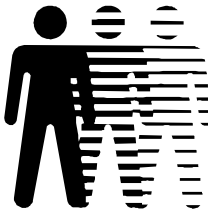
Datatilsynet

Datatilsynet



Senioringeniør Atle Årnes

Datatilsynet

Innhold

- Generell oversikt over personvernlovgivningen
- Lovverket i Norge (rettigheter og plikter)
- Spor som legges igjen av brukere
- Legge ut informasjon på Internett
  - Programvare for autopass og bruk
  - Programvare for lokalisering av mobiltelefoner og bruk
  - Programvare for å legge ut data fra databaser ut på Internett
  - Legge ut avisartikler med personnavn
  - Bilder fra studentfester
  - Studentweb (studieprogresjon og karakterer) ut på web (sikring)
  - Om studentenes kursdeltakelse
  - Deltakelsen i diskusjonsgrupper (news / studentportal)

Datatilsynet – i dag

- Uavhengig organ
- Aktiv innen råd og veiledning
- Fokus på operativt tilsyn
- Funksjon som ombud
- Hørings og konsultasjonspart
- Internasjonalt arbeid
- Meldeplikt

Viktigste funksjon

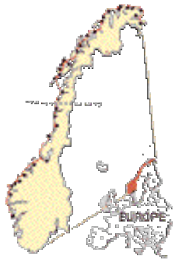
- **Bidra til tilfredsstillende beskyttelse av enkeltindividet ved trusler mot personvern fra statsmakten, offentlig virksomhet, næringsliv eller andre som behandler personopplysninger om oss.**

Virkemidler

- **Informasjon**
- **Påvirkning**
- **Regulering**
- **Tilsyn**
- **Sanksjon**

Datatilsynet

Personopplysningsloven



"Loven skal bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysningene"

Datatilsynet

Hva er din terskel for samtykke?

- Navn, adresse, telefon, kjønn
- Inntekt, formue, sivilstatus
- Vaner, adferd, holdninger
- Legning, rusvaner
- Helseplager, strafferegister
- Det private rom
- Indre tanker, intime detaljer

Datatilsynet

Grunnprinsipper

- **Beskytte enkelt-mennesket.**
- **Rettigheter til å kunne bestemme over informasjon.**
- **Det må foreligge rettslig grunnlag og saklig grunn.**

Datatilsynet

Personopplysningsbegreper

Personopplysning

- **Opplysninger og vurderinger som kan knyttes til en enkeltperson.**

Sensitive personopplysninger

- **Opplysninger om rase, etnisk bakgrunn, politisk, filosofisk, religiøs oppfatning, straffbare forhold, helse, seksuelle forhold eller fagforeningsmedlemskap.**

Datatilsynet

Tre aspekter

- Konfidensialitet

Informasjon skal ikke være tilgjengelig for uvedkommende. Personopplysninger skal være beskyttet mot uautorisert innsyn under behandlingen, for eksempel ved transport og lagring

- Integritet

Informasjon skal ikke kunne endres utilsiktet eller av uvedkommende. Krav til integritet må ikke forveksles med krav til kvalitet.

- Tilgjengelighet

Informasjon skal være tilgjengelig for rettmessige brukere når de har behov for å utføre sine oppgaver.

Forskriften forutsetter at alle tre aspekter blir vurdert med hensyn til eventuelle tiltak.

Datatilsynet

Risikovurdering

- **Hva slags opplysninger behandles?**
- **Hva kan skje? Trusselvurdering**
- **Hvor stor er sannsynligheten?**
- **Hva kan bli konsekvensene?**
- **Hvilke tiltak må treffes?**

R= S x K **Risiko er produkt av sannsynlighet og konsekvens**

Datatilsynet

Før en beslutning om valg av teknologisk løsning kan tas...

Virksomhetens ledelse skal utarbeide dette ansvaret blant annet ved å beskrive virksomhetens sikkerhets mål. Dette vil omfatte beslutninger om til hva, og hvordan informasjonsteknologi skal benyttes.

Sikkerhetsstrategi vil omfatte grunnlegende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet.

Datatilsynet

Kryptering

I alle overføringer hvor den behandlingsansvarlige ikke har fysisk kontroll over linjenettet skal overføringen sikres med kryptering eller tilsvarende.

Kryptering av data skal skje ende-til-ende mellom to sikrede soner, dvs at kryptering/dekryptering skjer i sikret sone.

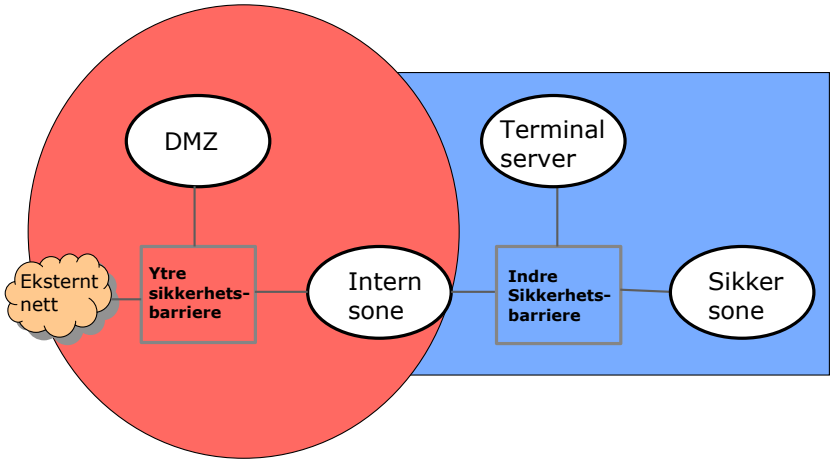
Datatilsynet

Sensitive personopplysinger

Sensitive personopplysinger skal behandles og lagres i sikrede soner hvor kun autoriserte brukere gis tilgang. En virksomhet kan opprette flere sikrede soner avhengig av behovet.

Datatilsynet

Sikkerhetsarkitektur



Datatilsynet

. . . planlagte og systematiske tiltak

- Betyr utarbeidelse av rutiner
- Rutinene skal dokumenteres
- Avviksrutiner

Datatilsynet

Organisatoriske aspekter

- Ledelsens ansvar
- Mål og strategi som vurderes jevnlig
- Kompetente, autoriserte medarbeidere
- Klare avtaler med parter

Datatilsynet

Viktige begreper

Behandling

•Enhver bruk av personopplysninger som f.eks. Innsamling, registrering, sammenstilling, lagring og utlevering eller kombinasjon av dette.

Databehandlingsansvarlig

•Den som bestemmer formål, hjelpemidler v/behandlingen

Databehandler

•Den som behandler personopplysninger på vegne av Databehandlingsansvarlig.

Datatilsynet

Databehandlingsansvarlige

Den databehandlingsansvarlige skal bare overføre personopplysninger til den som tilfredstiller kravene i forskriften.

Datatilsynet

Avtaleforhold tips

Databehandlingsansvarlig har ansvar:

- **Gir "databehandleren" klare oppgaver**
- **Pålegger "databehandler" sikkerhetskrav**
- **Kontrollerer "databehandlers" utførelse**

- **Databehandler er en virksomhet**
- **Databehandlingsansvarlig er en virksomhet**
- **Skriftlige avtaler....**

Datatilsynet

Akseptabelt risikonivå

Bruk styrende formuleringer, ikke tallkoder

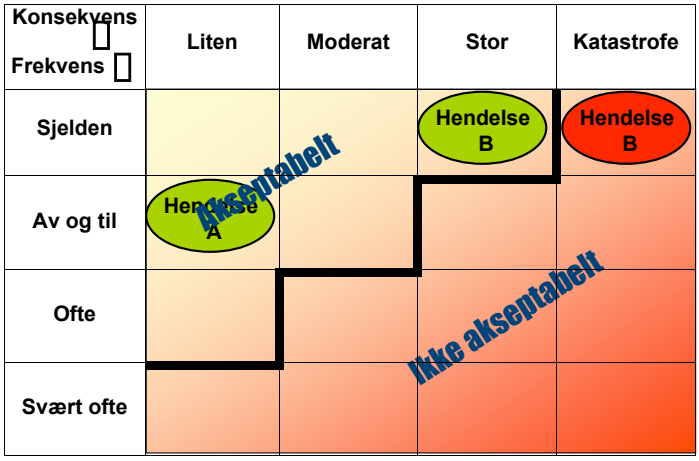
Sikkerhetstiltak skal iverksettes slik at personer utenfor virksomheten ikke skal kunne forårsake hendelser med katastrofale konsekvenser for enkeltmenneskers personvern.

egne medarbeidere uten gode resurser og god/fullstendig kjennskap til sikkerhetstiltak skal ikke kunne forårsake slike hendelser

...og heller ikke ved uaktsomhet eller forsett.....

Datatilsynet

Akseptkriterier



Datatilsynet

Loven skiller ikke mellom trådløs eller trådbasert kommunikasjon.

Samme krav til konfidensialiteten. Hvilke teknologiske løsninger virksomheten velger må være basert på resultatet av risikovurderingen.

Konfidensialitet når kommunikasjonen skjer utenfor den behandlingsansvarliges kontroll (Internett, radiolink eller trådløse nett).

Er kravet til konfidensialiteten høt må vi ikke bare ha kryptering, men også sterk autentisering.

Datatilsynet

Sikkerhetstiltak tips

§2-4 tilfredsstille risikovurderingen
§2-6 avvik: avdekke uautorisert bruk
§2-7 tilfredsstillende konfigurasjon
§2-8 autorisasjons mekanismer
§2-10 fysiske tiltak mot uautorisert adgang
§2-11 konfidensialitet inkl. kryptere, slette
§2-12 tilgjengelighet (backup, alternativer)
§2-13 integritet (ødeleggende programvare)
§2-14 sikkerhetstiltak (ikke mulig å omgå)
§2-15 parter og leverandørers tiltak

Datatilsynet

Styringssystemet tips/erfaringer

Styrende dokumenter
- §2-3 ansvar, mål, strategi
- §2-15 avtale ansvar: parter/leverandører
- §2-7 organisering m/klart ansvar

Gjennomførende dokumenter
- §2-8 autorisere kompetent personell
- §2-9 taushetsplikt også for sikkerhet

Kontrollerende dokumenter
- §2-3 ledelsens gjennomgang
- §2-5 sikkerhetsrevisjon gjøres jevnlig
- §2-6 avviksrutine m/melding til DT
- §2-4 Risikovurdering

Dokumentasjon
- §2-16 sikkerhet i 5 år, registreringer 3 mnd.

Datatilsynet

Sikkerhetskultur

Opplæring
Holdninger
Avvikshåndtering
Sikkerhetsrevisjon
Internkontrollsystem

Datatilsynet

E-post og logger

Hvor går grensen?

Datatilsynet

Disposisjon videre

- **Hjemmelsgrunnlag for e-postsystemer og logger**
  - Samtykke – hvilke krav stilles til dette?
  - Uten samtykke?

Datatilsynet

Lovens utgangspunkt

Behandling av personopplysninger
Forbudt

E-post og P-post

Hva er forskjellen?

Elektronikk	Papir
Tekst, bilde, film og lyd	**Tekst, bilder, lukt og følelse**

"Personlig"

E-post og P-post

Hva er forskjellen?

Elektronikk	Papir
Tekst, bilde, film og lyd	Tekst, bilder, lukt og følelse

"Virksomhet"

Datatilsynet

Elektroniske dokumenter

- Den ansattes forventning om diskresjon

Liten /ingen forventning

- **Fellesområde**, ”f:\felles*.*”
  - hvor samtlige eller en gruppe av ansatte har tilgang

Stor forventning

- **”Personlig” område**, ”g:\atle*.*”
  - hvor kun den ansatte selv har tilgang

Datatilsynet

Hjemmelsgrunnlag

- Personopplysningsloven
  - Samtykke, §8, 1. Ledd,1.pkt.
  - Interesseavveining, §8, bokstav f.)
- Formell lov
  - F.eks politiets hjemmel til å ta beslag (straffeprosessloven)
- Begrensninger
  - Straffelovens § 145
    - *”Den som uberettiget… skaffer seg adgang til innholdet… straffes med bøter eller fengsel inntil 6 måneder.”*

Datatilsynet

Aktivitetslogger

- **Register over hendelser internt i et edb-system eller datanett**

Aktiviteter som kan knyttes til enkeltpersoner, omfatter loggføring av:

- Internettbruk (web og e-post)
- Programmer, dokumenter mv.
- "Rettetasten" m.v.

Datatilsynet

Interesseavveining
- aktivitetslogger og e-post -

÷

- Fare for misbruk
- Personprofiler
- Datakvalitet
- Følelsesaspektet
- Tillitsbrudd

+

- Forutsetning for drift av edb-systemet
- Overvåkning av informasjonssikkerhet
- Bevismateriale ved straffbare forhold
- Arbeidsverktøy
- Preventivt

Datatilsynet

Administrasjon av system og sikkerhet

Personvernulempene

- –ingen beslutninger fattes
- –brukes sjelden
- –forventning om bruk

Nytte av behandlingen

- –Stor nytte av verktøy
- –Nødvendig for funksjon
- –Kritisk for infosikkerhet

Konklusjon: uten samtykke

Datatilsynet

Overvåkning av de ansatte

Personvernulempene

- –Informasjonskvaliteten
- –Beslutninger fattes
- –Diskresjonsforventning
- –Maktmisbruk

Nytte av behandlingen

- –Straffe de ansatte
- –Mer effektiv arbeidstid (??)
- –Kontroll med ulovligheter

Konklusjon: Samtykke

Datatilsynet

Krav til samtykke

Aktivt informert samtykke

- den ansatte skal vite hva han samtykker til
- frivillig

- **Forhåndsavtale mellom arbeidsgiver og arbeidstaker.**
- **Oppfyllelse av generell arbeidskontrakt er ikke nok.**

Datatilsynet

Retningslinjer

- **Klar informasjon**
  - Gjøre systemet forutsigbart
  - Frivillig
  - Oppfylle informasjonsplikten i §§19 og 20
- **Informasjon om**
  - Når andre kan se i postkassa
  - Hva andre kan ”se på ” i postkassa
  - Prosedyre ved aksessering

Datatilsynet

Autopass

Behandlingsansvarlig: **"den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes".**

Databehandler: **"En som behandler personopplysninger på vegne av den behandlingsansvarlige"**

Etter personopplysningsloven § 15 kan ikke databehandler behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Opplysningene kan heller ikke overlates til andre for lagring eller bearbeidelse uten slik avtale.

Datatilsynet

Utlevering til Politiet

Utlevering av billedopptak følger reglene i pol § 39 og kan skje "ved etterforskning av straffbare handlinger eller ulykker hvis ikke lovbestemt taushetsplikt er til hinder".

For øvrige opplysninger forutsettes at politiet har rettslig kjennelse for utleveringen.

- Utlevering til andre:

Utlevering til andre instanser forutsetter enten at den registrerte samtykker til utleveringen, eller at det foreligger en lovhjemmel til slik utlevering.

Datatilsynet

Innsyn

Etter § 18 i personopplysningsloven har den enkelte krav på å få vite hvilke opplysninger som er registrert om en selv.

Å for eksempel utvikle og drifte en løsning som via Internett gir den enkelte kunde en fullstendig og løpende oversikt over egne opplysninger har Datatilsynet ingen innvendinger mot, forutsatt at det opprettholdes en kostnadsfri og sikker innsynsmulighet.

Datatilsynet

Sletting

Personopplysningsloven § 28 forutsetter at opplysninger ikke skal lagres lenger enn det som er nødvendig for å gjennomføre formålet med behandlingen. Opplysningene skal deretter slettes.

Datatilsynet

Anonymt alternativ

Til hvert registreringssystem skal det i den grad det er praktisk mulig, eksistere et anonymt alternativ som er økonomisk like gunstig for brukeren.

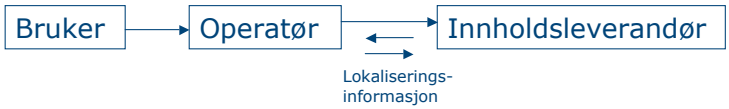
Den registrerte skal vite hva som registreres og i hvilken hensikt registreringen foretas.

Det må alltid være klare ansvarsforhold med hensyn til oppbevaring og bruk av personopplysningene.

Maskin- og programvare som håndterer personopplysningene må til enhver tid være av en slik kvalitet at de minimaliserer risikoen for uautorisert tilgang.

Datatilsynet

Lokalisering av mobiltelefoner



Brukeren må informeres og gi samtykke.

Datatilsynet

Hjemmesider på Internett må forholde seg til POL

Hjemmesider med personopplysninger (tekst, bilder osv.) anses ikke å ha et personlig og privat formål, de kan dermed ikke unntas fra personvernlovgivningen.

Skaff samtykke

Datatilsynet

Sikring av nettsteder

Kryptering

SSL (Secure Sockets Layer) 128 bit
HTTPS (The secure hypertext transfer protocol)

https er http som bruker SSL
Krever en secure server for å kunne håndtere forespørselen.

Datatilsynet

Aktivitet på Internett

Informasjon.

Informasjonen til brukerne bør være klar med tanke på hvordan de bør oppføre seg på nettet.

Det bør gis klar veiledning, i de tilfeller det foregår ukryptert kommunikasjon, at kommunikasjonen kan leses av andre.

For nyhetsgrupper og for andre informasjonstjenester hvor informasjonen vil være tilgjengelig for andre (chat-tjenester osv.) bør brukerne informeres om sikkerheten og hva de bør unngå å legge ut om.

Datatilsynet

Bilder på Internett

Situasjonsbilder kan defineres som bilder der selve situasjonen eller aktiviteten er det egentlige formålet med bildet. Trenger ikke samtykke så lenge bildene er harmløse.

Portrettbilder hvor hovedformålet er å avbilde en eller flere bestemte personer, hovedregelen er da at man alltid skal ha samtykke fra de avbildede før bildet legges ut på nett.