerende direktør, eller den han bemyndiger, kan beordre eller godkjenne tilintetgjørelse av dokumenter gradert etter Sikkerhetsinstruksen.

Materiale gradert etter Beskyttelsesinstruksen (STRENGT FORTROLIG eller FORTROLIG) skal tilintetgjøres under betryggende kontroll og det må gjøres anmerkning om tilintetgjørelsen i den journal som skal føres for slike dokumenter.

Materiale gradert KONFIDENSIELT eller BEGRENSET og som er godkjent for tilintetgjørelse, og materiale som er gradert STRENGT FORTROLIG eller FORTROLIG, må merkes med «farlig makulatur» på innpakningen og behandles som beskrevet i det følgende:

Dokumenter som er unntatt offentlighet i medhold av lov av 19. juni 1970 nr. 69 om offentlighet i forvaltningen (offentlighetsloven), må på samme måte behandles og merkes som «farlig makulatur».

Dette gjelder også annet materiale som ikke er gradert eller unntatt offentlighet, men hvor det likevel kan antas at noe av innholdet kan forårsake skade for det offentlige/SSBs interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent.

Datalister og annet papir som inneholder navn på personer, firmaer osv. bør i utgangspunktet alltid behandles og merkes med «farlig makulatur».

4. Oppbevaring
Makulaturen legges i egne låste beholdere som er utplassert i en del printer-/kopirom i Oslo. I Kongsvinger legges makulatur i eget avlåst rom i kjelleren.

5. Avhending
Farlig makulatur transporteres til godkjent mottakersted for tilintetgjørelse. En ansatt i SSB skal følge transporten samt overvære prosessen. SSB

Kongsvinger kan dersom det er kostnads- og miljømessig forsvarlig, makulere på egen makuleringsmaskin.

8.2. Fysisk sikring og adgangskontroll i SSBs lokaler

1. Alle tilsatte skal alltid ha med seg adgangskort og bruke dette, eventuelt sammen med kode, ved passering av låste dører. Kortet skal alltid brukes eller vises uoppfordret ved passering av resepsjonen på eget arbeidssted. Ved besøk på SSBs andre arbeidssted skal den besøkende registreres ved inn- og utpassering.

2. Tap av adgangskort må straks meldes til administrasjonskontoret ved avdelingen eller til resepsjonsvakten i Oslo og til Postekspedisjonen i Kongsvinger.

3. Adgangskort og tilhørende kode må ikke lånes eller utleveres til andre.

4. Dersom alarm utløses ved passering av alarmbelagte dører, skal den som forårsaket dette vente på stedet til vaktpersonale kommer.

5. Ingen skal slippe personer uten synlig adgangs- eller besøkskort gjennom låste dører. Alle tilsatte *har et ansvar for å påse* at uvedkommende ikke får tilgang til Statistisk sentralbyrås lokaler.

6. Den som får disposisjon over kantine eller annet lokale utenfor kontortiden skal følge den instruksen som blir gitt i det enkelte tilfellet.

7. Den som blir påtruffet av SSBs mobilvakt, skal oppgi navn og vise nødvendig legitimasjon etter at vakten har legitimert seg.

8. Den som mottar besøk, er ansvarlig for vedkommende fra besøket blir varslet fra resepsjonen til vedkommende forlater SSBs lokaler.

8.3. Utlevering og tilbakelevering av nøkler og adgangskort

Utlevering
Alle nyansatte og andre personer med kortere engasjement for SSB, som ikke regnes som besøk, får utlevert nøkkel til sitt kontor og adgangskort til dører med kortleser.

Det må kvitteres for mottatte nøkler og adgangskort i Oslo og for tilsvarende i Kongsvinger.

Tilbakelevering
- Engasjement opphører:

Når engasjementet for SSB opphører, skal adgangskortet leveres tilbake siste arbeidsdag.

- Oppsigelse

I brevet som bekrefter oppsigelsen fra medarbeider, tas det med en setning om at SSBs nøkler og adgangskort skal leveres til administrasjonskontoret ved avdelingen senest siste arbeidsdag. Ved tilbakelevering gjøres det anmerkning på listen for utleverte nøkler/adgangskort om at disse er mottatt.

- Permisjon

Når det innvilges permisjon i tre måneder eller mer, følges samme rutine for tilbakelevering som ved oppsigelse.

8.4. Merking av utstyr

IT-utstyr, og ikke minst stasjonære PC-er og bærbare PC-er, er enkelt å frakte med seg. Slikt utstyr er også lett omsettelig, hvilket gjør det fristende for eventuelle innbruddstyver. For å redusere risikoen for tyveri og forenkle eventuell oppklaring av tyverier skal alt IT-utstyr merkes med dertil egnet merkeutstyr.

For tiden betyr det at alle PC-er (bærbare og stasjonære), skrivere, skjermer og tilleggsutstyr til slikt, skal merkes med «Statistisk sentralbyrå». Egnet merkeutstyr er anskaffet av Administrasjonsavdelingen, og IT-drift har tilgang til dette.

Merkeutstyret benytter en etsende lakk som ved siden av farge, også lager relieff i materialet. Dette gjør det vanskelig å fjerne.

Eksisterende utstyr, herunder hjemlåns-PC-er, skal merkes i henhold til dette. Nyanskaffet utstyr skal merkes før utplassering.

8.5. Beredskaps- og katastrofesikring

I tilfelle nasjonale eller internasjonale krisesituasjoner er det utarbeidet en særskilt generell beredskapsplan for Statistisk sentralbyrå. Denne er gradert BEGRENSET i henhold til Sikkerhetsinstruksen.

Planen er gitt den laveste gradering i henhold til Sikkerhetsinstruksen og innebærer at alle ansatte i Statistisk sentralbyrå som har behov for det i sitt arbeid, er autorisert til å få denne til utlån. Beredskapsplanen inneholder derfor ikke opplysninger som anses for å være svært sensitive.

Det er imidlertid også utarbeidet særskilte beredskapsplaner for det sentrale IT-utstyret og annet

viktig utstyr som inneholder retningslinjer og regler for hvilke rutiner som skal følges ved f.eks. brann eller strømstans.

8.6. Branninstruks

1. Alle ansatte i SSB plikter å gjøre seg kjent med og følge branninstruksen.

2. Hver enkelt plikter å gjøre seg kjent med:
   - Rømningsveier
   - Utganger og trapper
   - Plassering av slukningsutstyr
   - Plassering av brannmeldere

3. Ved brann eller brannalarm skal lokalene forlates øyeblikkelig. Om mulig skal dører og vinduer lukkes.

4. Oppdages brann skal det om mulig slås alarm ved nærmeste brannmelder. Den enkelte skal om mulig varsle alle i sin nærhet ved f.eks. rop, og om mulig sjekke om rommene i nærheten er tomme.

5. Dersom det synes forsvarlig å prøve og slukke brannen før brannvesenet kommer til stedet, husk at vannslanger ikke må benyttes mot elektriske installasjoner.

6. Ta fremfor alt hensyn til at liv er viktigere enn verdier.

7. Brannvarsling *skal* respekteres og bygningene rømmes ved enhver utløsning av brannalarmen. Ved brann eller utløsning av alarm, skal heiser ikke benyttes. Følg de instrukser som eventuelt seksjonssjef/kontorsjef eller de ansvarshavende for fløy/etasjen, gir.

8. Seksjonssjef/kontorsjef eller ansvarshavende for fløy/etasje, skal straks bli varslet av den enkelte når vedkommende har kommet utenfor faresonen. Den enkelte skal møte på avtalt oppmøtested.

9. Feil eller mangler ved brannsikkerheten (f.eks. blokkerte rømningsveier, manglende slukningsutstyr) må meldes snarest til seksjonssjef/kontorsjef eller ansvarshavende for fløy/etasje.

9. IT-messige sikringstiltak

9.1. Sikkerhetsinstruks for dataeier

Dataeier plikter å tilse at sikringstiltak blir iverksatt og betryggende ivaretatt innenfor sitt ansvarsområde.

Hvert enkelt datasett i SSB "eies" av den enhet som har ansvaret for statistikken/opplysningene på det feltet datasettet primært skal dekke. Lederen for enheten har ansvaret for de datasettene/opplysningene enheten eier, inkludert ansvar for at nødvendige meldinger blir sendt Datatilsynet ved opprettelse av nye registre og ved endring eller kobling av eksisterende registre.

Lederen av den ansvarlige enheten avgjør hvem som skal gis tilgang til datasett/opplysninger. Tilsatte ved den enkelte enhet skal bare gis tilgang til de datasett/opplysninger vedkommende har et tjenestemessig behov for.

Den samme vurdering skal også foretas dersom personer ved *andre* enheter ønsker tilgang til datasettene/opplysningene. For datasett som inneholder individualdata, er det en forutsetning for at tillatelse blir gitt at det foreligger et prosjektskriv godkjent av administerende direktør og/eller fremgår av godkjent arbeidsprogram.

Melding om innvilget tillatelse sendes Seksjon for IT-drift på eget skjema. Skjemaet ligger som mal i Word, og sendes som e-post med ansvarlig dataeier som avsender. Dataeier vil motta tilbakemelding pr. e-post fra Seksjon for IT-drift når tillatelse er opprettet.

Personer ved andre enheter får som standard bare tillatelse til å lese ovennevnte datasett, og kan således ikke fjerne eller endre data. For datasett som ikke inneholder individualopplysninger er det tilstrekkelig at brukeren som eier datasettet/opplysningene gir tillatelse.

Ved tildeling av lesetilgang skal det fastsettes for hvor lang tid den skal gjelde og når dataene skal slettes. Eieren av datasettet skal påse at datasettet blir slettet hos den nye brukeren etter tidens utløp. Den som får tilgang til datasettet er ansvarlig for eventuelle nødvendige meldinger til Datatilsynet. I tillegg skal eier av det opprinnelige registeret gis melding om hvilken bruk som gjøres av det.

9.2. Sikkerhetsinstruks for data- og programbrukere

1. Brukeren skal oppbevare passord på en betryggende måte og ikke overlate det til andre. Velg passord som er vanskelig å gjette. Bruk minimum 6 tegn, som ikke skal være et ord eller navn, men en blanding av bokstaver, tall og spesialtegn. Bruk skjermbeskytter med passord slik at din terminal ikke er tilgjengelig for andre hvis du må forlate arbeidsplassen.

2. Brukeren skal ikke gi fra seg beskyttede data til andre enn de som har fått tillatelse fra registereier, eller medvirke til at slike data kommer uvedkommende i hende.

3. Brukeren skal ikke bringe fremmede data eller program inn i datamaskinen uten at dette er godkjent og virustest er foretatt. Dersom brukeren benytter egen PC hjemme, må det kjøres virustest før bruk i SSB.

4. Beskyttede data, skal ikke kopieres i lokalnett/PC uten at dette er godkjent av registeransvarlig.

5. Brukeren skal holde skjema, lister og flyttbare elektroniske lagringsmedia med beskyttede data nedlåst når de ikke er under betryggende tilsyn.

9.3. Sikkerhetsinstruks for systemutviklere og programmerere

1. Program og programsystemer (applikasjoner) som utvikles for produksjon av statistikk, analyse mv. skal utvikles slik at data lagres på fastsatt sted i samsvar med gjeldende instrukser.
2. Applikasjonene skal utvikles slik at ingen uautoriserte får tilgang til data i systemet.
3. Programmene og de data som anvendes og produseres av applikasjonene skal være dokumentert.

Systemutvikler og programmerer skal normalt ikke ha adgang til produksjonsdata i systemet. Det innebærer at systemendringer og testinger normalt skal utføres i egne testsystemer med anonymiserte eller syntetiske data. Avvik fra dette kan aksepteres hvis det er nødvendig for å rette, teste eller forstå feilsituasjoner.

9.4. Sikkerhetsinstruks for systemadministratorer

1. Systemadministratoren har ikke adgang til andre program og data enn de vedkommende skal vedlikeholde.

2. Systemadministratoren skal påse at det ikke er andre adkomstmuligheter til data, program eller passord enn det som tillates av sikkerhetsprogrammet. Dersom han/hun ser slike

muligheter, skal han/hun rapportere til nærmeste overordnede med kopi til Sikkerhetsutvalget.

9.5. Sikkerhetsinstruks for maskindrift

Den som er ansvarlig for drift av felles datamaskiner eller lokalnett, skal:

1. Sørge for at det blir tatt sikkerhetskopi etter fastsatt mønster.
2. Oppbevare sikkerhetskopier forskriftsmessig som kun autorisert personell har tilgang til.
3. Sørge for fjernarkivering av data etter registereierens krav.
4. Begrense fysisk adkomst til det sentrale utstyret så langt som mulig.
5. Legge frem for Sikkerhetsutvalget alle endringer i kommunikasjon over linje til omverdenen og skifte av operativsystem eller sikkerhetsprogram.
6. Sørge for at Statistisk sentralbyrås brukeridentifikasjoner bare kan brukes fra Statistisk sentralbyrås PC/arbeidsstasjon/terminaler.
7. Bare bruke autorisert personale til systemprogrammering, til å operere maskinene og til å holde dem vedlike. Forslag til autorisering legges frem for seksjonssjef.
8. Gradere materiale for systemprogrammering BEGRENSET og begrense utleveringen bare til autoriserte systemprogrammerere.
9. Sørge for at nødvendige sikkerhetsbestemmelser kommer inn i avtaler med eksterne leverandører.

9.6. Regler for sletting av data på PC

Ved vanlig sletting av filer på lokale disker vil det fremdeles være mulig å gjenskape informasjonen ved hjelp av spesielle programmer som er allment tilgjengelige.

Benyttes det spesielt utstyr vil det også være mulig å gjenskape informasjon som også er overskrevet et visst antall ganger. Det betyr at dersom disken (eller disketten) av en eller annen grunn har blitt benyttet i kortere eller lengre tid til å lagre sensitiv informasjon, må disken eller disketten makuleres.

Dog kan gjenbruk internt i SSB i visse tilfeller aksepteres. Det betyr at harddisken i PC-er som har vært benyttet til slik lagring ikke kan selges uten at harddisken fjernes og makuleres (eventuelt gjenbrukes internt).

9.7. Bruk av telenett og Internett for informasjonsoverføring

Informasjonsoverføring med elektronisk post
Elektronisk post til og fra Statistisk sentralbyrå må i dag anses som et usikkert medium. Dette gjelder både X400 og SMTP (Internett).

På grunn av dette må ikke elektronisk post brukes til å formidle taushetsbelagt eller gradert materiale.

Dersom sensitive personopplysninger skal overføres i datanett som SSB ikke kontrollerer (f.eks. telenett), skal opplysningene krypteres. Dette gjelder også tilsvarende opplysninger som overføres pr. telefaks, diskett eller lignende.

Bruk av PC med Internett-tilkobling
En del PC-er i Statistisk sentralbyrå er enten permanent koblet til Internett eller kan kobles om ved å flytte veggkontakten. I begge tilfeller må det utvises forsiktighet av de som bruker disse PC-ene:

- Dersom du har taushetsbelagt eller gradert materiale eller beskyttede data lagret på PC-en, skal denne PC-en ikke under noen omstendighet knyttes til Internett.
- Det må utvises vanlig forsiktighet ved nedlasting av programvare, for å unngå at datavirus o.l. spres i byrået.
- Normalt må PC-en kobles fri fra det interne nettet for å nå Internett. Det er imidlertid strengt forbudt å koble PC-er slik at man samtidig har kontakt både med det lokale nettet og Internett.
- Automatisk videresending av mail ut av SSBs lokalnett, er ikke tillatt.

Alle eksterne tilknytninger som f.eks. e-post, Internett eller modem, skal godkjennes av Datatilsynet. SSBs e-posttilknytning er forelagt Datatilsynet for slik godkjenning og spørsmålet er for tiden under utredning. Eventuelle vilkår for slik kommunikasjon vil derfor kunne bli fastsatt.

10. Sikringstiltak i henhold til Sikkerhets- og Beskyttelsesinstruksen

10.1 Informasjonsmateriale i henhold til sikkerhets- og beskyttelsesinstruksen

Generelt
Det er utarbeidet instrukser fra sentralt hold i statsforvaltningen som gir regler for behandling og tilgang til informasjon som bør beskyttes. Regelverket er bygget opp under den forutsetning at forskjellig informasjon fordrer ulik behandling.

Informasjonsmediet er uten betydning fordi det er informasjonen som skal beskyttes. Når instruksene snakker om "dokument", kan dette godt være en PC eller en diskett.

Sikkerhetsinstruksen av 17.03.72 med senere endringer gir regler om behandling av dokumenter som av sikkerhetsmessige grunner (hensynet til rikets sikkerhet) må beskyttes. Utsteder av materialet er ansvarlig for gradering.

Generelt gjelder disse reglene en type informasjon SSB har lite av, og vil derfor få liten betydning for informasjonsbehandlingen. Det er likevel nødvendig for noen å kjenne litt til reglementet for å kunne behandle den type informasjon som blir berørt av regelverket.

Beskyttelsesinstruksen av 17.03.72 gir regler om behandling av dokumenter som av andre grunner enn de som er nevnt i Sikkerhetsinstruksen trenger beskyttelse. Informasjonen må i tillegg også være unntatt offentlighet etter offentlighetsloven, se punkt 7.2.

Datasikkerhetsdirektivet av 01.02.90 gir regler for elektronisk databehandling av informasjon som er gradert i henhold til Sikkerhetsinstruksen og Beskyttelsesinstruksen.

Leder ved den enkelte administrative enhet vil være ansvarlig for gradering av informasjonsmateriale etter Sikkerhets- og Beskyttelsesinstruksen. Der det er tvil om beskyttelsesgrad forelegges spørsmålet Sikkerhetsutvalget.

Gradering av informasjon
Gradering i henhold til Sikkerhetsinstruksen
Sikring av data i henhold til Sikkerhetsinstruksen har til hensikt å hindre at opplysninger som angår Norges eller våre alliertes sikkerhet, kommer til uvedkommendes kjennskap, dvs. i fremmed makt.

De beskyttelsesgrader som skal nyttes for dette formål er følgende:
STRENGT HEMMELIG
HEMMELIG
KONFIDENSIELT
BEGRENSET

For å få tilgang til data/informasjon gradert KONFIDENSIELT eller høyere må man være sikkerhetsklarert og autorisert for tilgang, se punkt 10.1.

Ved vurdering av om noe skal graderes etter Sikkerhetsinstruksen, bør den som har ansvar for dette ha for øye at en samlet oppstilling av visse data i vesentlig omfang kan gi opplysninger som det kan være nødvendig å gradere.

Beskyttelsesgraden skal påføres dokumentets øverste og nederste høyre hjørne med rød farge. Hvis dokumentet inneholder flere sider, skal disse være behørig sammenheftet og beskyttelsesgraden skal påføres med rødt på dokumentets forside og bakside.

Dersom den enkelte enhet mottar sikkerhetsgraderte dokumenter utenfra, må spørsmålet om behandling av dokumentene tas opp med Sikkerhetsutvalget.

Gradering i henhold til Beskyttelsesinstruksen
Beskyttelsesinstruksen kommer til anvendelse ved behandling av dokumenter som trenger spesiell beskyttelse av andre grunner enn av hensynet til Rikets sikkerhet.

Gradering etter Beskyttelsesinstruksen skal bare foretas når et dokument kan unntas fra offentlighet i medhold av offentlighetsloven og skadevirkninger for offentlige interesser, en bedrift, institusjon eller enkeltperson, kan inntreffe. Det må da nyttes en av følgende beskyttelsesgrader:
STRENGT FORTROLIG
FORTROLIG

STRENGT FORTROLIG nyttes dersom det vil kunne forårsake *betydelig skade* for offentlige interesser, en bedrift, institusjon eller enkeltperson, at dokumentets innhold blir kjent for uvedkommende.

FORTROLIG nyttes dersom det vil kunne *skade* offentlige interesser, en bedrift, institusjon eller enkeltperson, at dokumentets innhold blir kjent for uvedkommende.

For å få tilgang til data/informasjon gradert etter Beskyttelsesinstruksen er det ikke nødvendig å være sikkerhetsklarert og autorisert.

Når et dokument graderes, skal det angis hvilken bestemmelse i offentlighetsloven som gir hjemmel for å unnta dokumentet fra offentlighet. Videre skal det angis at graderingen er foretatt i henhold til Beskyttelsesinstruksen.

Det meste av SSBs statistiske data og dokumenter omfattes av Beskyttelsesinstruksens bestemmelser og er gradert FORTROLIG.

Beskyttelsesgrad skal etter reglene påføres dokumentene på første side øverst til høyre med blå farge (stempel). Omfanget av materialet tilsier imidlertid at beskyttelsesgrad bare rent unntaksvis påføres statistikkskjemaene o.l.

Påføring av beskyttelsesgrad gjelder først og fremst beskyttede dokumenter/informasjon som unntaksvis blir sendt ut fra SSB.

Oppbevaring
Opplysninger gradert etter Sikkerhetsinstruksen skal som en generell regel ikke lagres i PC som har egen lagringsenhet med diskettstasjon.

Dokumenter/data gradert STRENGT HEMMELIG og HEMMELIG skal oppbevares i godkjente sikkerhetsskap, hvelv e.l.

Dokumenter/data gradert STRENGT FORTROLIG og KONFIDENSIELT skal være nedlåst i sikkerhets- eller stålarkivskap.

Dokumenter/data gradert FORTROLIG og BEGRENSET skal oppbevares avlåst.

Dokumenter/data gradert STRENGT FORTROLIG OG FORTROLIG må oppbevares slik at de ikke er tilgjengelige for uvedkommende. Når kontoret forlates, skal slikt materiell være nedlåst, om mulig i arkivskap o.l.

Opplysninger gradert STRENGT FORTROLIG og KONFIDENSIELT eller høyere, skal ikke lagres på frittstående PC. I de tilfeller en lagrer data gradert FORTROLIG på en PC skal hele maskinen behandles som ett fortrolig dokument.

I tillegg skal disketter som inneholder fortrolige data låses inn i skap/skrivebord ved arbeidsdagens slutt.

Den enkelte medarbeider har personlig ansvar for at gradert materiell som han/hun selv nytter i arbeidet oppbevares etter ovennevnte punkter.

Forsendelse
Dokument gradert STRENGT HEMMELIG skal alltid sendes med godkjent bud/kurer.

Dokument merket HEMMELIG og KONFIDENSIELT samt STRENGT FORTROLIG sendes med bud/kurer eller som rekommandert post.

Når dokumentene sendes med bud/kurer, skal det innhentes kvittering. Dokumenter gradert STRENGT HEMMELIG og HEMMELIG vedlegges dessuten en ugradert kvitteringsblankett som mottakeren uten opphold skal returnere i kvittert stand.

Dokumenter merket KONFIDENSIELT kan sendes i enkel konvolutt når de bringes med bud.

Sendes ovennevnte dokumenter i posten (rek) skal det skje i dobbel konvolutt. Den indre konvolutten skal forsegles og påføres beskyttelsesgrad. Den ytre konvolutten skal være umerket.

De ansatte som skal behandle materiale som er gradert STRENGT HEMMELIG, HEMMELIG, KONFIDENSIELT eller STRENGT FORTROLIG må gis spesiell beskjed om gradering og regler for behandlingen.

Forsendelse av dokumenter merket BEGRENSET og FORTROLIG kan skje på vanlig måte i umerket, lukket konvolutt.

Forsendelse og mottak av fortrolig data på alt maskinlesbart medium skal registreres av en ansvarlig ved den aktuelle avdeling/seksjon/gruppe.

All forsendelse av fortrolig data på maskinlesbart medium skal registreres som rekommandert post, verdipost eller sendes med bud.

Oversikt over forsendelse/mottak av data skal på forespørsel kunne legges frem for Sikkerhetsutvalget for kontroll.

Merk: Gradert datakommunikasjon skal være beskyttet mot uautorisert tilgang til informasjon eller dataressurser. Det vises til Datasikkerhetsdirektivet og til Forsvarets overkommando for nærmere retningslinjer.

11. Prosedyremessige sikringstiltak

11.1. Sikkerhetsklarering og autorisasjon av personale

Direktivet for personellsikkerhetstjenesten og personkontrolltjenesten innen den sivile forvaltning av 04.11.83 gir regler om fremgangsmåten ved sikkerhetsklarering og autorisasjon av personell som skal behandle/ha adgang til materiale gradert etter Sikkerhetsinstruksen, se punkt 9.5.

Informasjon gradert STRENGT HEMMELIG, HEMMELIG eller KONFIDENSIELT, kan bare behandles og gjøres kjent for personer som er sikkerhetsklarert og autorisert for å kunne behandle slik informasjon. Før klarering og autorisasjon gis, skal sikkerhetssamtale og personkontroll finne sted.

Sikkerhetsklarering innebærer at en person generelt ansees for å være sikkerhetsmessig skikket til å bli gitt adgang til gradert informasjon på et bestemt nivå etter at *sikkerhetssamtale* og *personkontroll* er foretatt.

Sikkerhetsautorisasjon er den konkrete beslutning som fattes om at en person etter å ha blitt sikkerhetsklarert kan få tilgang til en bestemt type gradert informasjon.

Før sikkerhetsklarering og autorisasjon kan foretas må vedkommende person gjennom en *sikkerhetssamtale*. Denne utføres av avdelingslederen eller den han/hun utpeker i samarbeid med Sikkerhetsutvalget.

Personkontroll foretas av Politiets overvåkningstjeneste bl.a. basert på opplysninger fremkommet i sikkerhetssamtalen. Sikkerhetsutvalget har nødvendige skjemaer som skal fylles ut, og er ellers ansvarlig for at forespørsel om personkontroll blir effektuert.

Utfylt skjema for personkontroll skal arkiveres hos Sikkerhetsutvalget.

Sikkerhetsklarering og *autorisasjon* foretas av den enkelte avdelingsleder når personkontroll er gjennomført, og "intet ufordelaktig" er funnet om den aktuelle person. Dette gjelder ikke dersom informasjonen er gradert STRENGT HEMMELIG eller dersom personen er utenlandsk statsborger. I disse tilfellene foretas sikkerhetsklarering/autorisasjon av Finansdepartementet.

11.2. Bruk av kopimaskin og skrivere

Ved kopiering/utskriving på skriver skal det bare tas de kopier/utskrifter som er nødvendige, og hver enkelt må påse at kopier og utskrifter ikke blir liggende i kopimaskin/skriver lenger enn høyst nødvendig.

Det er viktig å påse at kopiering og forsendelser av gradert informasjon etter Sikkerhets- og Beskyttelsesinstruksen foretas etter de regler som følger av disse instruksene, se punkt 10.

Datatilsynet 

Konsesjon for opprettelse av personregister

I medhold av Lov om personregistre mm av 9. juni 1978 nr 48 § 9, jf Kgl res av 21. desember 1979 pkt 1 gis

STATISTISK SENTRALBYRÅ

konsesjon for å opprette personregister.

Konsesjonen gjelder for
Statistisk sentralbyrås personregistre opprettet i medhold av Lov om offisiell statistikk og Statistisk sentralbyrå av 16. juni 1989

Konsesjonsdokumentet er lagt ved. Regler og vilkår som er fastsatt i konsesjonen, skal gjøres kjent for ansatte i virksomheten.

Georg Apenes
Direktør

KONSESJON
FOR OPPRETTELSE AV
PERSONREGISTER

Konsesjonssnr.: 97/1805-1 25.06.97

I medhold av Lov om personregistre mm av 9. juni 1978 nr 48 § 9, jf Kgl res av 21. desember 1979 pkt 1 gis

STATISTISK SENTRALBYRÅ

konsesjon til å opprette personregistre.

Dersom virksomheten eller føringen av registeret opphører, skal Datatilsynet ha melding om dette, se konsesjonens pkt 4.4 siste ledd.

Vilkår gitt med hjemmel i personregisterloven § 8 b og § 9, jf § 11 skal gjøres kjent for alle personer som behandler personopplysninger for registereier, og ellers være tilgjengelig for den som ber om det.

Konsesjonen gjelder for:

Statistisk sentralbyrås personregistre opprettet i medhold av Lov om offisiell statistikk og Statistisk sentralbyrå av 16. juni 1989.

Datatilsynet har fastsatt følgende regler for konsesjonen:

1 REGLER ETTER PERSONREGISTERLOVEN § 11

1.1 Formålet med de enkelte registre

Registrene skal benyttes i den virksomhet Statistisk sentralbyrå er pålagt i henhold til Lov om offisiell statistikk og Statistisk sentralbyrå (statistikkloven) §§ 1-1 og 3-1.

Dersom registeret skal brukes utover dette, må den registeransvarlige innhente ny tillatelse fra Datatilsynet.

1.2 Registrenes innhold

De enkelte registre kan bare inneholde opplysninger innhentet

- etter pålagt oppgaveplikt jf statistikkloven § 2-2,
- opplysninger innhentet fra administrative datasystemer i statsforvaltningen og landsomfattende kommunale organisasjoner, jf statistikkloven § 3-2,
- opplysninger innhentet med hjemmel i andre lover som gir SSB rett til å kreve opplysninger samt
- opplysninger innhentet på frivillig grunnlag.

1.3 Registeransvarlig (personregisterloven § 11 siste ledd)

Som registeransvarlig oppnevnes leder for den avdeling som fører det enkelte register.

Registeransvarlig plikter å sørge for at bestemmelsene i personregisterloven med forskrifter og denne konsesjonen blir fulgt. Registeransvarlig kan delegere sine oppgaver til annen kompetent person innen virksomheten. Det overordnede ansvar i henhold til denne konsesjonen påhviler likevel registeransvarlig fullt ut.

2 VILKÅR ETTER PERSONREGISTERLOVEN § 11 ANNET LEDD

2.1 Registermedium

Registeret kan føres både manuelt og ved bruk av elektroniske hjelpemidler.

2.2 Innsamling av opplysninger

Opplysningene i registeret kan innhentes med hjemmel i lov når lovbestemt taushetsplikt ikke er til hinder for det, eller på frivillig grunnlag fra den registrerte selv. For øvrig kan opplysninger innhentes fra kilder som er offentlig tilgjengelige.

Frivillige undersøkelser
Ved innsamling av personopplysninger gitt på frivillig grunnlag gjelder følgende vilkår:

- innsamling av personopplysninger fra den registrerte selv kan bare skje gjennom informert samtykke. Retur av spørreskjema regnes i denne sammenheng som samtykke

- i informasjonen til respondenten skal det framgå at deltakelse er frivillig, og at man på hvilket som helst tidspunkt kan trekke seg fra undersøkelsen uten å måtte gi noen grunn eller bli erstatningsrettslig ansvarlig. Det skal også gis orientering om sletteadgangen, jf konsesjones punkt 2.5.

- respondenten skal dessuten informeres om formålet med prosjektet, om opplysningene senere skal kobles mot andre opplysninger, herunder hvilke typer opplysninger, og formålet med koblingen

- respondenten kan ikke avkreves frafallsårsak, eller årsak til at respondenten ikke ønsker å delta i undersøkelsen. Dersom respondenten, etter å ha blitt gjort uttrykkelig oppmerksom på at det er frivillig, likevel oppgir frafallsårsak, kan dette registreres i en av følgende grupper: intervjuobjektet indisponert, kommunikasjonsproblemer eller nekting. Dersom intervjuobjektet ikke treffes, kan dette registreres i en av følgende grupper: ingen kontakt med intervjuobjektet eller intervjuobjektet utilgjengelig.

- bare den som har rettslig evne til å forplikte seg selv, kan avgi samtykke

- er respondenten under 15 år skal foresatte/foreldre gi samtykke til deltakelse. Er vedkommende over 15 år og under 18 år kan han/hun selv gi slikt samtykke, men foresatte/foreldre kan motsette seg dette og skal derfor også informeres.

2.3 Melding til Datatilsynet

2.3.1 Sensitive opplysninger
Innhenting av sensitive personopplysninger, jf personregisterloven § 6, annet ledd, etter pålagt oppgaveplikt eller fra administrative datasystemer, skal meldes Datatilsynet på fastsatt skjema i god tid før innsamlingen.

Meldingen skal inneholde hjemmel for innsamling, kopi av vedtak om pålagt oppgaveplikt samt en redegjørelse for forholdet til avgivers taushetsplikt. Det skal også redegjøres for formålet med og bruken av registeret, herunder om registeret skal kobles med andre personregistre.

2.3.2 Frivillige undersøkelser

Opprettelse av personregistre der opplysningen er innsamlet på frivillig grunnlag skal alltid meldes Datatilsynet i god tid før opprettelsen.

Meldingen skal inneholde kopi av den informasjon som gis respondentene, samt angivelse av registerets innhold. Det skal også redegjøres for formålet med og bruken av registeret, herunder om registeret skal kobles med andre personregistre.

2.3.3 Generelt

Datatilsynet kan på bakgrunn av meldingene sette ytterligere vilkår for opprettelse av registerene. Datatilsynet har, i særlige tilfeller jf personregisterloven § 9 jf §§ 6 og 10, adgang til å nekte opprettelse av registre inneholdende opplysninger innhentet på frivillig grunnlag.

Innhenting av personopplysninger som nevnt i konsesjonens punkt 2.3.1 og 2.3.2 skal ikke finne sted før kvittering fra Datatilsynet foreligger.

I tillegg til ovennevnte meldinger skal det sendes halvårlig rapport til Datatilsynet inneholdene kortfattede meldinger om alle personregistre som er opprettet i Statistisk sentralbyrå de siste seks måneder. Rapporten skal kort redegjøre for registrenes innhold, samt angi hjemmel for innhenting og om registrene tidligere er meldt Datatilsynet.

2.4 Utlevering av personopplysninger

Som personopplysninger regnes direkte identifiserbare og avidentifiserte, herunder krypterte, personopplysninger. Avidentifiserte personopplysninger er opplysninger som indirekte kan tilbakeføres til en identifiserbar enkeltperson.

Anonyme opplysninger er ikke å regne som personopplysninger. Begrensningene i utleveringsadgangen i dette punktet gjelder derfor ikke anonyme opplysninger. Som anonyme opplysninger regnes opplysninger som verken direkte eller indirekte kan knyttes til en identifiserbar enkeltperson.

2.4.1 Hovedregel

Personopplysninger fra registeret må ikke utleveres, uten i nedenforstående tilfelle.

2.4.2 Unntak - forskning og offentlig planlegging

Pålagt oppgaveplikt/administrative datasystemer

Opplysninger innhentet etter pålagt oppgaveplikt jf statistikkloven § 2-2, i henhold til andre lovbestemmelser som gir Statistisk sentralbyrå rett til å kreve opplysninger utlevert, eller fra administrative datasytemer jf statistikkloven § 3-2, kan likevel utleveres til statistisk bruk for forskningsformål og offentlig planlegging på følgende vilkår:

- mottaker må ha nødvendig konsesjon fra Datatilsynet
- opplysningene skal avidentifiseres i den grad formålet tillater
- når opplysningene er hentet fra andre offentlige organer, og det er tvil om utlevering bør finne sted, skal Statistisk sentralbyrå forelegge utleveringsspørsmålet for det avgivende organ

Mottaker av opplysningene er underlagt taushetsplikt, jf statistikkloven § 2-5 jf § 2-4, og må således ikke utlevere/offenliggjøre personidentifiserbare opplysninger. Når særlige grunner tilsier det kan Datatilsynet likevel gjøre unntak fra mottakers taushetsplikt.

Statistisk sentralbyrå kan ved utlevering stille vilkår blant annet om bruken av opplysningene, hvem som skal ha ansvar for og adgang til opplysningene, om oppbevaring og tilbakelevering av utlånt materiale, om tilintetgjøring av avskrifter m.m.

Frivillige undersøkelser

Personopplysninger innhentet på frivillig grunnlag kan utleveres til statistisk bruk for forskningsformål og offentlig planlegging på følgende vilkår:

- den registrerte skal særskilt ha samtykket i utleveringen
- mottaker må ha nødvendig konsesjon fra Datatilsynet
- opplysningene skal avidentifiseres i den grad formålet tillater

Mottaker av opplysningene er underlagt taushetsplikt, jf statistikkloven § 2-5 jf § 2-4, og må således ikke utlevere/offenliggjøre personidentifiserbare opplysninger. Når særlige grunner tilsier det kan Datatilsynet likevel gjøre unntak fra mottakers taushetsplikt.

Statistisk sentralbyrå kan ved utlevering stille vilkår blant annet om bruken av opplysningene og om hvem som skal ha ansvar for og adgang til opplysningene, om oppbevaring og tilbakelevering av utlånt materiale, om tilintetgjøring av avskrifter m.m.

2.4.3 Unntak - næringslivsopplysninger

Med hjemmel i statistikkloven § 2-5 godkjenner Datatilsynet at følgende næringslivsopplysninger utleveres til bruk for opprettelse og oppdatering av offentlige og private registre:

- navn, adresse, eierform (enhetstype) for juridiske personer og for andre som driver næringsvirksomhet
- adresseopplysninger
- bransje (næringsgruppekode), sektorkode
- sysselsetting (i grupper etter antall sysselsatte/årsverk)
- status-kode (om virksomheten er i vanlig drift, ute av drift, opphørt, m v).
- foretaks-/enhets-/organisasjonsnummer
- datoer for stiftelse/registrering og endring av ovennevnte opplysninger

Følgende vilkår gjelder for utlevering:

- mottaker må ha nødvendig konsesjon fra Datatilsynet, eventuelt være fritatt fra konsesjonsplikt jf personregisterloven § 41 eller forskriftene til personregisterloven. Registreringshjemmelen må omfatte innhenting av opplysningene fra Statistisk sentralbyrå, samt lagring og bruk av opplysningene til det aktuelle formålet.

Statistisk sentralbyrå skal dessuten påse at opplysningene oppdateres jevnlig og at tidligere versjoner skal slettes ved mottak av nye opplysninger. Mottakere skal også gjøres oppmerksom på at opplysningene ikke kan legges til grunn ved avgjørelser i enkeltsaker.

Når oppdatering som nevnt ovenfor skal skje ved kobling av registre skal koblingen skje ved Statistisk sentralbyrå.

2.4.4 Overføring til utlandet

Ved overføring av personopplysninger til utlandet skal dette meldes Datatilsynet på fastsatt skjema, jf personregisterlovens forskrifter § 8-1 jf personregisterloven § 36, såfremt Norge ikke har plikt til å foreta slik overføring etter folkerettslig overenskomst eller som følge av medlemsskap i internasjonal organisasjon.

2.4.5 Databehandlingsforetak

Utleveringsbestemmelsene i punktene 2.4.1 til 2.4.4 gjelder ikke for opplysninger som Statistisk sentralbyrå oppbevarer i egenskap av databehandlingsforetak. Det vises forøvrig til vilkår i SSBs konsesjon for databehandlingsvirksomhet.

Kobling av to eller flere registre med anonymt resultat, dvs at det ikke oppstår et nytt register og det ikke tilføres nye opplysninger til noen av de medvirkende registre, regnes ikke som opprettelse av et nytt register.

2.6.1 Pålagt oppgaveplikt/administrative datasystemer

Registre inneholdende opplysninger innhentet etter pålagt oppgaveplikt eller fra administrative datasytemer må bare kobles med egne eller andres registre, når dette anses nødvendig for å gjennomføre de oppgaver Statistisk sentralbyrå er pålagt i medhold av statistikkloven.

2.6.2 Frivillige undersøkelser

Registre inneholdende opplysninger innhentet på frivillig grunnlag må bare kobles med egne eller andres registre etter særskilt samtykke fra den registrerte. Det presiseres at også kobling av krypterte registre opprettet på frivillig grunnlag krever særskilt samtykke fra den registrerte.

2.6.3 Generelt

Det er ikke tillatt å koble registre i strid med formålet se pkt 1.1.

Foruten de tilfeller som er nevnt ovenfor, kan kobling bare skje med Datatilsynets tillatelse.

2.7 Taushetsplikt

Ansatte, personale og representanter som får tilgang til personregistre eller deler av disse, har taushetsplikt om forhold de får kjennskap til, jf statl § 2-4.

Autoriserte brukere nevnt under pkt 3, som ikke er underlagt lovbestemt taushetsplikt, skal undertegne særskilt taushetserklæring. Erklæringen skal oppbevares av den registeransvarlige.

Det samme gjelder personer som utfører service- eller vedlikeholdsoppdrag som nevnt i pkt 3 om bruk av eksterne konsulenter.

2.8 Innsynsrett etter personregisterloven § 7, tredje ledd

Innsynsrett etter personregisterloven § 7, tredje ledd gjelder for registre opprettet i henhold til denne konsesjonen.

2.5 Sletting av opplysninger

Den registeransvarlige skal slette eller anonymisere opplysninger som ikke lenger har betydning for formålet. Manuelt grunnlagsmateriale skal anonymiseres eller makuleres når registrering og kontroll har funnet sted.

Opplysninger om frafallsårsak skal slettes så snart analyse av det øvrige materialet innsamlet i den aktuelle undersøkelsen er gjennomført. Opplysningene skal likevel slettes senest et år etter innsamling.

Dersom navn, fødselsnummer eller annen personidentifikasjon ikke blir erstattet med kryptert nummer, må registrene anonymiseres så snart som mulig, senest innen et år.

Datatilsynet kan i forbindelse med den enkelte melding, på bakgrunn av opplysningenes art, fastsette lenger oppbevaringstid slik at opplysningene må anonymiseres innen annen fastsatt frist.

Det skal tas hensyn til gjeldende arkiveringsbestemmelser.

Frivillige undersøkelser
Personopplysninger innhentet på grunnlag av frivillighet skal slettes/anonymiseres innen 6 måneder, så fremt det ikke er innhentet særskilt samtykke fra respondenten til oppbevaring utover dette. Slettefrist for materialet skal i sistnevnte tilfelle fastsettes i forbindelse med den enkelte melding, jf konsesjonens punkt 2.3.2.

Enhver som ber om det kan, så lenge materialet er personidentifiserbart, kreve seg slettet fra registre inneholdende opplysninger innhentet på frivillig grunnlag.

2.6 Kobling

I denne konsesjonen er kobling ment som elektronisk samkjøring av personregistre i den hensikt å opprette et nytt register, eller å tilføre nye typer opplysninger til de personregistre som kobles.

Dersom to eller flere registre kobles slik at det oppstår et tredje, anses dette som opprettelse av et nytt konsesjonspliktig personregister jf personregisterlovens § 9. Registeret skal meldes innenfor rammene som er satt i konsesjonens punkt 2.3 om melding til Datatilsynet.

Innsynsretten gjelder kun hvilke typer opplysninger som er tatt inn i registrene.

3 SIKKERHET

SSBs håndbok i datasikkerhet og fysisk sikring skal danne grunnlag for de sikkerhetstiltakene som SSB iverksetter.

Den registeransvarlige skal sørge for at det iverksettes tiltak for nødvendig sikring av konfidensialitet, kvalitet og tilgjengelighet for personopplysninger og registre.

3.1 Sikkerhetsstrategi

Det skal utarbeides en sikkerhetsstrategi som skal beskrive de overordnede mål og hensyn som skal ivaretas ved informasjonsbehandlingen. Denne kan omfatte taushetspliktsregler, behandlingsregler for informasjon og virksomhetens egne overordnede mål.

3.2 Autorisasjon

Autorisasjon er en administrativ bestemmelse om at noen kan få tilgang til informasjon.

Den registeransvarlige skal autorisere alle brukere av registeret slik at enhver bare har tilgang til den informasjon og de funksjoner som han eller hun har bruk for. Drifts- og vedlikeholdspersonale skal også autoriseres av registeransvarlig.

3.3 Kommunikasjon

Registeret skal føres i et edb-system (maskin, nett og program) som kun er, eller kan være, tilgjengelig for ansatte i SSB.

Eksterne tilknytninger som f eks E-post, Internett eller modem, skal forelegges Datatilsynet for godkjenning.

Dersom sensitive personopplysninger fra registeret skal overføres i datanett som virksomheten ikke kontrollerer (f eks telenett), skal opplysningene krypteres. Dette gjelder også registeropplysninger som overføres pr telefaks, disketter e l.

3.4 Tilgangskontroll

Tilgangskontroll innebærer at tekniske tiltak i edb-systemet sørger for at gyldige autorisasjoner følges i systemet. Tilgangskontrollen sørger for at ingen kan få tilgang utover sin autorisasjon eller at personopplysninger gjøres tilgjengelig for uautoriserte brukere. Dette omfatter ulike typer tilgang (lese, skrive, endre, utlevere osv).

Tilgangskontrollen skal gjennomføre kontroll av all tilgang til personopplysninger som lagres, behandles eller overføres i systemet. Kontrollen skal sikre at bare autorisert tilgang kan gjennomføres. Ved endring eller bortfall av en brukers autorisasjon skal brukerens tilgang reguleres tilsvarende.

3.5 Autentisering

Autentisering betyr å identifisere seg for edb-systemet slik at systemet til enhver tid kjenner riktig identitet til dem som bruker det. Brukernes identitet benyttes ved tilgangskontroll og logging.

Enhver bruker av edb-systemet skal autentiseres før han eller hun gis tilgang til systemet. Autentisering kan f eks skje ved at brukeren oppgir et passord.

3.6 Fysisk sikring

Skjermbilder, utskrifter e l som inneholder personopplysninger skal beskyttes mot innsyn fra uvedkommende.

Lokaler der registrering, utskrift og behandling foregår, skal være fysisk sikret.

Utenom arbeidstiden skal registre som bare føres manuelt eller manuelle deler av registeret, holdes under den registeransvarliges kontroll og være nedlåst. Det samme gjelder manuelle navne- og kodelister.

3.7 Frigivelse av lagringsmedia

Lagringsmedia (disk, diskett, tape e l) kan ikke frigis til uvedkommende uten at personopplysningene er slettet på en slik måte at rekonstruksjon er umulig.

3.8 Tilgjengelighet

Det skal gjennomføres tiltak som sikrer at register og opplysninger er tilgjengelige når det er behov for dem.

Kopier av opplysninger og annet nødvendig materiale skal finnes med tanke på rekonstruksjon av registeret etter tap. Sikkerhetskopier må oppbevares trygt og adskilt fra edb-systemet.

3.9 Kryptering av fødselsnummer for lagring internt hos SSB

Kryptering skal følge retningslinjene i SSBs håndbok i datasikkerhet og fysisk sikring.

De nøkler/programmer som benyttes til kryptering av fødselsnummer, skal oppbevares/brukes slik at de må initieres av SSBs administrerende direktør eller personlig oppnevnt vararepresentant og personal- og økonomidirektør eller personlig oppnevnt vararepresentant.

3.10 Bruk av eksterne konsulenter

Foretak som skal drive service eller vedlikehold på maskin- eller programvare skal ha konsesjon fra Datatilsynet som databehandlingsforetak, jf personregisterloven § 22.

Slik konsesjon er ikke nødvendig når følgende tre vilkår er oppfylt:

- Når tilgang til personopplysninger ikke er påkrevd for oppdraget.
- Når oppdraget utføres i den registeransvarliges (eiers) lokaler under oppsyn av registeransvarlig eller den vedkommende bemyndiger.
- Når den som skal utføre oppdraget har underskrevet taushetserklæring. Se pkt 2.7 i denne konsesjonen.

3.11 Rapport ved sikringsbrudd

Datatilsynet skal ha en rapport ved følgende sikringsbrudd:

- datainnbrudd i edb-system som inneholder personregister,
- datainnbrudd i edb-system som kommuniserer med edb-system som inneholder personregister,
- innbrudd i lokaler hvor edb-utstyr er plassert,
- tyveri eller tap av edb-utstyr som inneholder personregister.

Rapporten skal inneholde en beskrivelse av hvordan innbruddet har skjedd og hvilke personregistre som er eller kan ha vært berørt.

4 KONTROLL

Datatilsynet kan uten hinder av taushetsplikten kreve de opplysningene som er nødvendige for å kontrollere at konsesjonsvilkårene oppfylles, jf personregisterloven § 5. For å kunne gjennomføre kontrollen, kan Datatilsynet kreve å få adgang til de steder der opplysninger er lagret og utstyret finnes. Datatilsynet kan kreve å få nødvendig bistand fra personalet på slike steder for å få utført prøvene eller kontrollene.

5 STRAFF

Brudd på Lov om personregistre av 9. juni 1978 nr 48 og forskrifter gitt i medhold av dette og betingelser satt i denne konsesjonen, straffes med bøter eller fengsel i inntil 1 år eller begge deler, jf personregisterloven § 38.

6 FORBEHOLD OM ENDRINGER

Dersom det skjer endringer i foretakets virksomhet som går ut over bestemmelsene i denne konsesjonen, må det søkes om ny konsesjon. Dersom foretakets virksomhet skal opphøre, må det meldes til Datatilsynet. Det må også gis melding om adresseendringer.

Datatilsynet tar forbehold om å trekke konsesjonen tilbake, eller gi nye og endrede vilkår når dette er nødvendig ut fra personvernhensyn, herunder av hensyn til sikring av de registrerte personopplysninger.

Knut-Brede Kaspersen (e f)
rådgiver

Åste Marie Bergseng
førstekonsulent

Vedlegg: Taushetserklæring
Informasjonsskriv om sikkerhetsstrategier

DATATILSYNET

TAUSHETSERKLÆRING FOR PERSONER SOM HAR ADGANG TIL KONSESJONS-PLIKTIG PERSONREGISTER, JF. LOV OM PERSONREGISTRE M.M. AV 9.6.1978 § 11 ANNET LEDD

Firma: .....

Navn: .....

Stilling: .....

Jeg forplikter meg med dette til å bevare taushet om personopplysninger jeg får kjennskap til ved at jeg har adgang til register som er konsesjonspliktig etter ovennevnte lovs § 9, første ledd.

Dette er ikke til hinder for utlevering av personopplysninger i samsvar med konsesjonsvilkår gitt i medhold av personregisterloven § 11, annet ledd. Slik utlevering skal bare skje i samråd med registeransvarlig.

Jeg er kjent med at forsettlig eller uaksomt brudd på taushetsplikten, eller medvirkning til dette, kan straffes med bøter eller fengsel inntil ett år eller begge deler etter Lov om personregistre m.m. av 9.6.1978 nr. 48 § 38 nr. 2.

NB! **Erklæringen skal oppbevares av den registeransvarlige etter at den er underskrevet.**

Sted: ..... den / 19

.....

underskrift

Datatilsynet

Søknad om tillatelse (konsesjon) til å drive databehandlingsvirksomhet

Jf personregisterloven § 22 første ledd, jf forskrifter gitt av Justisdepartementet 21. desember 1979 kapittel 5

Datatilsynet
Postboks 8177 Dep
0034 OSLO

Tlf 22 42 19 10

S	Person	Navn (fylles ikke ut av organ/foretak)		Fødselsdato
Ø	Organ/foretak	Navn		Foretaksnr/organisasjonsnr
K		Gate/vei		Telefon
E		Postadresse	Kontaktperson	
R		Postnummer / Poststed	Telefon	

1. Hva gjelder søknaden?

☐ Ny virksomhet som ikke tidligere har søkt om tillatelse

☐ Endring av eksisterende tillatelse

2. Tidspunkt for igangsettelse

Når er det planlagt at virksomheten skal starte?

3. Har foretaket tidligere vært i kontakt med Datatilsynet?

☐ Ja. Hvis ja, oppgi Datatilsynets referansenr _____

_____

☐ Nei

4. Hvilke tjenester tilbyr søker

☐ Service og vedlikehold

☐ Informasjonsformidling

☐ Overtakelse av drift (i kundens lokaler)

☐ Overtakelse av drift og flytting av edb-system til søkers lokaler

☐ Utbytting/reparasjon av lagringsmedia

☐ Annet, gi beskrivelse

_____

_____

_____

5. Har foretaket annen virksomhetskonsesjon fra Datatilsynet?

☐ Ja. Hvis ja, oppgi Datatilsynets referansenr _____

_____

☐ Nei

6. Hvilke registre får søker tilgang til eller skal behandle som gjør at det er nødvendig med databehandlingsvirksomhetskonsesjon?

_____

_____

_____

_____

_____

_____

Utarbeidelse av en sikkerhetsstrategi

Hva er en sikkerhetsstrategi?
Sikkerhetsstrategier danner grunnlaget for tiltak og gir føringer for hvordan organisasjonen skal ivareta informasjonssikkerheten. Strategien skal være nedfelt i et dokument. Strategien skal også være en motivasjonskilde for de ansatte i arbeidet med informasjonssikkerhet. Gjennom arbeidet med strategien skal de ansatte få et bevisst forhold til hva informasjonssikkerhet er og hvorfor organisasjonen trenger det.

For å sikre informasjonen og edb-systemet må vi vite hvilken informasjon og hvilke deler av edb-systemet som skal beskyttes, hvordan vi kan beskytte det og hvor mange ressurser som skal brukes. Sikkerhetsstrategien skal gi svar på disse spørsmålene.

Toppledelsens ansvar
Informasjonssikkerhet er et ledelsesansvar. Gjennom utarbeidelsen av en sikkerhetsstrategi har ledelsen mulighet til å sette sikkerhet på dagsordenen, og gi sin støtte til arbeidet med informasjonssikkerhet i organisasjonen.

Informasjonssikkerhet
Informasjonssikkerhet er tiltak og rutiner som etableres for å beskytte informasjon og edb-systemets konfidensialitet, tilgjengelighet og kvalitet.

- *Konfidensialitet* innebærer at data og informasjon gjøres tilgjengelig bare for autoriserte personer, enheter og prosesser, til fastsatte tider og etter fastsatte rutiner.
- *Tilgjengelighet* innebærer at autoriserte personer har tilgang til informasjon og systemer, og kan bruke dette på tilsiktet måte når det er behov for det.
- *Kvalitet* innebærer at data og informasjon er korrekt, oppdatert og fullstendig i forhold til det de skal representere, og at denne tilstanden opprettholdes over tid.

Forarbeider til en sikkerhetsstrategi
Som forarbeider til en sikkerhetsstrategi hører følgende oppgaver:

(1) Identifisere informasjonen og ressursene som skal sikres, og klassifisere informasjon. (Se under for forklaring.)
(2) Gjennomføre sikkerhetsanalyser (risikovurderinger, sårbarhetsanalyser).
(3) Definere ansvarlige.
(4) Klarlegge rapporteringsveier og rapporteringssituasjoner.

1 Før det kan iverksettes sikkerhetstiltak, må organisasjonens informasjon kartlegges og klassifiseres etter beskyttelsesbehov. Klare indikasjoner på beskyttelsesbehov er f eks taushetsplikt og ulike graderinger.

Å klassifisere informasjon innebærer at vi vurderer den informasjonen vi håndterer for å se hvor viktig det er å sikre den mot at uvedkommende får tak i eller kjennskap til den, om informasjonen er tilgjengelig når vi har behov for det eller at informasjonen er korrekt.

På samme tid er det viktig å se på avhengigheten av edb-systemet. Hvor viktig er det at systemet er tilgjengelig, trenger vi tilgang til skriverne hele tiden, osv.

2 Sikkerhetsanalyser er et godt verktøy for å få oversikt over dagens sikkerhetsnivå, se hvor organisasjonen er mest sårbar, hvilke hendelser organisasjonen må beskytte seg mot og hvilken skade organisasjonen kan akseptere. Målsettingen med sikkerhetsanalyser er blant annet å få en oversikt over og anslå:

- Organisasjonens avhengighet av informasjonen og edb-systemet.
- Hvilket skadeomfang organisasjonen kan akseptere. Dette er en kombinasjon av organisasjonens vurderinger og lover og regler på området. F eks at organisasjonen kan akseptere et driftsavbrudd på maksimalt 2 dager.
- Hendelser som kan føre til brudd på informasjonssikkerheten, og hvor sannsynlige disse hendelsene er.

- Konsekvenser/skade ved brudd på informasjonssikkerheten. F eks hvilke konsekvenser får det for organisasjonen hvis systemet er ute av drift i 12 timer.
- Hvilke mottiltak finnes, og hva koster det å beskytte seg?
- Hvilke sikkerhetstiltak skal organisasjonen iverksette gjennom en kost/nytte vurdering av de ulike tiltakene.

3 Blant de funksjonene som bør besettes er:

- *Registeransvarlig* - Utpekes i konsesjonen fra Datatilsynet. Som regel den faglig ansvarlige for området, f eks medisinsk ansvarlig for et journalsystem.
- *Sikkerhetsansvarlig* - Vedkommende skal ha hovedansvaret for totalsikkerheten i organisasjonen. Det være seg den fysiske (adgangskontroll, låser, brannvarsling), administrative (sikkerhetsklarering av personalet) eller den edb-tekniske sikkerheten.
- *Systemansvarlig* - Ansvarlig for et fagsystem, f eks gi tilgang til nye brukere. Hvis dette systemet er et personregister skal systemansvarlig være autorisert av registeransvarlig.
- *Driftsansvarlig* - Har ansvaret for drift og vedlikehold av de ulike edb-systemene.

4 Klarlegge rapporteringsveier og rapporteringssituasjoner. Med dette menes at det er klart hvem det skal rapporteres til når et sikkerhetsbrudd oppstår, og at det er klart definert hva som anses som et sikkerhetsbrudd.

Eksempler på sikkerhetsbrudd som skal rapporteres kan være: nettverket er "nede" lenger enn 20 min eller mer enn fem mislykkede innloggingsforsøk.

Når organisasjonen har gjort disse oppgavene vil utarbeidelsen av en sikkerhetsstrategi kun være å bestemme hvem som skal ha de ulike funksjonene, hvilke tiltak som skal iverksettes og fastsette dato for neste gjennomgang av informasjonssikkerheten.

Kostnader og sikringsgrad
Sikringstiltakene som iverksettes, skal ikke koste mer enn kostnaden ved de sikkerhetsbruddene de skal beskytte mot. Vurderingen av kostnader ved immaterielle skader som f eks følelsen hos den registrerte hvis sensitiv opplysninger kommer på avveie, eller negativ omtale i media av organisasjonen pga sikkerhetsbrudd, kan være vanskelig.

Datatilsynet vurderer det slik at hvis sensitive personopplysninger blir gjort kjent for uvedkommende, eller manipuleres med, kan skaden være så stor at sensitive personopplysninger må defineres som opplysninger som skal ha det høyeste nivå av sikkerhet.

All erfaringer tilsier at de fleste sikkerhetsbrudd blir begått av egne ansatte. Datatilsynet anbefaler at man konsentrerer sikkerhetstiltakene til dette området.

En sikkerhetsstrategi skal ha følgende innhold:

- En oversikt over den informasjonen og de edb-ressursene som skal beskyttes.
- En beskrivelse av hvorfor organisasjonen skal sikre informasjonen og edb-ressursene, og en erklæring fra ledelsen hvor den støtter arbeidet med informasjonssikkerhet.
- En beskrivelse av de hovedtiltakene som er gjort/skal gjøres, og de målsettingene organisasjonen ønsker å oppnå.
- Fordeling av ulike roller og oppgaver i forbindelse med informasjonssikkerheten.
- Definere hva som regnes som sikkerhetsbrudd, og hvem vi rapporterer ulike former for sikkerhetsbrudd til.
- Oppfølging av sikkerhetsarbeidet. Når skal strategien revideres, hvordan skal vi sjekke om tiltakene er effektive, o a.

Statistisk sentralbyrå
Statistics Norway

Melding om opprettelse av personregister med sensitivt innhold og andre registre opprettet på frivillig grunnlag jfr. rammekonsesjon 97/1805-1 av 25.6.97

SSBs reg. nr.:

Eier av registeret

Navn (organ, foretak, person): Statistisk sentralbyrå
Arbeidsgivernr: 3444 7837

Gate-/veiadresse: Kongensgate 6

Postadresse: Postboks 8131 Dep.
Postnr. og -sted: 0033 OSLO
Telefon: 22 86 45 00

Ansvarlig for registeret
Leder i sikkerhetsutvalget:
Telefon:

Kontaktperson:
Seksjonssjefen ved:
Telefon:

Meldingen gjelder

☐ **Nytt register** ☐ **Endring** ⇨ **Datatilsynets saksnr på opprinnelig melding:**

Tidspunkt for opprettelse/-hjemmelsgr.lag

Oppstartingsdato: **Dag** **Mnd** **År**

Hjemmelsgrunnlag:
☐ **Frivillig**
☐ **Oppgaveplikt (jfr. Statistikkloven)**

Registerets navn/type undersøkelse

Navn:
Type undersøkelse:

Omfanget av registeret

Enhet:
Tall på enheter:
Identifikasjonsbegrep:

Kilder/metode

Hvor opplysningene hentes fra:
☐ **Enhetene selv** ☐ **Register:**
Hvordan opplysningene hentes inn:

Ajourhold/ anonymi-sering/sletting

Tidspunkt for sletting/anonymisering:
☐ **6 mnd** ☐ **Krypteres**
☐ **1 år**
☐ **Annet, spesifisér** **Dag** **Mnd** **År**

Ajourhold:
☐ **Engangsprosjekt**
☐ **Holdes ajour til:** **Dag** **Mnd** **År**

Vedlegg

☐ **Kopi av informasjonsbrev**
☐ **Spørreskjema**
☐ **Kopi av vedtak om oppgaveplikt**
☐ **Beskrivelse av endring**
☐ **Kopi av dispensasjon fra avgivers taushetsplikt**
☐ **Annet, spesifiser:**

Undertegnede er kjent med de vilkår som er gitt konsesjon samt personregisterloven og forskrifter. Melding vil bli sendt Datatilsynet dersom det skjer endringer i registeret i forhold til det som er angitt i denne melding.

Dato, ansvarlig for registeret

Veiledning til meldeskjema for opprettelse/endring av personregistre som inneholder sensitive personopplysninger og for personregistre der opplysningene er innhentet på frivillig grunnlag.

I den nye rammekonsesjonen er det fastsatt nye regler for melding av personregistre til Datatilsynet. Bare personregistre der opplysningene er innhentet på frivillig grunnlag og personregistre som inneholder sensitive personopplysninger skal meldes fortløpende til Datatilsynet. Andre registre skal bare rapporteres hvert halvår på egne halvårsskjemaer. Her skal alle nyopprettede/endrede personregistre rapporteres, m.a.o også de registre som allerede er meldt på egne skjemaer.

Eier av registeret

Eier av registeret er SSB. Som ansvarlig for registeret angis navnet på leder av sikkerhetsutvalget. I praksis vil registeransvaret bli delegert fra leder i sikkerhetsutvalget til seksjonssjef.
Som kontaktperson angis navnet på seksjonssjefen i den seksjon som skal opprette/endre registeret.

Meldingen gjelder

Her krysses det av for hvorvidt det dreier seg om et nytt register eller en endring av et allerede eksisterende register.

- Det vil være en endring dersom registeret f.eks. er tilført nye opplysninger, skal oppbevares lenger enn tidligere angitt, brukes på annen måte enn tidligere angitt mv.
- Dersom det er foretatt koblinger som resulterer i et nytt register, skal registeret meldes som nytt. Koblinger som resulterer i statistikk skal ikke meldes.

Tidspunkt for opprettelse/ hjemmelsgrunnlag

Det er dato for opprettelse eller endring av registeret som her skal angis, evt. antatt oppstartingsdato.

Dersom det er snakk om endring av et register eller opprettelse av et register som resultat av en kobling, må det angis hjemmelsgrunnlag for de opprinnelige registre.

Registerets navn/ type undersøkelse

Her er det navnet på det nye registeret, evt. det endrede registeret, som skal angis.

Med *type undersøkelse* menes hvorvidt det dreier seg om f.eks. intervjuundersøkelse eller skjemabasert spørreundersøkelse eller f.eks. innhenting av registeropplysninger.

Omfanget av registeret

Med *enheter* siktes det til hvorvidt registeret er systematisert på personer, bedrifter, husstander mv.

Tall på enheter vil vise registerets omfang og vil kunne være omtrentlig.

Identifikasjonsbegrep vil f.eks. kunne være fødselsnummer eller bedriftsnummer.

Kilder/metoder

Kilde for opplysningene vil være enten enhetene selv eller et eller flere registre.

Ved frivillige undersøkelser vil det være enhetene selv som angis som kilde. Dersom det dreier seg om oppgavepliktige undersøkelser vil kilde også kunne være enhetene selv, f.eks. bedrifter.

Det skal også opplyses om hvordan opplysningene hentes inn. Her vil det være aktuelt å opplyse om hvorvidt opplysningene innhentes manuelt eller elektronisk, evt. også hvorvidt opplysningene innhentes ved intervju eller ved utfylling av skjemaer. (Dersom dette ikke allerede er oppgitt ovenfor.)

Ajourhold/anonymisering/ sletting

Anonymisering kan skje i stedet for sletting. Kryptering regnes ikke som anonymisering, men dersom det ikke er satt en særskilt frist for sletting kan kryptering skje isteden for anonymisering/sletting.

I henhold til den nye rammekonsesjonen skal opplysninger som er innhentet på frivillig grunnlag slettes/anonymiseres innen 6 måneder såfremt det ikke er innhentet særskilt samtykke fra respondenten til oppbevaring utover dette. Dersom lagringstiden har kommet klart frem i informasjonsbrevet til respondenten vil samtykke til deltagelse i undersøkelsen anses som tilstrekkelig samtykke til den angitte lagringstid.

Når det gjelder andre registre enn de frivillige er konsesjonens hovedregel at opplysninger skal slettes/anonymiseres snarest mulig og senest innen ett år. Datatilsynet vil på bakgrunn av opplysningenes art kunne fastsette særskilt anonymiserings-/slettefrist.

Dersom registeret hverken skal slettes, anonymiseres eller krypteres innen 6 måneder eller 1 år, skal det krysses av for *annet*. Det må i såfall angis dato for *når* et av alternativene er aktuelt. Det må også i eget vedlegg redegjøres for hvorfor det anses som nødvendig å opprettholde registeret i fullt ut identifiserbar form utover 6 måneder eller 1 år.

Vedlegg

- *Kopi av informasjonsbrev.* Det er kopi av det informasjonsbrev som sendes oppgavegiverne/intervjuobjektene ved frivillige undersøkelser som skal vedlegges meldingen.

- Kopi av *Spørreskjema* skal også alltid vedlegges ved frivillige undersøkelser.

Datatilsynet aksepterer at spørreskjema ikke alltid er ferdig utformet på det tidspunkt det er aktuelt å sende meldingen. Det vil være anledning til å foreta mindre justeringer/endringer i spørreskjemaet også etter at Datatilsynet har godkjent opprettelse av personregister uten at dette utløser ny meldeplikt. Det er en forutsetning at det kun dreier seg om f.eks. språklige eller redaksjonelle endringer, og ikke realitetsendringer som f.eks. at det tilføres nye spørsmål eller at spørsmålene «endrer karakter».

- *Kopi av vedtak om oppgaveplikt.* Dette er nytt i forhold til tidligere. Vedtak om bruk av oppgaveplikt fattes av administrerende direktør

og vil inneholde henvisning til hjemmelsgrunnlag. Vedtaket vil fremgå av referat fra direktørmøtet. (Se for øvrig Interne Dokumenter 97/1: Lovhjemmel ved datainnsamling.

- *Beskrivelse av endring.* Dersom registeret f.eks. skal tilføres nye opplysninger må det redegjøres for på hvilken måte dette skjer, f.eks. ved kobling av to eller flere registre, eller ved annen type innhenting av tilleggsinformasjon. Navn på registre som kobles og angivelse av nummer på tidligere meldinger er nødvendig samt evt. hvilke opplysningstyper som tilføres/fjernes. Dersom endringen består i endring av formål eller bruk, eller endret lagringstid, må dette begrunnes.

- *Kopi av dispensasjon fra avgivers taushetsplikt.* I henhold til statistikkloven kan oppgaveplikt pålegges enhver såfremt taushetsplikt ikke er til hinder for det. Det vil være nødvendig å innhente dispensasjon fra taushetsplikten dersom det f.eks. skal innhentes administrative registre fra en annen etat og disse er regulert av en særlov som har en strengere taushetspliktbestemmelse enn forvaltningsloven, (dvs. der det ikke uten videre kan utleveres opplysninger til statistikk og forskning.) Det er vedkommende etats fagdepartement som behandler søknader om dispensasjon.

Taushetserklæring

Jeg forstår

- at jeg i mitt arbeide vil kunne få kjennskap til opplysninger som av hensyn til offentlige, enkeltpersoners, institusjoners og bedrifters interesser, ikke må bli kjent for uvedkommende.

- at jeg i mitt arbeide tilknyttet Statistisk sentralbyrå også vil kunne få kjennskap til sikkerhetsrutiner, sikkerhetsinstrukser og annet som regulerer Statistisk sentralbyrås sikkerhet og som ikke må bli kjent for andre.

- at arbeidet i Statistisk sentralbyrå krever ansvarsfølelse, lojalitet og respekt for oppgavegivernes rett til vern mot urettmessig eller skadelig bruk av opplysninger.

- at passord som gir tilgang til opplysninger ikke må overdras eller meddeles andre personer i eller utenfor Statistisk sentralbyrå.

Jeg forplikter meg til

- å vise aktsomhet i behandlingen av alle opplysninger som Statistisk sentralbyrå henter inn samt befinner seg i Statistisk sentralbyrås personregistre i samsvar med retningslinjer og instrukser gitt av Statistisk sentralbyrå og Datatilsynet.

- ikke å gi opplysninger til noen personer i eller utenfor Statistisk sentralbyrå som ikke har krav på å få disse i sitt arbeid. Personlig passord kan under ingen omstendigheter gis til andre.

- ikke gi opplysninger om resultater av statistiske undersøkelser før Statistisk sentralbyrå har frigitt dem til offentliggjøring.

Jeg er klar over

- at brudd på taushetsplikten og misbruk av den informasjon jeg ellers får kunnskap om kan medføre straffansvar og suspensjon/avskjed fra tjenesten.

- at taushetsplikten også gjelder etter at mitt arbeid tilknyttet Statistisk sentralbyrå er avsluttet.

Jeg er gjort kjent med

- de lovbestemmelser og instrukser som er gjengitt på baksiden.

_____ _____

Sted Dato

_____

Underskrift

Taushetserklæringen er underskrevet i mitt påsyn:

_____ _____

Underskrift Dato

MODELLAVTALER VED UTLEVERING AV DATA FRA STATISTISK SENTRALBYRÅ OG MODELLBREV FOR AVSLAG PÅ SØKNAD OM UTLEVERING.

Innhold:

- **Avtale 1:** **Innvilget utlevering til forskning.**
- **Avtale 2:** **Innvilget utlevering til offentlig planlegging.**
- **Avtale 3:** **Innvilget utlevering av registerdata.**
- **Avtale 4:** **Utlevering av anonymiserte data.**
- **Malbrev om avslag på søknad om data.**

Modellavtalene inneholder ikke økonomiske betingelser. Slike betingelser kan selvfølgelig tas med i et oversendingsbrev når det er praktisk. I brevet må det stå at avtalen skal undertegnes i to originaleksemplarer, og at partene beholder en original hver.

Statistisk sentralbyrå
Statistics Norway

1. Innvilget utlevering til forskning

(Til bruk ved utlevering av identifiserbare/avidentifiserte data)

Deres søknad av / 19 om utlevering av data til prosjektet
xxxx
er innvilget med hjemmel i Statistikklovens § 2-5 (1) og Datatilsynets Rammekonsesjon for Statistisk sentralbyrå av 27.4.1990 pkt 4.3.1 som følger vedlagt.

Dataene vil bli utlevert etter at De har bekreftet skriftlig at følgende betingelser vil bli overholdt:

a) Dataene skal behandles i samsvar med Deres konsesjon fra Datatilsynet datert / 199 som vi har mottatt en kopi av.

b) Forskningsresultatene må ikke offentliggjøres på en slik måte at den kan henføres til enkeltpersoner. Videre må forskningsresultatene heller ikke offentliggjøres på en måte som kan fryktes å være til skade for oppgavegiver eller annen identifiserbar enkeltperson dersom oppgavegiver eller enkeltpersonen er en offentlig virksomhet eller et foretak.

c) Opplysningene må behandles bare av personale som er underlagt taushetsplikt etter statistikklovens (lov av 16. juni 1989 nr 54) § 2-4, og brudd på denne taushetsplikten kan medføre straffeansvar etter samme lovs § 5-1 nr. 2 jfr. straffelovens § 121. Videre må opplysningene bare brukes til det formålet som er oppgitt i Deres søknad og må ikke overlates til andre.

d) (1) Opplysningene er samlet inn av Statistisk sentralbyrå på frivillig grunnlag. Oppgavegiverne har overfor Statistisk sentralbyrå samtykket i at opplysningene brukes til dette formålet. Uten samtykke fra Statistisk sentralbyrå må De ikke henvende Dem til oppgavegiverene.

eller:

(2) Opplysningene er samlet inn av XXX som har samtykket i at de brukes til dette formålet. (Dette gjelder bare når Statistisk sentralbyrå er i tvil om utlevering er forsvarlig, se rammekonsesjonen pkt. 4.3.1.)

Hvis Statistisk sentralbyrå har samlet inn opplysningene direkte fra oppgavegiver med hjemmel i statistikkloven, faller punkt d) bort.

e) Når prosjektet er avsluttet og senest innen ../.. 19.., må De slette alle mottatte data, inklusive alle utskrifter og kopier av disse og bekrefte dette skriftlig overfor Statistisk sentralbyrå.

For Statistisk sentralbyrå: **For:**

....

(registeransvarlig)

Statistisk sentralbyrå
Statistics Norway

2. Innvilget utlevering til offentlig planlegging.

(Bare avidentifiserte data kan utleveres.)

Deres søknad av ../.. 199 om utlevering av data til prosjektet
xxxx
er innvilget med hjemmel i Statistikklovens prgr. 2-5 (1) og Datatilsynets Rammekonsesjon for Statistisk sentralbyrå av 27.4.1990 pkt 4.3.2 som følger vedlagt.

Dataene vil bli utlevert etter at De har bekreftet skriftlig at følgende betingelser vil bli overholdt:

a) Dataene må bare brukes til statistisk formål. Resultater må ikke offentliggjøres på en slik måte at den kan henføres til enkeltpersoner. Videre må resultatene heller ikke offentliggjøres på en måte som kan fryktes å være til skade for oppgavegiver eller annen identifiserbar enkeltperson dersom oppgavegiver eller enkeltpersonen er en offentlig virksomhet eller et foretak.

b) Opplysningene må behandles bare av personale som er underlagt taushetsplikt etter statistikklovens (lov av 16. juni 1989 nr 54) § 2-4, og brudd på denne taushetsplikten kan medføre straffeansvar etter samme lovs § 5-1 nr. 2 jfr. straffelovens § 121. Videre må opplysningene bare brukes til det formålet som er oppgitt i Deres søknad og må ikke overlates til andre.

c) (1) Opplysningene er samlet inn av Statistisk sentralbyrå på frivillig grunnlag. Oppgavegiverne har overfor Statistisk sentralbyrå samtykket i at opplysningene brukes til dette formål.

(2) Opplysningene er samlet inn av XXX
som har samtykket i at de brukes til dette formålet. (Dette gjelder bare når Statistisk sentralbyrå er i tvil om utlevering er forsvarlig, se rammekonsesjonen pkt 4.3.2.)

Hvis Statistisk sentralbyrå har samlet inn opplysningene direkte fra oppgavegiver med hjemmel i statistikkloven, faller punkt c) bort.

d) Når prosjektet er avsluttet, senest innen ../.. 19.., må De slette alle mottatte data, inklusive alle utskrifter og kopier av disse og bekrefte dette skriftlig overfor Statistisk sentralbyrå.

For Statistisk sentralbyrå: **For :**

....
(registeransvarlig)

Statistisk sentralbyrå
Statistics Norway

3. Innvilget utlevering av registerdata.

(Dette er ikke fortrolige data. Det er bare Seksjon for bedriftsregister som skal levere data fra Bedrifts- og fortaksregisteret.)

Deres søknad av xxxx om utlevering av data til prosjektet
xxxx
er innvilget med hjemmel i Statistikklovens prgr. 2-5 (1) og Datatilsynets Rammekonsesjon for Statistisk sentralbyrå av 27.4.1990 pkt 4.3.3. som følger vedlagt.

Følgende data vil bli utlevert fra vårt register: Her følger en spesifikasjon av hvilke deler av registeret det gjelder, hvilke data, hyppighet og tidspunkt for levering.

Dataene vil bli utlevert etter at De har bekreftet skriftlig at følgende betingelser vil bli overholdt:

a) Dataene skal behandles i samsvar med Deres konsesjon fra Datatilsynet datert xxxx som vi har mottatt en kopi av.

b) Dataene kan ikke overlates til andre uten tillatelse fra Statistisk sentralbyrå.

c) Dersom de finner feil i de mottatte data, skal feilene meldes slik vedlagte skjema/instruks beskriver. (Dette punktet tas bare med der seksjonen finner det gunstig.)

d) De mottatte data kan brukes i .. dager/måneder og skal da erstattes av nye data fra Statistisk sentralbyrå som behandles etter samme regler.

e) Denne avtalen kan sies opp fra begge parter med .. måneders varsel.

For Statistisk sentralbyrå: **For:**

....
(registeransvarlig)

Statistisk sentralbyrå
Statistics Norway

4. Utlevering av anonymiserte data.

Deres søknad om data til xxx er innvilget ved utlevering av anonymiserte data til formålet. Dataene vil bli utlevert etter at de skriftlig har bekreftet å godta følgende betingelser:

a) Dataene må bare brukes til statistisk formål. Resultater må ikke offentliggjøres på en slik måte at den kan henføres til enkeltpersoner. Videre må resultatene heller ikke offentliggjøres på en måte som kan fryktes å være til skade for oppgavegiver eller annen identifiserbar enkeltperson dersom oppgavegiver eller enkeltpersonen er en offentlig virksomhet eller et foretak.

b) Opplysningene må behandles bare av personale som er underlagt taushetsplikt. De må bare brukes til det formålet som er oppgitt i Deres søknad og må ikke overlates til andre.

d) Når prosjektet er avsluttet, må De slette alle mottatte data, inklusive alle utskrifter og kopier av disse og bekrefte dette skriftlig overfor Statistisk sentralbyrå.

Når vi stiller slike krav til anonymiserte data, skylles det at vi aldri kan se helt bort fra at personer med stor forhåndskunnskap om de individer dataene dekker, kan identifisere enkelte personer/foretak i det utleverte materialet.

For Statistisk sentralbyrå: **For:**

....

Adressatens navn
Postboks 1234
Postnummer Poststed

Seksjon eller avdeling
Oslo, 17. mars 1994
Deres ref.: AD, Vår ref.: 123456 ABC/DEF
Saksbehandler: Fornavn Mellomnavn Etternavn

Malbrev om avslag på søknad om utlevering av data

Deres søknad om data til xxxx er behandlet etter reglene i statistikkloven prgr 2-5 (1) og Datatilsynets rammekonsesjon for Statistisk sentralbyrå pkt 4.3.1/4.3.2/4.3.3 som følger vedlagt. (referer til det punkt som passer). Statistisk sentralbyrå har ikke funnet det riktig å innvilge søknaden ut fra disse reglene. (det bør her gis en begrunnelse for avslaget, f.eks.: Deres prosjekt faller ikke innenfor begrepet forskning/offentlig planlegging slik vi mener regelverket forutsetter.

Vårt avslag er et enkeltvedtak etter forvaltningslovens § 2 bokstav b, og kan påklages etter reglene i forvaltningslovens kapitel VI. Vedtaket påklages til Finansdepartementet som klageinstans, men klagen skal sendes til Statistisk sentralbyrå, Seksjon for..... Klagen må være skriftlig.

Fristen for å klage er 3 - tre - uker, og klagen skal angi det vedtak som det klages over, begrunnelsen for å klage og eventuelle andre opplysninger som kan ha betydning for bedømmelsen av klagen.

Med hilsen

(registeransvarlig)

Statistisk sentralbyrå
Sikkerhetsutvalget
10.03.97

UTLEVERING/TILBAKELEVERING AV DATA

Statistisk sentralbyrå kan på visse vilkår utlevere data som ikke er anonymisert, til forskning og offentlig planlegging. SSB har til nå ikke hatt noen rutiner for å følge opp at utleverte data blir tilbakelevert og/eller slettet. Sikkerhetsutvalget har sammen med Postekspedisjonen, utarbeidet et skjema til bruk for dette formålet. Skjemaet ***må brukes*** i alle tilfeller hvor det leveres ut data med betingelser om at dataene bare skal brukes til et bestemt formål og/eller skal returneres eller slettes på et gitt tidspunkt. ,

Skjemaet skal fylles ut av saksbehandler og sendes til Postekspedisjonen, sammen med følgebrevet til mottaker av dataene. Skjemaet blir liggende i saksmappen på Postekspedisjonen.

Postekspedisjonen har et system for påminnelse til seksjonene, ca 2 uker før retur-/slettedato. Posten vil da ta kopi av skjemaet i saksmappen og sende det til seksjonsleder ved ansvarlig seksjon. Seksjonene må selv følge opp i forhold til mottaker av dataene.

Det er nå sendt ut skjema til hver seksjonsleder ved fagseksjonene og kopi av skjema til alle avdelingsledere.

Ekstra skjemaer kan hentes på rekvisitarommmet i Oslo eller bestilles hos Erik Engebretsen.

Ordningen trer i kraft fra 1. mars 1997.

Statistisk sentralbyrå
Statistics Norway

Tilbakelevering av data

S.nr.:

Ansvarlig seksjon:	**Saksbehandler:**	**Utleveringsdato:**

Mottakers navn:
Adresse:
Postadresse:
Kontaktperson:

Hvilke data (tabell, individualdata, anonymisert,avidentifisert mv på diskett/lister e.l.)	**OBS-dato[1] (purredato):**

Seksjonsleder ved ansvarlig seksjon, vil få kopi av dette skjema som en påminnelse for purring av utlevert materiale, ca 2 uker før materiale er avtalt slettet eller tilbakelevert (OBS-dato).

[1] OBS-dato er den datoen utlevert materiale skal slettes eller returneres til SSB.

Statistisk sentralbyrå
Statistics Norway

Sikker databehandling i Statistisk sentralbyrå

1. Passord
Velg passord som er vanskelig å gjette. Hold det for deg selv.

2. Logg ut og lås etter deg
Logg ut når du avslutter arbeidet for dagen. Sørg for at uvedkommende ikke får adgang til terminalen din. Lås PCen hvis det er mulig.

3. Følg rutinene for reservekopiering
Ta backup regelmessig - det kan redde mye hvis ulykken er ute.

4. Beskytt dataene
Oppbevar diskettene slik at de ikke blir stjålet, misbrukt eller skadet.

5. Beskyttede data må ikke komme på avveie
Du har selv ansvar for at beskyttede data ikke kommer uvedkommende i hende. Makuler utskrifter med følsom informasjon du ikke lenger har behov for. Slett filer du ikke trenger.

6. Kopier ikke data uten tillatelse
Data som lagres sentralt i stormaskin skal ikke kopieres i lokalnett eller på PC uten at dette er godkjent av registereier.

7. Innføring av fremmede data må godkjennes
Bring ikke fremmede data eller programvare inn i datamaskinene uten at dette er godkjent på forhånd.

8. Unngå søl
Datautstyret tåler ikke kaffe, brus eller annet søl.

9. Hold utstyret fritt for støv
Statisk elektrisitet kan ødelegge data og utstyr. Støv er en av årsakene.

10. Respekter sikkerhetsbestemmelsene
Gjør deg kjent med Statistisk sentralbyrås sikkerhetsrutiner og instrukser.

MAL FOR ÅRLIG SIKKERHETSRAPPORT FRA AVDELINGENE

I sikkerhetsinstruks for avdelingsledere heter det i punkt 6:
" Avdelingslederen skal i januar hvert år sende en melding til Sikkerhetsutvalget om sikkerhetsarbeidet ved avdelingen". Rapporten skal bidra til å oppfylle Sikkerhetsutvalgets rapportering- og orienteringsplikt overfor administrerende direktør som gjelder i alle sikkerhetssaker.

Sikkerhetsrapporten skal dekke de områder avdelingsleder har ansvaret for iht. sikkerhetsinstruksen for avdelingsleder. Ut fra dette bør rapporten minst gi opplysninger om følgende:

1. Hvem som har ansvaret for sikkerheten (inkl. gitte fullmakter) ved avdelingen.

2. Hvilke sikkerhetstiltak som er gjennomført i løpet av året, opplæring, nye instrukser,m.v.

3. Antall meldinger sendt til Datatilsynet.

4. Praksis ved utlevering av data i året som gikk

5. Informasjon til nye medarbeidere - hva som blir gitt.

6. Kryptering av fødselsnummer - bruk av dette innen avdelingen.

7. Problemer som det arbeides med, opprydding i dataarkiv, nye instrukser m.v.

8. Spesielle problemer som avdelingen trenger hjelp til.

SL0, 18.12.96

Retningslinjer for:
Etablering av ny statistikk, frigiving av statistikk og forholdet til pressen

«Statistikk er tallfestede opplysninger om en gruppe eller et fenomen, som framkommer ved sammenstilling og bearbeiding av opplysninger om de enkelte enhetene i gruppen eller et utvalg av disse enhetene, eller ved systematisk observasjon av fenomenet.» (Statistikklovens § 1-2, første ledd.)

Med *statistikk* fra Statistisk sentralbyrå skal vi i disse retningslinjene mene:
- Tallfestede resultater fra produkter med egen datainnsamling, med oppgaveplikt ifølge statistikkloven eller basert på frivillighet
- Resultater fra regnskapssystemer basert på slike produkter

Analyser og forskningsresultater som bygger på ikke tidligere frigitte statistikker eller regnskaper, som Økonomisk utsyn og konjunkturrapportene, omfattes av det samme regelverk som for statistikk.

1. Etablering av ny statistikk

Vedtak om etablering av *ny løpende statistikk* eller gjennomføring av *engangsundersøkelser* gjøres ved godkjenning av Virksomhetsplanen (VP) eller direkte av administrerende direktør (DM). Slike saker skal fremmes, f.eks. i form av prosjektskriv, med dokumentasjon av prinsipper, definisjoner, bruk av oppgaveplikt og tvangsmulkt, opplegg for innsamling, revisjon/bearbeiding og publisering.

I god tid før *første gangs publisering* må publiseringsopplegget og resultatene godkjennes av ansvarlig avdelingsleder og administrerende direktør.

For enkelte statistikker/statistikkområder, f.eks. oppdragsbaserte intervjuundersøkelser, kan ansvaret delegeres til avdelingsleder, samtidig som forslag om undersøkelser som er kontroversielle forelegges administrerende direktør. Forslag om delegering fremmes av ansvarlig avdelingsleder.

2. Frigiving av statistikk

- Statistisk sentralbyrå bestemmer på helt selvstendig grunnlag *hva, når* og *hvordan* når det gjelder frigiving av statistikk
- Før statistikk frigis skal den godkjennes i henhold til de retningslinjer som er gitt nedenfor
- Statistikk skal frigis på et på forhånd annonsert tidspunkt så snart som mulig etter at den er ferdigstilt, og samtidig overfor alle brukere

2.1. Godkjenning og former for formidling

Normalt skal frigiving av statistikk skje ved en *pressemelding*, i *Ukens statistikk* og/eller gjennom *webtjenesten.* Pressemeldinger, bidrag til Ukens statistikk og bidrag til webtjenesten skal være godkjent av avdelingsleder eller den avdelingsleder delegerer ansvaret til. Kontroversielt stoff forelegges og utkast til pressemeldinger oversendes administrerende direktør. Pressemelding benyttes hvis statistikken inneholder en nyhet som det haster med å få publisert, og som antas å være så interessant for allmennheten at mediene formidler den videre.

Samtidig, eller i etterkant, kan det også foreligge en publikasjon, enten som en utgivelse i serien *NOS*, som artikler i *Økonomiske analyser* eller *Samfunnsspeilet*, eller de «gule seriene» *Månedsstatistikk over*

utenrikshandelen, Bank- og kredittstatistikk, Byggearealstatistikk, Aktuelle befolkningstall og *Bygginfo*. En nærmere omtale av de ulike publikasjonsseriene og godkjenningsprosedyrer er gitt i *Publiseringshåndboka* og i *SSB-info*.

Analyser og forskningsresultater vil normalt presenteres i form av en publikasjon, og godkjennings-prosedyrene følger de retningslinjene som gjelder for de ulike publikasjonene.

Etter frigiving vil brukere kunne få resultater basert på *nye uttak fra primærmaterialet eller fra databaser*. Dette regnes ikke som ny statistikk. For hver statistikk og for statistikk sammenstilt i databaser skal det foreligge retningslinjer som kvalitetssikrer slike uttak.

2.2. Statistikk-kalender

Fra og med 1. januar 1997 er det etablert en *statistikk-kalender*. Den viser *når* (hvilken dato) ny statistikk frigis de neste 3-4 månedene. Kalenderen viser dessuten *hvor* og *hvordan* statistikken frigis, dvs. om det er pressemelding, Ukens statistikk og/eller webtjenesten. Nærmere retningslinjer er gitt i *SSB-info*.

2.3. Adgang til statistikker før frigiving

For ansatte i SSB

Fagenhet, seksjons- og avdelingsleder og administrerende direktør kan få adgang til statistikken før den frigis. Også andre i SSB kan etter avtale få slik adgang hvis det er faglig begrunnet, men statistikken kan ikke direkte eller indirekte gjøres kjent utenfor SSB før den er formelt frigitt.

For spesielle brukere

Ordninger med forhåndsadgang til statistikk for spesielle brukere skal som hovedregel avvikles. Fra 1. januar 1997 er det bare ordninger som er godkjent av administrerende direktør (DM) som gjelder.

Følgende ordning er godkjent:

- Finansdepartementet får oversendt nasjonalregnskapets «marsregnskap» før frigiving av hensyn til arbeidet med revidert nasjonalbudsjett. Annen bruk av tallene er ikke tillatt før nasjonalregnskapstallene er frigitt fra SSB (DM, 25/9-1996).

Eiere av administrative data brukt til statistikkproduksjon

En rekke av våre produkter med egen datainnsamling er basert på administrative data. Dataeier vil i slike tilfeller (i prinsippet) selv kunne løpende ha kjennskap til tallmaterialet før vår frigiving. Slike tall kan også bli løpende publisert av registereiere, men vår statistikk kan avvike fra registereiers ved tilførsel av nye kjennetegn eller andre kontroller og revisjoner.

Ofte er det et samarbeid med dataeier om bearbeidingen av materialet for å sikre datakvaliteten. Slik kontakt er ikke i strid med reglene for frigiving av statistikk. Det er prinsipielt uheldig om de i denne sammenheng faktisk får adgang til vår bearbeidede statistikk før den frigis, men det kan være hensiktsmessig som et ledd i kvalitetssikringen. Det er imidlertid viktig at dataeier ikke videreformidler vår statistikk eller utnytter den i sin saksbehandling før den er frigitt fra SSB. Dette kan unngås hvis vi strikt holder oss til regelen om at statistikken skal frigis så snart som mulig etter at den er ferdigstilt.

De tilfeller der eiere av administrative data gis adgang til vår bearbeidede statistikk før den frigis, forelegges administrerende direktør (DM) til godkjenning.

Oppdragsfinansierte statistikker

Når bestemmelsen om oppgaveplikt i statistikkloven blir benyttet, skal frigiving av statistikken følge hovedregelen for frigiving, selv når den er oppdragsfinansiert. For oppdragsfinansierte statistikker uten oppgaveplikt, for eksempel en rekke intervjuundersøkelser, er det ofte en del av kontraktsvilkårene at oppdragsgiver får adgang til resultatene før de frigis. Men det er et ufravikelig prinsipp at frigivingen av

statistikken overfor andre enn oppdragsgiver skal gjøres av SSB, eventuelt samtidig med publisering fra oppdragsgiver. Etter frigiving av statistikken fra SSB er den tilgjengelig for alle. Før frigiving kan oppdragsgiver bare utnytte resultatene internt hos seg.

Sperrefrister
Hovedregelen er at frigiving av statistikk skjer uten bruk av sperrefrist, det vil si at ingen utenom SSB får se statistikken før den er frigitt, med de unntak som er nevnt ovenfor. Det skal imidlertid være mulig med sperrefrist for nyhetsmedier for enkelte statistikker. Sperrefristen brukes kun når følgende forhold er innfridd:

- Undersøkelsene som skal offentliggjøres kommer sjelden, som hovedregel sjeldnere enn en gang i året
- Materialet er av et omfang som gjør at pressen trenger tid til å forberede oppslag
- Nyhetsverdien vurderes som svært høy

Beslutning om bruk av sperrefrist tas i hvert enkelt tilfelle av administrerende direktør (DM) i god tid før offentliggjøring.

3. Forholdet til pressen

Spørsmål om nærmere beskrivelse eller tolking av tall, analyser eller forskningsresultater utover det som direkte framgår av det som er offentliggjort, kan besvares av den saksbehandler som er best inne i saken eller av dennes seksjonsleder. Henvendelser som kan antas å være kontroversielle eller som på andre måter krever ekstra varsomhet, skal forelegges administrerende direktør eller avdelingsleder. Spørsmål av allmenn art eller om SSB arbeidsprogram generelt, skal besvares av administrerende direktør eller avdelingslederne.

Som en rettesnor og hjelp for SSB-ansatte i sin kontakt med presse og kringkasting er det utarbeidet en «Vær-varsom-plakat».

3.1. Vær-varsom-plakat for SSB-ansatte

Formålet med denne plakaten er ikke å redusere SSB-ansattes kontakt med presse og kringkasting. Den kontakten er snarere for sjelden enn for hyppig. Plakaten gir imidlertid veiledning og råd om hvilke situasjoner en bør unngå, om hvordan medarbeiderne bør opptre og om hvem som kan uttale seg om hva.

- ***SSB-ansatte vet ikke alt og SSB besvarer ikke alle slags spørsmål***
  Dette betyr at SSB-ansatte som hovedregel skal nøye seg med å svare på spørsmål på områder der SSB lager statistikk, driver analysevirksomhet eller har forskningserfaring. Avklar om journalisten er ute etter intervju/uttalelser eller bakgrunnsinformasjon. Det er i det første tilfellet du bør være særlig aktsom.

- ***Hold deg til saken***
  Fall ikke for fristelsen til å henge på (egne) tolkninger som ikke direkte framgår av forskningsrapporten/statistikken du uttaler deg om.

- ***Vær forsiktig med å gi anbefalinger og vurderinger***
  SSB har bare unntaksvis oppfatninger i kontroversielle spørsmål når disse ikke angår selve arbeidsområdet til SSB, dvs. beskrivelser av den faktiske situasjon og utvikling, økonomiens virkemåte og sosiale og økonomiske prosesser og framskrivinger og analyser basert på SSBs analyseapparat. SSB har ikke til oppgave å gi politiske råd eller delta med partsinnlegg i den politiske debatt.

- ***Jo sterkere innslag av vurdering, jo høyere opp i hierarkiet bør henvendelsen besvares***
  Seksjonsleder er et rimelig startnivå for henvendelser som ikke har klar adresse i utgangspunktet. Han eller hun bør så vurdere om henvendelsen skal avvises, om den angår «facts» som eventuelt kan besvares av en saksbehandler som vet bedre eller om den angår vurderinger som eventuelt må besvares på høyere hold.

- ***Personlige synspunkter må ha faglig integritet***
  Når du blir spurt på personlig basis, men klart fordi du innehar en ledende stilling i SSB, er det særdeles viktig at uttalelsene har faglig integritet, dvs. at de er basert på den innsikt som institusjonen forvalter.

- ***Insister på å få intervjuet opplest før det trykkes hvis du ikke er helt trygg på å bli korrekt gjengitt***
  Om mulig bør en også be om å få opplest tittel og ingress; det er ofte der et intervju «gjøres interessant». Det er en rettighet å få intervjuet opplest (eller fakset over til gjennomlesing), men overskrift/ingress er ikke intervjuobjektets ansvar. Det er bare direkte sitater du har rett til å bestemme innholdet i.

- ***Overhold reglene for frigiving av statistikk***
  Det må ikke under noen omstendighet gis tall som ikke er frigitt til offentliggjøring. Heller ikke må det gis opplysninger om at statistikk som er under utarbeiding, vil gi tall som trolig vil avvike fra eller stort sett være i samsvar med tilsvarende tall fra tidligere år.

- ***Dokumentasjon bør foreligge***
  En bør være varsom med å utlevere resultater av pågående prosjekter selv om de ikke inneholder ny statistikk eller er av sensitiv art, dersom publikasjon eller dokumentasjon i annen form ikke er tilgjengelig.

- ***Informer dine nærmeste overordnede om uttalelser/intervjuer du har gitt hvis innholdet kan være kontroversielt***

Indeks

V

De sist utgitte publikasjonene i serien Statistisk sentralbyrås håndbøker

45 Håndbok i datasikkerhet og fysisk sikring. 1994. 53s.

46 Telefonkatalog. 1998. 89s.

47 EØS-avtalen. Det statistiske samarbeid og konsekvenser for Statistisk sentralbyrås statistikkproduksjon. 1994. 55s.

48 Håndbok i tilsettingssaker. 1994. 32s.

49 Oppgaveplikt og tvangsmulkt. 1995. 55s.

50 Emneinndeling 1995. 1995. 43s.

51 Intervju: EDB-arbeidsbok. 1995.

52 Intervju: EDB-oppslagsbok. 1995.

53 Intervju: Opplæring og administrasjon. 1995.

54 Internkontroll: Revidert utgave 1997. 25s.

55 Nordisk statistikk på CD-ROM: Veiledning. 20s.

56 PC-Axis versjon 2.2: Brukerhåndbok. 69s.

57 Produktregister versjon 4.0: Brukerveiledning. 49s.

58 Håndbok i prosjektstyring. 20s.

59 Personalreglement for Statistisk sentralbyrå. 22s.

60 Produktnummerkatalog pr. 28.02.1996. 55s.

61 Innkjøpshåndbok. 1996.

62 Timeplan versjon 3.0: Brukerveiledning. 16s.

63 Håndbok i EDB-metode. 52s.

64 Publiseringshåndbok: Regler og retningslinjer for publisering i Statistisk sentralbyrå. 93s.

65 Håndbok i utvikling av statistikksystemer: Med vekt på IT-metode. 52s.

Statistisk sentralbyrå
Statistics Norway