KiNS
foreningen kommunal informasjonssikkerhet

Ove Skåra, fagdirektør Datatilsynet
Steinar Nørstebø, styreleder KiNS

Først en øvelse:
Hva er det første du tenker på når jeg sier:

Informasjons sikkerhet

2

Hva er KiNS

- Foreningen Kommunal Informasjonssikkerhet KiNS 2003
- **Over 280** kommuner/fylkeskommuner som medlemmer
- Samarbeider nært med Datatilsynet, DiFi, DSB, NSM, eHelse, Senter for IKT i undervisningen og KS.
- KiNS arrangerer årlig én stor konferanse
- KiNS arrangerer også regionale dags-/flerdags kurs gratis for medlemmer

NYPE

nye personvernregler

NYPE
nye personvernregler

KiNS og KS startet i 2016 et to-årig prosjekt

- Informere rådmennene (forankring)
- Lage roadtrip (Opplæring)

- Bidragsytere er
  - Datatilsynet Difi
  - e-Helse Undervisningsdirektoratet

Fylkesvis:	Ant komm.	Komm. pmldt	Ant ikke	Påmeldte	%-vis påmeldt komm.
Østfold	19	13	6	44	68,4 %
Akershus	23	17	6	86	73,9 %
Oslo	1	1	0	10	100,0 %
Hedmark	23	12	11	37	52,2 %
Oppland	27	23	4	82	85,2 %
Buskerud	22	13	9	42	59,1 %
Vestfold	13	6	7	34	46,2 %
Telemark	18	15	3	93	83,3 %
Aust-Agder	16	16	0	75	100,0 %
Vest-Agder	16	14	2	54	87,5 %
Rogaland	27	25	2	171	92,6 %
Hordaland	34	24	10	101	70,6 %
Sogn og Fjordane	27	13	14	28	48,1 %
Møre og Romsdal	37	23	14	68	62,2 %
Sør-Trøndelag	26	19	7	153	73,1 %
Nord-Trøndelag	24	14	10	38	58,3 %
Nordland	45	29	16	105	64,4 %
Troms	25	21	4	100	84,0 %
Finnmark	21	17	4	114	81,0 %
HELE LANDET	444	315	129	1435	70,9 %

Hele 118 rådmenn i to dager om personvern og informasjons-sikkerhet

NYPE
nye personvernregler

Kursinnhold dag 1

- 09:00 Åpning
- 09:15 Hva er personvern, Datatilsynet og det nye regelverket
- 09:45 Grunnleggende jus + *Øvelse*
- 10:30 Pause
- 10:40 Rettigheter
- 12:00 Lunsj
- 13:00 Ansvarlighet, systematikk og informasjonssikkerhet + *Øvelse*
- 14:00 Pause
- 14:15 Personvernombud etter nytt regelverk
- 15:15 Kort om andre nyheter + *Øvelse*

NYPE
nye personvernregler

Kursinnhold dag 2

- 09:00 Åpning
- 09:10 Styring og kontroll - + Øvelse Difi
- 10:30 Beinstrekk
- 10:40 Risikovurdering og skole - Utdanningsdirektoratet
- 11:30 Pause med pausemat
- 11:50 Risikovurdering fortsetter
- 12:15 Beinstrekk
- 12:30 Databehandleravtale/ leverandøroppfølging - Utdanningsdirektoratet
- 13:00 Lunsj
- 14.00 Helse – e-helse
- 14:50 Beinstrekk
- 15.00 Oppsummering og KAHOOT

NYPE
nye personvernregler

Uoffisiell norsk lovtekst
- og offisiell engelsk

- Linken til denne finner dere ved å gå inn på
  facebook.com/kins.no
  .... dere kan jo følge oss samtidig
- youtube.com
  - Søk etter Foreningen KiNS
- Narvestad-videoen til e-helse

NYPE
nye personvernregler

Og nå over til...

- Fagdirektør Ove Skåra – Datatilsynet

Ny personvernlovgivning fra 2018

2

Forum for kontroll og tilsyn, 21. mars 2018

Ove Skåra - Datatilsynet

Datatilsynet

IT-sikkerhetssjef i Atea, Thomas Tømmernes.

De som ikke har fått med seg dette risikerer bøter på inntil 20 millioner euro

Bare to prosent av bedriftsledere har satt seg inn i EUs nye personvernregler som innføres til neste år.

TU STORY LABS Dette er en annonse. Journalistene i Tu.no er ikke involvert i produksjonen.

Norske bedrifter er dårlig forberedt på personvernlov

En av fire selskaper er ikke forberedt på den nye personvernloven, viser en undersøkelse.

Agenda

- Litt om status i norske kommuner
- Bakgrunn for nye personvernregler
- Hva er personvern og personopplysninger
- De viktigste endringene i ny lovgivning
- Hva kan kontrollutvalgene bidra med?

Hvor trykker skoen?

- Manglende oversikt over egne behandlinger
- Hull i kunnskapen om innsyn og informasjon
- Manglende eller for dårlige risikovurderinger
- Usikkerhet knyttet til konfigurasjonsstyring
- Vertskommuner i regionale samarbeid er ikke alltid bevisst sin rolle som databehandler for de øvrige kommunene
- Databehandleravtaler
- Publisering og postlister

Personvernforordningen – GDPR – personopplysingsloven

Bakgrunn – personvernregelverket

Personopplysningsloven 2001

Nye norske personvernregler 2018

Personregisterloven 1978

EUs personverndirektiv 1995

EUs personvernforordning 2016

16

Personopplysninger og høstes og analyseres..

Nye rammer for behandling av personopplysninger! (EU 2016/679)

- **Hvorfor?**
  - ✓ Styrke den europeiske borgers rettigheter
  - ✓ Gjøre det lettere å utveksle personopplysninger over landegrensene
  - ✓ Sikre samarbeid mellom personvernmyndigheter
  - ✓ Styrke tilliten til digitale tjenester

- **Hvordan?**
  - ✓ Gjennom en forordning
  - ✓ Erstatter nasjonal lovgivning
  - ✓ Direkte gjeldende i EU/EØS
  - ✓ Begrenset spillerom for nasjonale tilpasninger

Mye videreføres og noe er helt nytt

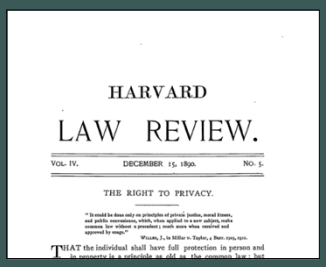
For de registrerte

- Informasjon og samtykke
- Innsynsrett
- Korrigering – og informere tredjeparter
- Retten til å bli glemt - sletting
- Retten til begrenset behandling
- Innsigelsesrett
- Retten til dataportabilitet
- Rett til å nekte profilering og automatiserte avgjørelser
- Barn gis styrkede rettigheter

For virksomhetene:

- Likere regler i Europa
- Virksomheter skal kunne forholde seg til en personvernmyndighet
- Melde- og konsesjonsplikt faller bort
- Ansvarlighetsprinsippet – mer selvstendighet og ansvar
- Kraftigere økonomiske sanksjoner og mulighet for gruppesøksmål
- Databehandlere får flere plikter
- Personvernombud blir obligatorisk for mange
- Krav om innebygd personvern og personvern som standardinnstilling
- Plikt til å utrede personvernkonsekvenser
- Plikt til å rapportere sikkerhetsbrudd til Datatilsynet og til å informere de berørte

19



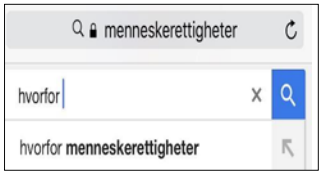
HARVARD
LAW REVIEW.
VOL. IV. DECEMBER 15, 1890. NO. 5.
THE RIGHT TO PRIVACY.

Hva er person(opplysnings)vern og noen definisjoner

Personopplysninger – mer enn du kanskje tror?

Ove Skåra
Granåsen 72b
1362 Hosle
Tlf 917 917 97

Fødselsnummer: 090361 46271
IP-adresse: 195.159.103.82
Bilens registreringsnummer: BL 23456
Bluetooth MAC:
17:35:52:78:4B:CA
Wi-Fi-adresse MAC:
12:44:32:45:7B:C9
Autpass-brikke-ID:
7483920983278394
Vurderinger og profiler



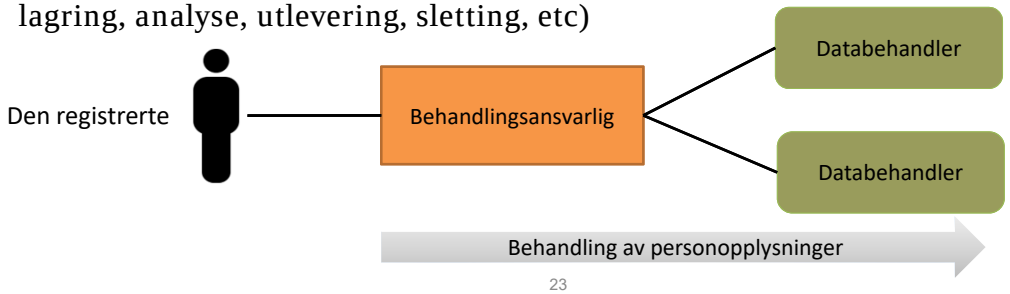
Hva er en sensitiv personopplysning?

Art. 9 og 10

- Særlige kategorier av personopplysninger
  - Rasemessig eller etnisk opprinnelse
  - Politisk oppfatning, religion, overbevisning
  - Fagforeningsmedlemskap
  - Genetiske opplysninger
  - Biometriske opplysninger med det formål å entydig identifisere en fysisk person
  - Helseopplysninger
  - Seksuelle forhold eller seksuell orientering
- Personopplysninger om straffedommer og lovovertredelser

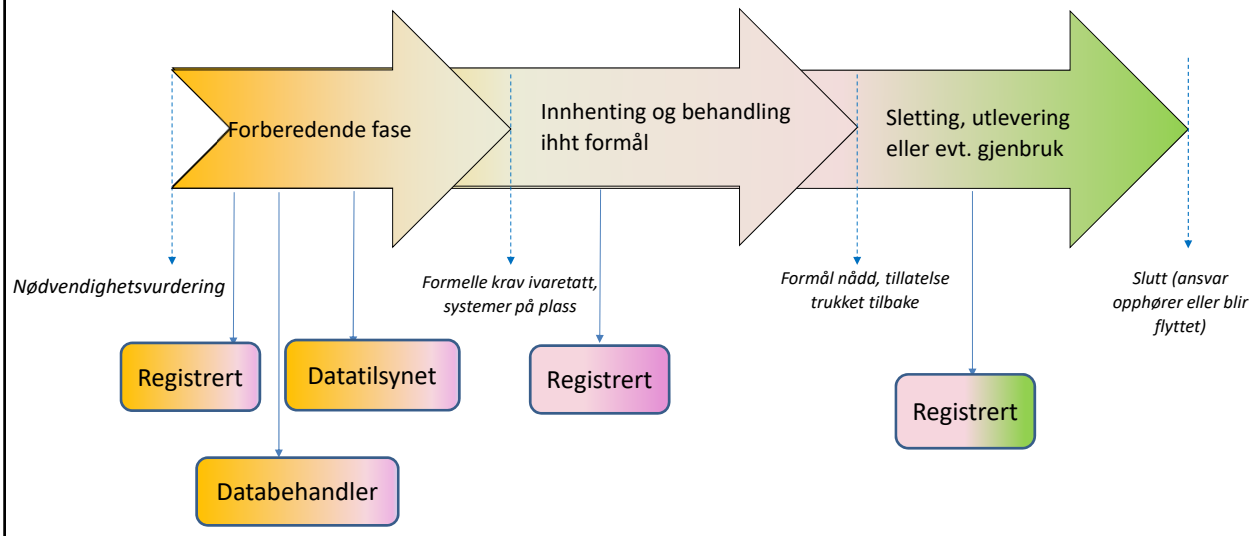
Noen andre begreper

- **Den registrerte:** Enkeltperson som det behandles personopplysninger om
- **Behandlingsansvarlig:** Virksomheten som bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes
- **Databehandler:** Virksomhet som behandler personopplysninger på vegne av, og etter avtale med behandlingsansvarlig
- **Behandling (av personopplysninger):** Enhver prosessering (innhenting, lagring, analyse, utlevering, sletting, etc)



23

Personopplysninger har et livsløp



24

Gamle personvernprinsipper i ny drakt

Lovlig, rimelig og gjennomsiktig
Opplysningene skal behandles lovlig, rimelig og på en gjennomsiktig måte. Respekter de registrertes interesser og rimelige forventninger. Informasjon skal gis på en tilgjengelig og forståelig måte.

Formålsbegrensning
Opplysningene skal brukes til uttrykkelig angitte og legitime formål. Opplysningene skal ikke brukes til andre uforenlige formål.

Dataminimering
Personopplysningene skal være tilstrekkelige, relevante og begrenset til hva som er nødvendig for formålet.

Korrekte og oppdaterte
Opplysningene skal være korrekte og om nødvendig ajourførte. Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes.

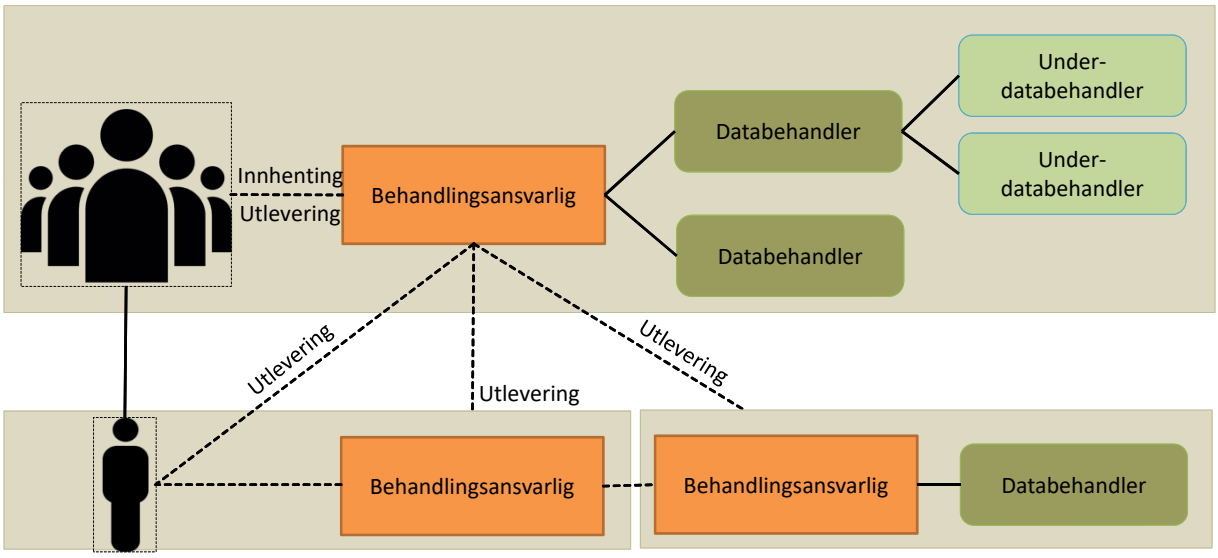
Rutiner for lagring og sletting
Det skal være rutiner som sikrer at det ikke er mulig å identifisere de registrerte lenger enn hva som er nødvendig for de formål de er samlet inn for.

Integritet og konfidensialitet
Personopplysninger sikres mot uautorisert eller ulovlig tilgang og mot utilsiktet tap, ødeleggelse eller skade. Det skal brukes egnede tekniske og organisatoriske tiltak.

Ansvarlighet
Den behandlingsansvarlige har ansvar for, og må kunne dokumentere, at personvernprinsippene blir etterlevd.

(Artikkel 5)

Behandlingsansvarlig, databehandler og tredjeparter



26

Lovlig behandling (krav til behandlingsgrunnlag)

Art. 6

a) Samtykke
b) Nødvendig for å inngå kontrakt (med den registrerte)
c) Nødvendig for å oppfylle en rettslig forpliktelse
d) Nødvendig for å verne den registrertes vitale interesser
e) Nødvendig for å utføre en oppgave i offentlighetens interesse eller utøve offentlig myndighet
f) Nødvendig for formål knyttet til rettmessige interesser (interesseavveining)

NB!

Interesseavveiing er ikke aktuelt behandlingsgrunnlag for behandling av personopplysninger som foretas av det offentlige for deres oppgaveløsning

Datatilsynet

Noen sentrale rettigheter (med tilhørende plikter)

Retten til informasjon (hva)

Art. 13 og 14

- Kontaktdetaljer for behandlingsansvarlig
- Kontaktdetaljer for PVO
- Formål og behandlingsgrunnlag
  - Dersom interesseavveiing (art. 6 nr. 1 f) hva den berettigede interessen er
  - Rett til å trekke samtykke
- Eventuelle mottakere av opplysningene
- Overføring til tredjeland/internasjonal organisasjon og beskyttelsestiltak

Retten til informasjon (hva)

Art. 13 og 14

- Lagringstid og hva som avgjør lagringstiden
- Hvilke rettigheter man har
- Klagerett til Datatilsynet
- Automatiske avgjørelser som nevnt i art 22

- **Ny informasjonsplikt når behandling for nye formål**

- Kun art 13: Om det å gi fra seg opplysningene er obligatorisk ihht. lov eller kontrakt, og ev. konsekvenser av å ikke gi fra seg opplysningene
- Kun art 14: Opplysningenes kilde, de berørte personopplysningskategorier

Rett til informasjon (hvordan)

Art. 13 og 14

- Form
  - Kortfattet, gjennomsiktig, lett forståelig og lett tilgjengelig
  - "Layered notices"
  - "Just in time notices"
- Språk
  - Klart og enkelt
  - Tilpasset barn
- Skriftlig, elektronisk

NÅR?

✓Ved første gangs kommunikasjon med den registrerte,

✓eller ved første gangs utlevering til en tredjepart,

✓men senest innen en måned etter innhenting av dataene

= Mer åpenhet → økt tillit fra brukeren

Samtykke

Art. 6 nr. 1 a)

Frivillig

Reelt valg, ikke noe press, ingen negative konsekvenser av å si nei

Ikke frivillig hvis klar skjevhet mellom den registrerte og den behandlingsansvarlige (særlig hvis den behandlingsansvarlige er en offentlig myndighet)

Spesifikt

Mulig å gi særskilt samtykke til forskjellige behandlingsaktiviteter / formål

Informert

Informasjon om alle relevante sider av behandlingen (hva, hvem, hvorfor, hvor lenge, etc.

Utvetydig

Inaktivitet eller passivitet vil ikke kunne gi grunnlag for et lovlig samtykke

Dokumentert

Datatilsynet

Retten til innsyn

Art. 15

- Bekreftelse på om personopplysninger behandles
- Rett til tilgang til kopi
- Rett til informasjon om
  -formål og lagringstid
  -kategorier av opplysninger og hvor de stammer fra
  -mottakere
  -om automatiske avgjørelser, inkl. profilering
  -om opplysningene skal overføres til utlandet

  -retten til korrigering og sletting
  -retten til å klage til Datatilsynet

Retten til retting

Art. 16 og 19

- Opplysninger
  – Unøyaktige
- Rett til å få ufullstendige opplysninger komplettert ved å fremlegge en tilleggserklæring
- Skal gjøres uten ugrunnet opphold

Retten til sletting (å bli glemt)

Art. 17

- Ikke lenger er nødvendig for formålet
- Samtykket trekkes tilbake
- Ved innsigelser
- Personopplysningene er behandlet ulovlig
- Må slettes for å oppfylle en rettslig forpliktelse
- Opplysningene er samlet inn ifm. med barns bruk av informasjonssamfunnstjenester

Retten til begrenset behandling

Art. 18 og 19

- Den registrerte ønsker ikke at opplysninger skal slettes eller bestrider at opplysningene er korrekte
- Opplysningene kan KUN lagres
- Noen unntak:
  - med den registrertes samtykke,
  - for å forsvare et rettskrav,
  - for å forsvare en annens rettigheter
  - for å ivareta viktige samfunnsinteresser.

Virksomheten må informere tredjeparter

Art. 18 og 19

- Varsle tredjeparter som har mottatt personopplysningene dersom retting, sletting eller begrensing er etterkommet
- Unntak:
  - Umulig/uforholdsmessig vanskelig
  - Som et minimum, plikt til å oppgi identiteten til tredjepartsmottakere hvis den registrerte ber om det

37

Innsigelse – Retten til å motsette seg behandling

Art. 21

- Gjelder i tre situasjoner:
  - Nødvendig for offentlig myndighet eller oppgaver i allmenhetens interesse
  - Nødvendig for å vareta en berettiget interesse som veier tyngre enn den registrertes personvern
  - Formålet er direkte markedsføring
- Ved innsigelse skal behandlingen opphøre (sletting)
- Uttrykkelig gjøres oppmerksom på innsigelsesretten

Dataportabilitet

Art. 20

- Rett til å få utlevert opplysninger om **seg selv** som man har **gitt** til den behandlingsansvarlige
  - Samtykke
  - Nødvendig for avtale
- Rett til å overføre personopplysningene uten hinder
- Strukturert, alminnelig anvendt og maskinlesbar form

Automatiserte avgjørelser

Art. 22

- Fullt ut automatisert
- Avgjørelse med rettsvirkning eller på tilsvarende måte betydelig påvirker vedkommende
- **Hovedregel: Forbudt***
- Unntak
  - Nødvendig for å inngå eller gjennomføre en avtale med de registrerte
  - Hjemlet i lov *som samtidig gir tilfredsstillende garantier* for personvernet til de registrerte
  - Eksplisitt og gyldig samtykke

Noen nye plikter for virksomheten

Protokoll over behandlingsaktiviteter

Art. 30

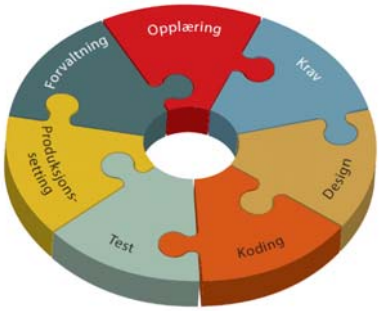
- Kontaktinformasjon til behandlingsansvarlig
- Formål
- Kategorier av registrerte og kategorier av personopplysninger
- Kategorier av mottakere
- Evt. overføringer til tredjeland eller internasjonale organisasjoner, og dokumentasjon på tilstrekkelig beskyttelse
- Tidsfrister for sletting
- Tekniske og organisatoriske sikkerhetstiltak

Formål med behandlingen	**Kategorier av registrerte**	**Kategorier av personopplysninger**	**Kategorier av mottakere** Hvis aktuelt også i tredjestater eller internasjonale organisasjoner	**Planlagte tidsfrister for sletting** Av de forskjellige kategorier av personopplysninger Hvis mulig	**Generell beskrivelse av tekniske og organisatoriske sikkerhetstiltak** Som nevnt i artikkel 32. nr 1 Hvis mulig
Lønnskjøring og utbetaling	Ansatte	Kontaktopplysninger	Regnskapsbyrået (lønnskjører)	x år etter avslutning av arbeidsforhold	Kryptert lagring og overføring
Lønnskjøring og utbetaling	Ansatte	Opplysninger om skattetrekk	Regnskapsbyrået (lønnskjører)	x år etter avslutning ar	Kryptert lagring og overføring

Innebygd personvern og personvern som standard

Art. 25

- Vær i forkant, forebygg fremfor å reparere.
- Gjør personvern til standardinnstilling.
- Bygg personvern inn i designet.
- Skap full funksjonalitet: Både-og, ikke enten-eller.
- Ivareta informasjonssikkerhet fra start til slutt.
- Vis åpenhet.
- Respekter den registrertes personvern.



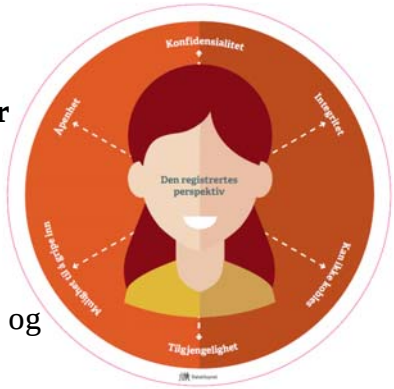
Oppsummert art 25:

- Obligatorisk
- Tekniske og organisatoriske tiltak.
- Sett det minst personverninngripende alternativet som standard, mht mengde, omfang, lagringstid, tilgjengelighet.
- Ivareta personvernprinsipper og den registrertes rettigheter.

43

Vurdering av personvernkonsekvenser (DPIA)

- En prosess for å **etterleve lovgivningen**, samt **demonstrere** etterlevelse (fortale nr. 84)
- I prosessen skal den behandlingsansvarlige **beskrive behandlingen**, **nødvendigheten** av behandlingen, **forholdsmessigheten** og **håndtere risikofaktorer** for enkeltpersoners rettigheter og friheter, og deretter vurdere og bestemme tiltak for å redusere risikoen.
- **Rettigheter**: art 12-22
- **Friheter**: retten til privatliv, men også retten til kommunikasjon, tanke- tros og religionsfrihet, ytrings- og informasjonsfrihet, jf. EMK.



44

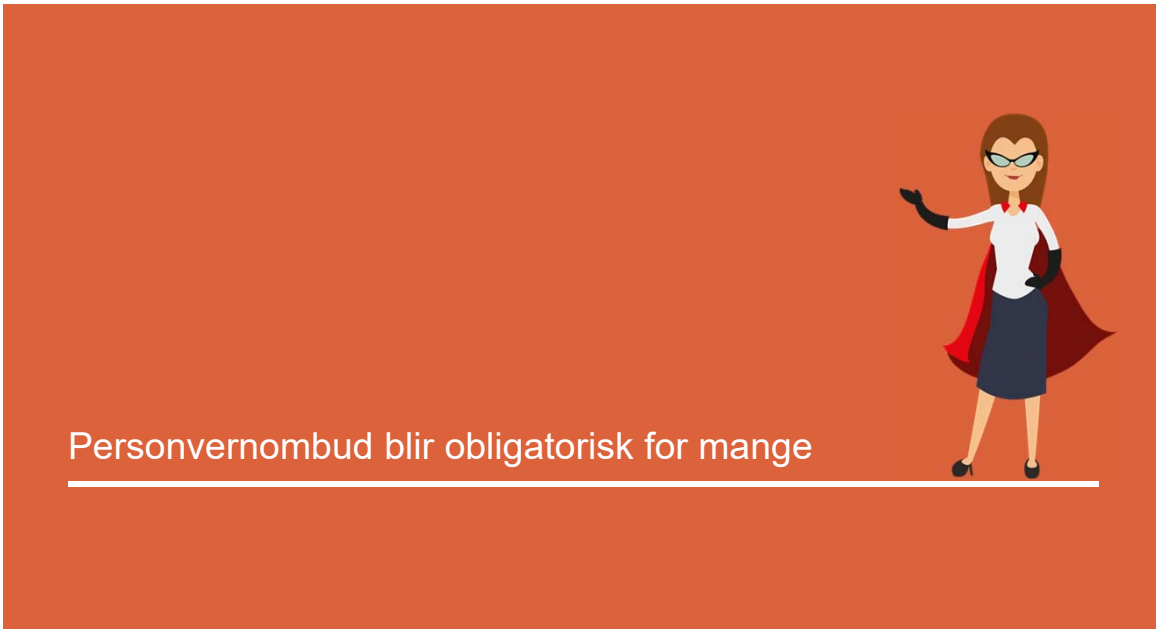
Hvilke behandlingsaktiviteter er omfattet av en DPIA?

«Dersom det er sannsynlig at en **type behandling**, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens **art, omfang, formål og sammenhengen den utføres i**, vil medføre en **høy risiko** for fysiske personers **rettigheter og friheter**, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.» (Art. 35.1)

+ typetilfeller i art. 35.3 og MÅ-liste i art. 35.4

- Hva er risikoen relatert til? → de registrertes rettigheter og friheter
- Hva skal ligge til grunn for vurderingen av om risikoen er høy?
  → type behandling (art, omfang, formål og kontekst)

45



Personvernombud (data protection officer)

Viktige endringer med GDPR

- Fremhevet og lovregulert
- Fra frivillig til obligatorisk for mange
- Skjerpede krav og tydeligere rolle

- Artikkel 37, 38 og 39
- Retningslinjer fra WP29

Hvem må ha?

- Alle offentlige virksomheter (unntatt domstoler)
- Virksomheter, som ledd i/konsekvens av sin kjerneaktivitet
  - regelmessig og systematisk monitorerer personer, eller
  - behandler sensitive personopplysninger eller opplysninger om straffbare forhold

  i stor skala.
- NB: Gjelder både behandlingsansvarlige og databehandlere
- De som ikke må kan opprette frivillig

47

Oppgaver

- Ha oversikt over behandlingsaktiviteter
- Involvere seg tidlig, informere og gi råd
- Kontrollere overholdelse av personvernregelverket og interne retningslinjer, deriblant ansvarsfordeling, opplæring, holdningsskapende tiltak mv,
- Gi råd og delta ved vurdering av personvernkonsekvenser (DPIA)
- Være kontaktpunkt for de registrerte
- Være et kontaktpunkt for, og samarbeide med Datatilsynet
- Skal ha en risikobasert tilnærming til sitt arbeide

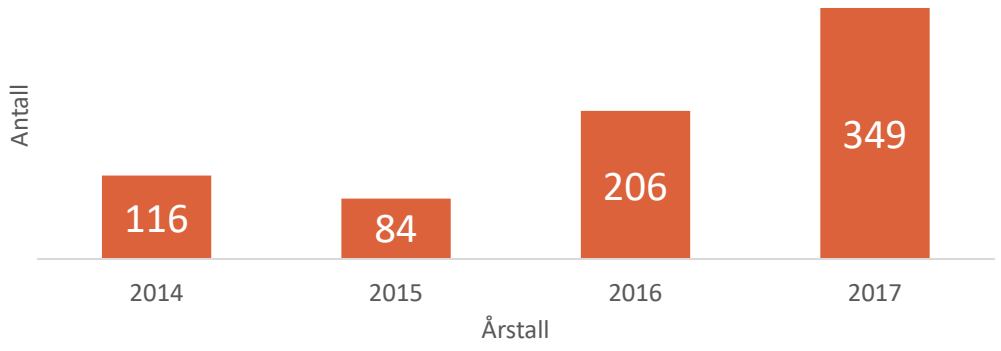
Mao: En viktig støttende funksjon for å sikre behandlingsansvarliges etterlevelse av kravene i personvernlovgivningen, men PVO overtar ikke behandlingsansvarliges rolle eller ansvar!

Art. 39

48

Avviksmeldinger til DT og informasjon til berørte

Antall registrerte avviksmeldinger de siste årene



Meldte avvik fra kommuner og fylkeskommuner i 2017

Bergen (4)
Tønsberg
Malvik
Melhus
Buskerud FK
Moss (2)
Luster
Vest Agder FK
Lyngdal
Oslo (2)
Kristiansand
Strand
Vadsø
Bodø
Farsund
Østfold FK (2)
Dovre
Nes
Trondheim
Nittedal
Rendalen
Jevnaker
Drammen
Odda
Bjugn
Ballangen
Sogndal

Meldte avvik kommunal sektor 01.01-09.03.2018

- Hordaland FK
- Lunner
- Ørland (2)
- Bergen (2)
- Stavanger
- Moss
- Songdalen
- Os (2)

Lørenskog (2)
Nes
Tønsberg (2)
Hordaland FK
Vadsø
Strand (4)

Og de som ikke feiler?

- Tromsø
- Lillehammer
- Fredrikstad
- Sandefjord
- Sandnes
- Bærum
- Osv.....

- Og 16 fylkeskommuner

Avviksmeldinger

Art. 33

Når må virksomheten sende melding om avvik til Datatilsynet?

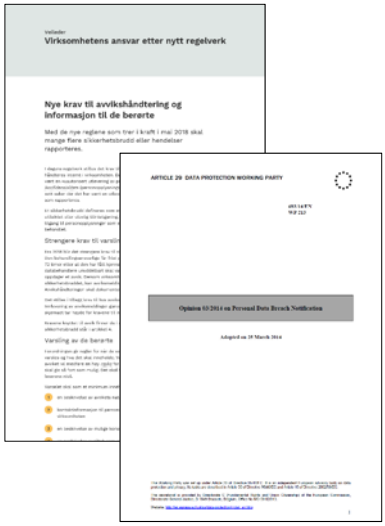
«Ved brudd på personopplysningssikkerheten ..., med mindre det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter.»

Ikke bare konfidensialitet, men også tilgjengelighet og integritet

Definisjon: *«brudd på personopplysningssikkerheten» - er et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet* (art. 4 (12))

53

Avviksmeldinger – art. 33 og 34



- Melde avvik innen 72 timer. Kan meldes trinnvis.
- Databehandler melder til behandlingsansvarlig
- Krav til innholdet i avviksmeldingen. Vårt skjema i Altinn tar høyde for dette.
- Berørte skal informeres så raskt som mulig, slik at de skal kunne foreta seg noe for å begrense skaden. (Noen unntak fra informasjonsplikt.)

54

Hvordan dokumentere ansvarlighet?

Ansvarlighet - ‘accountability’

Den behandlingsansvarlige er ansvarlig for og skal kunne påvise at personvernprinsippene overholdes. Artikkel 5 (2)

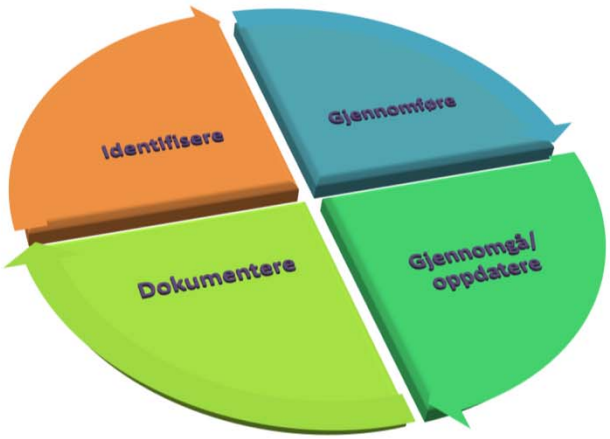
«gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. » Artikkel 24 (1)

Risikobasert tilnærming, som er viktig også i dagens regelverk, forsterkes i nytt regelverk.

Datatilsynet

56

Internkontrollplikt i art 24, 30, 32..



Identifisere
- Roller
- Opplysninger
- Formål
- Kilder
- Mottakere
- Begrensninger

Gjennomføre
- Tekniske tiltak
- Organisatoriske tiltak

Oppdatere
- DPIA
- Forhåndsdrøftelser

Dokumentere
- Jf. art 30
- Bransjenormer/ sertifisering

57

Har kommunen dokumentert kontroll på dette?

Internkontroll

- **Styrende** (gir føringer for arbeidet)
- **Utførende** (oversikt, risikovurderinger og rutiner)
- **Kontrollerende** (kontroll, gjennomgang, avvikshåndtering, evaluering)

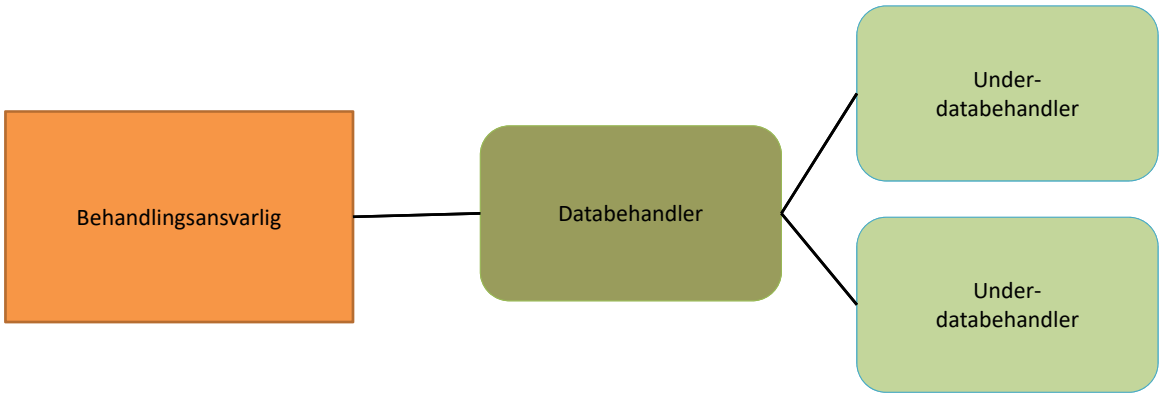
58

Eksempler på rutinebeskrivelser

- Rutiner for systematisk gjennomgang og sletting av personopplysninger
- Ivaretakelse av informasjonsplikten
- Innhenting av samtykke
- Rutiner for å oppdage, melde og håndtere avvik
- Hvordan håndtere krav om innsyn, retting og sletting
- Rutiner for varsling til tredjeparter
- Håndtering av retten til dataportabilitet
- Opplæring

59

Hold orden på databehandlerne



60

Lykke til!

- Datatilsynet
- Ove Skåra, fagdirektør
- Tlf 22 39 69 30
- Mobil 917 91 797
- Epost osk@datatilsynet.no

www.datatilsynet.no
www.personvernbloggen.no
Twitter.com/datatilsynet

Husk å abonnere på nyhetsbrevene fra Datatilsynet og personvernbloggen!

Rådmannens skrekk

62

Behandlingsoversikt eksempel

Tjeneste	Formål	Hjemmel	Person-opplysninger	Behandlings-ansvarlig	Databe-handler
Personalarkiv	Personal-forvalt.	Person-opplysnings-lov § 8	Personoppl	Kristin W	
Hjemmehjelp	Pasientjournal	Helsepersonell-lov § 39-40	Sensitive personoppl	Morten S	
Grunnskole	Spesial-undervisning	Opplæringslov § 5-1	Sensitive personoppl	Siw H	IST

Tips til behandlingsoversikt

- I tillegg til forordningskravene, vil det være fornuftig å inkludere:
  - Kobling mot fagsystemer
  - Hvem er databehandler
  - Link til databehandleravtalen i de tilfeller en databehandler er involvert
  - Link til samtykke i de tilfeller behandlingsaktiviteten er samtykkebasert
  - Link til DPIA-rapport og ROS-analyse
  - Link til interne dokumentasjonssystemer, ressurssider for fagsystemet etc
- Behandlingsoversikten bør også:
  - Være i et strukturert format som gjør det mulig å publisere (deler av) behandlingsoversikten internt og eksternt
  - Mulig å gruppere og sortere ut fra ulike formål

Oversikt over personopplysninger i Bærum kommune

Format (digital(USB, CD), papir, system)	Leverandør/database handler	Behandlingsansvarlig (navn/kontaktinformasjon/tjenestested)			Orgkode	Formål med behandling	Behandling grunnlaghjemmel samtykke	Hvilke personopplysninger samles inn		Type behandling	Volum (hvor mange)	Oppbevaringstid på datarutiner for sletting	Databehandleravtale med leverandør	Geografisk plassering av eksternpersonell med tilgang til data	Plassering database	Overføringsmekanisme til land utenfor EU/EØS	Deles dataene internt i kommune	Utlevering av opplysninger til medlepart
		Navn på ansvarlig/data forvalter	Kontaktinformasjon	Tjenestested				Personopplysninger	Sensitive personopplysninger									
Eitens skole-ad	IST	Siv Herlistad	siv.herlistad@baerum.kommune.no	Grunnskole-avdelingen		Elevadmini-strasjon	Opplærings-loven §13-1	Personnummer, navn, adresse, telefon, epostadresse elev og foresatte. Karakterer, fravær, anmerkninger, vurderinger. Klassetilhørighet, fag, lærere.	Kan forekomme - helseopplysninger.	Elevadministrasjon	Skolekonsulenter, ledere, systemforvalter, DigIT - ca 200 personer	Ihht bevarings og kassasjonsvedtekten	Ikke nødvendig				til IAM, WebSak, Factum. Henter data fra LØP.	Itslearning, Conexus. Udir
Visma Kulturskol	Visma	Siv Herlistad	siv.herlistad@baerum.kommune.no	Grunnskole-avdelingen		Administrering av kommunens kulturskoletilbud.	Opplæringslov §13-6	Navn, adresse, telefon og epostadresse til elev og foresatt. Personnummer.	Nei	Administrasjon av Kulturskolen	Alle ansatte i Kulturskolen, ca 50 stk	Vi arkiverer planer og tilbud, resten slettes.	Ikke nødvendig				Nei	Nei
MS Skoleadmi	MS	Siv Herlistad	siv.herlistad@baerum.kommune.no	Grunnskole-avdelingen		Elevadministrasjon	Opplæringslov §13-1	Navn, adresse, telefon og epostadresse til elev og foresatt. Personnummer.	Kan forekomme	Elevadministrasjon	Benyttes kun av 2 rektorer ved Skarva og Sandvikstubakken	Ihht bevarings og kassasjonsvedtekten	Ikke nødvendig	on-premise lagring	on-premise	Nei	Nei	Nei
Kikora - Digital	Kikora	Siv Herlistad	siv.herlistad@baerum.kommune.no	Grunnskole-avdelingen		Opfylle kompetansemål i læreplan	Opplæringslov § 2-3	Feide-pålogging. Læringsdata - adaptiv læring. Lærer kan følge progresjon til elever i sin klasse	Nei	Opplæring	Lisenser for 2017/2018 - alle elever og lærere 5. - 10. trinn		Ja				Nei	Nei
Conexus Engag	Conexus	Siv Herlistad	siv.herlistad@baerum.kommune.no	Grunnskole-avdelingen		Kartleggingsprøver og kartleggingsverktøy	Opplæringslov § 2-3	Ansatte: Navn og fødselsnummer, skoletilhørighet, epost, feide, mobilnr. Elev: Navn og fødselsnummer, skole og gruppetrinn-tilhørighet, resultater av kartlegginger og vurderinger.	Nei	Kartlegging og vurdering av opplæring	Kommuneansatte for alle skoler	Data lagres 1 år	Ja	Norge - Conexus og Basefarm	Norge - Conexus og Basefarm	Nei	Nei, kun resultater pr skole	underleverandør - Basefarm. Henter opplysninger fra Eitens, fra høst 2018 - Tieto.
Clarity - Digital	Clarity	Siv Herlistad	siv.herlistad@baerum.kommune.no	Grunnskole-avdelingen		Opfylle kompetansemål i læreplan	Opplæringslov § 2-3	Feide-pålogging. Lagring av søkerdata	Nei	Opplæring	Lisenser for 2017/2018 - alle elever og lærere 5. - 10. trinn		Ja				Nei	Nei
Digital læringspl	Showbie	Siv Herlistad	siv.herlistad@baerum.kommune.no	Grunnskole-avdelingen		Kommunikasjon lærer - elev, vurdering av og for læring	Opplæringslov § 2-3	Feide-pålogging. Elevens navn og klassetilhørighet, lærer og klassetilhørighet. Elevens besvarelser, lærerens vurderinger	Kan være, i elevens besvarelser.	Opplæring og vurdering	Alle elever og lærere ved skoler som har nettbrett. Fra høsten 2018 vil det gjelde alle skoler.	Under etablering.	Ja. Kommer ny nå oppdatert med GDPR	Canada	Canada	Nei	Nei	Nei

E-post til 378 rådmenn

Hva er det viktigste for deg som øverste leder med hensyn til informasjonssikkerhet?

Steinar Nørstebø

Stort spenn, men to sider av samme sak

- **Rådmann 1:** At det må være enkelt for organisasjonen å gi ut korrekt informasjon så rask som mulig, helst så tilgjengelig at hvem som helst kan finne informasjonen når de selv trenger den. Vi må framstå som åpne, etterrettelige og gi god service og informasjon.
- **Rådmann 2:** At dét som skal være tilgjengelig er tilgjengelig for den som skal ha tilgang og utilgjengelig for alle andre.

Hva er rådmannens mareritt?

- «Jeg håper virkelig jeg unngår å havne i medienes søkelys på grunn av at kommunens systemer ikke fungerer og sensitiv informasjon om innbyggere med spesielle behov og kommunale rettigheter havner på avveie!»

Fredag 12. april 2013 NYHETER 3

FYLKESMANNEN I [redacted]
Sosial- og helseavdelingen

[redacted] kommune
v/Rådmannen

TILBAKEMELDING - TILBUD VED BEHOV FOR AKUTT PSYKIATRISK HJELP

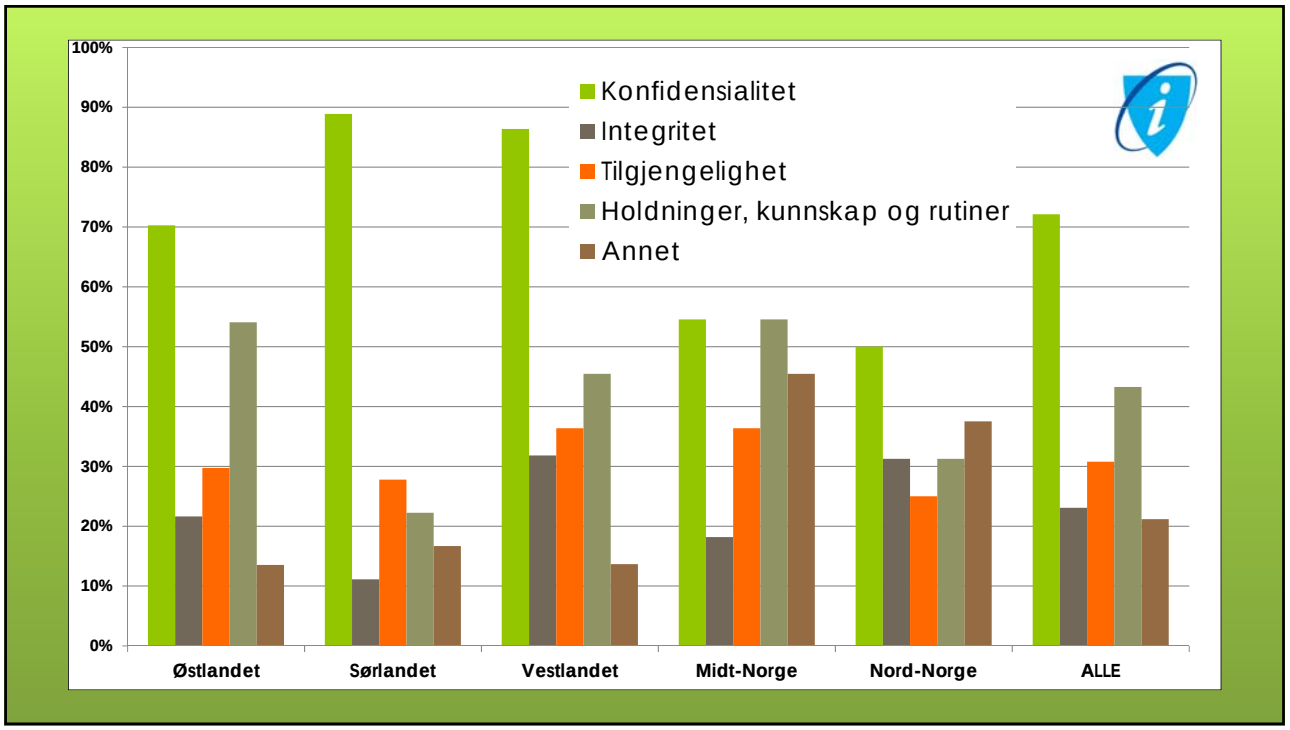
Fylkesmannen i [redacted] mottok den 21.01.13 brev fra [redacted] kommune.

Journalutskrift og rapport knyttet til en henvendelse fra en dypt fortvilet pasient med selvmordstanker og kjæresteproblemer ble i sin helhet publisert på kommunes postliste. Navn, adresse og fødselsdato på personen sto fullt leselig på et av vedleggene til hoveddokumentet. Brevet fra fylkesmannens helse- og sosialavdeling var merket unntatt offentlighet.

ALVORLIG AVVIK: [redacted] kommune publiserte sen
tatt offentlighet. [redacted] i kommunen [redacted]

La ut sensitive opplysninger

● Dokumentet var merket unntatt offentlighet, men kommunen publiserte det



Gullkorn fra rådmennene

- … men vi kan ikkje ha eit så strengt regime at informasjonsflyt blir hindra på tvers av etatar/ tenester som skal samarbeida til beste for brukaren (eks. barnevern)
- ….. at det er mulig for mine medarbeidere å forholde seg til de retningslinjer vi har for informasjonssikkerhet.
- Interne rutinar så ikkje opplysningar blir liggjande lett tilgjengelege på pc, skrivar, kopimaskin m.m.
- Persondata på avveie er ei krise for kommunen ***og for den som vert råka.***

Hva er informasjonssikkerhet?

- **Dette sier dere:**

Hjertesukk fra én rådmann:

- Mitt intuitive svar er «at våre brukere/innbyggere har en garanti for at personlig opplysninger om dem ikke kommer uvedkommende i hende». Eks informasjon i lege/pasientjournal.

… selv har jeg opplevd at ansatte hos min fastlege (i en annen kommune) har snoket i *min* legejournal.

Det var noe skikkelig dritt, selv om jeg ikke har noen spennende sykdommer…

- **KiNS-konferansen i Tromsø**
  12. – 13- juni 2018
  Topp foredragsholdere
  Stort fagmiljø
  Mange leverandører
  Tur til Sommarøy
  Midnattssol