Sikkerhetsbestemmelsene i personopplysningsforskriften

med kommentarer

Datatilsynet

Desember 2000

INNHOLD

Del I Innledning

Fra 1. januar 2001 gjelder *personopplysningsloven* for behandling av personopplysninger – som erstatning for *personregisterloven* fra 1978. Sammen med loven gjelder utfyllende bestemmelser gitt i en egen personopplysningsforskrift. Denne forskriften omfatter krav til informasjonssikkerhet ved behandling av personopplysninger (kapittel 2), og erstatter kravene i *Retningslinjer for informasjonssikkerhet ved behandling av personopplysninger (TR-100:1998).* Sikkerhetsbestemmelsene i personopplysningsforskriften er i hovedsak en videreføring og oppgradering av dette regelverket.

Bestemmelsene gjelder kun for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler. For manuelle behandlinger som omfattes av personopplysningsloven, gjelder kun de generelle reglene om informasjonssikkerhet i personopplysningsloven § 13. Bestemmelsene gjelder videre kun for behandlinger der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet, er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene.

Sikkerhetsbestemmelsene angir krav til det styringssystem den enkelte behandlingsansvarlige må etablere for å oppnå tilfredsstillende informasjonssikkerhet. Et viktig element i dette systemet er kravet om sikkerhetsledelse: Utarbeidelse av sikkerhetsmål og –strategi, og jevnlig revurdering av disse gjennom ledelsesgjennomganger og sikkerhetsrevisjoner.

En sentral bestemmelse er at den behandlingsansvarlige må gjennomføre risikovurdering for å klarlegge den risiko behandlingen av personopplysninger innebærer i forhold til behovet for konfidensialitet, tilgjengelighet eller integritet. Resultat fra risikovurdering skal sammenlignes med det nivå for akseptabel risiko den behandlingsansvarlige på forhånd har fastsatt. Den behandlingsansvarlige skal etter slik sammenligning iverksette sikkerhetstiltak der dette er nødvendig. Datatilsynet kan gi pålegg om sikring av personopplysninger og herunder overprøve den behandlingsansvarliges valg av akseptabelt risikonivå.

Sikkerhetsbestemmelsene i personopplysningsforskriften skal være oppfylt før behandlingen av personopplysninger igangsettes. Den behandlingsansvarlige skal for eget bruk dokumentere informasjonssystemet og informasjonssikkerheten. For konsesjonspliktige behandlinger skal deler av denne dokumentasjonen vedlegges konsesjonssøknaden. For meldepliktige behandlinger skal dokumentasjon – utover meldeskjema – ikke oversendes. Datatilsynet vil uansett kunne be om ytterligere dokumentasjon. Informasjon om konsesjonspliktens og meldepliktens omfang og gjennomføring vil være tilgjengelig hos Datatilsynet.

Datatilsynet vil som før veilede behandlingsansvarlige som skal etablere informasjonssikkerhet i samsvar med bestemmelsene i personopplysningsforskriften. De eksisterende veiledningsdokumenter vil være tilgjengelig hos Datatilsynet som referansedokumenter.

Del II Sikkerhetsbestemmelsene med kommentarer

1 Generelle kommentarer

De innledende kommentarer til personopplysningsforskriftens kapittel 2 (sikkerhetskapittelet) gjengis her ordrett:

I personopplysningsloven § 13 pålegges den behandlingsansvarlige å sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Dette omfatter å sørge for at tilstrekkelig sikkerhetsfaglig kompetanse er tilgjengelig hos den behandlingsansvarlige. I tillegg til ansvar for sikkerheten i egen organisasjon, må den behandlingsansvarlige også forsikre seg om at informasjonssikkerheten er tilfredsstillende hos kommunikasjonspartnere og leverandører.

Begrepet informasjonssikkerhet omfatter:

- Sikring av konfidensialitet, dvs. beskyttelse mot at uvedkommende får innsyn i opplysningene.
- Sikring av integritet, dvs. beskyttelse mot utilsiktet endring av opplysningene.
- Sikring av tilgjengelighet, dvs. sørge for at tilstrekkelige og relevante opplysninger er til stede.

Tilfredsstillende informasjonssikkerhet skal oppnås ved hjelp av "planlagte og systematiske tiltak". Begrepet innebærer at kjente teknikker og anerkjente standarder for kvalitetsstyring, internkontroll, og informasjonssikkerhet, skal legges til grunn ved sikkerhetsarbeidet. De tiltak som etableres, skal være både organisatoriske og tekniske.

Sikkerhetstiltakene og selve informasjonssystemet skal dokumenteres. Dokumentasjonen skal omfatte beskrivelse av organisering, rutiner for bruk samt registrering av hendelser.

Som beskrevet i Ot.prp. nr. 92 (1998-99) side 114 i merknadene til personopplysningsloven § 13, er det ikke mulig å pålegge uttømmende og detaljerte regler for informasjonssikkerhet. Sikkerhetstiltak må etableres etter en konkret vurdering av de personopplysninger som behandles i forhold til de trusler mot informasjonssikkerheten som er til stede. Denne vurderingen skal utføres av den behandlingsansvarlige med utgangspunkt i et styringssystem for sikkerhet. Det er kravene til dette styringssystemet som beskrives i dette kapittelet i forskriften.

Videreføring av dagens sikkerhetskrav

Datatilsynet vedtok i 1998 nye sikkerhetsregler til bruk som utgangspunkt for sikkerhetsvilkår i konsesjoner, som grunnlag for enkeltvedtak etter personregisterloven § 8b, samt til bruk som kontrollgrunnlag. *Retningslinjer for informasjonssikkerhet ved behandling av personopplysninger (TR-100:1998)* er basert på kjente teknikker, og anerkjente standarder for kvalitetsstyring, internkontroll, og informasjonssikkerhet. Ved utforming av bestemmelsene i dette kapittelet er det blant annet tatt utgangspunkt i eksisterende sikkerhetsregler. Bestemmelsene er derfor en naturlig videreføring og oppgradering av dette regelverket.

Sertifisering av informasjonssikkerhet

Planleggings- og samordningsdepartementet, og senere Nærings- og handelsdepartementet, har siden 1996 forberedt etablering av to sertifiseringsordninger for informasjonssikkerhet. Den ene av disse gjelder sertifisering av informasjonssikkerhet i organisasjoner, det vil si tredjeparts

vurdering av organisasjonenes styringssystem for sikkerhet. Som sertifiseringsgrunnlag er valgt den engelske standarden *BS-7799, A code of practice for information security management*.

Departementets arbeid har blant annet som mål å harmonisere sikkerhetsregler, samt å sørge for en generell heving av sikkerhetsnivået. Ved behandling av personopplysninger er denne målsettingen sammenfallende med formålet med bestemmelsene i dette kapittelet. Det er derfor valgt å benytte den samme sikkerhetsstandard som en del av grunnlaget ved utarbeidelsen av forskriften. Felles grunnlag for sertifisering og for sikkerhetsregler, vil gjøre det mulig for den behandlingsansvarlige å benytte sertifiseringsordningen for å vise samsvar med bestemmelsene i dette kapittelet.

Harmoniserte sikkerhetskrav

Som beskrevet i forarbeidene til personopplysningsloven § 13 skal sikkerhetskravene i loven tjene som grunnlag for å harmonisere sikkerhetsnivået for behandling av personopplysninger som er hjemlet i annen lovgivning. Slik harmonisering er nødvendig for å oppnå et felles gjenkjennbart sikkerhetsnivå, og for å legge til rette for elektronisk samhandling mellom forskjellige sektorer. Bestemmelsene i kapittelet beskriver et styringssystem for sikkerhet som kan anvendes i alle sektorer.

Som nevnt foran er bestemmelsene koordinert med Nærings- og handelsdepartementets arbeid med sikkerhetssertifisering. Også i andre land, som f.eks. England, Nederland, Sverige med flere, etableres nå tilsvarende sertifiseringsordninger med BS-7799 som sertifiseringsgrunnlag. I England har "The privacy comissioner" oppfordret behandlingsansvarlige til å benytte slik sertifisering for å vise samsvar med sikkerhetsreglene i den engelske personvernlovgivningen.

Harmoniserte personvernregler, herunder sikkerhetsregler, innen EU/EØS er et av hovedformålene med personverndirektivet 95/46/EF. Som grunnlag for bestemmelsene i dette kapittelet er det derfor valgt kjente teknikker og anerkjente standarder som har og får, internasjonal tilslutning.

2 De enkelte bestemmelser med kommentarer

Sikkerhetsbestemmelsene i personopplysningsforskriften (§§ 2-2 til 2-16), sammen med kommentarer til de enkelte bestemmelser, gjengis her ordrett:

§ 2-1 Forholdsmessige krav om sikring av personopplysninger

Bestemmelse	Kommentarer
Reglene i dette kapittelet gjelder for behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler der det for å hindre fare for tap av liv og helse, økonomisk tap eller tap av anseelse og personlig integritet er nødvendig å sikre konfidensialitet, tilgjengelighet og integritet for opplysningene.	Bestemmelsen avgrenser reglene i dette kapittelet til kun å gjelde behandling av personopplysninger som helt eller delvis skjer med elektroniske hjelpemidler. For manuelle behandlinger som omfattes av personopplysningsloven, gjelder kun de generelle reglene om informasjonssikkerhet i loven § 13. Bestemmelsen avgrenser sikkerhetsreglene til kun å gjelde for behandlinger der det av hensyn til den enkeltes personvern er nødvendig å sikre konfidensialitet, tilgjengelighet eller integritet for opplysningene. Videre skal sikkerhetstiltak implementeres i forhold til sannsynlighet for og konsekvens av sikkerhetsbrudd

Der slik fare er til stede skal de planlagte og systematiske tiltakene som treffes i medhold av forskriften, stå i forhold til sannsynligheten for og konsekvens av sikkerhetsbrudd.

konsekvens av sikkerhetsbrudd.

Avgrensningene er viktig for å unngå at det etableres for omfattende sikkerhetstiltak. I vurderingen av om sikkerhetstiltak er nødvendig, er opplysningenes art og den fare for tap av liv og helse, økonomisk tap, eller tap av anseelse og personlig integritet behandlingen kan medføre, avgjørende.

Det faktum at sensitive personopplysninger behandles, gir ikke alene en anvisning av hvilke sikkerhetstiltak som er nødvendig. Videre vil også andre opplysninger enn sensitive personopplysninger kunne være omfattet av taushetsplikt og dermed ha behov for sikring av konfidensialitet. Som eksempler på vurdering av sikkerhetsbehovet, kan nevnes at konfidensialitets-sikring normalt vil være mindre nødvendig ved behandling av opplysninger om fagforeningstilhørighet enn for behandling av sensitive personopplysninger for øvrig. Videre vil det for enkelte spesielle behandlinger av helseopplysninger være like nødvendig å sikre opplysningenes tilgjengelighet som konfidensialitet, for å hindre fare for tap av liv og helse.

§ 2-2 Pålegg fra Datatilsynet

Bestemmelse

Datatilsynet kan gi pålegg om sikring av personopplysninger og herunder fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.

Kommentarer

Bestemmelsen understreker Datatilsynets påleggskompetanse etter personopplysningsloven § 46 når det gjelder informasjonssikkerhet. Datatilsynet kan gi pålegg om at bestemmelsene i dette kapittelet følges. Videre kan Datatilsynet stille sikkerhetsvilkår, og herunder pålegge etablering av konkrete sikkerhetstiltak for en bestemt behandling av personopplysninger.

Den behandlingsansvarlige skal fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger, jf. § 2-4. Av hensyn til et harmonisert og tilfredsstillende sikkerhetsnivå, kan slike beslutninger overprøves i de tilfeller der Datatilsynet ikke finner informasjonssikkerheten tilfredstillende, jf. personopplysningsloven § 13. I arbeidet med å beskrive nivåer for akseptabel risiko, bør Datatilsynet samarbeide med de berørte virksomheter, bransjeorganisasjoner og myndigheter.

§ 2-3 Sikkerhetsledelse

Bestemmelse

Den som har den daglige ledelsen av virksomheten som den behandlingsansvarlige driver, har ansvar for at bestemmelsene i dette kapittelet følges.

Kommentarer

Bestemmelsen understreker at det er den behandlingsansvarlige, ved virksomhetens daglige ledelse, som skal sørge for tilfredsstillende informasjonssikkerhet, jf. personopplysningsloven § 13, og dermed har ansvar for at bestemmelsene i dette kapittelet følges.

Formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål.

Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi.

Bruk av informasjonssystemet skal jevnlig gjennomgås for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.

Resultatet fra gjennomgangen skal dokumenteres og benyttes som grunnlag for eventuell endring av sikkerhetsmål og strategi.

Virksomhetens ledelse skal utøve dette ansvaret blant annet ved å beskrive virksomhetens sikkerhetsmål. Sikkerhetsmål vil omfatte beslutninger om til hva, og hvordan informasjonsteknologi skal benyttes i virksomheten. Eksempler på slike beslutninger kan være valg av hvilke behandlinger av personopplysninger som skal skje med elektroniske hjelpemidler, hvordan virksomheten forholder seg til opplysninger som må sikres både med hensyn til konfidensialitet og tilgjengelighet, og føringer for medarbeideres eventuelle private bruk av informasjonssystemet.

Videre skal virksomhetens ledelse beskrive valg og prioriteringer i sikkerhetsarbeidet i en sikkerhetsstrategi. Sikkerhetsstrategien vil omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Eksempler på slike beslutninger kan være fordeling av arbeidsoppgaver for drift og informasjonssikkerhet mellom ledelse, drifts- og sikkerhetspersonell og den enkelte bruker, eventuelt krav til at konfidensielle personopplysninger behandles i informasjonssystem uten tilkobling til eksterne datanett, og bruk av leverandører for å få utført sikkerhetsoppgaver.

Virksomhetens ledelse skal jevnlig, eksempelvis årlig, gjennomgå sikkerhetsmål og strategi. Slik ledelsesgjennomgang vil ha som formål å vurdere hvorvidt de beslutninger som er tatt, er i samsvar med virksomhetens behov for informasjonsteknologi og informasjonssikkerhet. Gjennomgangen vil danne grunnlag for eventuelle endringer av sikkerhetsmål eller strategi. Praktisk kan ledelsesgjennomgang gjennomføres innenfor rammen av årlig økonomi- eller virksomhetsplanlegging.

§ 2-4 Risikovurdering

Bestemmelse

Det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger.

Den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten.

Resultatet av risikovurderingen

Kommentarer

Bestemmelsen pålegger den behandlingsansvarlige å holde oversikt over de personopplysninger som behandles med elektroniske hjelpemidler, sammen med angivelse av hvilke opplysninger det er nødvendig å sikre konfidensialitet, tilgjengelighet eller integritet for. Oversikten benyttes som del av grunnlaget for risikovurderingen.

Den behandlingsansvarlige skal fastlegge kriterier for den risiko som kan aksepteres, eller eventuelt må reduseres ved hjelp av sikkerhetstiltak. Slike beslutninger kan overprøves i de tilfeller der Datatilsynet ikke finner informasjonssikkerheten tilfredsstillende, jf. § 2-2.

Den behandlingsansvarlige skal klarlegge sannsynlighet for, og konsekvens av sikkerhetsbrudd ved hjelp av risikovurdering. Begrepet ”risikovurdering” er valgt i stedet for den mer formelle betegnelsen ”risikoanalyse”. Dette for å signalisere at

skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandling av personopplysninger, jf. første ledd og § 2-2.

Resultatet av risikovurderingen skal dokumenteres.

arbeidet med å avdekke risiko ikke bør være mer omfattende eller formalisert en strengt tatt nødvendig. Begrepet "risikovurdering" er også valgt i stedet for "sårbarhetsanalyse" som normalt benyttes kun til å beskrive vurdering av motstandsdyktighet mot uønskede hendelser.

Risikovurdering skal gjennomføres før behandling av personopplysninger med elektroniske hjelpemidler settes i gang, og deretter ved endringer med betydning for informasjonssikkerheten. Dette kan være endringer som følger av beslutninger hos den behandlingsansvarlige, eller hendelser den behandlingsansvarlige ikke har herredømme over, eksempelvis endringer i trusselbildet, feil i standard programvare eller lignende. Risikovurdering kan utføres med utgangspunkt i norsk standard *NS-5814, Krav til risikoanalyser.*

Resultat av risikovurdering skal sammenlignes med de fastlagte kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. Resultatet benyttes som del av grunnlaget for valg av de konkrete sikkerhetstiltak som må etableres.

§ 2-5 Sikkerhetsrevisjon

Bestemmelse

Sikkerhetsrevisjon av bruk av informasjonssystemet skal gjennomføres jevnlig.

Sikkerhetsrevisjon skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører.

Dersom sikkerhetsrevisjonen avdekker bruk av informasjonssystemet som ikke er forutsatt, skal dette behandles som avvik, jf. § 2-6.

Resultat fra sikkerhetsrevisjon skal dokumenteres.

Kommentarer

Bestemmelsen pålegger den behandlingsansvarlige jevnlig, eksempelvis årlig, å etterprøve sikkerhetsarbeidet for å verifisere at de sikkerhetstiltak som er besluttet etablert, faktisk er iverksatt og fungerer etter sin hensikt. Ved sikkerhetsrevisjon sammenlignes faktisk bruk av informasjonssystemet med de retningslinjer for slik bruk som er besluttet. Slik revisjon må ikke blandes sammen med ledelsens gjennomgang av sikkerhetsmål og strategi, jf. § 2-3, hvor formålet er å vurdere ledelsens beslutninger opp mot virksomhetens behov for informasjonsteknologi og informasjonssikkerhet. Resultatet fra sikkerhetsrevisjonen vil imidlertid være del av grunnlaget for slike gjennomganger.

Sikkerhetsrevisjon er et viktig grunnlag for kontinuerlig forbedring av informasjonssikkerheten. Praktisk kan sikkerhetsrevisjoner gjennomføres etter de samme fremgangsmåter som benyttes i HMS-arbeidet, jf. forskrift 6. desember 1996 nr. 1127 om systematisk helse-, miljø- og sikkerhetsarbeid i virksomheter (internkontrollforskriften).

§ 2-6 Avvik

Bestemmelse

Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og

Kommentarer

Bestemmelsen pålegger den behandlingsansvarlige å behandle uønskede hendelser i informasjonssystemet med formål å gjenopprette normal tilstand og å hindre

sikkerhetsbrudd, skal behandles som avvik.

Avviksbehandlingen skal ha som formål å gjenopprette normal tilstand, fjerne årsaken til avviket og hindre gjentagelse.

Dersom avviket har medført uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet varsles.

Resultat fra avviksbehandling skal dokumenteres.

med formål å gjenopprette normal tilstand og å hindre gjentagelse. Avviksbehandling iverksettes ved sikkerhetsbrudd og/eller når oppgaver er utført i strid med de rutiner som er besluttet.

Avviksbehandling vil normalt omfatte rapportering, strakstiltak, permanent korrigering av avvik og oppfølging av korrigerende tiltak over tid for å vurdere om dette fungerer etter sin hensikt.

For de tilfeller der avviksbehandlingen har avdekket uautorisert utlevering av personopplysninger hvor konfidensialitet er nødvendig, skal Datatilsynet meddeles resultatet fra avviksbehandlingen.

§ 2-7 Organisering

Bestemmelse

Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.

Ansvars- og myndighetsforhold skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.

Informasjonssystemet skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås.

Konfigurasjonen skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.

Bruk av informasjonssystemet som har betydning for informasjons-sikkerheten, skal utføres i henhold til fastlagte rutiner.

Kommentarer

Bestemmelsen pålegger den behandlingsansvarlige å organisere arbeidet med informasjonssystemet slik at tilfredsstillende informasjonssikkerhet oppnås. Det skal etableres klare ansvars- og myndighetsforhold med utgangspunkt i beslutninger tatt av virksomhetens ledelse. Ansvars- og myndighetsforhold skal dokumenteres og gjøres kjent for virksomhetens medarbeidere.

Det er viktig at ansvar og myndighet relatert til drift av informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeid (sikkerhetsledelse), er klarlagt. Disse funksjoner er henholdsvis ”utøvende” og ”kontrollerende” og bør ideelt sett tillegges forskjellige medarbeidere i virksomheten. For mindre virksomheter kan det likevel være nødvendig å legge begge funksjoner til en og samme person. Arbeidsoppgaver for sikkerhetsleder vil normalt omfatte forberedelse av ledelsesgjennomganger, gjennomføring av sikkerhetsrevisjoner samt kontroll med risikovurdering og avviksbehandling.

Den behandlingsansvarlige pålegges videre å konfigurere informasjonssystemet slik at tilfredsstillende informasjonssikkerhet oppnås. Med ”konfigurasjon” menes informasjonssystemets utforming, det vil si utstyr og program samt sammenkoblinger mellom disse. Informasjonssystemet konfigureres med utgangspunkt i beslutninger tatt av virksomhetens ledelse. Konfigurasjonen skal dokumenteres.

Ved valg av konfigurasjon skal virksomhetens behov for informasjonssikkerhet tillegges vekt, i tillegg til vurdering av økonomi og behov for funksjonalitet. Eksempelvis vil slik vurdering omfatte etablering av sikkerhetsbarrierer, bruk av nettverkssegmentering for å skille forskjellige behandlinger av

personopplysninger fra hverandre i informasjonssystemet eller lignende.

Den behandlingsansvarlige pålegges å beslutte hvordan arbeidet med informasjonssystemet skal foregå. Slike beslutninger må gjøres kjent for virksomhetens medarbeidere i form av rutiner for bruk. Rutiner må ha et omfang og en detaljeringsgrad som sikrer at arbeidsoppgaver utføres med tilfredsstillende sikkerhet som resultat, og at de utføres likt hver gang de repeteres.

§ 2-8 Personell

Bestemmelse

Medarbeidere hos den behandlingsansvarlige skal bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk.

Medarbeiderne skal ha nødvendig kunnskap for å bruke informasjonssystemet i samsvar med de rutiner som er fastlagt.

Autorisert bruk av informasjonssystemet skal registreres.

Kommentarer

Den behandlingsansvarlige pålegges å begrense bruk av informasjonssystemet til det som er tjenstlig nødvendig. Som hovedregel vil all bruk av informasjonssystemet medføre risiko. Slik risiko reduseres til akseptabelt nivå ved hjelp av sikkerhetstiltak. Ved å begrense bruk av informasjonssystemet oppnås:

– minst mulig eksponering av personopplysninger overfor trusler.

– at den behandlingsansvarlige kjenner til, og har vurdert risiko forbundet med den bruk av informasjonssystemet som pågår.

Bestemmelsen innebærer ikke et absolutt forbud mot medarbeideres private bruk av informasjonssystemet. Privat bruk må imidlertid være kjent for den behandlingsansvarlige, og kunne gjennomføres uten at behandling av personopplysninger utsettes for ytterligere trusler. Eksempelvis vil privat bruk av internett-tjenesten ”world wide web” kunne tillates forutsatt at det ikke er nødvendig å etablere egne sikkerhetstiltak for å muliggjøre slik bruk, og at ”WWW” også benyttes for tjenstlige formål.

Den behandlingsansvarlige skal registrere autorisert bruk av informasjonssystemet i den grad dette er nødvendig for gjennomføring av avviksbehandling, herunder oppklaring av sikkerhetsbrudd, og for drift av informasjonssystemet.

Bestemmelsen pålegger videre den behandlings-ansvarlige å sørge for at virksomhetens medarbeidere har tilstrekkelig kompetanse til å bruke informasjonssystemet, samt å legge til rette for vedlikehold og heving av denne kompetansen. Bruk av avanserte datatekniske løsninger for behandling av personopplysninger, og rask datateknisk utvikling, stiller strenge krav til medarbeidernes kompetanse. Den behandlingsansvarlige vil ha behov for oversikt over medarbeideres kunnskaper om informasjonsteknologi og informasjonssikkerhet i forhold til kravene for den enkelte stilling/funksjon.

§ 2-9 Taushetsplikt

Bestemmelse	Kommentarer
Medarbeidere hos den behandlingsansvarlige skal pålegges taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten skal også omfatte annen informasjon med betydning for informasjonssikkerheten.	Bestemmelsen pålegger taushetsplikt for personopplysninger hvor konfidensialitet er nødvendig. Taushetsplikten omfatter også informasjon om informasjonssystemet og om sikkerhetstiltak i den grad utlevering av slik informasjon kan få betydning for informasjonssikkerheten. Taushetsplikten er ikke til hinder for at den behandlingsansvarlige kan informere om sikkerhetstiltak, jf. personopplysningsloven § 18, eller sende melding til Datatilsynet, jf. § 32. Det forutsettes at det ved risikovurdering er klarlagt at informasjon kan gis uten at dette truer informasjonssikkerheten. Til sammenligning kan nevnes at Datatilsynets taushetsplikt omfatter all informasjon om sikkerhetstiltak hos den behandlingsansvarlige, jf. personopplysningsloven § 45. Dette fordi Datatilsynet kun unntaksvis vil besitte nok informasjon til å foreta en fullstendig risikovurdering. Den behandlingsansvarlige pålegges å informere medarbeideren om behovet for konfidensialitet og om de konsekvenser - både for egen del, for den behandlingsansvarlige, og for de personer opplysningene kan knyttes til - brudd på taushetsplikten kan medføre.

§ 2-10 Fysisk sikring

Bestemmelse	Kommentarer
Det skal treffes tiltak mot uautorisert adgang til utstyr som brukes for å behandle personopplysninger etter forskriften her. Sikkerhetstiltakene skal også hindre uautorisert adgang til annet utstyr av betydning for informasjonssikkerheten. Utstyr skal installeres slik at ikke påvirkning fra driftsmiljøet får betydning for behandlingen av personopplysninger.	Bestemmelsen pålegger den behandlingsansvarlige å hindre uautorisert adgang til utstyr benyttet for behandling av personopplysninger eller med betydning for informasjonssikkerheten. Eksempelvis skal tjener- og klientmaskiner, og utstyr benyttet som sikkerhetsbarrierer i virksomhetens datanett, fysisk sikres mot uautorisert adgang. Fysisk sikring kan gjennomføres ved tilsyn/vakt, låsing/skjerming av det enkelte utstyr eller låsing/skjerming av lokaler. Tilsyn/vakt etableres eksempelvis ved hjelp av resepsjonstjeneste og ledsagelse av uautorisert personell (besøkende). Låsing/skjerming av utstyr oppnås eksempelvis ved fysiske sikkerhetsmekanismer integrert i utstyret. For låsing/skjerming av lokaler er det som hovedregel tilstrekkelig å etablere normal bygningsmessig sikkerhet.

§ 2-11 Sikring av konfidensialitet

Bestemmelse

Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig.

Sikkerhetstiltakene skal også hindre uautorisert innsyn i annen informasjon med betydning for informasjonssikkerheten.

Personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig.

For lagringsmedium som inneholder personopplysninger hvor konfidensialitet er nødvendig, skal behovet for sikring av konfidensialitet fremgå ved hjelp av merking eller på annen måte.

Dersom lagringsmediet ikke lenger benyttes for behandling av slike opplysninger, skal opplysningene slettes fra lagringsmediet.

Kommentarer

Begrepet konfidensialitet i denne bestemmelsen er ikke sammenfallende med konfidensialitetsbegrepet i sikkerhetsinstruksen.

Bestemmelsen pålegger den behandlingsansvarlige å hindre uautorisert innsyn i personopplysninger. Også informasjon om informasjonssystemet og om sikkerhetstiltak skal sikres mot uautorisert tilgang når dette kan få betydning for informasjonssikkerheten. Valg av hvilke opplysninger som det skal sikres konfidensialitet for, og hvilke sikkerhetstiltak som må etableres, følger av resultatet av risikovurderingen.

Den behandlingsansvarlige skal ved kryptering eller på annen møte sørge for nødvendig konfidensialitet ved overføring av personopplysninger i offentlige telenett. Reglene for kryptering gjelder også for overføring via private datalinjer som er utenfor det området virksomheten har sikret mot uautorisert adgang, jf. § 2-10. I slike tilfeller skal kryptering velges som nødvendig erstatning for konfidensialitetssikring som normalt oppnås ved fysisk sikring. Eksempel på annen sikring enn kryptering kan være anonymisering eller oppsplitting av teksten slik at teksten kun gir mening når en har tilgang til hele teksten.

Det skal tydelig fremgå om et lagringsmedium (harddisk, magnetbånd, kompaktdisk, diskett eller lignende) inneholder personopplysninger som det er nødvendig å sikre konfidensialitet for. Bestemmelsen inneholder ingen detaljerte krav til utforming eller metode. Den behandlingsansvarlige må selv velge merking som gir tilstrekkelig informasjon om konfidensialitetsbehovet, eksempelvis ved utveksling av lagringsmedia eller for å vurdere behovet for sletting av personopplysninger.

Bestemmelsen pålegger den behandlingsansvarlige å sørge for sletting av personopplysninger fra lagringsmedium som ikke lenger benyttes for behandling av personopplysningene. Bestemmelsen inneholder ingen detaljerte krav til metode. Valg av metode for sletting vil blant annet avhenge av om lagringsmediet skal benyttes til annen behandling av personopplysninger eller avhendes.

Ved avhending av lagringsmedia skal personopplysninger slettes fullstendig og permanent fra lagringsmediet, slik at det ikke er mulig, selv ved bruk av tekniske hjelpemiddeler, å gjenopprette tilgang til opplysningene. Som alternativ til sletting kan det være nødvendig å destruere lagringsmediet fysisk.

§ 2-12 Sikring av tilgjengelighet

Bestemmelse	Kommentarer
Det skal treffes tiltak for å sikre tilgang til personopplysninger hvor tilgjengelighet er nødvendig. Sikkerhetstiltakene skal også sikre tilgang til annen informasjon med betydning for informasjonssikkerheten. Alternativ behandling skal forberedes for de tilfeller informasjonssystemet er utilgjengelig for normal bruk. Personopplysninger og annen informasjon som er nødvendig for gjenoppretting av normal bruk, skal kopieres.	Bestemmelsen pålegger den behandlingsansvarlige å sikre nødvendig innsyn i opplysninger slik at behandling av personopplysninger kan gjennomføres som besluttet. Det skal også sikres tilgang til informasjon om informasjonssystemet og om sikkerhetstiltak når dette er nødvendig for sikkerhetsarbeidet. Valg av hvilke opplysninger som det skal sikres tilgjengelighet for, og hvilke sikkerhetstiltak som må etableres, følger av resultatet av risikovurderingen. For personopplysninger som det skal sikres tilgjengelighet for, må den behandlingsansvarlige forberede alternativ behandling for de tilfeller informasjonssystemet ikke er tilgjengelig. Alternativ behandling kan gjennomføres ved duplisering av utstyr/program, eller ved hjelp av manuelle behandlingsrutiner. Den behandlingsansvarlige skal reservekopiere (ta "backup" av) personopplysningene. Kravet til reservekopiering gjelder også for annen informasjon når dette er nødvendig for sikkerhetsarbeidet, eksempelvis for program og innstillinger av program, benyttet i sikkerhetstiltak.

§ 2-13 Sikring av integritet

Bestemmelse	Kommentarer
Det skal treffes tiltak mot uautorisert endring av personopplysninger der integritet er nødvendig. Sikkerhetstiltakene skal også hindre uautorisert endring av annen informasjon med betydning for informasjonssikkerheten. Det skal treffes tiltak mot ødeleggende programvare.	Bestemmelsen pålegger den behandlingsansvarlige å hindre utilsiktet endring av personopplysninger. Også informasjon om informasjonssystemet og om sikkerhetstiltak skal sikres mot uautorisert endring når dette er nødvendig for informasjonssikkerheten. Valg av hvilke opplysninger som det skal sikres integritet for, og hvilke sikkerhetstiltak som må etableres, følger av resultatet av risikovurderingen. Den behandlingsansvarlige skal sørge for beskyttelse mot ødeleggende program, eksempelvis "datavirus" eller "malicious software". Slike program kan påvirke integritet for program benyttet for behandling av personopplysninger eller i sikkerhetstiltak, og medføre driftsforstyrrelser og gjøre informasjonssystemet utilgjengelig.

§ 2-14 Sikkerhetstiltak

Bestemmelse	Kommentarer
Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk.	Bestemmelsen understreker at sikkerhetstiltak skal etableres både med formål å hindre sikkerhetsbrudd, og for å avdekke hendelser som kan forårsake sikkerhetsbrudd. Dette medfører at alle forsøk på uautorisert bruk av informasjonssystemet må registreres.
Forsøk på uautorisert bruk av informasjonssystemet skal registreres.	Sikring av konfidensialitet, tilgjengelighet eller integritet kan ikke utelukkende baseres på rutiner den enkelte medarbeider forutsettes å følge. Den behandlingsansvarlige må også etablere tiltak som fungerer uavhengig av medarbeidernes handlinger, eksempelvis i form av nettverks- eller applikasjonskontroll i sikkerhetsbarrierer. Sikkerhetstiltak bør etableres slik at funksjonen til to uavhengige tiltak må påvirkes før et sikkerhetsbrudd får betydning for konfidensialitet, tilgjengelighet eller integritet for personopplysningene.
Sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne, og ikke være begrenset til handlinger som den enkelte forutsettes å utføre.	
Sikkerhetstiltak skal dokumenteres.	Sikkerhetstiltak skal dokumenteres. De handlinger den enkelte forutsettes å utføre for å oppnå tilfredsstillende informasjonssikkerhet, skal fremgå av rutiner.

§ 2-15 Sikkerhet hos andre virksomheter

Bestemmelse	Kommentarer
Den behandlingsansvarlige skal bare overføre personopplysninger elektronisk til den som tilfredsstiller kravene i forskriften her.	Bestemmelsen understreker at den behandlingsansvarlige kun kan overføre personopplysninger til kommunikasjonspartnere, eksempelvis databehandlere, som tilfredsstiller bestemmelsene i dette avsnittet. Formålet med bestemmelsen er blant annet å sikre et harmonisert sikkerhetsnivå i hele kommunikasjonsskjeden.
Den behandlingsansvarlige kan overføre personopplysninger til enhver dersom overføringen skjer i samsvar med reglene i personopplysningsloven §§ 29 og 30, eller når det er fastsatt i lov at det er adgang til å kreve opplysninger fra et offentlig register.	Unntaket fra bestemmelsen gjelder bl.a. ved overføring til utlandet, jf. personopplysningsloven §§ 29 og 30. Overfor mottakere utenfor Norge gjelder ikke bestemmelsene i dette kapittelet.
	Som hovedregel skal den behandlingsansvarlige selv etablere nødvendige sikkerhetstiltak. For enkelte virksomheter, spesielt mindre virksomheter uten tilstrekkelige ressurser, vil dette ofte ikke være praktisk å gjennomføre. Et alternativ til egen etablering av sikkerhetstiltak kan være å få utført sikkerhetsoppgaver hos underleverandør. Fordeling av sikkerhetsoppgaver mellom virksomheten og leverandøren, skal i "sum" gi informasjonssikkerhet som minst tilfredsstiller kravene i dette kapittelet.
Leverandører som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i dette kapittelet.	Forholdet mellom den behandlingsansvarlige og kommunikasjonspartnere eller leverandører, skal være klarlagt og beskrives i avtale.
Den behandlingsansvarlige skal etablere klare ansvars- og	Den behandlingsansvarlige skal være kjent med sikkerhetsarbeidet hos kommunikasjonspartnere eller

myndighetsforhold overfor kommunikasjonspartnerer og leverandører. Ansvars- og myndighetsforhold skal beskrives i særskilt avtale.

Den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartner og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.

leverandører gjennom kunnskap om sikkerhetsstrategien til slike virksomheter. Videre skal den behandlingsansvarlige forsikre seg om at informasjonssikkerheten hos partner/leverandør er tilfredsstillende. Dette kan oppnås ved at den behandlingsansvarlige meddeles de resultater fra ledelsesgjennomganger, sikkerhetsrevisjoner og avviksbehandling som er relevant for forholdet til partner/leverandør.

§ 2-16 Dokumentasjon

Bestemmelse

Rutiner for bruk av informasjonsystemet og annen informasjon med betydning for informasjonssikkerheten, skal dokumenteres.

Dokumentasjon skal lagres i minst 5 år fra det tidspunkt dokumentet ble erstattet med ny gjeldende utgave.

Registrering av autorisert bruk av informasjonssystemet og av forsøk på uautorisert bruk, skal lagres minst 3 måneder. Det samme gjelder registreringer av alle andre hendelser med betydning for informasjonssikkerheten.

Kommentarer

Bestemmelsen understreker kravet til dokumentasjon, jf. personopplysningsloven § 13. Dokumentasjonskravet omfatter i tillegg til beskrivelse av tekniske sikkerhetstiltak, også rutiner for arbeid med informasjonssystemet og registrering av hendelser. Dokumentasjonens omfang og detaljeringsgrad må være i samsvar med sikkerhetsbehovet.

Den behandlingsansvarlige skal arkivere dokumentasjon med betydning for informasjonssikkerheten. Formålet med slik lagring er å muliggjøre sporing og korrigering av avvik over tid. Lagringstid er 5 år fra det tidspunkt dokumentet, eksempelvis en rutinebeskrivelse, ble tatt ut av bruk, eller fra tidspunktet for registrering av en hendelse. Lagringstiden er harmonisert med de krav som normalt stilles innen kvalitetsstyring, eksempelvis i *ISO-9001, Kvalitetssystemer, Modell ved utvikling, konstruksjon, tilvirkning, installasjon og ettersyn*.

For hendelsesregistre gjelder en lagringstid på 3 måneder. Den relativt korte lagringstiden er begrunnet ut fra den store mengde data som akkumuleres ved slik registrering.