GDPR-status fra en kommune

«Hvordan har vi det med etterlevelsen i dag?»

NKRF fagkonferanse
Hamar, 13.06.2019

Knut J. Eggen, Personvernombud
Sarpsborg kommune

Hvor gyldig er mitt «værvarsel»?

Kort om Sarpsborg

- Norges 10. største by – 56.000 innbyggere
- Lave inntekter og eldrebølge
- Mottiltak: Innovasjon og utvikling
- 4.100 kommunalt ansatte
- Budsjett 2020: 3.1 mrd.

Kilde: https://upload.wikimedia.org/wikipedia/commons/8/81/Sarpsborg_r%C3%A5dhus.jpg

Kort om Knut

- Yrkesaktiv i 30 år hittil
  - IT-drift og -ledelse
  - Salg og rådgivning
  - «Kommunemann»

  - Roller i Sarpsborg kommune:
    - Rådgiver IKT-strategi
    - Personvernombud
    - Sikkerhetsansvarlig
    - Prosjektleder digitalisering

Akademiske krumspring

- 2013 – 2016: Erfaringsbasert Master i IT og ledelse

- Oppgave i Ledelse av informasjonssikkerhet
  «Hvorfor har vi så få avvik på informasjonssikkerhet og personvern?»

- Masteroppgave 2016
  «Kompetanse om informasjonssikkerhet og personvern i grunnskolen - En casestudie fra en kommune»

25. mai som ble 20. juli

«Nå blir det bøter på 4 % av omsetningen! Kommunens budsjett er 3 mrd…»

«Dere må kjøpe vår programvare for å være compliant.»

«Nå blir det forbudt å håndtere sensitive personopplysninger!»

«Hvordan skal vi klare å få oversikt?»

«Dette er så komplisert at dere må kjøpe tjenester fra oss.»

«Hvordan skal vi sikre at alle får nødvendig opplæring?»

«Nå kommer ALLE til å be om innsyn i ALT vi har lagret…. :-O»

En god start er viktig

Sigmund Falch (født 21. april 1965[1] i Kongsberg) er en norsk regissør, manusforfatter og forfatter.
Mer om forfatteren på https://sigmundfalch.no Bildet er gjengitt med eksplisitt (og festlig) tillatelse gitt av forfatteren.

Vårt GDPR-prosjekt

- Fulgte i stor grad anbefalingene fra Datatilsynet

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

Kilde: www.datatilsynet.no

Personvernombudets bekymring

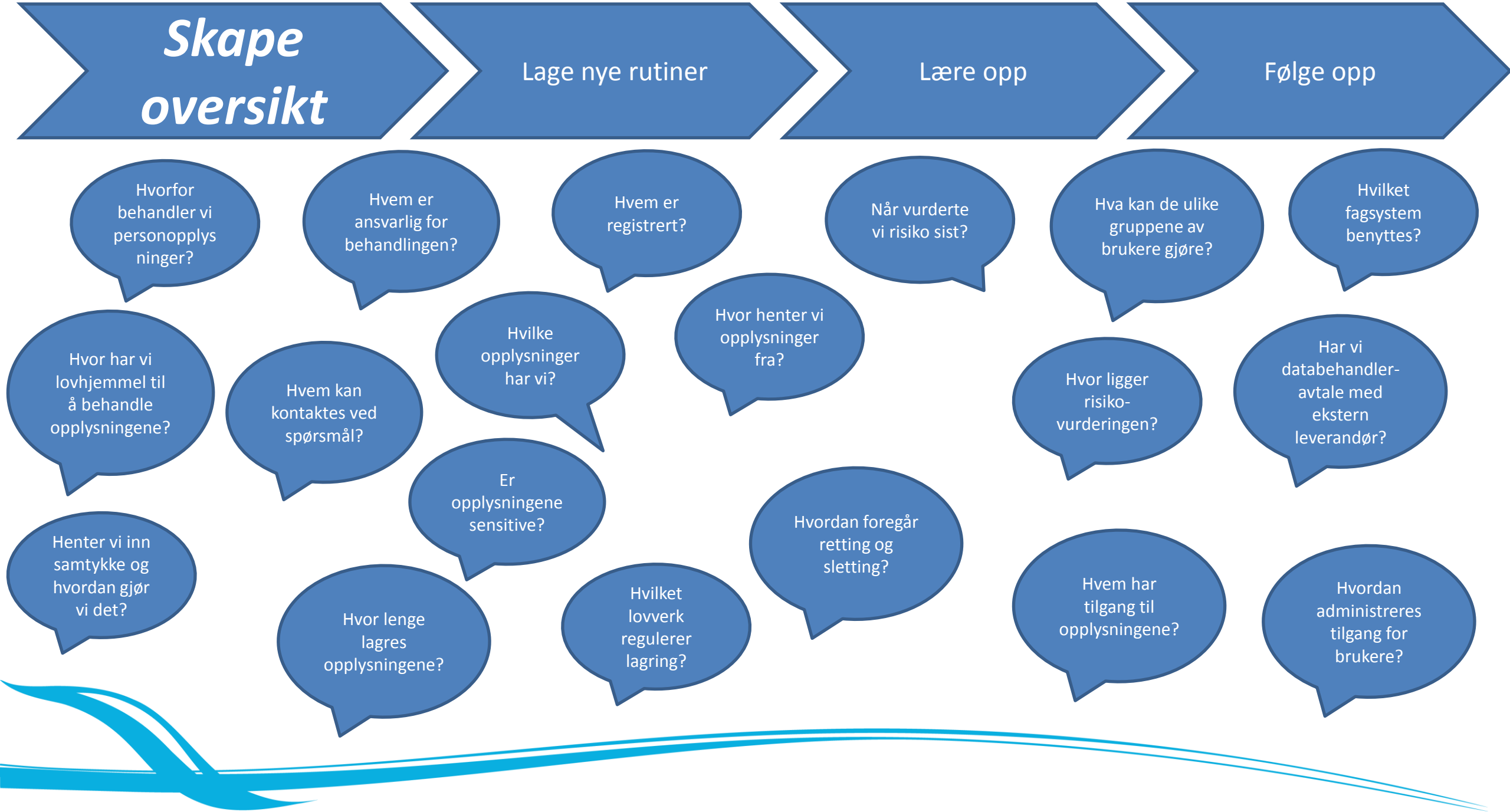
(Basert på akademiske studier og flere års observasjon)

Kommunen er til dels…

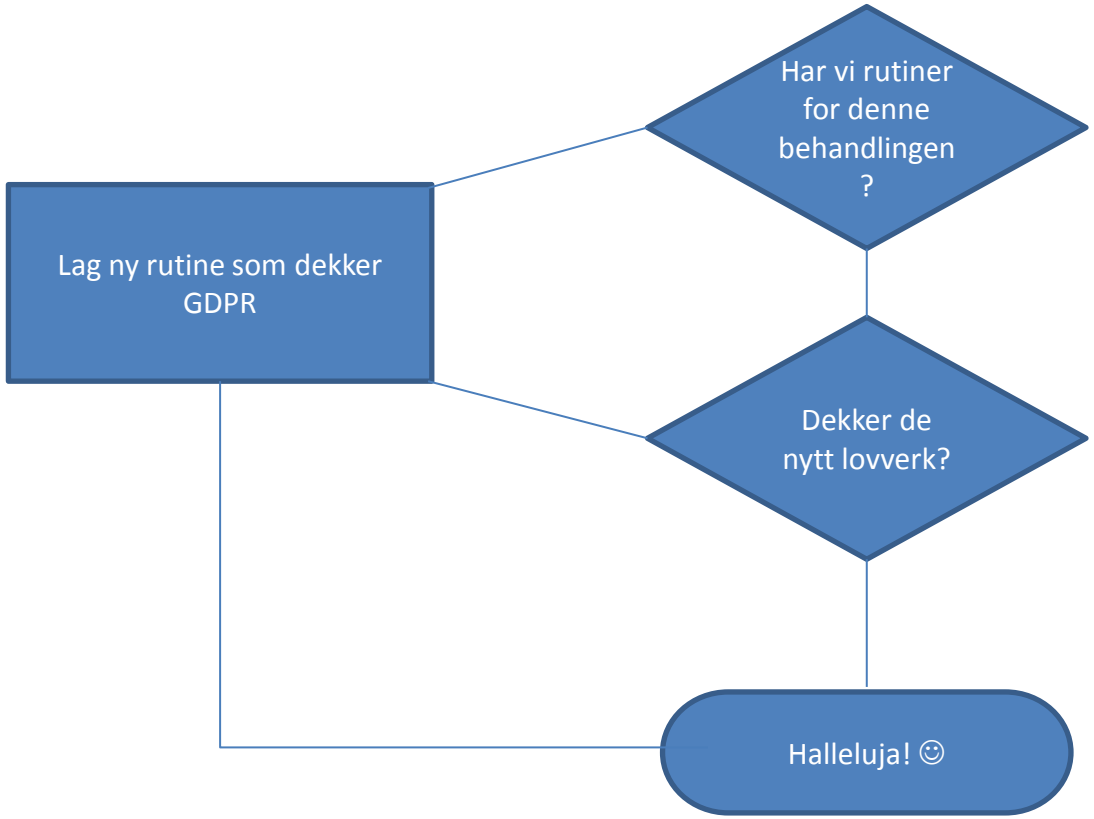
G anske **D** årlige **P** å **R** isiko

Prosjektet

- Skape oversikt
- Lage nye rutiner
- Lære opp
- Følge opp


Skape oversikt
Lage nye rutiner
Lære opp
Følge opp
Hvorfor behandler vi personopplys ninger?
Hvem er ansvarlig for behandlingen?
Hvem er registrert?
Når vurderte vi risiko sist?
Hva kan de ulike gruppene av brukere gjøre?
Hvilket fagsystem benyttes?
Hvor har vi lovhjemmel til å behandle opplysningene?
Hvem kan kontaktes ved spørsmål?
Hvilke opplysninger har vi?
Hvor henter vi opplysninger fra?
Hvor ligger risiko-vurderingen?
Har vi databehandler-avtale med ekstern leverandør?
Er opplysningene sensitive?
Henter vi inn samtykke og hvordan gjør vi det?
Hvordan foregår retting og sletting?
Hvor lenge lagres opplysningene?
Hvilket lovverk regulerer lagring?
Hvem har tilgang til opplysningene?
Hvordan administreres tilgang for brukere?

Skape oversikt → **Lage nye rutiner** → Lære opp → Følge opp



Krav til dokumentasjon

Etter GDPR bør det foreligge dokumentasjon på:

- Protokoll (register) over beh.aktiviteter (behandlings-oversikt) (se artikkel 30)
- Informasjonssikkerhet og rutiner for å ivareta sikkerheten for personopplysninger
- Brudd på personopplysnings-sikkerheten og utbedringstiltak
- Rutine for varsling ved brudd på personopplysningssikkerheten
- Egnede tekniske og organi-satoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med regelverket, herunder risikovurdering
- Vurdering av personvernkonsekvenser
- Rutiner for hvordan behandlingens lovlighet sikres, som lovlig behandlingsgrunnlag (herunder sikring av samtykke, interesseavveining mv.), samt for særlige kategorier opplysninger, og sikring av at behandlingen kun skjer innenfor og så lenge formålet for innsamlingen av opplysningene foreligger
- Rutine for oppstart og opphør av behandling av personoppl., herunder at behandlingen skal inntas i behandlingsoversikten, se nedenfor, hvem som beslutter behandling, hvilke plikter som foreligger ved behandlingen mv.
- Rutiner for å sikre personoppl. riktighet, dvs. hvordan person-opplysningene oppdateres, rettes, endres og slettes (når relevant)
- Rutiner for hvordan lagrings-begrensning, herunder når sletting, psedonymisering og anonymisering skal gjøres og hvordan dette skal gjøres.
- Rutiner for informering av registrerte
- Rutiner for at rettighetene til de registrerte blir fulgt, som retten innsyn, retting og sletting, og hvordan krav om begrensning av behandling, innsigelsesrett og dersom de registrerte motsetter seg automatiserte individuelle avgjørelser, herunder profilering.
- Rutiner for dataportabilitet
- Rutiner for overholdelse av adferdsnormer og sertifisering
- Rutiner for bruk av databehandlere
- Rutiner for overføring av personopplysninger, herunder til land utenfor EU/EØS
- Rutiner for utpeking, stilling og oppgaver for personvernrådgiver
- Rutine for innsyn i arbeidstakers e-postkasse mv.

Dokumentasjon skal være skriftlig og på et klart og enkelt språk.

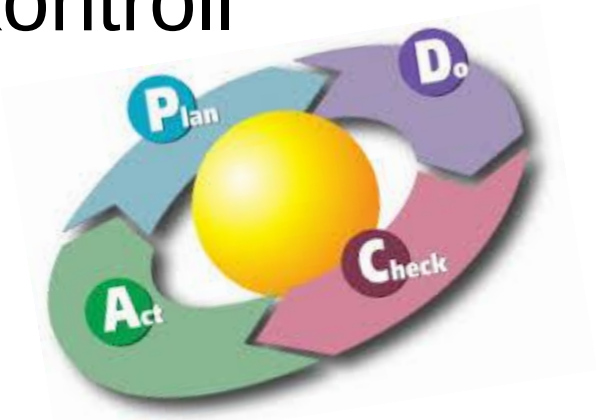
Artikkel 32 til 34, jf. 26, 28, 29, 71, 73, 75, 78, 83, 85, 86, 87, 88, 156.

Krav til dokumentasjon etter GDPR. Kilde: Teknologiadvokat Jan Sandtrø www.sandtro.no

Skape oversikt → Lage nye rutiner → ***Lære opp*** → Følge opp

Skape oversikt → Lage nye rutiner → Lære opp → ***Følge opp***

- Løpende bevissthetstrening
- Workshops, møter, nettverk
- Interne revisjoner
- Egenkontroll
- Fokus



Kilde: en.wikipedia.org

Prosjektet er ferdig; hva nå?

«Gjennom prosjektet har vi fått en god oversikt over behandling av personopplysninger i kommunen.

Vi har også revidert eksisterende retningslinjer og har laget noen nye.

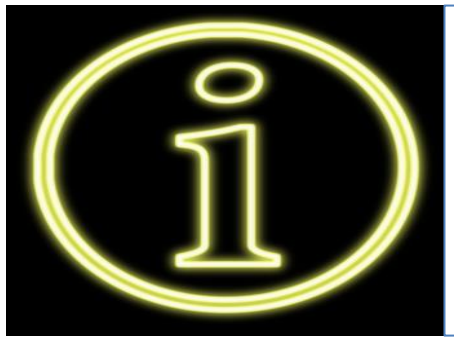
Samtidig ser vi at etterlevelse av det nye lovverket vil kreve mye. Det handler om kompetansebygging, rutiner og verktøy; å bygge en god sikkerhetskultur i Sarpsborg kommune.»

GDPR-veien videre

1. Bevissthet om behandlingsansvaret
2. Bygge mer kompetanse
3. Bygge god sikkerhetskultur
4. Sikre personvernombudets uavhengighet
5. Holde behandlingsoversikten levende
6. Ta eierskap til databehandleravtaler

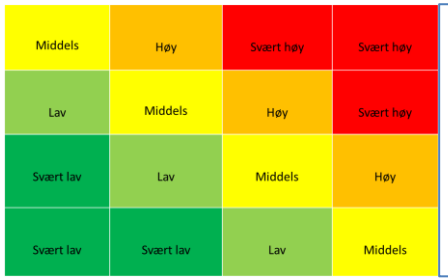
Så; hva er status?

All behandling av personopplysninger må være lovlig, rettferdig og gjennomsiktig



Innbyggere har krav på
Informasjon
Innsyn
Retting / Sletting
Begrensning

Vi må ha
oversikt over person-opplysningene



Vi må vurdere risiko og dokumentere vurderingene

Vi må ha tilstrekkelig sikkerhet, både teknisk og organisatorisk

Vi må melde alvorlige avvik til Datatilsynet innen 72 timer

1. Kvartal 2019

To reelle overskrifter og en fiktiv

sa.no

Prøv oss! 5 kr for 5 uker

SA:TV Podkast Direkte sport (+) Dødsannonser (+) Knut Joar Eggen | Meny

SARPSBORG KOMMUNE NYHET BARN OG UNGE

Årsoppgaven til to personer ble sendt til 21 sarpinger ved en feil

Av Vetle Granath Magelssen 25. januar 2019, kl. 09:24

Det oppstod en teknisk feil, da kemnerkontoret i Sarpsborg skulle sende ut årsoppgave for «pass og stell av barn», som gjelder for dem som har barn i barnehage og SFO i 2018.

Avviket meldt til Datatilsynet.
Årsak: Teknisk feil i Visma Enterprise

sa.no

Prøv oss! 5 kr for 5 uker

SA:TV Podkast Direkte sport (+) Dødsannonser (+) Knut Joar Eggen | Meny

Kommune-ansatt snoket i taushetsbelagte opplysninger

SNOKET: Den kommuneansatte snoket i kollegaers tilsettingsforhold. Foto: Jarl M. Andersen

Av Stina Mikalsen 05. februar 2019, kl. 14:20

Den ansatte har blant annet lest taushetsbelagte opplysninger som omhandler tre kollegers tilsettingsforhold.

Avviket meldt til Datatilsynet.
Årsak: Misbruk av tilganger til å gjøre oppslag uten tjenstlig behov

sa.no

Prøv oss! 5 kr for 5 uker

SA:TV Podkast Direkte sport (+) Dødsannonser (+) Knut Joar Eggen | Meny

Medarbeider tok med seg sensitive utskrifter hjem på siste arbeidsdag

Bare tilfeldigheter forhindret en personvernskandale i Sarpsborg kommune.

Avviket meldt til Datatilsynet.
Årsak: Brudd på interne rutiner / menneskelig svikt

Bedring, men ikke bra

	2016	2017	2018
Enheter som har gjort risikovurdering	20	19	34 (69 %)

Kommuneområde	Har behandlet avvik	Har gjort risikovurdering
Velferd	9 av 17 (53 %)	13 av 17 (76 %)
Oppvekst	8 av 25 (32 %)	14 av 25 (56 %)

Fanger vi opp alt som går galt?

	2012	2013	2014	2015	2016	2017	2018
Antall avvik totalt	1460	1127	1144	2285	1825	2306	2726
Personvern og info.sikk.	28	22	19	31	30	40	80

Velferd	Oppvekst	Teknisk	Samfunn	Organisasjon
64	8	1	0	7

Værmelding

Hva trekker i retning av godvær?

Jobben som er gjort hittil

Økende oppmerksomhet

Økende kompetanse

Økende erfaring

Økende samarbeid

Flere involverte

Hvilke truende skyer finnes i horisonten?

Kommuner er komplekse virksomheter
Økende digitalisering utfordrer personvernet
Temaet er omfattende og faguttrykkene mange

Spørsmål:
Hvordan lære opp både feieren, lederen og læreren?
Dokumenterer vi det vi skal?
Har vi tilstrekkelig forståelse for risiko?
Hvem ivaretar den behandlingsansvarliges plikter?
Hva når «alt» ligger i skyen?
Hva med alt som ikke ligger i fagsystemer?
Blir personvernombudet involvert?
…og mange fler…

Spørsmål? Innspill? Kommentarer?

knut.eggen@sarpsborg.com

924 19 408