

Håndbok i datasikkerhet og fysisk sikring



Håndbok i datasikkerhet og fysisk sikring

ISBN 82-537-4001-8

Design: Enzo Finger Design
Trykk: Falch Hurtigtrykk

Forord

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

"Sikkerheshåndbok for Statistisk sentralbyrå" inneholder de regler og interne retningslinjer som styrer sikkerheten i Statistisk sentralbyrå og som er av almen 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.

Sikkerheshåndboka 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.

I denne 2. utgaven av håndboka er det foretatt en del viktige endringer og presiseringer når det gjelder tekstlig innhold. Det er dessuten gjort flere redaksjonelle endringer som jeg håper skal øke bruken av boka som et verktøy i arbeidet med å oppnå best mulig sikkerhet i Statistisk sentralbyrå.

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 en av Sikkerhetsutvalgets medlemmer eller din avdelings sikkerhetskonsulent (se vedlegg 1 om hvem dette er).

Statistisk sentralbyrå,
Oslo, 14. mars 1994

Svein Longva

Innhold

Forord	3
1. Innledning	7
1.1. Mål for sikkerheten i Statistisk sentralbyrå	7
1.2. Krav til datavern i Statistisk sentralbyrå	7
1.3. Om Statistisk sentralbyrås sikkerhetsorganisasjon og ansvar/oppgavefordeling	8
2. Hovedinstruks	10
2.1. Hovedinstruks for sikkerhet i Statistisk sentralbyrå	10
2.2. Sikkerhetsinstruks for avdelingsleder	10
2.3. Mandat for Statistisk sentralbyrås sikkerhetsutvalg	11
3. Andre instruks	12
3.1. Sikkerhetsinstruks for fysisk sikring og adgangskontroll i Statistisk sentralbyrås lokaler	12
3.2. Sikkerhetsinstruks for data- og programbruker	12
3.3. Branninstruks	13
3.4. Instruks for behandling av makulerings- og returpapir i Statistisk sentralbyrå	13
3.5. Sikkerhetsinstruks for systemprogrammerer	14
3.6. Sikkerhetsinstruks for maskindrift	14
4. Generelle administrative rutiner	15
4.1. Sikkerhetsklarering og autorisasjon av personale	15
4.2. Taushetsplikten	15
4.3. Utlevering og tilbakelevering av Statistisk sentralbyrås nøkler og nøkkelkort	16
4.4. Forsendelse av informasjon over telenettet, bruk av kopieringsmaskiner og skrivere	16
4.5. Beredskaps- og katastrofesikring	16
4.6. Revisjons- og kontrollrutiner	17
5. Informasjonsbehandling i Statistisk sentralbyrå	18
5.1. Generelt	18
5.2. Om personopplysninger og personregistre i Statistisk sentralbyrå	18
5.3. Plikter pålagt den registeransvarlige i Statistisk sentralbyrå	19
5.4. Statistisk sentralbyrås rammekonsesjon og rutiner i forbindelse med søknad/melding om konsesjon	20
5.5. Rutiner for kryptering av fødselsnummer	20
5.6. Publikums innsynsrett i Statistisk sentralbyrås personregistre	21
5.7. Personregistre unntatt konsesjon	21
5.8. Gradering, beskyttelse og bruk av informasjonsmateriale iht. sikkerhets- og beskyttelsesinstruksen	21
5.9. Informasjonsmateriale i Statistisk sentralbyrå som kan være offentlig/ikke offentlig	23
6. Offentliggjøring av statistikk og utlevering av statistiske opplysninger generelt	26
6.1. Offentliggjøring av statistikk/informasjon fra statistiske registre	26
6.2. Utlevering av individualopplysninger/mikrodata fra statistisk grunnmateriale	27
6.3. Utlevering av data innenfor EØS-området	29
Vedlegg	
1. Navneliste over aktuelle personer i Statistisk sentralbyrås sikkerhetsorganisasjon	31
2. Datatilsynets rammekonsesjon for Statistisk sentralbyrå	33
3. Kryptering av fødselsnummer i Statistisk sentralbyrås registre	37
4. Mal for melding til Datatilsynet om opprettelse/endring av personregister	41
5. Statistisk sentralbyrås taushetserklæringer	43
6. Modellavtaler til bruk ved utlevering av data	47
7. Mal for årlig sikkerhetsrapport fra avdelingene	53

1. Innledning

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 informasjon blir:

- Ødelagt
- 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. 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 viktig å redusere sikkerhetsrisikoen og dermed sikkerhetstiltakene så langt som mulig. Dette kan særlig gjøres ved å slette data som det ikke lenger er bruk for, kryptere identifikasjonsnumre eller aidentifisere 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 for at uvedkommende tar seg inn i Statistisk sentralbyrås bygninger mest mulig.

Arbeidet med å sikre den enkeltes arbeidsplass, arbeidsmiljø, helse o.l. vil ellers ikke bli behandlet i

denne håndboken 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. Krav til datavern i Statistisk sentralbyrå

Statistikkloven inneholder regler om hvordan alle data som er hentet inn med sikte på å utarbeide offisiell statistikk skal behandles. Personregisterloven og rammekonsesjon fra Datatilsynet regulerer behandling og bruk av personopplysninger. Statistikkloven har regler for taushetsplikt for den enkelte ansatte. Både statistikkloven og Datatilsynet setter rammen for bruk og utlevering av opplysninger. Lovens bestemmelser vil både kunne ramme den enkelte ved brudd på taushetsplikten og institusjonen dersom opplysningene brukes til andre formål enn utarbeiding av offisiell statistikk uten godkjenning fra Datatilsynet, eller offentliggjøres slik at de kan føres tilbake til oppgavegiver eller annen identifiserbar enkeltperson til skade for denne.

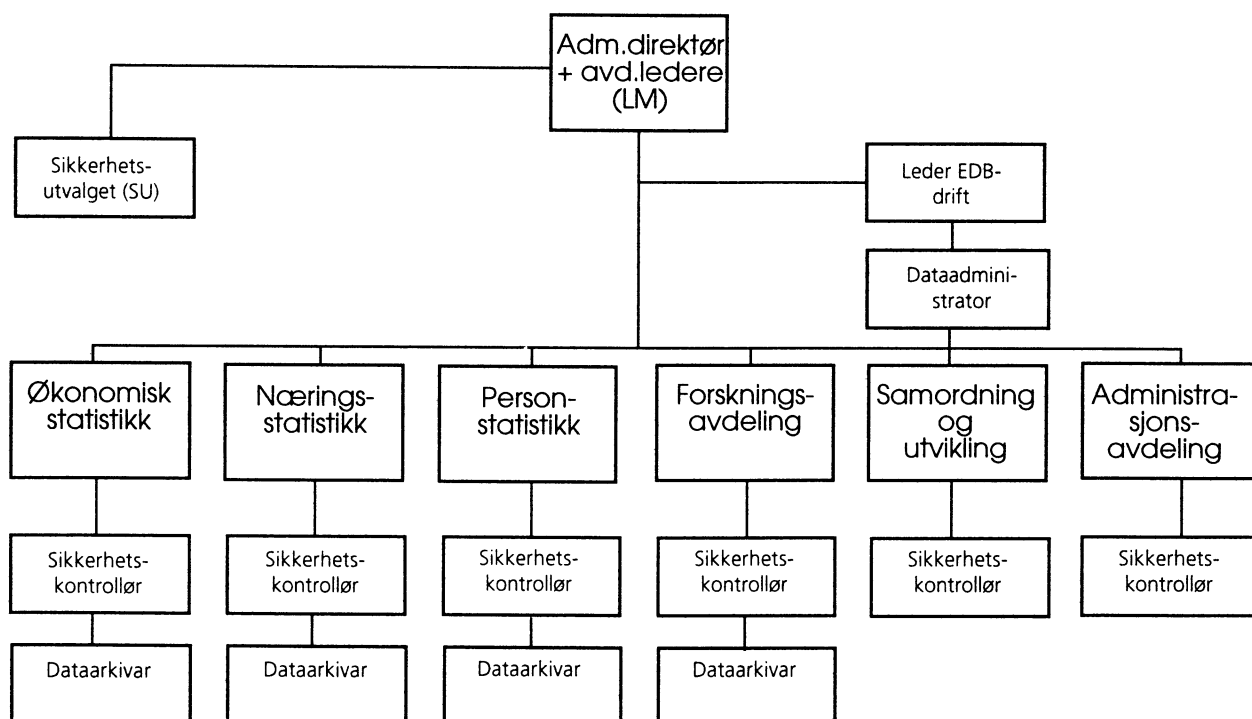
På denne bakgrunn må det stilles følgende krav til Statistisk sentralbyrås datavern:

1. Medarbeiderne i Statistisk sentralbyrå må kjenne til og overholde bestemmelsene i statistikkloven og Datatilsynets rammekonsesjon. Det må ikke kunne stilles spørsmål ved Statistisk sentralbyrås eller medarbeidernes etterlevelse av disse bestemmelser.
2. Det skal ikke kunne påvises feil i Statistisk sentralbyrås statistikk eller andre data som Statistisk sentralbyrå leverer fra seg som følge av at statistiske data er endret i strid med gjeldende rutiner.
3. Data som skal oppbevares til framtidig bruk må ikke bli ødelagt.

Det må være en realistisk målsetting at disse kravene også blir oppfylt i framtida, selv om risikoen for brudd på de krav som stilles skulle øke som følge av :

- større og mer verdifulle samlinger av data i Statistisk sentralbyrå,
- større interesse for slike data utenfor Statistisk sentralbyrå og
- økte muligheter for kopiering og flytting av data.

1.3. Om Statistisk sentralbyrås Sikkerhetsorganisasjon og ansvar/oppgavefordeling



Forklaringer til sikkerhetsorganisasjonen:

1. Generelt for linjeledelsen:

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

Avdelingslederne har ansvaret for sikkerheten innen sin avdeling. Avdelingsleder ved Administrasjonsavdelingen er hovedansvarlig for den fysiske sikkerheten i Statistisk sentralbyrås lokaler. Se forøvrig punkt 2.2 nedenfor.

Seksjonsledere i avdelingene skal sørge for at alle ved seksjonen kjenner og etterlever det regelverket som gjelder for den enkeltes arbeidsområde og foreslå spesielle tiltak og instruksjoner for områder som er spesielle for seksjonen.

Seksjonssjef for Seksjon for EDB - drift har det overordnede ansvaret for den daglige datasikkerheten i Statistisk sentralbyrå. Dette inkluderer bl.a ansvar for systemprogrammering og driftsansvar for felles programvare og datatamaskiner.

Kontorsjef ved EDB-gruppene i avdelingene vil ha ansvar for datasikkerheten i avdelingen for de EDB - rutiner som utvikles ved avdelingene og ved tildeling av brukerprofiler for ansatte i EDB - gruppen.

2. Spesielle ledd/funksjoner:

Sikkerhetsutvalget er direkte underlagt administrerende direktør og har en rapporterings- og orienteringsplikt overfor administrerende direktør i alle sikkerhetssaker. Se forøvrig punkt 2.3 nedenfor.

Utvalget er ansvarlig for at regler og retningslinjer godkjennes og blir fulgt opp av avdelingene. Videre er utvalget ansvarlig for at saker av sikkerhetsmessig betydning behandles i Sikkerhetsutvalget og for at prinsipielt viktige saker tas opp til behandling av Statistisk sentralbyrås ledelse.

Statistisk sentralbyrås kontakt med Datatilsynet skal skje gjennom Sikkerhetsutvalget og administrerende direktør, unntatt rutinemessige meldinger om opprettelse av personregistre.

Dataadministratoren skal føre en journal over alle Statistisk sentralbyrås registre. Journalen skal vise hvem som eier registeret, hvilke restriksjoner som er lagt på registeret og referere til de enkelte datafiler. Denne journalen er en del av datadokumentasjonssystemet i Statistisk sentralbyrå.

Dataadministratør skal kontrollere at restriksjonene i journalen blir overholdt og melde fra til registreieren og Sikkerhetsutvalget ved mangler.

Dataadministrator skal sørge for at rutiner for kryptering av identifikasjonsnummer blir holdt ajour, tilfredsstillende beskrevet, og at informasjonen om bruken av rutinen er tilfredsstillende.

Dataarkivaren skal føre ajour lese- og skrevetillatelse i sikkerhetsprogrammet bare etter skriftlig ordre fra registereier.

Dataarkivaren skal kontrollere at slike ordre er undertegnet av ansvarlig person ved den seksjonen som eier registeret.

Ved innlasting av data fra sikkerhetskopi skal dataarkivaren kontrollere at de data som lastes inn ikke er slettet eller kryptert ifølge ajourført datadokumentasjon.

Sikkerhetskrollørene er den enkelte avdelings "sikkerhetssjef". Avdelingslederne oppnevner en eller flere sikkerhetskrollører ved hver avdeling.

Sikkerhetskrolløren(e) skal overvåke alle sider av sikkerheten ved avdelingen. Dette innebærer bl.a. at vedkommende skal sette i verk de kontroller avdelingen er pålagt i følge vedtak av administrerende direktør, til de tidspunkter og i det omfang avdelingslederen bestemmer.

Sikkerhetskrolløren(e) har rapporteringsplikt overfor avdelingslederen, og kan videre fremme forslag overfor avdelingslederen om sikringstiltak, instruksjoner og kontroller.

2. Hovedinstrukser

2.1. Hovedinstruks for sikkerhet i Statistisk sentralbyrå

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 framtiden blir arkivert på en forsvarlig måte.

Alle tilsatte i Statistisk sentralbyrå skal følge de regler og instruksjoner de blir pålagt av sine overordnede. Hver tilsatt har et eget ansvar for at sensitiv eller beskyttet informasjon ikke blir gjort tilgjengelig for personer som ikke har tilgang til dette. 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 instruksjoner.

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 instruksjoner 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 instruksjoner for områder som er spesielle for seksjonen/gruppa.

2.2. Sikkerhetsinstruks for avdelingsleder

1. Avdelingslederen skal sette seg inn i alle lover, regler og instruksjoner 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 instruksjoner 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 instruksjoner som skal gjelde for den enkelte seksjon eller gruppe og påse at disse blir etterlevet.
3. Avdelingslederen er ansvarlig for at saker forelegges Sikkerhetsutvalget der hvor dette følger av gjeldende regelverk og instruksjoner.
4. Avdelingslederen skal sørge for klarering og autorisasjon av sitt personale.
5. Avdelingslederen skal oppnevne en eller flere sikkerhetskontrollører som skal overvåke sikkerheten ved avdelingen og gi disse instruksjoner for dette arbeidsområdet.
6. Avdelingslederen skal i januar hvert år sende en melding til Sikkerhetsutvalget om sikkerhetsarbeidet ved avdelingen.
7. Avdelingslederen er innenfor gjeldende regelverk ansvarlig for:
 - 7.1 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
 - 7.2 Bruk og vedlikehold av eget frittstående teknisk utstyr og EDB-utstyr (utstyr som ikke er koblet til lokalnett eller sentral stormaskin).
 - 7.3 Fysisk sikkerhet i avdelingens lokaler og adgangskontroll til disse, se imidlertid punkt 9 nedenfor.

- Ansvar for dette kan avdelingslederen delegeres til avdelingens seksjons- og kontorsjefer.
8. Avdelingslederen skal påse at avdelingen følger forsvarlige regler for publisering innen 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.
 9. Avdelingsleder ved Administrasjonsavdelingen er hovedansvarlig for sikkerheten i Statistisk sentralbyrås lokaler, kontroll av adgang til bygningene og rutiner for makulering av sensitiv informasjon og utlevering av nøkkelkort og adgangstegn.
 10. Den avdelingsleder som administrerende direktør peker ut er ansvarlig for sikring av den sentrale databehandling og beskyttelse av det sentrale arkiv.
5. Utvalget kan sette igang sikkerhetstiltak etter godkjenning av administrerende direktør.

Sikkerhetsutvalget oppnevnes av administrerende direktør og skal ha følgende sammensetning:

 - 1 person som kjenner Statistisk sentralbyrå godt
 - 1 EDB - ekspert
 - 1 jurist

Administrerende direktør velger ut leder for utvalget fra en av disse.

 - Administrasjonsavdelingen er ansvarlig for utvalgets sekretariat.

2.3. Mandat for Statistisk sentralbyrås sikkerhetsutvalg

1. Sikkerhetsutvalget skal være direkte underlagt administrerende direktør. 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 EDB-sikkerhet og organisatorisk sikkerhet ved å utarbeide regler, retningslinjer og instruksjoner som:
 - 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
 - Legge fram en vurdering av de økonomiske og administrative konsekvenser utvalgets forslag medfører.
3. Utvalget har ansvaret for å holde ajour Statistisk sentralbyrås Beredskapsplan.
4. Utvalget skal holde jevnlig kontakt med avdelingenes sikkerhetskontrollører.

3. Andre instruksjer

3.1. Sikkerhetsinstruks for fysisk sikring og adgangskontroll i Statistisk sentralbyrås lokaler

1. Alle tilsatte skal alltid ha med seg nøkkelkort 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 Statistisk sentralbyrås andre arbeidssted skal den besøkende skrive seg inn i besøksprotokollen ved inn- og utpassering.
2. Tap av nøkkelkort må straks meldes til avdelingens administrative gruppe.
3. Nøkkelkort og tilhørende kode må ikke lånes eller utleveres til andre.
4. Dersom alarm utløses ved passering av alarmbelagte dører (dører merket med ALARM), skal den som forårsaket dette vente på stedet til vaktpersonale kommer.
5. Ingen skal slippe noen gjennom låste dører uten at det er sikkert at vedkommende har adgang. Alle tilsatte har et ansvar ved 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 instruksjonen som blir gitt i det enkelte tilfellet.
7. Den som blir påtruffet av Statistisk sentralbyrås 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 Statistisk sentralbyrås lokaler.

3.2. Sikkerhetsinstruks for data- og programbruker

1. Brukeren skal oppbevare passord på en trygghetssik måte og ikke overlate det til andre.
2. Brukeren skal ikke gi fra seg beskyttede data til andre enn de som har fått tillatelse fra

registreier, 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 datavirustest er foretatt. Dersom brukeren benytter egen PC hjemme, må det kjøres virustest før bruk.
4. Brukeren skal holde skjema, lister og flyttbare elektroniske lagringsmedia med beskyttede data nedlåst når de ikke er under betryggende tilsyn.
5. Beskyttede data som lagres sentralt, skal ikke kopieres i lokalnett/PC uten at dette er godkjent av registreier.

Utfyllende bestemmelser:

Generelt

Alle dataprogram som brukes på Statistisk sentralbyrås datamaskiner (inkl. PC'er) forelegges EDB-gruppen ved avdelingen/Seksjon EDB - drift på forhånd. Dette for å sikre Statistisk sentralbyrå mot bl.a. datavirus.

Adgang til opplysninger via dataskjerm

Hver person tildeles brukerområde og passord. Avdelings-/seksjons-/kontorsjef er ansvarlig for tildeling av brukerområde og at passord blir gitt. Når en person slutter eller har permisjon vil alle tillatelser til Statistisk sentralbyrås data og datamaskiner bli trukket tilbake, noe enhetens leder er ansvarlig for at skjer.

Dataskjermen skal være avslått (logget av lokalnettet) når brukeren forlater rommet.

Lagring/tilintetgjøring av taushetsbelagt materiell

Sletting og makulering skal skje på en forsvarlig måte.

Opplysninger/data skal ikke lagres lenger enn nødvendig. Kassert materiell samles i kartonger eller sekker som merkes spesielt og oppbevares i seksjonens arkivrom inntil det kan overleveres til Administrasjonsavdelingen for makulering. Det må påses at dette ikke gjelder materiell som skal oversendes Riksarkivet.

Ved skriving av FORTROLIG data på tekstbehandling eller PC (f.eks. opplysninger om ansatte), skal dokumentet ikke lagres i maskinen,

men slettes etter at det er tatt i bruk til det formål det ble skrevet for.

Lagringsmedia (magnetisk, elektronisk, optisk o.l.) som lånes ut, selges eller sendes ut av Statistisk sentralbyrå til reparasjon, må på forhånd gjennomgå en sletteprosess der dette er nødvendig.

Spesielle sikringstiltak ved bruk av PC og andre lett transportable maskiner

Eier av dataene tillegges ansvaret for at rutiner for bl.a. sikkerhetskopiering (back-up) blir fulgt. Viktige sikkerhetskopier bør oppbevares brannsikkert. Dersom det ikke er tilgang til slik lagerplass ved kontoret/avdelingen, kan avtale om oppbevaring av disketter gjøres med Seksjon for EDB - drift.

Når en PC skal skiftes ut, må vi regne med at den gamle skal tas i bruk igjen. Selv om PC'en skal makuleres, vil harddisken være fullt lesbar. Leder av enheten er ansvarlig for at nødvendig sletteprosess blir gjennomført. Vedkommende avgjør også om dataene på PC'en må slettes før den sendes til service.

Når data på disketter sendes ut av Statistisk sentralbyrå skal det alltid brukes nye disketter. Ved forsendelse må reglene i punkt 6.2 nedenfor følges.

3.3. Branninstruks

1. Alle ansatte i Statistisk sentralbyrå plikter å gjøre seg kjent med og å 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, slå om mulig 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 framfor 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 instruksjoner 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.
9. Feil eller mangler ved brannsikkerheten (f.eks. blokkerte rømningsveier, manglende slukkeutstyr) må meldes snarest til seksjonssjef/kontorsjef eller ansvarshavende for fløy/etasje.

3.4. Instruks for behandling av makulerings- og returpapir i Statistisk sentralbyrå

1. Innledning

Denne instruksjonen er retningsgivende for hvordan makulering/kasting 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 trygghetssikret måte før det blir levert til sentralt oppbevaringssted.

Den enkelte medarbeider må selv sørge for at slikt papir blir brakt til sentralt sted, dette gjelder også returpapir. Avdelingene v/avdelingsleder har det formelle ansvaret for at instruksjonen blir fulgt. Administrasjonsavdelingen har ansvaret for sentralt oppbevaringssted og for å avhende materiellet.

3. Sikkerhetsgradert materiale

Det gjelder særskilte regler med hensyn til makulering/tilintetgjøring av materiale som er gradert etter Sikkerhetsinstruksjonen som STRENGT HEMMEIG, HEMMELIG, KONFIDENSIELT eller BEGRENSET, og etter Beskyttelsesinstruksjonen som STRENGT FORTROLIG eller FORTROLIG. Det vises forøvring til pkt. 5.8 nedenfor om gradering, beskyttelse og bruk av informasjonsmateriale i henhold til Sikkerhets- og Beskyttelsesinstruksjonen.

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

Bare administrerende direktør, eller den han bemynder, 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/Statistisk sentralbyrås 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".

Materiell som ikke kommer inn under ovennevnte behandles som "returpapir" og legges i esker merket "returpapir".

4. Oppbevaring

Makulaturen/returpapiret legges i esker, merkes og oppbevares på den enkeltes kontor inntil esken er full og bringes til angitt sentralt sted. Makulatur som er merket med "farlig makulatur" oppbevares i låste rom.

5. Avhending

Farlig makulatur transporteres til godkjent mottakersted for tilintetgjørelse. En ansatt i Statistisk sentralbyrå skal følge transporten, samt overvære prosessen. Statistisk sentralbyrå Kongsvinger kan dersom det er kostnads-/miljømessig forsvarlig makulere på egen makuleringsmaskin.

3.5. Sikkerhetsinstruks for systemprogrammerer

1. Systemprogrammereren har ikke adgang til andre program og data enn de vedkommende skal vedlikeholde.
2. Systemprogrammereren 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.
3. Systemprogrammereren skal ikke utlevere materiale for systemprogrammering til andre.

3.6 Sikkerhetsinstruks for maskindrift

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

1. Sørge for at det blitt tatt sikkerhetskopi etter fastsatt mønster.
2. Utlevere sikkerhetskopier bare gjennom dataarkivar.
3. Sørge for fjernarkivering av data etter registereierens krav.
4. Begrense fysisk adkomst til det sentrale utstyret så langt som mulig.
5. Legge fram for Sikkerhetsutvalget alle endringer i kommunikasjon over linje med omverdenen og skifte av operativsystem eller sikkerhetsprogram.
6. Sørge for at Statistisk sentralbyrås brukeridentifikasjoner bare kan brukes fra Statistisk sentralbyrås terminaler.
7. Bare bruke autorisert personale til systemprogrammering, til å operere maskinen og til å holde den vedlike (forslag til autorisering legges fram for avdelingsleder).
8. Sørge for at systemprogrammering bare kan foregå fra bestemte terminaler.
9. Gradere materiale for systemprogrammering BEGRENSET og begrense utleveringen bare til autoriserte systemprogrammerere.
10. Sørge for at nødvendige sikkerhetsbestemmelser kommer inn i avtaler med eksterne leverandører.

4. Generelle administrative rutiner

4.1. Sikkerhetsklarering og autorisasjon av personale

Direktiv for personellsikkerhetstjenesten og personkontrolltjenesten innen den sivile forvaltning av 4.11.83 gir regler om fremgangsmåten ved sikkerhetsklarering og autorisasjon av personell som skal behandle/ha adgang til materiale gradert etter Sikkerhetsinstruksen, se punkt 5.8.

Informasjon gradert STRENGT HEMMELIG, HEMMELIG eller KONFIDENSIELT, kan bare behandles av 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 overvåkingstjeneste bl.a. basert på opplysninger fremkommet i sikkerhetssamtalen. Sekretariatet i Sikkerhetsutvalget har nødvendige skjemaer som skal fylles ut, og er ellers ansvarlig for at forepørsel om personkontroll blir effektivert. 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 tilfeller foretas sikkerhetsklarering/autorisasjon av Finansdepartementet.

4.2. Taushetsplikten

Generelt

Statistikklovens § 2-4 pålegger taushetsplikt for ansatte i Statistisk sentralbyrå når disse forbereder eller utarbeider offisiell statistikk. Dette gjelder opplysninger om personlige forhold, drifts-, forretningsforhold eller tekniske innretninger og fremgangsmåter. I tillegg kan ansatte i Statistisk sentralbyrå 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 taushetsplikten gjelde også for denne type opplysninger.

Alt personale tilknyttet Statistisk sentralbyrå skal derfor undertegne en taushetserklæring og gjøres kjent med det straffeansvar som følger av brudd på taushetsplikten, jfr. statistikklovens § 5-1, straffelovens § 121 og vedlegg 5.

Når det gjelder innhenting av informasjon, vil oppgavegiverens taushetsplikt som hovedregel ikke være til hinder for utlevering til Statistisk sentralbyrå, jfr. forvaltningslovens § 13b nr. 4 ("opplysningene kan brukes for statistisk bearbeiding"). Unntak gjelder hvis særlov sier det (eks. legelovens og tannlegelovens § 31).

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

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

- er medlem av et utvalg tilknyttet Statistisk sentralbyrå
- er deltager i et internt prosjekt
- har konkret tilgang til opplysninger i forbindelse med eksterne prosjekter
- har tilgang til utstyr som kan inneholde sensitiv informasjon (reparasjons- og servicepersonale).

Innhold

- * Taushetserklæringen pålegger alle ansatte i Statistisk sentralbyrå og andre med tilknytning til Statistisk sentralbyrå å vise aktsomhet i behandlingen av alle opplysninger som Statistisk sentralbyrå henter inn.
- * Taushetsplikten gjelder overfor uvedkommende; det vil si også overfor andre personer i Statistisk sentralbyrå som ikke har behov for å kjenne til en bestemt type informasjon i sitt arbeide.
- * Det må ikke gjøres kjent for andre opplysninger som av hensyn til offentlige, enkeltpersoners, institusjoners og bedrifters interesser er å anse som fortrolige.
- * Passord som gir tilgang til graderte eller beskyttede opplysninger må ikke overdras eller meddeles andre personer i eller utenfor Statistisk sentralbyrå.
- * Alle blir også pålagt å ikke gi opplysninger om resultater av statistiske undersøkelser før Statistisk sentralbyrå har frigitt dem til offentliggjøring.
- * Taushetsplikten gjelder også etter at man har sluttet i Statistisk sentralbyrå eller oppdraget for Statistisk sentralbyrå 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- og forretningsforhold.

4.3. Utlevering og tilbakelevering av Statistisk sentralbyrås nøkler og nøkkelkort

Utlevering

Alle nyansatte og andre personer med kortere engasjement for Statistisk sentralbyrå som ikke regnes som besøk, får utlevert nøkkel til sitt kontor og nøkkelkort til inngangsdørene.

Det må kvitteres for utleverte nøkler.

Tilbakelevering

- Engasjementet opphører:

Når engasjementet for Statistisk sentralbyrå opphører skal nøkkelkortet leveres tilbake siste arbeidsdag.

- Oppsigelse:

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

- Permisjon:

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

4.4. Forsendelse av informasjon over telenettet, bruk av kopieringsmaskiner og skrivere

Alle plikter å påse at taushetsbelagt eller gradert informasjon blir behandlet slik at uvedkommende ikke får tilgang til denne informasjonen.

Ved forsendelse av slikt materiale på telenettet; enten ved bruk av telefaks, fra PC, ved bruk av telefon eller annet, må den enkelte forvise seg om at mottaker har tilgangsrett til den aktuelle informasjonen, og at det faktisk er rette vedkommende som mottar informasjonen.

Ved kopiering/utskrivning 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 Beskyttelsesinstruksjonen foretas etter de regler som følger av disse instruksene, se punkt 5.8.

Ved overføring av sensitive opplysninger generelt må spesielle forholdsregler ivaretas. Nærmere retningslinjer er under utarbeidelse, bl.a. retningslinjer for kryptering av høyhastighetslinje mellom Oslo og Kongsvinger.

4.5. 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 Sikkerhetsinstruksjonen. Planen er gitt den laveste gradering i henhold til Sikkerhetsinstruksjonen, 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 EDB-utstyret og annet viktig utstyr som inneholder retningslinjer og regler for hvilke rutiner som skal følges ved f.eks. brann eller strømstans.

4.6. Revisjons- og kontrollrutiner

For at sikkerheten i Statistisk sentralbyrå skal være så god og hensiktsmessig som mulig til enhver tid, er det viktig at det skjer jevnlig revisjoner av rutinene og regelverket.

Gjennom å konkretisere hvem som har ansvar for hva, er det forholdsvis enkelt å pålegge de enkelte ledd i Statistisk sentralbyrås sikkerhetsorganisasjon rapporteringsplikt til overordnet ledd. Sikkerhetsutvalget vil ha en koordinerende rolle ved at de er ansvarlig for å sammenfatte de ulike rapportene til en årlig sikkerhetsrapport som legges fram for administrerende direktør.

Både rapportene og observasjonene fra de ulike ledd i organisasjonene samt rapporten fra Sikkerhetsutvalget danner grunnlag for de revisjoner av rutiner og regelverk som er nødvendige.

Viktige rutiner vil være:

1. Revisjon av lese- og skrevetillatelsen
2. Kontroll av datafiler utenfor gyldige registre
3. Revisjon av meldinger til Datatilsynet
4. Journal for forsendelse av graderte data
5. Stikkprøvekontroller og inspeksjoner
6. Informasjonsbehandling i Statistisk sentralbyrå.

5. Informasjonsbehandling i Statistisk sentralbyrå

5.1. Generelt

Selv om de regler og rutiner som er nevnt nedenfor rettes mot behandling av informasjon til statistikkproduksjonen, er det viktig å huske at Statistisk sentralbyrå også behandler mye informasjon som skal brukes til annet enn dette. 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 nevnt nedenfor også i stor grad gjelde tilsvarende.

I Statistisk sentralbyrå er det nødvendig å gjøre mange unntak fra allmenhetens rett til innsyn i dokumenter mv. Primærdata og administrative data innhentet med hjemmel i statistikkloven, 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 være til skade for oppgavegiverne eller andre enkeltpersoner. Opplysningene som blir gitt frivillig eller 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 statistikkproduksjonen 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 ikke brukes, skal slettes.
5. Informasjonen skal ordnes i registre, og hvert register skal ha en ansvarlig eier.
6. Rutiner og informasjon skal dokumenteres på en fullstendig og oversiktlig måte.

5.2. Om personopplysninger og personregistre i Statistisk sentralbyrå

Lov om personregistre m.m av 9.6.78 nr. 48 og forskrifter fastsatt med hjemmel i denne samt Statistisk sentralbyrås rammekonsesjon for føring av personregistre av 2.5.90 inneholder bestemmelser som er av betydning for hvordan Statistisk sentralbyrå kan bruke den informasjon som befinner seg i Statistisk sentralbyrås 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 mm., bare skal registreres i den grad det er nødvendig. Disse krav vil være tilfredsstillt dersom opplysningene anses nødvendige for utarbeidelse av offisiell statistikk. Personregisterloven stiller m.a.o. et sterkere behovskrav når det er snakk om sensitiv informasjon. Dette bør 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.

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

Personopplysninger er opplysninger 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, A.S. ol.).

Personregistre er registre, fortegnelser m.m. der personopplysninger 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 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 aidentifisert register er navn, fødselsnummer eller andre direkte kjennetegn fjernet.

Et aidentifisert register vil likevel kunne være et personregister dersom det til tross for aidentifisering fortsatt ikke er tilstrekkelig anonymisert.

Således kan og må man i utgangspunktet skille mellom aidentifiserte og anonymiserte registre. Et aidentifisert 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 registreier sitter med krypteringsnøkkelen.

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

Det kreves som hovedregel samtykke (konsesjon) for å opprette personregistre 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 slektsskap 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 statistikklovens § 2-5 (spesifisert i Statistisk sentralbyrås rammekonsesjon, se vedlegg 2) behøves det imidlertid ikke å søke om konsesjon. Det skal istedet sendes en såkalt melding om opprettelse av nytt/ending i allerede meldt register. Se pkt. 5.3. nedenfor for nærmere veiledning

Hva er ett personregister 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 konsesjonsystemet gir mening. En samling opplysninger hvor den enkelte person/foretak/bedrift m.m. kan gjenfinnes må tilfredsstillende 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/foretaksnummer.
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.

5.3. Plikter pålagt den registeransvarlige i Statistisk sentralbyrå

Hvert enkelt register i Statistisk sentralbyrå "eies" av den enhet (normalt den enkelte seksjon) som har ansvaret for statistikken/ opplysningene på det feltet registeret primært skal dekke. Datasett/opplysninger som brukes av flere enheter eies av den enhet som har kontakten med den som leverer registeret/ opplysningene til Statistisk sentralbyrå. Lederen for enheten vil være den registeransvarlige, og denne skal:

- * Påse at melding om opprettelse og endring av personregister blir utarbeidet, behandlet i Statistisk sentralbyrås 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 og med visse mellomrom, 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 jfr. nedenfor under punkt 5.8.
- skal det sendes *en* melding som dekker de registrene som vil bli koblet. Meldingen om de 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.
- Litt om utfylling av skjemaet (skjemaet er lagt ved som vedlegg 4):*

Registereier er Statistisk sentralbyrå.

Kontaktperson er leder av Sikkerhetsutvalget.

Registeransvarlig er administrative leder for den enhet som har ansvaret for statistikken/-opplysningene på det felte datasettet primært skal dekke.

Meldingen sendes fra registeransvarlig til avdelingsleder via dataadministratoren.

5.4. Statistisk sentralbyrås rammekonsesjon og rutiner i forbindelse med søknad/melding om konsesjon

Hvordan melde registre?

Statistisk sentralbyrås rammekonsesjon har fastsatt rammen for hva slags type registre Statistisk sentralbyrå kan ha, hvordan informasjon skal samles inn, oppbevares og brukes. Datatilsynet har imidlertid et system hvor nye registre/endringer i tidligere etablerte registre bare behøver å *meldes* før opplysninger kan samles inn og lagres. Disse meldingene skal skje på et fastsatt skjema, jf. vedlegg 4. 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.

Innenfor de regler rammekonsesjonen setter og utifra det som her er sagt om hva som er et personregister i Statistisk sentralbyrå, er det fortsatt stor frihet i forhold til hva som skal meldes som et register til Datatilsynet. Følgende regler kan imidlertid legges til grunn:

- * Det skal ikke meldes unødig mange registre, dvs. en melding skal alltid dekke minst det omfang og det datainnhold registeret skal ha.
- * Når det meldes et nytt register og det regnes som sikkert at det nye registeret vil bli koblet med et eksisterende eller framtidig register,

5.5. Rutiner for kryptering av fødselsnummer

Om kryptering og begrunnelse for dette

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 en beredskap for statistikkproduksjonen fordi det ofte vil være behov for å ta vare på muligheten for kobling av data fra ulike tidsperioder. Dersom fødselsnummeret er koblingsnøkkelen vil kobling være vanskelig, og ved å kryptere vil Statistisk sentralbyrå

også kunne bygge opp en høyere beredskap for tilfeldige oppdrag der det er behov for det.

- * Imøtekomme krav fra Datatilsynet. Statistisk sentralbyrås rammekonsesjon fra Datatilsynet tillater kobling av registre når det er "absolutt nødvendig". Denne begrensningen gjelder ikke når fødselsnummer, navn og annen identifikasjon er erstattet med kryptert nummer (jf. konsesjonens pkt 4.2).

For øvrig vises det til vedlegg 3 for utfyllende informasjon om de mer tekniske sider av krypteringsrutinene.

Interne rutiner

Informasjon om kryptering fås hos Statistisk sentralbyrås dataadministrator (se vedlegg 1).

Forøvrig gjelder følgende rutiner:

- * Den registeransvarlige er selv ansvarlig for å overføre fra Fnr. til Snr. Benytt standardrutine som ligger på COMPAREX.
- * 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 kontrollør som kjenner registeret kontrollerer innholdet i det krypterte registeret og bekrefter at bare det datainnholdet som skal være med har kommet med og at ingen form for identifikasjon er kommet med.
- * Den registeransvarlige kontrollerer at det krypterte registeret inneholder riktig antall records, at det er katalogisert på riktig filident, bekrefter at register med fødselsnummer er

slettet, signerer krypteringsblanketten og sender kopi av blanketten til dataadministrator og Sikkerhetsutvalgets sekretariat.

5.6. Publikums innsynsrett i Statistisk sentralbyrås personregistre

Personregisterloven § 7 sier at alle har rett til å få opplyst hvilke opplysninger om dem selv som lagres eller bearbeides ved elektroniske hjelpemidler. For personregistre i organ for stat eller kommune gjelder denne innsynsretten også for manuelle registre.

Registre som utelukkende brukes til statistikk, forskning eller generelle planleggingsformål, er imidlertid unntatt fra innsynsrett.

Bakgrunnen for unntaksregelen er at data som samles inn kun for statistisk bruk, forsknings- eller generelle planleggingsformål, ikke benyttes som grunnlag for å fatte beslutninger om den enkelte registrerte. Behovet for innsyn er ikke det samme fordi man ikke har samme interesse i å få rettet opp eventuelle feil og mangler ved det registrerte som ved andre registre hvor opplysningene og bruken av dem får konsekvenser direkte for den enkelte person.

Alle har imidlertid rett til å få opplyst hvilke typer opplysninger generelt som er tatt inn i registrene.

5.7. Personregistre unntatt konsesjon

En rekke typer personregistre til ulike formål er unntatt konsesjonsplikt. Forskriftenes kapittel 2 til personregisterloven 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. Viktige unntak for Statistisk sentralbyrå er registre over nåværende eller tidligere ansatte, bibliotekets lånerregister og kunde-, abonnent- og leverandørregistre.

5.8. Gradering, beskyttelse og bruk av informasjonsmateriale iht. sikkerhets- og beskyttelsesinstruksen

1. Generelt

Det er utarbeidet instruksjoner fra sentralt hold i statsforvaltningen som gir regler for behandling og tilgang til endel typer informasjon som bør beskyttes. Regelverket er bygget opp under den forutsetning at forskjellig informasjon har krav på ulik behandling. Generelt gjelder disse reglene en type informasjon Statistisk sentralbyrå har lite av, og vil derfor få liten betydning for informasjonsbehandlingen. Det er likevel nødvendig at en del kjenner litt til reglementet for å kunne behandle den type informasjon som blir berørt av regelverket.

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

Sikkerhetsinstruksen av 17.3.72 og 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.

Beskyttelsesinstruksen av 17.3.72 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 5.9.

Datasikkerhetsdirektivet av 1.2.90 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 tilfellet *Sikkerhetsutvalget*.

2. 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

Det er viktig å presisere at for å få tilgang til data/informasjon gradert KONFIDENSIELT eller høyere, må man være sikkerhetsklarert og autorisert for dette, se 4.1.

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 *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 **b e t y d e l i g s k a d e** for offentlige interesser, en bedrift, institusjon eller enkeltperson at dokumentets innhold blir kjent for uvedkommende.

FORTROLIG nyttes dersom det vil kunne **s k a d e** 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 angis at graderingen er foretatt i henhold til *Beskyttelsesinstruksen*.

Det meste av Statistisk sentralbyrås 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 Statistisk sentralbyrå.

3. 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 arbeidshagens slutt.

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

4. 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 og

STRENGT FORTROLIG må gis spesiell beskjed om gradering og 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 media skal registreres som rekommandert post, verdipost eller sendes med bud.

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

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

5.9. Informasjonsmateriale i Statistisk sentralbyrå som kan være offentlig/ikke-offentlig

1. Om offentlighetens rett til innsyn i Statistisk sentralbyrås dokumenter

Hovedregel: Alt er offentlig. Lov om offentlighet i forvaltningen av 19.6.70 nr. 69 (Offentlighetsloven) sier i § 2 at hovedregelen er at alle offentlige dokumenter er offentlige. Det vil si at enhver kan kreve å få gjøre seg kjent med innholdet i slike dokumenter.

Dokumentbegrepet: Begrepet dokument må ikke tolkes snevert. Som dokument regnes ikke bare brev, uttalelser o.l., men også journaler, registre, utskrift fra dataregistre og tekstbehandlingssystem, kart, skisser, fotografier m.m. som er relevante for saksområdet som vedkommende ønsker innsyn i.

I forhold til materiale som er utarbeidet, overført eller lagret ved hjelp av elektronisk databehandling (EDB) vil innsynsretten gjelde den naturlige enhet av tekst eller opplysninger som på utskrift fra systemet framstår som ett dokument. Med slik naturlig enhet sikter man f.eks. til den tekst som behandles som en enhet i et tekstbehandlingssystem, eller den enhet som gjenfinnes ved hjelp av et tekstsøkesystem eller et annet informasjonssystem.

Unntak fra regelen om full offentlighet:

Offentlighetslovens §§ 5 og 6 har regler om hva som kan unntas fra offentlighet. Det er viktig å merke seg at det er bestemte typer opplysninger som kan

unntas, ikke dokumentene i seg selv. De øvrige delene av et dokument vil være offentlig tilgjengelig såfremt det ikke gir et åpenbart misvisende bilde av innholdet. Dersom et saksdokument er unntatt fra offentlighet kan hele saken unntas fra offentlighet dersom de øvrige saksdokumenter vil gi et åpenbart misvisende bilde av saken og offentlighet kan skade samfunnsmessige eller private interesser.

Blir en begjæring om å få gjøre seg kjent med innholdet av et dokument avslått, skal det vises til den bestemmelse som er grunnlag for avslaget samt opplyse om klageadgang og klagefrist.

Nedenfor er nevnt endel unntak fra offentlighetsprinsippet. Hovedregelen er at all annen informasjon er offentlig. Tvilsspørsmål kan tas opp med Sikkerhetsutvalget.

2. Nærmere om hva som er unntatt eller kan unntas offentlighet

Opplysninger belagt med taushetsplikt

Opplysninger undergitt taushet i medhold av lov. Dette gjelder i særlig grad opplysninger om:

- a) Personlige forhold
- b) Tekniske innretninger og fremgangsmåter samt drifts- eller forretningsforhold som det vil være av konkurransemessig betydning å hemmeligholde av hensyn til den opplysningen angår.

Det vises for øvrig også til bestemmelsene i *Forvaltningsloven* av 10.2.67 § 13a-13f som inneholder generelle regler om offentlig ansattes taushetsplikt generelt.

Statistisk materiale

Alt statistisk grunnmateriale (skjemaer, revisjons-skriv, navnekort o.l.) og arbeidstabeller, manuskripter o.l. er unntatt. Det gjelder også når opplysninger blir innhentet på frivillig grunnlag. Data som av andre institusjoner stilles til rådighet for statistisk bearbeiding i Statistisk sentralbyrå kan ikke av Statistisk sentralbyrå gjøres kjent for andre uten institusjonenes godkjennelse/samtykke.

Denne bestemmelse omfatter samtlige dokumenter som ikke spesielt er frigitt for offentliggjørelse i form av publikasjoner eller på annen måte.

Statistiske registre

Alle registre - både sentrale registre og delregistre som nyttes i samband med oppgaveinnhenting - uansett hvilken form de føres på, er unntatt.

Dokumenter som utarbeides på grunnlag av registeropplysninger, er ikke offentlige dokumenter før de er spesielt frigitt for offentliggjøring.

Dokumenter vedrørende folkeregistreringsloven

Alle dokumenter som danner grunnlag for registrering i henhold til folkeregistreringsloven, er unntatt.

Interne arbeidsdokumenter

Alle interne dokumenter, forslag, utkast, møtereferater og liknende arbeidsdokumenter kan unntas. Dette gjelder også korrespondanse med anmodning om faglig og teknisk rådgivning. Dokument som er innhentet fra underordnede organ eller utarbeidet av særlig sakkyndige/rådgivere, kan unntas.

Personal- og lønnsaker

Saksdokumenter vedrørende tilsetninger, engasjement, utnevninger, forfremmelser, bedret lønnsmessig plassering og lønnstillegg for navngitte funksjonærer, normeringer og justeringer og spesielle avtaler om lønns- og arbeidsvilkår, og korrespondanse med tjenestemannsorganisasjoner og trygdekantor kan unntas.

Hjemmel for innkreving av oppgaver

Korrespondanse som går forut for vedtak som gir hjemmel for innkreving av statistiske oppgaver, kan unntas.

Ileggelse av tvangsmulkt og anmeldelser av oppgavegivere

Dokumenter vedrørende ileggelse av tvangsmulkt og politianmeldelser av oppgavegivere og gjenparter av dommer og forelegg i samband med oppgavegivingen kan unntas.

Byråskolen/intern opplæring

Alle dokumenter vedrørende den interne kursvirksomheten i Statistisk sentralbyrå, besvarelser til eksamener og skriftlige prøver, eksamenspapirer o.l. kan unntas.

Budsjett og regnskap

Statistisk sentralbyrås budsjettframlegg og korrespondanse i den forbindelse. Korrespondanse om mer- og mindreutgifter under kap. 1620 og 4620, om etaten Statistisk sentralbyrå, og om Statistisk sentralbyrås regnskapssaker, kvitteringer, antegnelser, desisjoner, ettersyn o.l. kan unntas.

Kontrakter

Kontrakter om leie og service vedrørende maskiner, husleiekontrakter og korrespondanse om vedlikeholdskontrakter og om trykking av skjemaer og publikasjoner, kan unntas.

Etablering, omlegging eller utbygging av statistikk

Korrespondanse i samband med de årlige budsjetter eller langtidsbudsjetter som har nær tilknytning til budsjettene.

Når det gjelder saker av denne art, bør dokumenter eller følgeskriv som sendes til andre offentlig organer, påføres en opplysning om at saken er unntatt fra offentlighet. Øverst i høyre hjørne henvises til den bestemmelse som danner grunnlag for unntaket, dvs. til vedkommende paragraf og nr. eller ledd, f.eks. U.offl. § 6.7. ledd eller § 5.1. ledd.

Dersom dokumentet ikke under noen omstendighet er unntatt fra offentlighet, kan det likevel bli spørsmål om utskyting av tidspunktet for offentlighet. Vilåret for utskyting er at de foreliggende dokumenter antas å gi et åpenbart misvisende bilde av saken og videre at offentlighet kan skade samfunnsmessige eller private interesser. Begge disse vilkår må være oppfylt. Det er altså ikke nok at saken er ufullstendig opplyst eller på et forberedende stadium.

Representasjon

All korrespondanse om arrangementer med møter eller besøk kan unntas.

Innkjøp

Korrespondanse vedrørende anskaffelse av kontorutstyr, inventar, kontorrekvisita o.l. kan unntas.

Internasjonalt samarbeid

Møter i internasjonale organisasjoner, kan unntas.

Saker vedrørende Nordisk statistisk sekretariats budsjett og regnskap, personal- og lønnsaker o.l., kan unntas.

Arbeidsmiljøutvalget

Alle interne dokumenter og korrespondanse med Arbeidstilsynet kan unntas.

Graderte dokumenter

Alle graderte dokumenter er unntatt.

6. Offentliggjøring av statistikk og utlevering av statistiske opplysninger generelt

6.1. Offentliggjøring av statistikk/informasjon fra statistiske registre

Generelt

Retningslinjer for hva slags statistikk som kan publiseres reguleres først og fremst av bestemmelsen i statistikklovens § 2-6. Offentliggjøringen må imidlertid ses i sammenheng med alle de regler som finnes med det formål å beskytte oppgavegiverne mot misbruk av opplysninger de har gitt til Statistisk sentralbyrå.

Opgavegiverene skal i tillegg til bestemmelsen i § 2-6 også være beskyttet ved at det er gitt:

1. Regler om taushetsplikt for de som arbeider med opplysningene i Statistisk sentralbyrå (statistikklovens §§ 2-4 og 5-1, jfr. straffelovens § 121).
2. Regler som gir en snever angivelse av hva opplysningene kan brukes til annet enn å utarbeide offisiell statistikk (statistikklovens § 2-5 og rammekonsesjonens kapittel 4).

Offentliggjøring av opplysninger og forholdet til taushetspliktsbestemmelsene

Statistikklovens § 2-4 pålegger alle som utfører arbeid eller tjeneste taushetsplikt for visse typer opplysninger den enkelte får tilgang til i arbeidet med å utarbeide statistikk. I dette ligger også at Statistisk sentralbyrå generelt har et ansvar for at statistikk ikke offentliggjøres slik at opplysninger om enkeltindivider/bedrifter/foretak blir gjort kjent for uvedkommende.

Taushetsplikten etter statistikkloven er mer omfattende enn den generelle taushetsplikten etter forvaltningslovens § 13. Taushetsplikten i denne bestemmelsen er innskrenket til å gjelde opplysninger som det vil være av "konkurransmessig betydning å hemmeligholde".

Bestemmelsen i statistikkloven sier at uvedkommende ikke må få adgang til opplysninger som gjelder "drifts- eller forretningsforhold, eller tekniske innretninger og fremgangsmåter". Det vil derfor være et brudd på taushetsplikten og også brudd på regelen om forbud mot offentliggjøring til "urimelig skade" om f.eks. opplysninger om en

teknisk fremgangsmåte i en produksjonsprosess blir gjort kjent.

Offentliggjøring og forholdet til reglene om bruk av opplysninger.

Statistikklovens § 2-6 innebærer en innskrenkning av adgangen til bruk av opplysninger og dermed også en innskrenkning i rekkevidden av bestemmelsen i statistikklovens § 2-5. Hovedregelen er at innsamlet informasjon bare kan brukes til utarbeiding av offisiell statistikk eller annen bruk definert i rammekonsesjonens kapittel 4, jf. § 2-5.

Spørsmål kan stilles om offentliggjøring av detaljstatistikk i realiteten innebærer utlevering som nevnt i rammekonsesjonens punkt 4.3.1 - 4.3.3, og som derfor må følge de retningslinjer som er nevnt der. Grensen mellom utlevering av aidentifiserte individualopplysninger, jf. f.eks. konsesjonens punkt 4.3.2, og offentliggjøring av statistikk om spesielle deler av næringslivet kan innebære at muligheten for å identifisere oppgavegivere er stor. Offentliggjøring kan derfor tenkes å skje i strid med rammekonsesjonens bestemmelser, til tross for at offentliggjøring ikke skjer i strid med statistikklovens § 2-6. Dette må vurderes i det enkelte tilfellet.

Om krav til offentliggjøring av statistikk, jf. statistikklovens § 2-6

Det kan tenkes tilfelle hvor det av hensyn til statistikken og oppbygningen av denne må gjøres unntak fra hovedregelen om at opplysninger om enkeltpersoner/bedrifter ikke må gjøres kjent for andre. Det gjelder derfor en slags "siste skanse" ved at offentliggjøring uansett ikke må skje til skade for enkeltpersoner eller til urimelig skade for foretak/-offentlig virksomhet, jf. statistikklovens § 2-6. Se også rammekonsesjonen pkt. 3.2.1.

Det er oppgavegiveren som i utgangspunktet selv har bevisbyrden for at offentliggjøring av tall/tabeller vil være til skade/urimelig skade.

Om hva som kan regnes som "til skade" sier forarbeidene bl.a (Ot.prp.nr.58 1988-89 s. 31-32): "Departementet mener det er viktig å verne oppgavegiverne mot skadevirkninger som følge av oppgavegivingen. Departementet mener imidlertid

også at det kan tenkes tilfeller hvor offentliggjøring er lite betenkelig. Er opplysningene allerede offentlig kjent, som f.eks. regnskapsopplysninger fra et aksjeselskap, vil dette være et viktig moment. Er interessene og hensynene som taler for offentliggjøring overveiende, kan oppgavegivers interesser måtte vike."

Om vilkåret "*urimelig skade*" sies det på samme sted:

"Hva denne rettslige standard innebærer, vil avhenge dels av opplysningenes karakter, og dels av hvem oppgavegiver er. Personvern, dvs. vern om enkeltindividers forhold, vil stå særlig sterkt i vurderingen av om noe er til urimelig skade. Det vil være av særlig betydning - men ikke avgjørende - om oppgavegiveren (og den opplysningene gjelder, dersom dette er en annen) samtykker i offentliggjøring av opplysningene."

Oppsummering av reglene om publisering

Etter det som er sagt over, vil offentliggjøring av opplysninger i statistisk form svært vanskelig kunne hindres med hjemmel i statistikklovens § 2-6. Dersom detaljeringsgraden er stor, og det er lett å gjenfinne enkeltbedrifter i statistikken, vil offentliggjøring kunne være et brudd på taushetsplikten etter statistikklovens § 2-4. Videre må publisering heller ikke skje i strid med reglene om utlevering til "annen bruk" etter § 2-5.

Publisering av en for detaljert statistikk kan også medføre at Statistisk sentralbyrå går utenfor hva som er definisjonen av statistikk i statistikklovens § 1-2. Det er f.eks ikke Statistisk sentralbyrås oppgave å offentliggjøre omsetningsopplysninger i seg selv, men å gi opplysninger i en slik form at de er "tallfestede opplysninger om en gruppe eller fenomen, som fremkommer ved sammenstilling og bearbeiding av opplysninger om de enkelte enhetene i gruppen..."

Reglene for publisering må tilpasses det enkelte statistikkområde. Det skal tas hensyn både til det informasjonsbehov som foreligger og den skade som kan oppstå ved et utilsiktet innsyn i den enkelte oppgavegivers forhold.

Det vil ikke være mulig for Statistisk sentralbyrå, fullt ut å sikre at all statistikk som publiseres er fri for muligheter til å avlese opplysninger om enkelte oppgavegivere, basert på forhåndskunnskap om en eller flere oppgavegivere i en gruppe. Statistisk sentralbyrå bør derfor orientere oppgavegiverne, gjennom spørreskjemaet, om deres rett til å få fjernet

tall som etter statistikkloven kan være til skade for dem. Dette kan begrenses til økonomisk statistikk.

6.2. Utlevering av individualopplysninger/-mikrodata fra statistisk grunnmateriale

Adgangen til å levere ut opplysninger fra Statistisk sentralbyrås statistiske registre følger av statistikklovens § 2-5 og Statistisk sentralbyrås rammekonsesjon fra Datatilsynet (se vedlegg 2). Det vises også til punkt 5.1 - 5.3 over, som må sees i sammenheng med reglene om utlevering iht. til det som sies her.

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 personnummer/bedriftsnummer og/eller navn
- * *Aidentifiserte opplysninger*, dvs. opplysninger hvor de data som brukes som identifikasjonsnøkkel ved registeret er fjernet. Dette vil vanligvis være navn, adresse og personnummer/bedriftsnummer.
- * *Anonymiserte opplysninger*, dvs. opplysninger hvor så mye av en fil er fjernet at det med rimelige midler ikke er mulig å knytte opplysninger eller vurderinger direkte eller indirekte til identifiserbare enkeltpersoner, sammenlutninger eller stiftelser. Spørsmålet om en individfil er anonym eller ikke, må også ses i sammenheng med definisjonen av et personregister, se punkt 5.2. Selv om registrering av anonymiserte opplysninger ikke krever konsesjon, må det ved utlevering av denne type 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 6.

Det er viktig å merke seg at reglene åpner for en adgang til utlevering ("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 Statistisk sentralbyrå 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 Statistisk sentralbyrå kan utlevere opplysningene.

1. Hvem kan levere ut opplysningene?

Bare den som har ansvaret for et register og fullmakt til å levere ut 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.

2. Sammendrag av reglene om utlevering:

Statistikklovens § 2-5 gir Datatilsynet fullmakt til å bestemme at opplysningene i Statistisk sentralbyrås registre kan brukes til annet enn å utarbeide offisiell statistikk. I Statistisk sentralbyrås 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 Statistisk sentralbyrå skal eller kan stille.

Etter konsesjonens bestemmelser kan utlevering av informasjon i annen form enn som offisiell statistikk, foretas i følgende tilfelle:

- **Utlevering til statistisk bruk for forskningsformål (konsesjonens pkt. 3.2.3 og 4.3.1).**

- * Slik utlevering kan skje til etablerte forskningsinstitutter, forskere med forskerkompetanse og hovedfagsstudenter forutsatt at disse er under veiledning av en med forskerkompetanse ved undervisningsstedet.
- * Selv identifiserbare opplysninger kan utleveres til slikt formål om ikke Statistisk sentralbyrå selv har unntatt data fra utlevering. Dette kan være gjort for identifiserbare data fra frivillige undersøkelser. Slike unntak skal være registrert i registerdokumentasjonen. Det er viktig å merke seg at utlevering til slikt formål ikke kan skje uten at det er dispensert fra eventuell taushetsplikt. 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 identifiserbare data fra frivillige undersøkelser ikke kan utleveres uten samtykke fra informantene.

- * 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.
 - * Utlevering skjer etter skriftlig søknad, og øvrige vilkår følger av standardavtale nr. 1 i vedlegg 6 som registeransvarlig og søker skal undertegne.
- **Utlevering til statistisk bruk for offentlig planlegging (konsesjonens pkt. 3.2.3 og 4.3.2).**
- * Slik utlevering 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.
 - * Det kan bare utleveres aidentifiserte opplysninger for dette formålet. For opplysninger underlagt taushetsplikt etter særlovgivning, kan det være nødvendig med dispensasjon fra taushetsplikten også for utlevering av aidentifiserte opplysninger. Dette spørsmålet må forelegges det aktuelle fagdepartement.
 - * Hvor Statistisk sentralbyrå har mottatt opplysninger fra en annen offentlig institusjon, må Statistisk sentralbyrå også ha samtykke fra denne om det er tvil om utlevering bør finne sted.
 - * Det må påses at de registre som utleveres, ikke på noen måte kan kobles med andre registre hos mottakeren.
 - * Utlevering skjer etter skriftlig søknad, og øvrige vilkår følger av standardavtale nr. 2 i vedlegg 6 som registeransvarlig og søker skal undertegne.

- **Utlevering av næringslivsopplysninger for etablering og ajourhold av registre (konesjonens pkt. 3.2.4 og 4.3.3).**

- * Bestemmelsen åpner for adgang til utlevering av særskilte identifiserbare næringslivsopplysninger.
 - * Slik utlevering kan skje både til bruk i offentlige og private registre.
 - * Ved etablering eller ajourhold av et register må det kreves at det registeret som mottar opplysningene, har konsesjon fra Data-tilsynet til å motta disse opplysningene fra Statistisk sentralbyrå.
 - * Ved utlevering av opplysninger til ajourhold av et register er det naturlig å kreve at ajourholdet utføres tilstrekkelig ofte i forhold til bruken av registeret. Det vil ofte være gunstig å kreve tilbakemelding om feil eller mangler i registeret. Dette gjelder særlig feil i adresser og manglende enheter.
 - * Utlevering skjer etter skriftlig søknad, og øvrige vilkår følger av standardavtale nr. 3 i vedlegg 6 som registeransvarlig og søker skal undertegne.
3. *Saksbehandling*
- * Den som er ansvarlig for utlevering, skal alltid kreve en skriftlig søknad (husk journalføring). Det skal først vurderes om det finnes andre alternativ enn utlevering av identifiserbare opplysninger.
 - * Det må alltid undersøkes om det er knyttet spesielle vilkår til det registeret utleveringen skjer fra. Dette skal framgå av registerdokumentasjonen.
 - * De betingelser som skal stilles går fram av standardavtalene i vedlegg 6. Der man mener det er nødvendig, kan strengere vilkår tas inn, f.eks. i forbindelse med publisering. Alle betingelser nevnt i rammekonesjonens pkt. 4.3.1 - 4.3.3. må tilfredsstilles om modellavtalene i vedlegg 6 ikke brukes.
 - * Registeransvarlig skal registrere alle utleveringer og sørge for at sletting av utleverte opplysninger blir bekreftet etter at prosjektet er utført.
 - * 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. malbrevet i vedlegg 6.

- * Dersom Statistisk sentralbyrå godkjenner søknad om utlevering, kan opplysningene gjøres tilgjengelige for brukeren i Statistisk sentralbyrås lokaler, i Statistisk sentralbyrås datamaskin fra søkerens terminal eller de kan sendes i posten på papir eller i maskinlesbart medium. Det vil til enhver tid finnes mer detaljerte regler for hver av disse formene for oversendelse, se bl.a. punkt 5.8 over.

6.3. Utlevering av data innenfor EØS-området

- * I utgangspunktet skal overføring av personregistre til utlandet meldes til Datatilsynet på Statistisk sentralbyrås meldingsskjema, jf. Personregisterlovens § 36 og forskriftenes § 8-1 til loven (se vedlegg 4). Datatilsynet kan nekte overføring eller sette vilkår til slik overføring. Det foreligger imidlertid ikke meldeplikt dersom Norge "har plikt til å foreta slik overføring etter folkerettslig overenskomst eller som følge av medlemskap i internasjonal organisasjon".
- * 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 vedlegg 30 i avtalen mht. særlige bestemmelser om organiseringen av samarbeidet. Hverken protokoll 76 eller vedlegg 30 utpeker hvem som skal ha hovedansvar for produksjon og utarbeiding av statistikk for EØS-området eller gir klare og generelle regler om utleveringsplikt. Disse spørsmålene må derfor avklares gjennom konkrete rettsaker innenfor de områder hvor det skal utarbeides statistikk i henhold til EØS-avtalen og senere endringer i den.
- * Rådsforordning (EØF) nr. 1588/90 om oversendelse av fortrolige statistiske opplysninger til De europeiske fellesskaps statistikkbyrå (som er 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   p legge de enkelte nasjonale statistikkbyr er utleveringsplikt, jf. ogs  forordningens Art. 3 nr. 2, men om slik plikt foreligger i en spesifikk E S-rettsakt, skal personvern/taushetspliktsregler i de enkelte land ikke v re til hinder for slik utlevering.

For   kunne fastlegge om Statistisk sentralbyr  har plikt til   utlevere data, hvilket detaljeringsniv  m.v., er det derfor f rst og fremst de enkelte rettsakter innenfor de enkelte statistikkomr der som fastlegger pliktens omfang. Dersom rettsakten ikke sier noe om utlevering eller til hvem slik utlevering skal foretas, m  sp rsm let om utlevering avklares gjennom den lovbestemte meldingen som i disse tilfellene skal sendes til Datatilsynet. Dette skal skje ved at den registeransvarlige s ker Datatilsynet om tillatelse til utlevering dersom vedkommende mener dette er forsvarlig i henhold til gjeldende norsk regelverk.

Navneliste over aktuelle personer i Statistisk sentralbyrås sikkerhetsorganisasjon pr. 1. februar 1994

Statistisk sentralbyrås ledelse:

Administrerende direktør	Svein Longva
Avdelingsdirektør for Avdeling for økonomisk statistikk:	Gisle Skancke
Avdelingsdirektør for Avdeling for personstatistikk:	Gunvor Iversen
Avdelingsdirektør for næringsstatistikk:	Nils Håvard Lund
Forskningsdirektør for Forskningsavdelingen:	Olav Bjerkholt
Avdelingsdirektør for Administrasjonsavdelingen	Hanne Finstad

Andre sentrale personer i ledelsesstrukturen:

Seksjonsleder for Seksjon for EDB - drift:	Bent Vangli
--	-------------

Statistisk sentralbyrås Sikkerhetsutvalg:

Leder:	Sverre Hove
Medlemmer:	Mette Bredengen
	Bent Vangli

Statistisk sentralbyrås dataadministrator:

Fra Seksjon for EDB - drift:	Ole Førreisdahl
------------------------------	-----------------

Statistisk sentralbyrås dataarkivar:

Marit Hansen

Avdelingenes sikkerhetskontrollører:

Avdeling for økonomisk statistikk:	Rune Gløersen
Avdeling for personstatistikk:	Jon Holmøy
Avdeling for næringsstatistikk:	Sindre Børke
Forskningsavdelingen:	Bård Lian
Avdeling for administrasjon og fellestjenester:	Arne Gunnar Teigen
	Svein Erik Børslungen

Datatilsynets rammekonsesjon for Statistisk sentralbyrå

Saksnr.: 90/622-2

TG/KY datert 27.4.1990

I medhold av Lov om personregistre mm. av 9.6.78 nr. 48 § 9, jfr. Kgl. res. av 21.12.1979 pkt. 1 gis Statistisk sentralbyrå (Statistisk sentralbyrå) samtykke (konsesjon) til å føre personregistre som det Statistisk sentralbyrå anser nødvendig av hensyn til utarbeiding av offisiell statistikk og en rasjonell og formålstjenelig statistikk produksjon.

Konsesjonen gjelder fra 2.5.90 samtidig som konsesjon av 15.4.86 blir trukket tilbake.

Konsesjonen gjelder for:

PERSONREGISTRE TIL BRUK I
STATISTIKKPRODUKSJON OG ANNEN
NÆRMERE ANGITT BRUK GODKJENT MED
HJEMMEL I LOV OM OFFISIELL STATISTIKK
OG STATISTISK SENTRALBYRÅ AV 16. JUNI
1989 NR. 54 § 2-5.

Datatilsynet har fastsatt følgende vilkår for samtykket. Vilkårene skal gjøres kjent for personell som behandler personopplysninger for registreier.

1. Registeransvarlig (personregisterlovens § 11 siste ledd)

Ansvarlig for det enkelte register oppgis i den melding som sendes Datatilsynet for hvert enkelt register (se pkt. 4.6)

Registeransvarlig plikter å sørge for at betemmelsene i personregisterloven med forskrifter og denne konsesjon blir fulgt.

2. Registerets omfang/registrerings-medium

Konsesjonene gjelder for pesonregistre som opprettes i statistikkøyemed. Konsesjonen omfatter manuelle og EDB-førte registre.

3. Regler etter personregisterloven § 11 første ledd

3.1. Registerets innhold

Registeret kan bare inneholde følgende typer opplysninger:

1. Opplysninger innhentet med hjemmel i Lov om offisiell statistikk og Statistisk sentralbyrå av 16.6.1989 nr. 54 og i tidligere Lov om tilveiebringelse av oppgaver til den offisielle statistikk av 25. april 1907 nr. 2.
 2. Opplysninger innhentet med hjemmel i andre lover som gir Statistisk sentralbyrå rett til å kreve opplysninger.
 3. Opplysninger som Statistisk sentralbyrå har mottatt fra andre offentlige organer, herunder gjennom utnyttelse av administrative datasystemer i statsforvaltningen og i landsomfattende kommunale organisasjoner.
 4. Opplysninger innhentet på frivillig grunnlag (herunder markeds- og opinionsundersøkelser) som grunnlag for offisiell statistikk.
 5. Opplysninger innhentet fra offentlige tilgjengelige kilder.
- 3.2. *Hva registeret kan brukes til/formålet med registreringen*

3.2.1

Registrene skal som hovedregel bare nyttes i statistisk øyemend. Statistikk må ikke offentliggjøres på en slik måte at den kan fryktes å være til skade for enkeltpersoner.

3.2.2

Registrene kan videre nyttes i analyse- og forskningsvirksomhet internt i Statistisk sentralbyrå.

3.2.3

Registrene kan bare nyttes statistisk for forskningsformål utenfor Statistisk sentralbyrå og for offentlig planlegging.

3.2.4

Opplysninger som nevnt i konsesjonens pkt. 4.3.3 (særskilte næringsopplysninger) kan nyttes til opprettelse og oppdatering av andre offentlige og private registre i det omfang og til den bruk som er hjemlet i disse registrenes konsesjon gitt av

Datatilsynet. Det samme gjelder for registre opprettet med hjemmel i egen lov jfr. personregisterlovens § 41, såfremt særloven eller bestemmelser fastsatt av Datatilsynet tilater lagring og bruk av slike opplysninger.

3.2.5

Utlevering av opplysninger fra registrene kan skje som presisert under pkt. 4.3.

3.2.6

Om andres bruk av personopplysninger fra registeret, se konsesjonens punkt 4.3.

3.2.7

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

4. Vilkår etter personregisterloven § 11 annet ledd

4.1. Innsamlig/kontroll

Opplysningene i registeret kan innhentes fra fysiske og juridiske personer og fra offentlige organer dersom lovbestemt taushetsplikt ikke er til hinder for det. Ved innhenting av opplysninger på frivillig grunnlag (se ovenfor under pkt. 3.1.4), skal det gjøres uttrykkelig oppmerksom på at den enkelte kan nekte å delta i vedkommende undersøkelser e.l. (Jfr. også personregisterlovens §§ 32 og 33 hva gjelder opplysninger mottatt for opinions- og markedsundersøkelser.)

Dersom ikke navn, fødselsnummer eller annen personidentifikasjon blir erstattet med kryptert nummer, må registre som nevnt i pkt. 3.1, anonymiseres så snart som mulig.

4.2. Samkjøring (kobling)

Registre som inneholder opplysninger som nevnt i pkt. 3-1, må bare kobles med andres eller egne registre dersom det er absolutt nødvendig. For opplysninger innhentet på frivillig grunnlag forutsettes uttrykkelig samtykke fra informanten.

Denne begrensningen gjelder ikke når fødselsnummer, navn og annen identifikasjon er erstattet med kryptert nummer.

Som forarbeid til oppdatering av opplysninger som nevnt i pkt. 4.3.3, kan kobling bare utføres internt av Statistisk sentralbyrå med bruk av egne og andres registre.

4.3. Utlevering av opplysninger fra registeret

4.3.1

Opplysninger i registrene kan utleveres til statistisk bruk for forskning utenfor Statistisk sentralbyrå, når det finnes rimelig og ikke medfører uforholdsmessig ulemper for andre interesser.

For utlevering er det et vilkår at opplysningen blir anonymisert i den grad forskningsprosjektet tillater og at vedkommende forsker/forskningsinstitusjon har fått nødvendig konsesjon fra Datatilsynet til opprettelse av register. Dersom opplysninger innhentet på frivillig grunnlag skal utleveres på en slik måte at de kan føres tilbake til den enkelte oppgavegiver, skal det i tillegg innhentes særskilt samtykke fra informanten.

For opplysninger som Statistisk sentralbyrå har mottatt fra andre offentlige organer må disse i tillegg ha samtykke i dette dersom det er tvil om utlevering bør finne sted, og ellers dersom Statistisk sentralbyrå har mottatt opplysninger for bearbeiding fra andre.

Forskningsresultatene må ikke offentliggjøres på en slik måte som kan fryktes å være til skade for oppgavegiver eller annen identifiserbar enkeltperson, eller til urimelig skade dersom oppgavegiver eller enkeltperson er en offentlig virksomhet eller et foretak som nevnt i statistikklovens § 5-1, 3 ledd. Det er et vilkår at taushetsplikt etter statistikklovens § 2-4 skal gjelde for mottaker av opplysningene.

Statistisk sentralbyrå må også stille krav om hvem som skal ha ansvar for opplysningene, hvem som skal ha adgang til de, om oppbevaring og tilbakelevering av materialet, og tilintetgjøring av avskrifter, om forskere skal ha adgang til eller innhente nærmere opplysninger som dem det er gitt opplysninger om og om bruken ellers.

4.3.2

Aidentifiserte personopplysninger i registrene kan utleveres til statistisk bruk for offentlig planlegging. Dersom opplysninger innhentet på frivillig grunnlag skal utleveres på en slik måte at de kan føres tilbake til den enkelte oppgavegiver, skal det i tillegg innhentes særskilt samtykke fra informanten. For opplysninger som Statistisk sentralbyrå har mottatt fra andre offentlige organer må disse i tillegg ha samtykke i dette dersom det er tvil om utlevering bør finne sted, og ellers dersom Statistisk sentralbyrå har mottatt opplysninger for bearbeiding fra andre. Det er et viktig vilkår at taushetsplikt etter statistikklovens § 2-4 skal gjelde mottakere av opplysningene.

4.3.3

Med hjemmel i statistikklovens § 2-5 gjøres det unntak fra taushetsplikten i lovens § 2-4, slik at utlevering av særskilte næringslivsopplysninger kan skje til bruk som nevnt i pkt. 3.2.4. Adgangen skal begrenses til navn, adresse og eierform for juridiske personer og for andre som driver næringsvirksomhet, samt oversikt over den enkelte virksomhets beliggenhet, bransje (næringsgruppekode), sysselsetting (i grupper etter antall sysselsatte/årsverk) og status-kode (om virksomheten er i vanlig drift, ute av drift eller opphørt). Videre kan identifikasjonsnumrene for henholdsvis virksomheter (bedriftsnummer) og foretak (foretaksnummer såvel som Brønnøysundregistrenes nummer) leveres ut sammen med opplysningene foran og til de samme formål. Tilsvarende gjelder for datoer som vedrører tidspunkt for registrering og endring av ovennevnte opplysninger.

Før utlevering kan skje, skal Statistisk sentralbyrå bringe på det rene at mottageren av opplysningene har konsesjon fra Datatilsynet som både gir adgang til at de aktuelle opplysninger kan registreres og til at de kan mottas fra Statistisk sentralbyrå. Det skal også ved slik utlevering stilles krav om at opplysningene skal oppdateres jevnlig og at tidligere versjoner skal slettes ved mottak av nye opplysninger fra Statistisk sentralbyrå. Mottakere skal også gjøres oppmerksom på svakheter i de mottatte opplysningenes kvalitet, og at opplysningene ikke kan legges til grunn ved avgjørelser i enkeltsaker.

4.3.4

Opplysninger som Statistisk sentralbyrå mottar fra andre offentlige organer kan utleveres til andre når vedkommende organ ber om det.

4.3.5

Opplysninger i Statistisk sentralbyrås registre som er hentet fra offentlig tilgjengelige kilder (pkt. 3.1.5) kan utleveres til formål som ikke anses å være til skade for den enkelte.

4.3.6

Opplysninger fra registeret må ellers ikke gjøres kjent for andre på en slik måte at den kan henføres til enkeltperson.

4.3.7

Det må generelt påses at utlevering av enkeltopplysninger ikke skjer i strid med taushetsplikten.

4.4. Sletting av opplysninger

Den registeransvarlige skal slette/anonymisere opplysninger som ikke lenger har betydning.

Manuelt grunnlagsmateriale skal anonymiseres eller makuleres når registrering og kontroll har funnet sted.

Spørsmålet om avlevering til arkivverket er for tiden under utredning, og krav til sletting/anonymisering som nevnt ovenfor kan utstå inntil dette er avklart.

4.5. Adgang til registeret - sikring

Bare ansatte som har behov for opplysningene i sitt arbeid, skal ha tilgang til opplysningene.

Det samme gjelder personell i EDB-avdeling/EDB-foretak.

Den registeransvarlige må sørge for slik sikring av de registrerte opplysninger som hindrer at noen får tilgang til dem uten å ha rett eller krav på opplysningene.

Oppbevaring av personopplysninger skjer i samsvar med Statistisk sentralbyrås interne retningslinjer. Det skal ved melding om enkeltregistre opplyses hvilke tiltak som gjelder.

De nøkler/programmer som nyttes til kryptering, skal oppbevares/brukes slik at de må initieres av Statistisk sentralbyrås administrerende direktør eller personlig oppnevnt vararepresentant og personal- og økonomidirektør eller personlig oppnevnt vararepresentant. Statistisk sentralbyrå skal forelegge Datatilsynet rutiner for dette til godkjenning.

4.6. Melding til Datatilsynet

Byrået skal før opprettelsen av register gi melding til Datatilsynet i god tid på fastsatt skjema.

4.7. Straff

Brudd på Lov om personregistre av 9.6.1978 nr. 48 og forskrifter gitt i medhold av dette og betingelser satt i denne konsesjon straffes med bøter eller fengsel i inntil 1 år eller begge deler, jfr. personregisterloven § 38.

5. Forbehold om endringer i konsesjonsvilkårene

Datatilsynet tar forbehold om å trekke konsesjonen tilbake, eller gi nye og endrete vilkår når dette finnes nødvendig ut fra personvern hensyn.

Kryptering av fødselsnummer i Statistisk sentralbyrås registre

1. Bruk av fødselsnummeret og om kryptering av personregistre

Fødselsnummeret

I tillegg til å identifisere hver enkelt bosatt person i Norge gir fødselsnummeret informasjon om kjønn og fødselsdato. Ved feilregistrering av disse opplysningene på det tidspunktet identifikasjonsnummeret tildeles, må personen tildeles nytt fødselsnummer når feilene skal rettes. I dag forekommer dette praktisk talt bare for utlendinger som kommer fra land som bruker en annen tidsregning enn vår. Sentralkontoret for folkeregistrering som tildeler fødselsnummer, fører til enhver tid en oversikt (katalog) over fødselsnummer som er skiftet (og sammenhengen mellom dem). Fødselsnummer som er brukt blir aldri tatt i bruk på nytt.

Om kryptering og begrunnelse for dette

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

En annen begrunnelse for kryptering er de krav som stilles fra Datatilsynet ved kobling av registre. Statistisk sentralbyrås rammekonsesjon fra Datatilsynet tillater kobling av registre når det er "absolutt nødvendig". Denne begrensningen gjelder ikke når F.nr er erstattet av K-nr. (Se konsesjonen pkt 4.2).

Ellers er det selvfølgelig slik at krypteringen bidrar sterkt til en anonymisering av dataene og derved styrker vårt datavern. Kryptering er et godt alternativ til anonymisering (total fjerning av alle kjennetegn, S-nr. og K-nr.) som vil kunne avskjære Statistisk sentralbyrås mulighet til framtidig kobling. Der framtidig kobling helt klart ikke er aktuelt, bør imidlertid registeret anonymiseres. Der vi vil holde muligheten åpen for slik kobling, antas kryptering å være en akseptabel løsning for Datatilsynet. Statistisk sentralbyrå kan ikke regne med at kostnader ved kryptering vil bli godtatt av Datatilsynet som begrunnelse for ikke å kryptere der det blir gitt et pålegg.

2. Litt om S-nr og K-nr.

S-nr er en permanent identifikasjon av alle personer som er tildelt F-nr. Et program som er tilgjengelig for alle, skifter ut F-nr med S-nr. S-nr har, som F-nr, 11 siffer.

Det begynner med bokstav S, fortsetter med et løpenr. på 7 siffer, har ett siffer som kode for kjønn og århundre og avsluttes med fødselsår. De tre siste sifferne tilhører egentlig ikke S-nr, men det er praktisk å plassere disse her for å fylle opp plassen etter fødselsnr. Numrene tildeles i tilfeldig rekkefølge slik at det ikke ligger noen informasjon i nummeret. Statistisk sentralbyrå har bedt Sentralkontoret for folkeregistrering ta S-nr inn i databasen for det sentrale personregisteret og regner med at dette blir gjort. Dette tillater en overgang til S-nr i Befolkningsstatistikken og Statistisk sentralbyrås egen datainnsamling slik som i FOB 90.

K-nr. er en kryptering av S-nr og er derfor også permanent over tiden. Krypteringen foregår ved bruk av et program og en todelt nøkkel. Hver nøkkel gir en egen krypteringsserie som kjennetegnes ved en bokstav forskjellig fra S i første posisjon i K-nr. Ellers har K-nr. samme redigering som S-nr. Krypteringsprogrammet er godkjent av Datatilsynet. Programmet benytter seg av en kjent formel for generering av tilfeldige tall og trenger ikke behandles fortrolig. Det er bare nøklene som må beskyttes.

3. Krypteringsrutinene

Det er laget tre rutiner i forbindelse med kryptering av S-nr.:

- * Kryptering av S-nr. til K-nr.
- * Dekryptering av K-nr. til S-nr.
- * Omkryptering av K-nr. fra en serie (nøkkel) til en annen serie (nøkkel)

Kryptering av S-nr. til K-nr.

Krypteringen styres av en todelt nøkkel som kan velges fritt blant minst 1 million muligheter. Til hver nøkkel som blir brukt svarer det en krypteringsserie. Krypterings-serien identifiseres med en bokstav forskjellig fra S (S er reservert til S-nr). Denne bokstaven settes foran det krypterte nummeret i K-nr. i registeret og skrives på den plassen hvor S-nr. stod.

Registre som er kryptert med samme nøkkel kan kobles når de sorteres på K-nr.

Nøkkelen er den eneste informasjon som må behandles fortrolig i forbindelse med krypteringen. Hver halvpart av nøkkelen skrives på hvert sitt krypteringskort sammen med bokstaven som identifiserer krypteringsserien.

Krypteringen styres av to autoriserte personer som er ansvarlige for hver sin halvdel av nøkkelen. Etter Statistisk sentralbyrås konsesjon fra Datatilsynet er det bare adm. dir. og administrasjonsdirektøren og deres vararepresentanter som er autorisert til å styre krypteringen og oppbevare nøklene.

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 uforutsatt behov skulle dukke opp.

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.

Bruk av forskjellige krypteringsserier.

Hvert nytt sett av nøkler gir en ny krypteringsserie. Data som skal kobles etter kryptering må ha samme serie. Dersom Statistisk sentralbyrå ønsker å koble registre med forskjellig serie, må det ene registeret omkrypteres på forhånd ved bruk av nøkler for begge registrene. Det kan også lages program for kobling av registre med forskjellig K-nr eller hvor ett register har K-nr og det andre har S-nr. I slike tilfeller må det brukes flere sett med nøkler. Dette tilsier at Statistisk sentralbyrå bør bruke forskjellige serier der vi ikke kjenner til behov for kobling.

Normalt bør Statistisk sentralbyrå ikke levere data til eksterne brukere med K-nr. Dette skyldes at Statistisk sentralbyrå, med støtte av Datatilsynet, har ment at Statistisk sentralbyrås registre ikke skal leveres ut med mer identifikasjon enn nødvendig. Dersom det allikevel bli nødvendig å levere ut et register med K-nr, bør det velges en egen serie til et slikt register. Dersom det oppstår mistanke om at et kryptert register er helt eller delvis identifisert, bør det straks omkrypteres.

4. 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 aidentifisering, dvs. fjerning av fødselsnummer og den regnes ikke som sikker.

Det vil imidlertid alltid være visse muligheter for bakveisidentifisering, dvs. identifisering av personer gjennom andre data i registeret som er kjent sammen med sikker informasjon om identitet, utenfor registeret. Det er ikke mulig å vite hvor mye slik forhåndskunnskap den enkelte bruker av et slikt register sitter inne med. Siden Statistisk sentralbyrå har oversikt over hvilke registre hver bruker har adgang til, blir det derfor en oppgave å påse at registre som ikke er kryptert ikke brukes sammen med registre som inneholder data som kan brukes til å bryte krypteringen.

5. Kontroll av krypteringen

Vi kan dele denne kontrollen i fire deler:

- Kontroll av krypteringsprosessen
- Kontroll av hva som må krypteres
- Kontroll av fordelingen av registre på krypteringsserien
- Kontroll med spredning av K-nr. og kobling av registre

Kontroll av krypteringsprosessen

Når en ny krypteringsserie tas i bruk, beregner krypteringsprogrammet en veiet kontrollsum for hver halvdel av nøkkelen. Ved senere kryptering må både nøkkel og kontrollsum testes inn. Nøkkel og kontrollsum sammen med bokstav for krypteringsserie skrives ned på et kort som oppbevares nedlåst hos den som har foretatt krypteringen. Kopi av kortet oppbevares nedlåst i fjernarkiv.

En kontrollør som kjenner registeret og er uavhengig i forhold til eieren av registeret, må kontrollere innholdet i det krypterte registeret og bekrefte at bare det datainnholdet som skal være med har kommet med og at ingen form for identifikasjon er kommet med.

Kontroll av hva som må krypteres

De fleste registre i Statistisk sentralbyrå forekommer i flere utgaver med det samme eller delvis det samme innhold. Det må kontrolleres at alle disse utgavene blir kryptert, avidentifisert eller slettet.

Innholdet i et register kan, helt eller delvis, bli overført til et annen register. Kryptering av et register kan derfor få konsekvenser for et annet register. Det må i hvert enkelt tilfelle avgjøres hvor langt kryptering, avidentifisering eller sletting av registre må gå for at en kryptering skal være effektiv.

Med det store antall registre som finnes i Statistisk sentralbyrå, og behovet for kobling og behovet for å kopiere registrene i forskjellige utgaver under statistikkproduksjonen, er det nyttig å ha en systematisk identifisering av alle filer som det er nødvendig å opprette.

For å styrke Statistisk sentralbyrås datadokumentasjon, vil nå det registernummeret som brukes overfor Datatilsynet kunne knyttes til filidentifikasjonen. Filer med krypterte data vil få bokstav K som siste ledd i identifikasjonen. Etter kryptering av et register skal alle filer i arkivet for dette registeret ha en K i siste ledd eller være avidentifisert. Dersom dette ikke kan gjennomføres må registereier påse at ikke samme bruker har lesetillatelse til både kryptert og ikke-kryptert kopi av registeret.

Kontrollen med hvilke filer som må krypteres når et register skal krypteres, vil overvåkes av en sentral person, dataadministratøren, som har oversikt over hele dataarkivet.

Kontroll av fordelingen av registre på krypteringsserier

Det ville være mest praktisk å bruke bare en krypteringsserie for alle registre i Statistisk sentralbyrå. En slik praksis vil imidlertid gjøre det teknisk mulig å koble alle registre som en bruker (i praksis en seksjon) har adgang til. Det vil imidlertid av hensyn til dataleverandørens tillit til Statistisk sentralbyrå være gunstig å opprette flere krypteringsserier.

Flere serier gir derfor reelt en bedre beskyttelse. Det kan også tenkes at enkelte dataleverandører, f.eks. helsesektoren, selv ønsker å kontrollere krypteringen og overvåke nøkkelen. Slike leverandører må kunne tilbys å bruke en egen krypteringsserie. Dersom noen av Statistisk sentralbyrås krypterte registre skal omkrypteres til en slik serie av hensyn til kobling, må begge parter medvirke med sine nøkler under omkryptering av Statistisk sentralbyrås register.

Det vil kreve en omfattende oversikt over Statistisk sentralbyrås dataarkiv og planen for statistikkproduksjon i årene framover hos dem som skal avgjøre valg av krypteringsserie. Denne funksjonen må derfor plasseres sentralt hos dataadministratør.

Datatilsynet Postboks 8177 Dep OSLO 1 Tlf. 22 42 19 10	MELDING OM OPPRETTELSE AV PERSONREGISTER INNENFOR VILKÅR SATT I RAMMEKONSESJON			Reg. nr.
Meldingen sendes Datatilsynet i god tid før registeret opprettes				
Eier av registeret	Navn (organ, foretak, person) Statistisk sentralbyrå			Arbeidsgivernr. 3444 7837
	Gate-/veiadresse Kongens gt. 6			
	Postnr. Postboks 8131 Dep.	Poststed 0033 OSLO		Telefon 22 86 45 00
	Kontaktperson Leder i sikkerhetsutvalget			Telefon
Meldingen gjelder	<input type="checkbox"/>	Nytt register	<input type="checkbox"/>	Endring
Tidspunkt for opprettelse av registeret		Oppstartingsdato		
Registeret opprettes innen rammen av		Konsesjonsnr.	Ramme-konsesjon av 2.5 1990	Jnr. 90/622-2 TG/KY
Forslag til ansvarlig for registeret (jfr. lovens §4, 1. ledd, jfr. forskriften § 3-1)	Navn (organ, foretak, person) Statistisk sentralbyrå			
	Gate-/veiadresse			
	Postnr.	Poststed		Telefon
	Kontaktperson			Telefon
Registerets navn mv.	Registerets navn			
	Navn på de(t) databehandlingssystem registeret inngår i			
Omfanget av registeret	Enhet	Tall på enheter	Identifikasjonsbegrep	
Formål med registeret	Beskrivelse			
Hvordan opplysningene oppbevares	<input type="checkbox"/>	Manuelt (i kartotek, arkiv e.l.)	<input type="checkbox"/>	Maskinlesbart medium, oppgi type:

Kilder/ metoder	Hvor opplysningene hentes fra			
	Hvordan opplysningene hentes inn			
	Hjemmel for innhenting av opplysningene			
Innhold av registeret	Opplysninger eller dataelementer som inngår i registeret (Oppstilling av de opplysninger som inngår i registeret. Best mulig spesifikasjon.)			
Ajourhold av registeret	<input type="checkbox"/>	Engangsprosjekt	<input type="checkbox"/>	Holdes ajour fram til:
	<input type="checkbox"/>	Annet, spesifiser:		
Overføring til utlandet	Blir noen av opplysningene overført til utlandet?		<input type="checkbox"/>	Ja
			<input type="checkbox"/>	Nei
	Dersom ja, hvilke opplysninger			
	System:			
Land		Distrikt		
Sikring/ Sletting	Gjør rede for særlige sikringstiltak og sletting			
	Opplysningene behandles og oppbevares i overenstemmelse med bestemmelser gitt i SSBs håndbok i datasikkerhet og fysisk sikring. Opplysningene behandles og oppbevares i overenstemmelse med bestemmelser gitt i SSBs håndbok i datasikkerhet og fysisk sikring.			

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, underskrift

¹ Finnes tilgjengelig som tekstfil for WP51 på S:\dt-meld.w51.



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 arbeidet i Statistisk sentralbyrå krever ansvarsfølelse, lojalitet og respekt for oppgavegiverenes rett til vern mot urettmessig eller skadelig bruk av opplysninger.
- at passord som gir tilgang til graderte eller beskyttede 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 instruksjoner 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. Fortrolig 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
- at taushetsplikten også gjelder etter at mitt arbeid tilknyttet Statistisk sentralbyrå er avsluttet.

Jeg er gjort kjent med

- de vedlagte lovbestemmelser og instruksjoner

Sted..... , dato.....

.....
Underskrift

Taushetserklæringen er underskrevet i mitt påsyn: Dato: Navn:



T A U S H E T S E R K L Æ R I N G

for personer med annen tilknytning til Statistisk sentralbyrå enn midlertidig eller fast ansettelse

Jeg forstår

- at jeg i mitt arbeide tilknyttet Statistisk sentralbyrå vil kunne få kjennskap til opplysninger som av hensyn til offentlige, enkeltpersoners, institusjoners og bedrifters interesser ikke må bli kjent for andre personer som ikke har krav på å få opplysninger i sitt arbeide.
- at jeg i mitt arbeide tilknyttet Statistisk sentralbyrå også vil kunne få kjennskap til sikkerhetsrutiner, sikkerhetsinstruksjoner og annet som regulerer Statistisk sentralbyrås sikkerhet og som ikke må bli kjent for andre.

Jeg forplikter meg til

- ikke å gi opplysninger til noen personer i eller utenfor Statistisk sentralbyrå som ikke har krav på å få disse i sitt arbeid. Fortrolig 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

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

Jeg er gjort kjent med

- de vedlagte lovbestemmelser og instruksjoner

Sted..... , dato.....

.....
Underskrift

Taushetserklæringen er underskrevet i mitt påsyn: Dato: Navn:



O A T H O F S E C R E C Y

I understand

- that in the course of my work I may be privy to information which, in the interest of the public, individuals, institutions or companies, should not fall into the hands of unauthorised persons.

that my work for Statistics Norway demands that I feel a sense of responsibility, loyalty and respect for respondents' right to be protected against unlawful or injurious use of information.

that passwords which give access to classified or confidential information must not be transferred to or shared with anyone else, inside or outside Statistics Norway.

I pledge

- to exercise care in dealing with all information procured by Statistics Norway and all information located in Statistics Norway' personal data registers, in accordance with the guidelines and instructions issued by Statistics Norway and the Data Inspectorate.

not to disclose confidential information to anyone inside or outside Statistics Norway who is not authorised to access that information in the course of his/her work. Secret passwords shall not be disclosed to anyone else under any circumstances.

not to divulge the results of statistical investigations before Statistics Norway has released them for publication.

I am aware

- that any breach of the oath of secrecy, including the misuse of passwords, may lead to punishment and possibly to suspension or dismissal from Statistics Norway.

that the oath of secrecy shall continue to apply, even after I no longer work at/for Statistics Norway.

I am acquainted with

- the legal provisions and instructions reprinted on the back of this oath.

Name:

Birthdate:

Place:

Date:

Signature

.....

This oath of secrecy has been signed in my presence:

Date:

Name:.....

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

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.

¹ Finnes tilgjengelig som tekstfil for WP51 på S:\utlevavt.w51.



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.

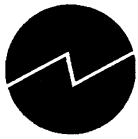
- e) Når prosjektet er avsluttet og senest innen ../. 19.., må De slette alle mottatte data, inklusive alle utskrifter og kopier av disse og bekrefte dette skriftlig overfor Statistisk sentralbyrå.

For Statistisk sentralbyrå:

.....
(registeransvarlig)

For:

.....



2. Innvilget utlevering til offentlig planlegging.

(Bare aidentifiserte 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.

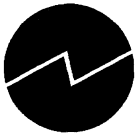
- d) Når prosjektet er avsluttet, senest innen ../. 19., må De slette alle mottatte data, inklusive alle utskrifter og kopier av disse og bekrefte dette skriftlig overfor Statistisk sentralbyrå.

For Statistisk sentralbyrå:

.....
(registeransvarlig)

For :

.....



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:

.....
(registeransvarlig)

For:

.....



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, 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.

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)

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 instruksjoner, 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 instruksjoner m.v.
8. Spesielle problemer som avdelingen trenger hjelp til.

