



# Når barn og barnevernsaker eksponeres i media

Barnevernkonferansen 2016

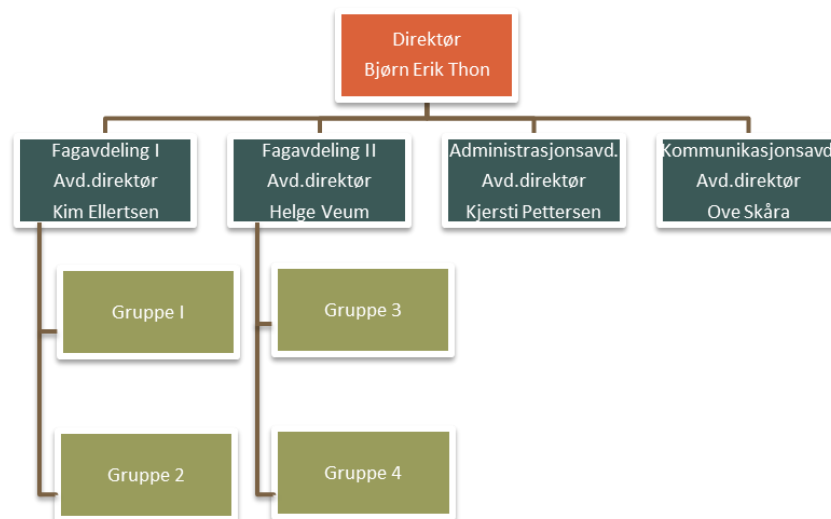
Radisson BLU Bodø 22. november 2016

Fagdirektør Knut B. Kaspersen



# Datatilsynet

- Opprettet 1980, lokalisert i Oslo
- 51 medarbeidere
- Særlig uavhengig forvaltningsorgan under KMD
- To roller – forvaltning og ombud
- Regelverk:
  - Personopplysningsloven
  - Helseregisterloven
  - Pasientjournalloven
  - Helseforskningsloven
  - Politiregisterloven
  - Lov om Schengen informasjonssystem
  - mv.
- Personvernemnda er klageorgan for våre vedtak

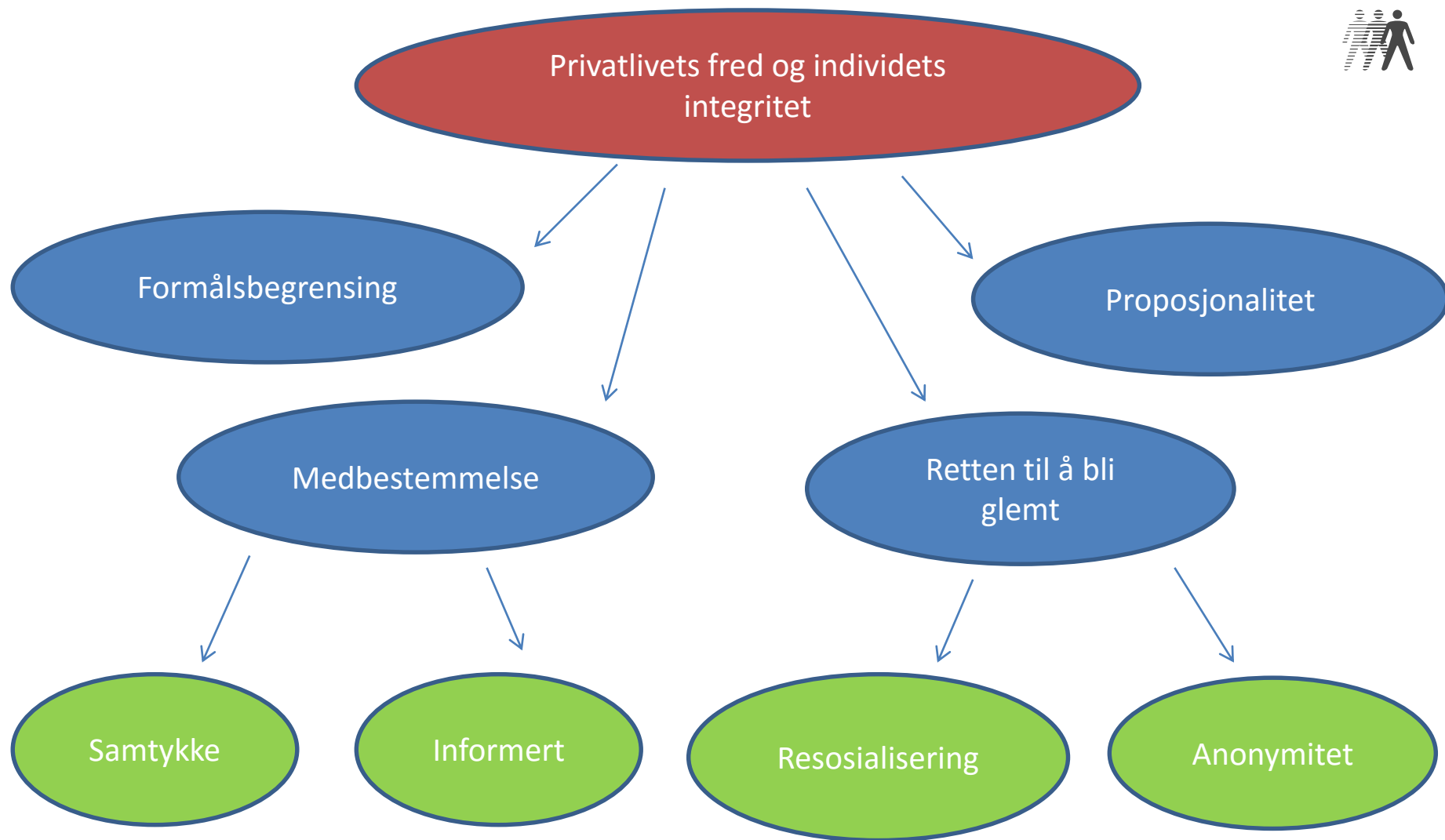




# Personvern

Hva er det?

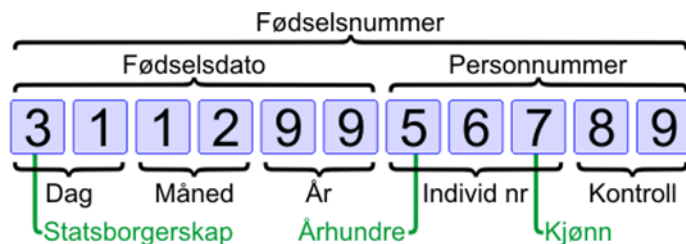






# Personopplysninger

Hva er det?





- Opplysninger og vurderinger som kan knyttes til en enkeltperson
  - Knut B. Kaspersen (180455 xxxxx)
- Direkte eller indirekte identifiserbart
  - Indirekte kan være opplysninger som beskriver en person uten bruk av identifikatorer.
    - Mann 61, lite hår, med briller ansatt i Datatilsynet

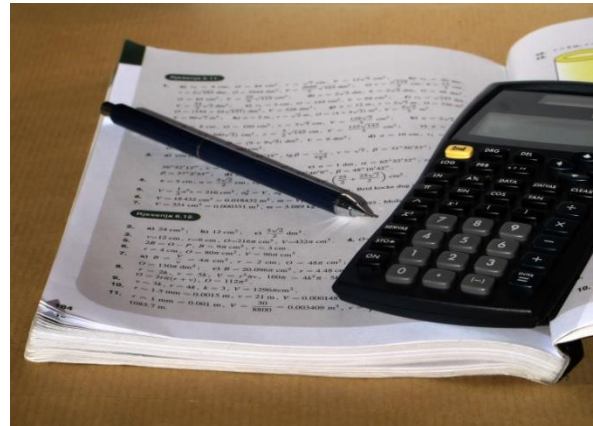


# Personopplysninger – hva er det?



Peder Aas  
2020 Lillevik

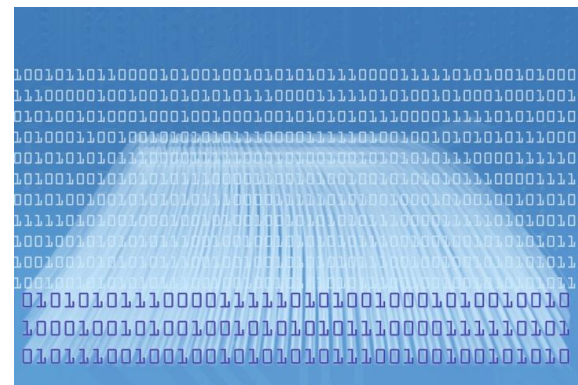
F.nr 180262 34997



# Personopplysninger

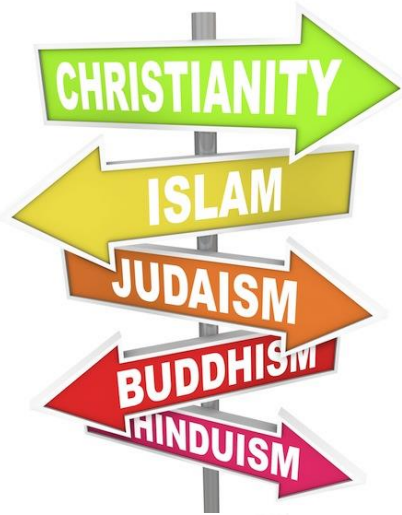
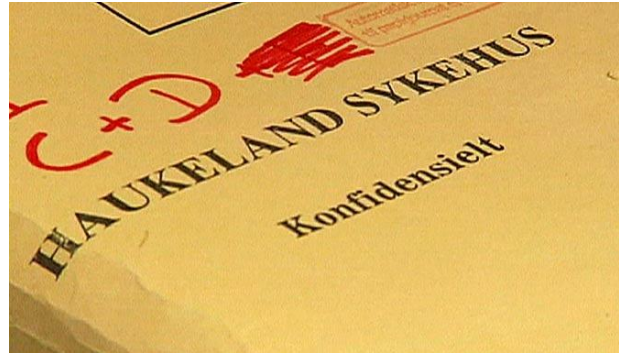


- **Fødselsnummer:** 13087846271
- **Telefonnummer:** 22396900
- **IP-adresse:** 195.159.103.82
- **Bilnummer:** BL 23456
- **Bluetooth MAC:** 17:35:52:78:4B:CA
- **Wi-Fi-adresse MAC:** 12:44:32:45:7B:C9
- **Autpass-brikke-ID:** 7483920983278394



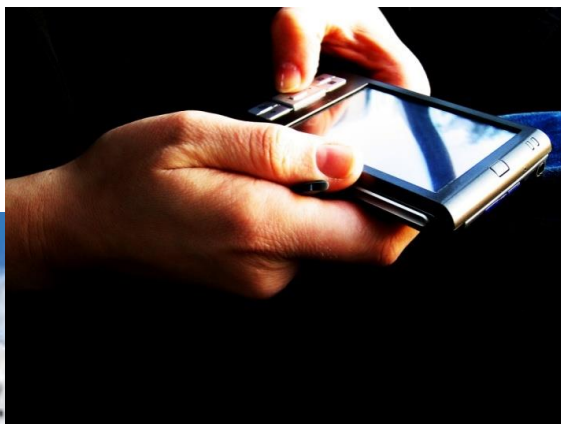


# Sensitive personopplysninger



# Personopplysninger – hvor er de?

---



# Hvordan etterleve loven?

---





- Få oversikt over hvilke personopplysninger som behandles og klassifiser dem fra sensitive til ikke-sensitive.
- Lag rutiner og regler for:
  - Innsyn
  - Samtykke
  - Retting og sletting
  - Informasjon



# Kartlegge virksomhetens behandlinger



Virksomheten skal ha oversikt over personopplysningene

- Nødvendig for å ivareta sine plikter.
- Grunnlag for sikkerhetsmål og sikkerhetsstrategi.
- Underlag for risikovurderinger.

Informasjon	Behandlingsgrunnlag	Melding/Konsesjon	Klassifikasjon	Sikkerhetstiltak	Lagring og kommunikasjon	Opplysningenes omfang	Avdeling	Databehandler
<b>Formål</b>								
<b>Lønn og personal:</b> lønnsopplysninger personalopplysninger	Personopplysning sloven, § 8f	Unntatt i forskriftens § 7-16	Personopplysninger			Ca. 130 ansatte		
<b>Barnevern:</b> vurdering og tiltak	Barnevernloven, § 3-1	Meldt 14.01.2009	Sensitive personopplysninger			Ca. 68 barn og foresatte		
<b>Helseopplysninger:</b> pasientjournal	Helsepersonelloven § 39	Meldt 14.01.2009	Sensitive personopplysninger			Ca. 413 pasienter		
<b>Elevadministrasjon</b> elever / foresatte lærere	Opplæringsloven § 13-5		Personopplysninger			Ca. 219 søkere		
<b>Hendelsesregister:</b> logg over brudd	Personopplysning sloven, § 13	Unntatt i forskriftens § 7-11	Personopplysninger			Arkivlogg, nettverkslogg og serverlogg, PC-logger		

# Dokumentasjon av internkontrollsystemet



- Det er et lovpålagt krav at internkontrollsystemet skal være dokumentert.
- Dokumentasjonen er delt i tre emner:
  1. Styrende dokumentasjon som ledelsen er ansvarlig for å utarbeide.
  2. Gjennomførende dokumentasjon med rutiner og tiltak for daglig drift.
  3. Kontrollerende dokumentasjon med rutiner for oppfølging, korrigering og forbedring av internkontroll og informasjonssikkerhet.





Den behandlingsansvarlige er pålagt å ha rutiner for å oppfylle den registrertes rettigheter.

- Plikt til å informere når det samles inn opplysninger fra den registrerte er beskrevet i personopplysningsloven § 19.
- Plikt til å informere når det samles inn opplysninger fra andre enn den registrerte, er beskrevet i personopplysningsloven § 20.
- Virksomheten skal ha rutine for behandling av forespørsel om innsyn fra mulig registrerte
- Virksomheten skal ha rutine for behandling av forespørsel om retting og sletting for en registrert.



# Bilder av barn

---







# Hva er problemet?

---



- Forholde seg til et regelverk som kan virke vanskelig tilgjengelig
- Tillatelse fra foreldrene





- På noen bilder er hovedfokus én eller flere bestemte personer. Da skal man alltid ha samtykke. Hvis de som er avbildet er under 15 år, må også de foresatte samtykke. På andre bilder er det selve situasjonen eller aktiviteten som er hovedfokus i bildet. Vanligvis kan slike bilder offentliggjøres uten samtykke fra de avbildede så lenge bildene er harmløse og ikke på noen måte kan føles krenkende for de som er avbildet. Bildene skal heller ikke skal virke krenkende ut fra sammenhengen de benyttes i.

Ha som hovedregel:  
Spør alltid om samtykke!





# Hva er problemet?

---



- Forholde seg til et regelverk som kan virke vanskelig tilgjengelig
- Tillatelse fra foreldrene
  - Passordbeskyttelse
  - Sletting – videre bruk
  - Journalistiske formål
    - Gruppebilder / klassebilder
    - Politiske sammenhenger
  - Misbrukspotensialet
  - Etske vurderinger
  - Den totale mengden bilder av barna på nett allerede i ung alder







- **Paradoks:**
- Barn og unge skal lære fornuftig bruk av Internett; de skal tenke seg om før de publiserer noe om seg selv eller andre
- Allerede fra dagen de er født opplever de at foreldre og andre (ukritisk?) teppelegger nettet med bilder av dem..
- Hvordan lære seg gode nettvvaner da?







# I beste mening . . .

Et veiledningshefte om bilder av barn på nett





- Sett av tid på et personalmøte til å gå gjennom Datatilsynets veileder, ”I beste mening...”
- Lag egne interne regler
- Lag et skreddersydd og tydelig samtykkeskjema
- Fremfor alt; vurder hvert enkelt bilde før det legges på nett. Er det virkelig nødvendig å legge det ut? Kan barnehagen vurdere å benytte andre måter å vise bildene på?







# Bilder av barn på nett



- Når vi voksne synes det bare er gøy

1. Feriebilder
2. Portrett vs. Lagbilde
3. Barnet gråter
4. Bløtkakebilde
5. Down syndrom



“He realized his caramel apple has an apple in it.”

Submitted By: XXXXX

Location: Wisconsin, United States





- Barnet brukes i de voksnes interesse
  1. Ved skilsmisse
  2. Mot barnevernet
  3. Protestarena
- Digital mobbing
- Barnet brukes for å verne om dets interesser
  1. Barneombudet – You Tube



# Barnevernssaker på nett

---



- Taushetsplikten
- Foreldrene gir opplysninger selv



- Hva kan barneverntjenesten gjøre
- Delta i debatten
- Begrensninger
- Barnets situasjon
- Hvilke opplysninger er offentlig kjent
- Korrigeringer
- Nye konkrete opplysninger
- Ingen berettiget interesse
- Saken skal ikke kommenteres
- Hva når foreldrene gir samtykke til barnevernet?

# Reaksjon

---



- Foreldre kan straffes – privatlivets fred strl. § 267
- Erstatningspliktig

# Barnevernssaker på nett - avvik

---



- Postjournal på nett
- Fulltekstdokumentasjon på nett

# Trakasering av ansatte (fagpersonale) på nett

## Norske leger henges ut på nettside om barnevern





# Trakasering av ansatte på nett

---



- Nettstedene inneholder lister med over 400 navn på psykologer, barnevernsansatte, politikere, advokater, journalister og andre, der disse kritiseres og karakteriseres. De fleste opplistede er offentlige tjenesteutøvere. Personopplysningene som finnes på sidene er personnavn, yrke, bosted og tittel. Noen av de opplistede er også avbildet.

# Trakasering av ansatte på nett

---



- Hvor går grensen?
- Når formålet utelukkende er ment for å påvirke opinionen og diskusjonen i det offentlige rom
- Grunnloven § 100 vern av ytringer
- Etske prinsipper i vern av enkeltindivid
- Grense mot det straffbare
- Sjikane vs. Trusler
- Informasjon om beredskapshjem – PVN-2010-11

# Sletting i barnevernjournal

---



- Kvalitetssikring av personopplysninger
- Sletting/retting/supplering/sperres/arkiveres
- Sosialrapport i sin helhet
- Oslo kommune – barnehageplass
- Lillehammer kommune
- Tysnes kommune PVN-2013-02
- Barnevernsenter – PVN -2003-04 (supplering)
- Barneverntjenesten – PVN-2013-06
- Fosterforeldre – PVN-2012-05

# Kontroll av Fylkesnemnda

---



- Informasjonssikkerhet
- Arkiv vs lagring på lokal server
- telefaks



# Tilgangsstyring

---



= autentisering, autorisasjon, sporbarhet

- Hvem skal ha tilgang til hvilke personopplysninger,
- for hvilke brukere,
- hvilke informasjonselementer,
- i hvilket tidsrom
- evt. andre forutsetninger

Disse fem faktorene må balanseres. Hva kan vi leve med og hvor bør grensene gå?



Hva skal til for å bevise at du er den du hevder du er?  
Kravet til autentisering avhenger av risiko.

Ved sensitive opplysninger eller andre opplysninger med behov for konfidensialitetsbeskyttelse:

- Brukernavn, passord og kontroll over nettverk eller
- På internett kreves to-faktor-autentisering, typisk brukernavn, passord og en ekstra faktor
- Passordkrav



- Autorisert bruk av informasjonssystemet skal registreres
- Forsøk på uautorisert bruk av informasjonssystemet skal registreres
- Bruk av logg
  - Ved henvendelser fra den registrerte
  - Ved tips om misbruk
  - Stikkprøveanalyse
  - Automatiserte analyser



# Saksbehandlere skal...

---



- ikke avgjøre hvordan opplysningen skal sikres
- forskånes fra å være i tvil om hvordan han skal håndtere opplysningene
  - Vite hvilke rutiner som finnes
  - Vite hvem som er ansvarlig for å gi hjelp
  - Vite hvem som skal orienteres om problemer
- følge ledelsens rutiner
- rapportere avvik
  - Avvik fra rutiner
  - Manglende eller ufullstendige rutiner





- Det forventes ikke alltid at øverste leder har inngående kunnskap om informasjonssikkerhet
- Derimot forventes det at personopplysninger er sikret på en forsvarlig måte, og at øverste leder kan garantere at dette blir gjort. I praksis betyr det å sørge for at virksomheten har oversikt over:
  - hvilke plikter som gjelder
  - hvordan opplysninger behandles og sikres
  - at alle rutiner knyttet til dette er godkjent og blir fulgt opp av alle ansatte

# Risikovurdering

---



Thinkstock.com

# Risikovurdering – trinn for trinn



- Kartlegg og klassifiser alle behandlinger
- Identifiser uønskede hendelser (og årsaker!)
- Konsekvensvurdering (1-4)
- Sannsynlighetsvurdering (letthet 1-4)

Sammenlign resultater og iverksett tiltak for å komme innenfor akseptabel risiko.

Konsekvens (K)/ Sannsynlighet (S)	S1	S2	S3	S4
K4				R4
K3			R3	
K2		R2		
K1	R1			



**AVVIK**



- Dersom personopplysninger håndteres i strid med fastlagte rutiner, eller det er mistanke om eller dokumentert brudd på informasjonssikkerhet, skal virksomheten iverksette avviksbehandling
  - Formålet med avviksbehandling er å lukke avviket så raskt som mulig, gjenopprette normal tilstand og hindre gjentakelse
- Når man behandler avvik er det viktig å:
  - Iverksette strakstiltak, blant annet med det formål å avgrense eventuelle følgeskader
  - Iverksette korrigerende tiltak for permanent å gjenopprette normal tilstand
  - Vurdere hvorvidt korrigerende tiltak fungerer etter sin hensikt
  - Varsle Datatilsynet når dette er pålagt (forskriften § 2-6, 3. ledd)

# Personopplysninger på avveie – eks.



The screenshot shows the NRK Nordland website interface. The main headline is "Fjernet personnummer på nett" (Removed personal number on net). The sub-headline reads: "Etter pålegg fra Datatilsynet har Bodø kommune nå fjernet fødsels- og personnumrene til ansatte fra internett." (After orders from the Data Inspectorate, Bodø municipality has now removed birth and personal numbers of employees from the internet). The article is dated 21.04.2005 13:08 and is by Ivar Jensen. A sidebar on the right lists "10 SISTE NRK NORDLAND" with various news items like "Skaptisk til ny minister" and "Minikraftverk under planlegging".

The screenshot shows the Østlandets Blad website. The main headline is "Kommunen hengte ut elev" (The municipality hung out student). Below the headline is a photograph of a man in a suit, likely a representative of the municipality. To the right of the photo is a sidebar with "VERKTØY" (Tools) including "Utskriftsvennlig versjon" (Print-friendly version) and "Bokmerk denne artikkelen" (Bookmark this article). Below that is "NYHETS BREV" (Newsletter) with a link to "Meld deg på vårt nyhetsbrev" (Sign up for our newsletter). At the bottom is "TIPS OSS OM OPPFØLGING" (Tip us on follow-up) with a link to "Til tips-skjema" (To tip form).

**Stikk i strid med lover og regler har Ski kommune offentliggjort navnet på en niendeklassing med det som betegnes som «stort fravær fra undervisningen».**



# Fulltekstpublisering av dokumenter

---



- Kommune
- Stat



- Tidlig ute med løsning
- Lite føringer fra sentrale ”myndigheter” (KS)
- Prøve og feile-metoden
- Hva gikk galt?



- HVA SKJER I DAG?
- OEP-LØSNING
- AKTUELLE ALTERNATIVER
- Innsendelse av lenke til OEP med opprettelse av lokal database
- Innsendelse av dokumentet til en sentral database i OEP



- VED PUBLISERING
- RISIKOVURDERING
- FØRINGER FOR PUBLISERING
- HINDRE SKYGGEDATABASER”
- HINDRE INDEKSERING FRA EKSTERNE SØKEMOTORER



- PERSONOPPLYSNINGSLOVEN GJELDER FULLT UT
- §§ 8 og 9
- § 11
- §§ 13 og 14



- HVILKE PERSONOPPLYSNINGER SOM PUBLISERES
- Hvilke tiltak er iverksatt for å hindre at det skjer avvik



- SKAL PERSONOPPLYSNINGER PUBLISERES
- HVILKE PERSONOPPLYSNINGER SKAL PUBLISERES
- VEILEDNING ELLER
- BESTEMTE OG KLARE FØRINGER
- KONSEKVENSER FOR BORGEREN
- PERSONVERNERKLÆRING



# HINDRE INDEKSERING FRA SØKEMOTORER

---



- Google, Kvasir o.a.
- Hvorfor er dette viktig?
- Hva må til?
- Ålesund-vedtaket
- No robot ikke nok



- ANDEBU KOMMUNE (spesialscole)
- RÅDE KOMMUNE (attføringsmappe)
- NORDFJORDEID KOMMUNE
- ST. OLAV HOSPITAL
- PPT – MINNEPENN
- RANA KOMMUNE
- OPPSIGELSE AV TRENER
- SYKEPLEIER TAUSHETSPLIKT



- Personalsak – ved bytte av system
- Journalmappe på 15 psykisk utviklingshemmede
- Universitetet i Oslo – fødselsnummer - gjentakelse
- Kommune – helseerklæring - handikaplass
- Hacking – politiske parti
- Kommune – skanning av «bunker» med dokumenter (skilleark)



## Det nye regelverket



- Noen sier at vi går fra hefte til bok
  - Her er det nok noen modifikasjoner
- Det sies også at det nye lovverket er som en Sveitserost
  - Like mye hull som ost - som kan fylles med nasjonale tilpasninger
  - Også her er det mange modifikasjoner
    - Det gamle direktivet var nok betydelig mer Sveitserost
    - Derfor er vår personopplysningslov med forskrift ganske forskjellig fra mange andre land i Europa
  - Forordningen gir oss betydelig mer enhetlig lovverk innenfor EU/EØS





- Arbeidet startet i 2012
- Vedtatt i 2016 og trer i kraft i 2018
- Felles regelverk for personvern i Europa
- Styrke den europeiske borgers rettigheter
- Gjøre det lettere å utveksle personopplysninger over landegrenser
- Styrke tilliten til digitale tjenester
- Sikre samarbeid mellom personvernmyndigheter



# Hva gjør Datatilsynet?

---



- Bistår Justis- og beredskapsdepartementet og Kommunal- og moderniseringsdepartementet
- Eget internprosjekt
  - IKT
  - Juridisk
  - WEB
  - Personvernombud
  - Kommunikasjon
- Deltar i internasjonalt arbeid og bidrar til utredninger





# Alle norske virksomheter får nye plikter

---



- Alle må finne ut hva regelverket betyr
- Nye rutiner er et ledelsesansvar
- Alle ansatte skal følge nye rutiner



# Alle skal ha en forståelig personvernerklæring

---



- Informasjonen skal være lett tilgjengelig
- Klart språk som er tilpasset leserens nivå
- Stilles krav til hvilke opplysninger som skal gis





- I tillegg til en risikovurdering skal man utrede tiltak med stor personvernrisiko
- Ved høy risiko, som ikke kan begrenses, skal vi involveres i forhåndsdrøftelser
- Forordningen stiller krav til vår behandlingstid
- Vi kan veilede eller forby behandlingen

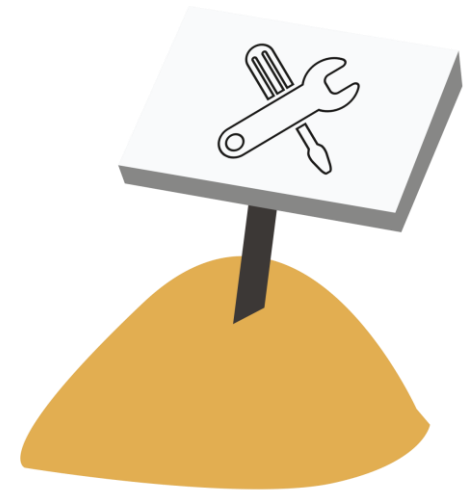


# Alle skal bygge personvern inn i nye løsninger

---



- Nye krav til løsninger, tiltak og systemer
- Skal utarbeides på mest mulig personvernvennlig måte
- Den mest personvernvennlige innstillingen som standard





- Personvernombudsordningen går fra frivillig til obligatorisk
- Alle offentlige virksomheter
- Mange private
- Krav til kompetanse
- Krav til å involvere ombudet



# Alle databehandlere får nye plikter

---



- Egne rutiner for behandling av personopplysninger
- Si ifra om instruksjer er i strid med loven
- Underleverandører skal godkjennes
- Melde avvik til behandlingsansvarlig
- Kan bli erstatningspliktige





- Sektorvis utforming av retningslinjer
- Sikrer at de viktigste rutinene er på plass
- Flere fordeler ved å følge disse
- Datatilsynet skal godkjenne bransjenormer





# Alle får nye krav til avvikshåndtering

---



- Strengere regler enn i dag
- Melde avvik innen 72 timer
- Stilles krav til innholdet i avviksmeldingen
- De berørte skal varsles i klart språk



# Hva bør alle virksomheter gjøre nå?

---



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





## Nye personvernregler fra 2018



### Hva betyr ny lov for personvernombudene?

Ombudsets uavhengighet og posisjon i virksomheten styrkes i den nye loven. Mens dagens ordning er frivillig, vil mange virksomheter etter 2018 plikte å ha personvernombud.

Mer om nytt lovverk og hva det betyr for ombudene. »

### Nyheter

- 14.04.2016  
Personvernforordningen vedtatt i EU  
Denne okun vedtok EU-parlamentet personvernforordningen. Det betyr at alle EU-land får ny og enhetlig personvernlovgivning fra 2018. Dette er den største styringen innen personvernlovgivning i Europa på over 20 år. »
- 09.03.2016  
Hvem gjør hva frem mot ny personvernforordning? »
- 16.12.2015  
Ny forordning for personvern gir flere rettigheter »
- 15.06.2015  
Enighet om ny personvernforordning »

Se alle sakene »



### Forordningens tekst

Her finner du lovkosten som er vedtatt i EU og publisert i "The Official Journal of the European Union".

Forordningen ble formelt vedtatt i EU-møtet den 14. april 2016 og vil tre i kraft 25. mai 2018.

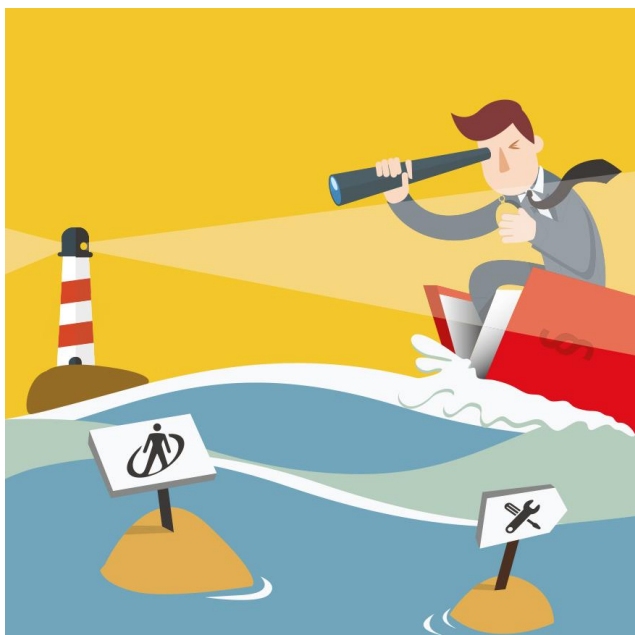
Forordningsteksten på engelsk »  
Forordningsteksten på dansk »  
Forordningsteksten på svensk »



### Hvem gjør hva frem mot ny personvernlovgiving?

Ette nye lovgivning for personvern er vedtatt. I 2015 vil det også erstatte dagens norske personvernregelverk. Hvordan jobber EU med implementering av forordningen, og hvordan forbereder vi oss i Norge? Vi gir deg innblikk i over hvilket arbeid som pågår.

Hvem gjør hva frem mot ny personvernlovgiving »



## Nye personvernregler fra 2018

# Hva betyr det for din virksomhet?



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 personopplysninger**  
Fra 2018 må ikke bare behandlingsansvarlige, 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 (innebygg 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 overføring og mottak av opplysninger.
- 4 Tilfredstillende 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 gjenoprettes på en sikker måte etter hendelser. I tillegg må dere ha prosedyrer 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.



# Takk for meg!



postkasse@datatilsynet.no  
Telefon: +47 22 39 69 00

**datatilsynet.no**  
**personvernbloggen.no**

hhu@datatilsynet.no