EUs nye forordning for personvern

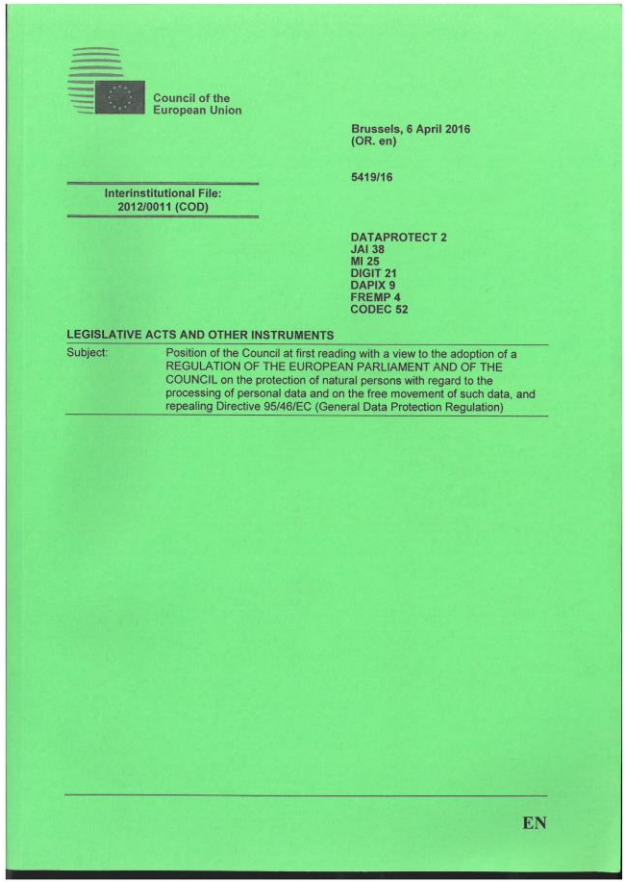
Tobias Judin, juridisk rådgiver

Norsk Arkivråds høstseminar, 2. november 2016

Datatilsynet

Nye personvernregler

1. Om de nye reglene
2. De nye reglene



Council of the European Union

Brussels, 6 April 2016
(OR. en)

5419/16

Interinstitutional File:
2012/0011 (COD)

DATAPROTECT 2
JAI 38
MI 25
DIGIT 21
DAPIX 9
FREMP 4
CODEC 52

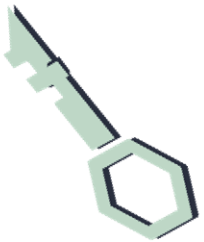
LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject: Position of the Council at first reading with a view to the adoption of a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

EN

1. Om forordningen

- Arbeidet startet i 2012
- Vedtatt i 2016 og gjelder fra 25. mai 2018
- Vil bli gjort til norsk lov og erstatte personopplysningsloven
- Formål
  - Harmonisering – like rettigheter og plikter i hele EU/EØS
  - Bedre samarbeid i EU/EØS
  - Styrke den europeiske borgers rettigheter



1. Om forordningen

- Direktiver og forordninger
  - I EU
    - Direktiver må tilpasses og vedtas av EU-landenes storting
    - Forordninger gjelder automatisk i EU-landene
  - I EØS
    - Forordningen inntas som et vedlegg til EØS-avtalen
    - Vedtas av Stortinget
  - = Norge må tolke den nye loven helt likt som resten av EU

- Noen spørsmål
  - Kan Norge beholde særregler?
  - Er særbestemmelsene i personopplysningsloven forenlige med forordningen? Hvor skal de plasseres?
  - Kan Norge delta i det europeiske samarbeidet?

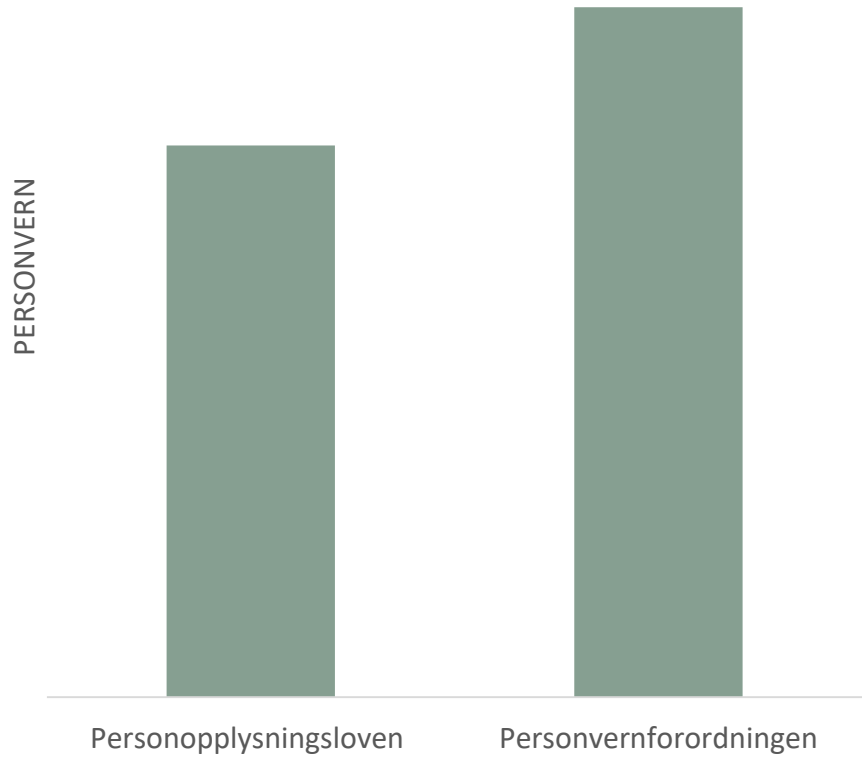
1. Om forordningen

- Bistår Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementet

- Eget internprosjekt

- Deltar i internasjonalt arbeid og bidrar til utredninger

1. Om forordningen



Dersom man følger dagens lov, er veien til etterlevelse av forordningen kort.

Dersom man ikke følger dagens lov, har man et problem…

Nye personvernregler

1. Om de nye reglene
2. De nye reglene

Alle norske virksomheter får nye plikter

- Bli kjent med de nye reglene
- Nye rutiner er et ledelsesansvar
- Alle ansatte skal følge nye rutiner

Krav til informasjon blir strengere

- Form
  - Kortfattet, klar og tydlig, lett forståelig og lett tilgjengelig
- Språk
  - Klart og enkelt
  - Tilpasset barn
- Skriftlig, elektronisk
- Stilles strengere krav til hvilke informasjon som skal gis

Plikt til å ha personvernombud (PVO)

- Plikt for
  - Offentlige organer
  - Virksomheter hvis kjerneaktivitet består i å regelmessig og systematisk overvåke personer i stort omfang
  - Virksomheter som behandler sensitive personopplysninger i stort omfang
- Krav til personvernkompetanse
- Personvernombudets stilling
  - Krav til å involvere ombudet
  - Kontaktpunkt for de registrerte
  - Uavhengig
  - Rapportere til øverste ledernivå
  - Taushetsplikt
  - Internt eller eksternt, andre oppgaver

Plikt til å utrede personvernkonsekvenser

- Dersom det er sannsynlig at behandlingen vil utgjøre en stor risiko for personvernet
  - Art, omfang og sammenheng og formål
  - Ny teknologi
- Påkrevet i visse typetilefeller opplistet i forordningen
  - systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser
  - behandling av sensitive personopplysninger i stort omfang
  - systematisk overvåking av offentlig område i stort omfang
- Privacy impact assesment (PIA)

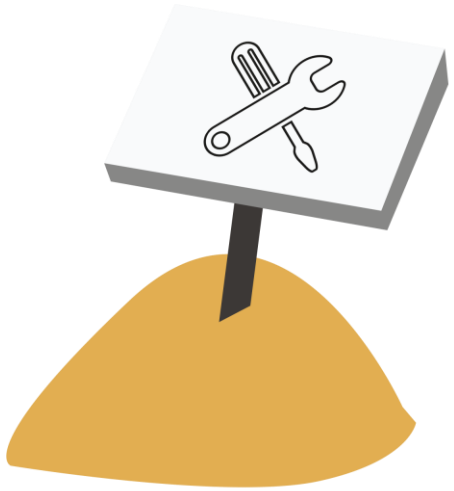
Plikt til å utrede personvernkonsekvenser

- Ved høy risiko, som ikke kan begrenses av interne tiltak, skal Datatilsynet involveres i forhåndsdrøftelser
- Vi kan veilede eller forby behandlingen
- Datatilsynet skal som hovedregel svare innen 8 uker
- Datatilsynet har plikt til å lage liste over typer behandlinger som krever en konsekvensutredning

Plikt til innebygget personvern

- Nye tiltak og systemer skal utarbeides på mest mulig personvernvennlig måte.
- Tenke personvern i innledende fasen, i fortsettelsen og så lenge det behandles personopplysninger
- Den mest personvernvennlige innstilingen som standard
  - Mengden personopplysninger
  - Omfanget av behandlingen
  - Lagringstid
  - Tilgjengelighet

  Psedonymisering



Teknologi
- Apper
- Big Data
- Biometri
- Dronar
- GPS og sporing
- **Innebygd personvern**
  - Sjekkliste for innebygd personvern
- Internett og sosiale medier
- Kameraovervåking
- Lydopptak av samtaler
- Skytjenester
- Strømavlesning

Syv steg til innebygd personvern

(Publisert: 15.02.2013 Sist endret: 05.03.2015)

Innebygd personvern betyr at det tas hensyn til personvern i alle utviklingsfaser av et system eller en løsning. Det er både kostnadsbesparende og mer effektivt enn å endre et ferdig system.

1. Vær i forkant, forebygg fremfor å reparere
2. Gjør personvern til standardinnstilling
3. Bygg personvern inn i designet
4. Skap full funksjonalitet: Både-og, ikke enten-eller
5. Ivareta informasjonssikkerheten fra start til slutt
6. Vis åpenhet
7. Respekter brukerens personvern

Når du lager et system som behandler personopplysninger, er det viktig at du kjenner til personvernprinsippene. Hvis du er *behandlingsansvarlig* eller *databehandler* for personopplysningene som skal behandles i systemet, må du også forholde deg til kravene i personopplysningsloven.

Se også sjekkliste for innebygd personvern

Brukerne forventer personvern

I dagens teknologiske samfunn utfordres grensene mellom personvern, brukervennlighet og *tilgjengelighet*. Datatilsynet ser at brukere av nettbaserte tjenester forventer at løsningene både er sikre, og ivaretar personopplysningene på en god måte. Personvern er ikke bare forventet, men også et mulig konkurransefortrinn for mange virksomheter. Dersom en virksomhet kan vise at de forvalter personopplysninger på en bedre måte enn en konkurrent som har tilsvarende løsning, vil brukerne foretrekke virksomheten med fokus på personvern.

Mer om

30.12.2011
Personvernprinsippene

Verktøy

Sjekkliste for innebygd personvern

Hvordan vurdere personvernkonsekvenser. Datatilsynets veileder

Regelverk

Personopplysningsloven (lovdata.no)

Personopplysningsforskriften (lovdata.no)

Annet

Resolution on Privacy by Design, 2010

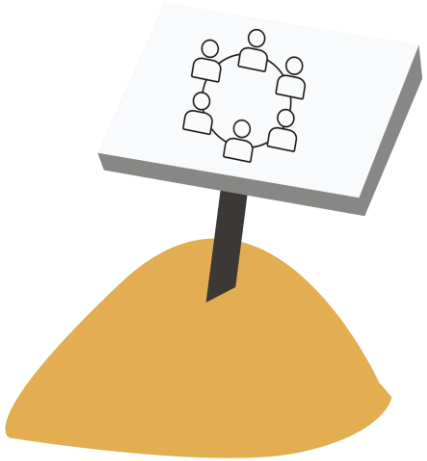
7 foundational principles by Ann Cavoukian, 2010

Krav til avvikshåndtering

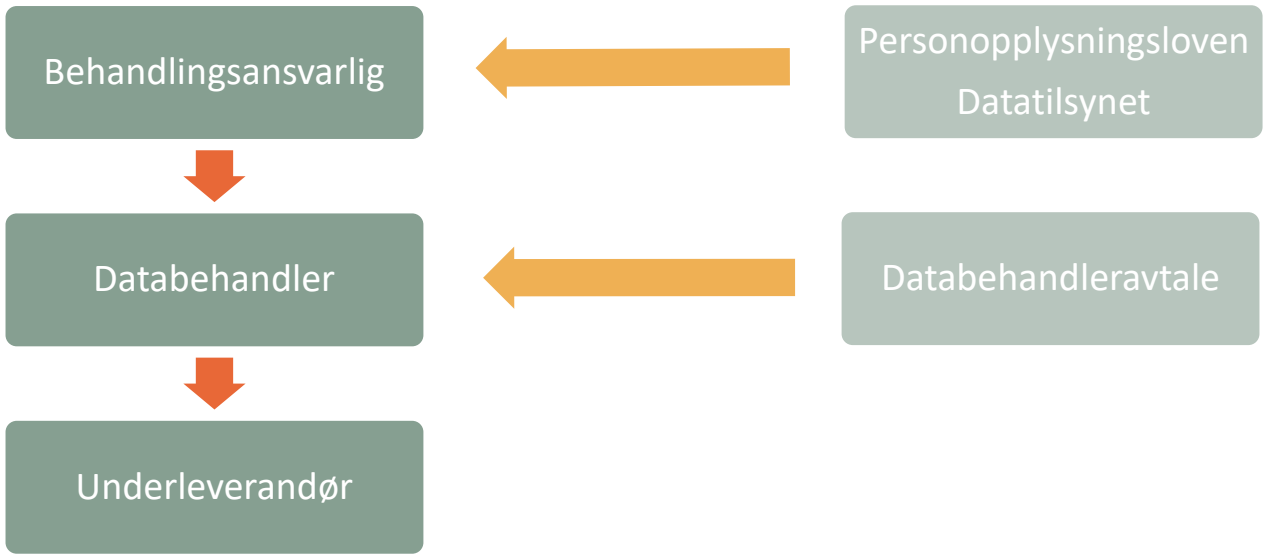
- Plikten til å melde avvik utvides
  - I dag: personopplysninger der konfidensialitet er nødvendig
  - I 2018: alle avvik med mindre usannsynlig at avviket medførte en risiko for personers rettigheter, personvernet
- Plikt til å melde raskere
  - Hovedregel: uten unødig opphold og innen 72 timer
  - Avviksmelding kan gis trinnvis
- Krav til avviksmeldingens innhold
- Krav til varsling av de berørte hvis høy risiko for deres rettigheter, personvernet
  - Noen unntak (kryptering eller andre tiltak eller uforholdsmessig)

Bransjenormer

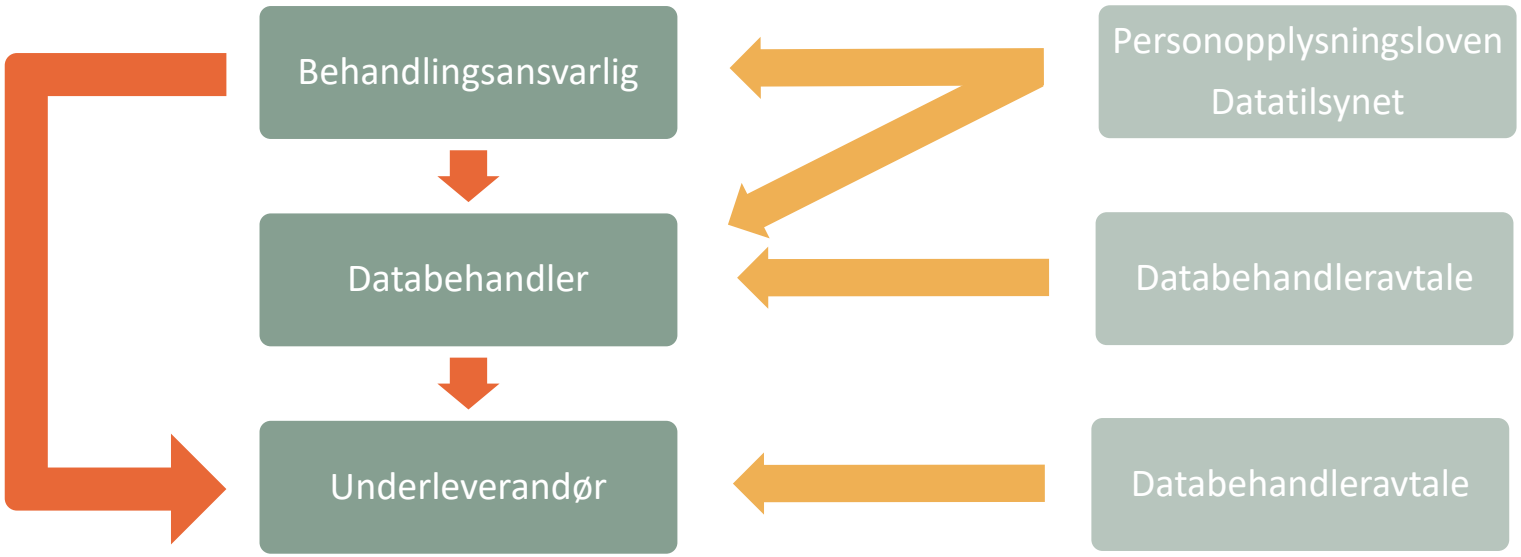
- De nye reglene oppfordrer til sektorvis utforming av retningslinjer og bransjenormer
- Tar hensyn til sektorens art og virksomhetens størrelse
- Bidra til etterlevelse av forordningen
- Flere fordeler ved å følge disse
- Datatilsynet skal godkjenne bransjenormer



Plikter for databehandlere



Plikter for databehandlere



Spesifikk godkjenning

Generell godkjenning med informasjon og reservasjonsrett

Plikter for databehandlere

- Loven gjelder direkte for databehandlere
  - Plikt til å sørge for informasjonssikkerhet
  - Plikt til å varsle den behandlingsansvarlige om avvik
  - Plikt til å utnevne PVO på lik linje med behandlingsansvarlige
  - Gi beskjed til behandlingsansvarlig om instrukser som er i strid med loven
  - Krav til databehandleravtalen og dens innhold
  - Kan blir erstatningspliktige

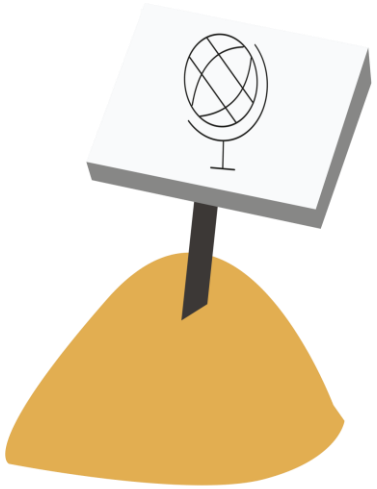
- Behandlingsansvarlige kan kun velge databehandlere som gir tilstrekkelige garantier for at loven følges (bransjenorm)

Internasjonalt

- De nye reglene gjelder også virksomheter utenfor EU-/EØS-området
  - Tilbyr varer eller tjenester til EU- eller EØS-borgere
  - Kartlegger EU- eller EØS-borgeres adferd

- Virksomheter skal kunne forholde seg til ett datatilsyn (hovedetablering)

- Den registrerte skal kunne klage i eget land



Bedre rettigheter for enkeltpersoner

Retten til å bli glemt og motsette seg profilering

Dataportabilitet

Bedre informasjon og oversikt

Klager kan rettes til Datatilsynet i landet man bor i

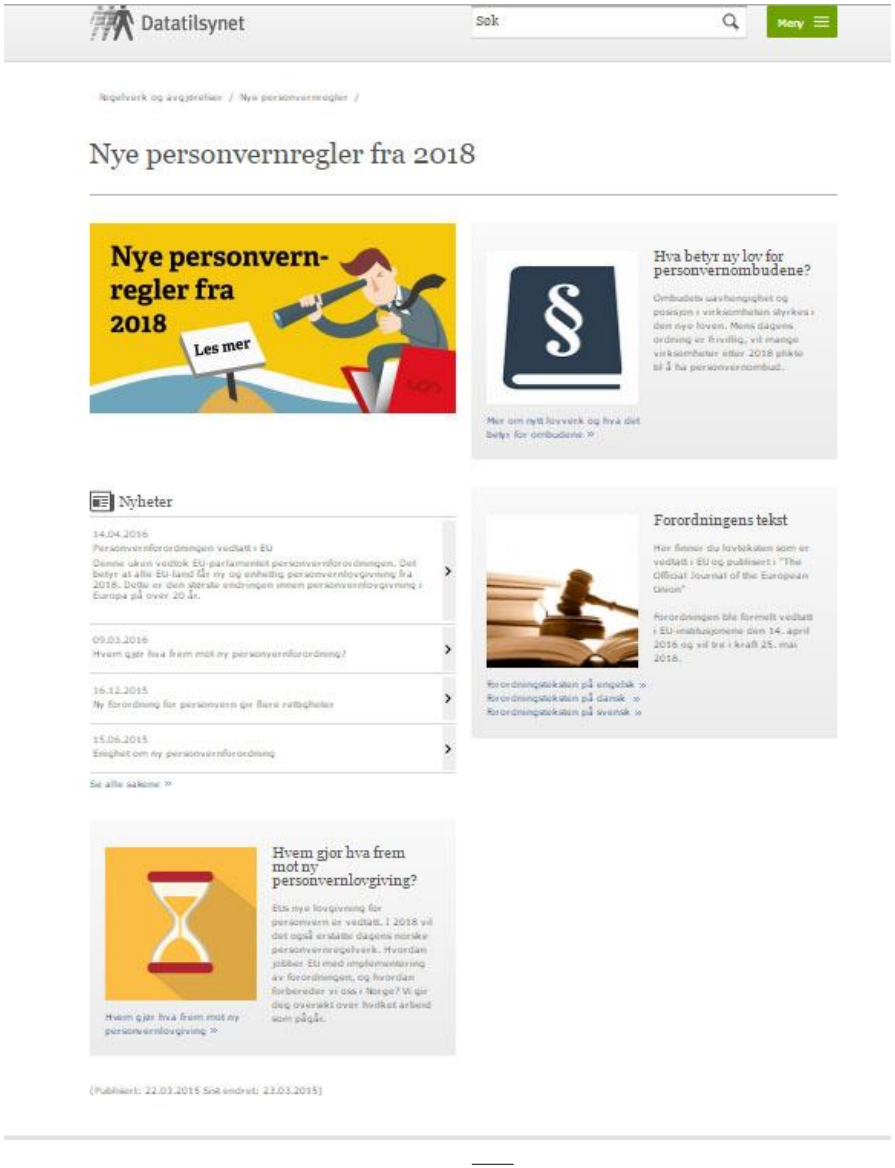
Nettjenester må innhente foreldres samtykke

Nye sanksjoner

Hvordan forberede seg?

- Sørge for å ha oversikt over hvilke personopplysninger som behandles
- Sørge for å oppfylle dagens lovkrav
- Sette seg inn i det nye regelverket
- Lage rutiner for å følge de nye reglene

Datatilsynet.no/forordning



Nye personvernregler fra 2018

Hva betyr det for din virksomhet?

Datatilsynet

Til ledere med ansvar for personvern, sikkerhet og utvikling

Er du klar for nytt regelverk?

I 2018 blir dagens personvernregelverk erstattet av EUs personvernforordning. Norske virksomheter bør derfor begynne å forberede seg på nye personvernregler allerede nå. Før de nye reglene trer i kraft må dere sørge for at dere har:

1

Internkontroll og oversikt over hvordan dere behandler person-opplysninger

Fra 2018 må ikke bare behandlings-ansvarlige, men også databehandlere ha oversikt over behandling av personopplysninger.

2

Systemer, tjenester og løsninger som oppfyller prinsippene om innebygd personvern

Velg den mest personvernvennlige innstillingen som standard. Bygg personvernet inn ved blant annet å begrense mengden informasjon som samles inn, pseudonymisere opplysninger så raskt som mulig, være åpen om innsamling og bruk av opplysninger, og tenke sikkerhet i alle utviklingsfaser (innebygd sikkerhet).

3

Systemer som er tilpasset for dataportabilitet

Alle registrerte skal som hovedregel kunne ta med seg personopplysninger de selv har oppgitt, fra en virksomhet til en annen. Systemene dere bruker må være tilpasset for overføringer og mottak av opplysninger.

4

Tilfredsstillende informasjonssikkerhet

Gjennomfør risikovurderinger og få på plass tekniske og organisatoriske tiltak som pseudonymisering og kryptering. Systemene må sikre konfidensialitet, integritet, tilgjengelighet og robusthet. Sørg for at tilgjengelighet og tilgang til personopplysningene dere behandler gjenopprettes på en sikker måte etter hendelser. I tillegg må dere ha prose-dyrer for å teste, vurdere og evaluere at tiltakene både er effektive og ivaretar sikring av alle personopplysninger virksomheten behandler.

5

Rammeverk og rutiner for å vurdere personvernkonsekvenser

Dersom et tiltak er inngripende, skal dere vurdere personvernkonsekvensene ved tiltaket ved hjelp av en Privacy Impact Assessment (PIA) før det iverksettes. Er risikoen høy og umulig for dere å redusere, skal Datatilsynet involveres i forhåndsdrøftelser.

6

Rutiner for avvikshåndtering

Forordningen stiller strengere krav til avvikshåndtering enn dagens regelverk. Ved brudd på sikkerheten skal dere varsle Datatilsynet innen 72 timer, og vi skal varsles oftere enn før. I tillegg skal dere informere alle som er berørt av sikkerhetsbruddet. Databehandlere skal også varsle behandlingsansvarlig umiddelbart ved avvik.

datatilsynet.no/forordning

Datatilsynet

veiledning@datatilsynet.no