INFORMASJONSSIKKERHET OG PERSONVERN

KOMMUNEDIREKTØRUTVALGET | MAI 2026

ERLEND KYDLAND FAANES

MINNER OM MANDATET

- GJENNOMFØRE OG OPPFØLGING AV FELLES ROS ANALYSER
- GJENNOMFØRE OG KVALITETSSIKRE FELLES PERSONVERNSKONSEKVENSVURDERINGER (DPIA)
- TILPASNING OG FORBEDRING AV KINS STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET OG PERSONVERN (PROSESS MED IKT AGDER)
- PLANLEGGING OG GJENNOMFØRING AV FELLES KOMPETANSETILTAK OG BEVISSTGJØRING I KOMMUNENE (MULIG 2027)
- INNFØRING AV BEHANDLINGSPROTOKOLLER OG INTERNKONTROLL SAMMEN MED KOMMUNENE (COMPILO 25/26)
- MÅLET ER Å SIKRE EN HELHETLIG OG KOORDINERT TILNÆRMING TIL GDPR OG INFORMASJONSSIKKERHET PÅ TVERS AV KOMMUNENE, SLIK AT REGIONEN STÅR STERKERE SAMLET I MØTE MED NYE KRAV, TILSYN OG DIGITALE TRUSLER.

Innføring av behandlingsprotokoller og internkontroll sammen med kommunene (Compilo 25/26)

Tilpasning og forbedring av KiNS styringssystem for informasjonssikkerhet og personvern (prosess med IKT Agder) 26/27

Et styringssystem sørger for at virksomheten jobber systematisk og kontinuerlig med sikkerhet og personvern – ikke tilfeldig eller bare når noe går galt.
Sikkerhetsloven §4-1 og virksomhetssikkerhetsforskriften §3

Et godt styringssystem gjør at ledelsen:

- vet hvilke risikoer virksomheten har,
- kan prioritere riktige tiltak,
- dokumenterer etterlevelse,
- og skaper trygghet for innbyggere, ansatte og samarbeidspartnere.

I kommunal sektor beskrives dette ofte som et kontinuerlig kretsløp:
Det viktigste er ikke store dokumentmapper, men at virksomheten faktisk har kontroll og jobber systematisk over tid.

En behandlingsprotokoll er en oversikt over hvordan en virksomhet behandler personopplysninger.

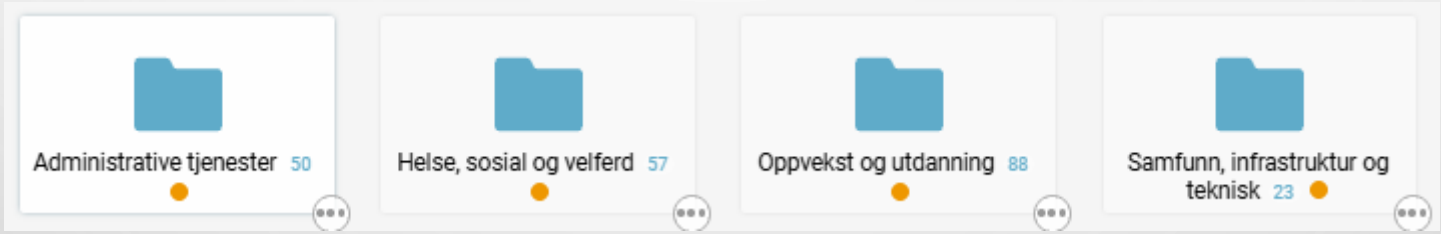
Den er et krav i personvernregelverket (GDPR artikkel 30), og fungerer som virksomhetens "kart" over behandlingene av personopplysninger.

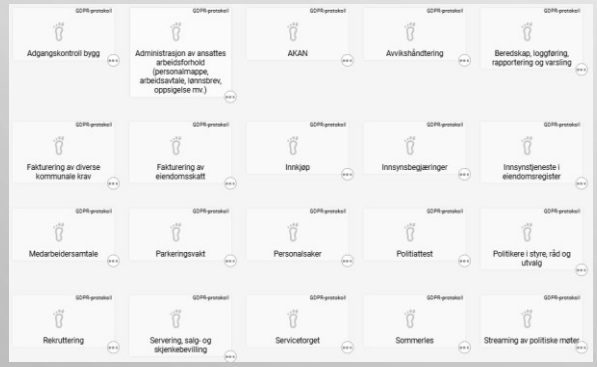
Typisk beskriver en behandlingsprotokoll:

- hvilke personopplysninger som behandles,
- hvorfor de behandles (formål),
- hvem opplysningene gjelder,
- hvilket rettslig grunnlag som brukes,
- hvem opplysningene deles med,
- hvor lenge de lagres,
- og hvilke sikkerhetstiltak som beskytter dem.

STATUS ARBEID

- BEHANDLINGSPROTOKOLLER:
  - INNFØRES ELLER ER INNFØRT I FØLGENDE KOMMUNER: (BLÅ= PÅBEGYNT, GRØNN=FERDIG)
    - ARENDAL, BYGLAND, BYKLE, EVJE OG HORNES, FROLAND, GJERSTAD, GRIMSTAD, IVELAND, RISØR, TVEDESTRAND, VALLE, VEGÅRSHEI, VENNESLA, ÅMLI





STYRINGSSYSTEM FOR INFORMASJONSSIKKERHET OG PERSONVERN (KINS)

- FORANKRET HOS KOMMUNENE (FLERE KOMMUNER HAR ALLEREDE TATT KINS SOM UTGANGSPUNKT I SITT ARBEID MED INFORMASJONSSIKKERHET OG PERSONVERN)
- VIKTIG AT IKT AGDER ER DELAKTIG I PROSESSEN, SIKRET GJENNOM SAMSTYRING PÅ TVERS OG KOMMENDE MØTE I REPRESENTANTSKAPET OG EIERMØTET.
- ETABLERT ARBEIDSGRUPPE: RONNY TELLEFSDAL SUNDE, JOHN HORVE, ERLEND KYDLAND FAANES, MARTE AARTHUN, RUNE OLSEN (PT).
- BEREDSKAP ER FØRSTE TENKTE OMRÅDE (BEREDSKAPSPLAN IT, SÅRBARHETSKARTLEGGING MED MER).

DATATILSYNET

- DATATILSYNET GJENNOMFØRER I 2026 NYE KOMMUNERUNDER
  - SPØRRESKJEMA → ALLE NORGES KOMMUNER
  - BOKTILSYN → 11 AV 14 IKT AGDER KOMMUNER
  - STEDLIG TILSYN → UKJENT PER NÅ ?
  - BISTÅTT KOMMUNENE I SVAR OG KOORDINERING MED IKT AGDER.

Datatilsynet

Spørreskjema om ivaretakelse av personopplysningssikkerhet

Viktig at dere leser «støtteteksten» (tekstbokser) gjennom hele dokumentet. Avkrysning er satt i lys av «Grimstad kommunes». Status er per nå.

Dere må selv ta stilling til om dette er gjeldende status hos egen kommune.

1. Generelt om kommunen

Navn på kommunen:

Grimstad kommune

Er kommunen en del av et formelt samarbeid knyttet til ivaretakelse av informasjonssikkerhet og personvern?

(•) Ja ( ) Nei

Hvis ja, angi hvilke samarbeid:

KiNS, KommuneCert, Norm for informasjonssikkerhet, KS, KS Fagråd f

2. Overordnet felles styringssystem for informasjonssikkerhet og personvern

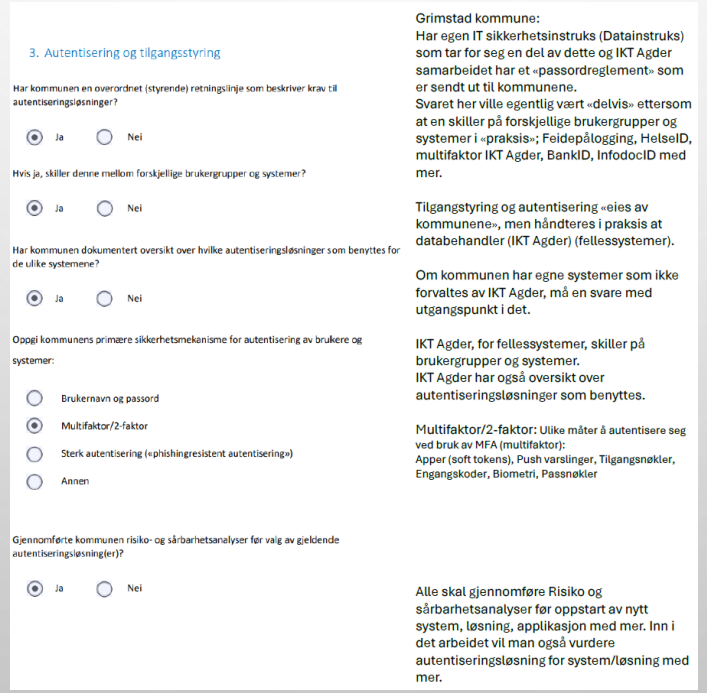
Har kommunen et etablert styringssystem for å ivareta arbeidet med informasjonssikkerhet og personvern?

( ) Ja ( ) Nei (•) Delvis

- KS (Støtteverktøy, malverk, dokumentasjon med mer.)
- KS Fagråd for informasjonssikkerhet og personvern
- KiNS (Foreningen kommunal informasjonssikkerhet). Dere må undersøke medlemskap)
- IKT Agder samarbeidet
- Andre?

Grimstad kommune:
Har en god del dokumentasjon, rutiner og overordnede retningslinjer på feltet. Men mangler et «fult» styringssystem for informasjonssikkerhet og personvern. Dette gjelder nok de fleste kommuner.

Det arbeides med å tilby KiNS styringssystem for kommunene i løpet av 2026/2027 og er også noe IKT Agder ser på.



3. Autentisering og tilgangsstyring

Har kommunen en overordnet (styrende) retningslinje som beskriver krav til autentiseringsløsninger?

(•) Ja ( ) Nei

Hvis ja, skiller denne mellom forskjellige brukergrupper og systemer?

(•) Ja ( ) Nei

Har kommunen dokumentert oversikt over hvilke autentiseringsløsninger som benyttes for de ulike systemene?

(•) Ja ( ) Nei

Oppgi kommunens primære sikkerhetsmekanisme for autentisering av brukere og systemer:

( ) Brukernavn og passord
(•) Multifaktor/2-faktor
( ) Sterk autentisering («phishingresistent autentisering»)
( ) Annen

Gjennomførte kommunen risiko- og sårbarhetsanalyser før valg av gjeldende autentiseringsløsninger(er)?

(•) Ja ( ) Nei

Grimstad kommune:
Har egen IT sikkerhetsinstruks (Datainstruks) som tar for seg en del av dette og IKT Agder samarbeidet har et «passordreglement» som er sendt ut til kommunene.
Svaret her ville egentlig vært «delvis» ettersom at en skiller på forskjellige brukergrupper og systemer i «praksis»; Feidepålogging, HelseID, multifaktor IKT Agder, BankID, InfodocID med mer.

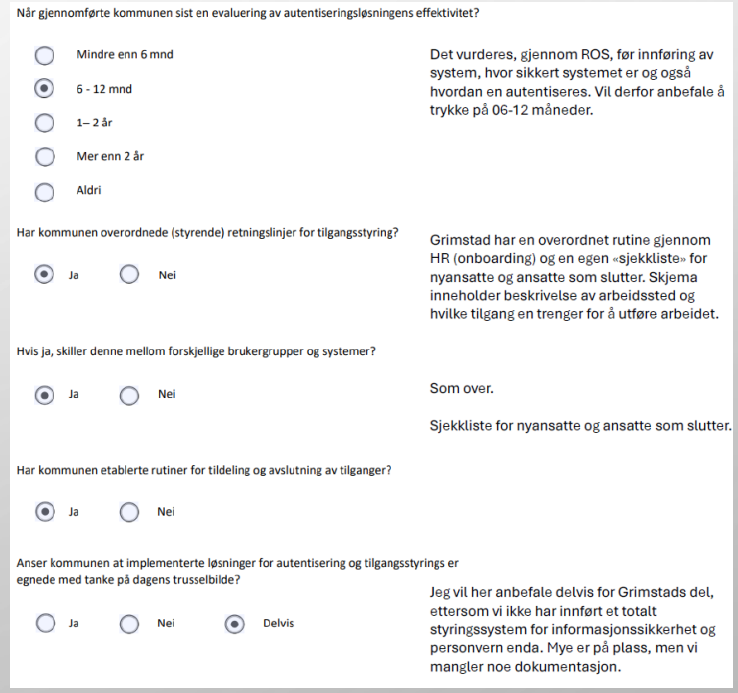
Tilgangstyring og autentisering «eies av kommunene», men håndteres i praksis at databehandler (IKT Agder) (fellessystemer).

Om kommunen har egne systemer som ikke forvaltes av IKT Agder, må en svare med utgangspunkt i det.

IKT Agder, for fellessystemer, skiller på brukergrupper og systemer.
IKT Agder har også oversikt over autentiseringsløsninger som benyttes.

Multifaktor/2-faktor: Ulike måter å autentisere seg ved bruk av MFA (multifaktor):
Apper (soft tokens), Push varslinger, Tilgangsnøkler, Engangskoder, Biometri, Passnøkler

Alle skal gjennomføre Risiko og sårbarhetsanalyser før oppstart av nytt system, løsning, applikasjon med mer. Inn i det arbeidet vil man også vurdere autentiseringsløsning for system/løsning med mer.



Når gjennomførte kommunen sist en evaluering av autentiseringsløsningens effektivitet?

( ) Mindre enn 6 mnd
(•) 6 - 12 mnd
( ) 1– 2 år
( ) Mer enn 2 år
( ) Aldri

Det vurderes, gjennom ROS, før innføring av system, hvor sikkert systemet er og også hvordan en autentiseres. Vil derfor anbefale å trykke på 06-12 måneder.

Har kommunen overordnede (styrende) retningslinjer for tilgangsstyring?

(•) Ja ( ) Nei

Grimstad har en overordnet rutine gjennom HR (onboarding) og en egen «sjekkliste» for nyansatte og ansatte som slutter. Skjema inneholder beskrivelse av arbeidssted og hvilke tilgang en trenger for å utføre arbeidet.

Hvis ja, skiller denne mellom forskjellige brukergrupper og systemer?

(•) Ja ( ) Nei

Som over.

Sjekkliste for nyansatte og ansatte som slutter.

Har kommunen etablerte rutiner for tildeling og avslutning av tilganger?

(•) Ja ( ) Nei

Anser kommunen at implementerte løsninger for autentisering og tilgangsstyrings er egnede med tanke på dagens trusselbilde?

( ) Ja ( ) Nei (•) Delvis

Jeg vil her anbefale delvis for Grimstads del, ettersom vi ikke har innført et totalt styringssystem for informasjonssikkerhet og personvern enda. Mye er på plass, men vi mangler noe dokumentasjon.

Faanes, Erlend Kydland 12.5. 15:08 Redigert

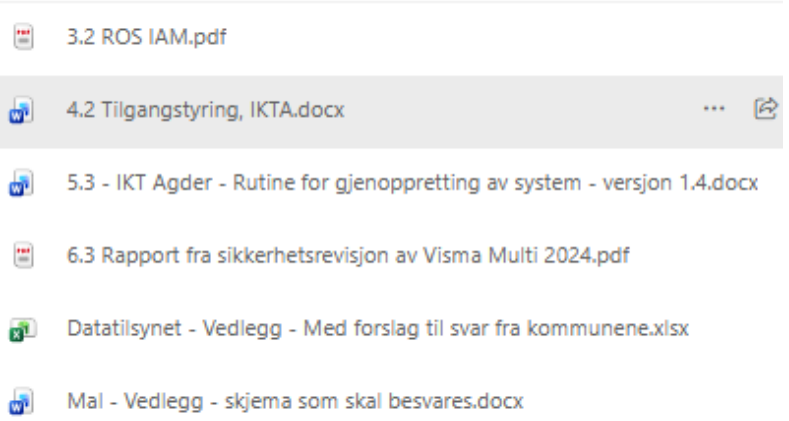
Datatilsynet - utgangspunkt til "forslag til svar fra kommunene"

hei Informasjonssikkerhet for kommunene i IKT Agder samarbeidet,

Vedlagt ligger en Excel fil som alle kan benytte i sitt arbeid med svar til Datatilsynet. Per nå er det fylt ut litt av undertegnede og Risør kommune v/Ståle Sjaavaag. Har lagd en fane til hver kommune bortover, slik at alle som ønsker det kan fylle inn og se hva de andre skriver. håper det kan være til hjelp i egen besvarelse. Dette er også gjort med tanke på å koordinere med IKT Agder. Fila ligger her inne på "delt", "brevtilsyn mai 2026"

mvh Erlend

Datatilsynet - Vedlegg - Med forslag til svar fra kommunene.xlsx



FORANKRING I KOMMUNENE

- ØSTRE AGDER ✓
- SETESDAL (ALLE FORUTEN BYGLAND → MØTE 15.06)
- VENNESLA ✓

VIDERE ARBEID

- VIDERE BISTAND TIL KOMMUNENE VED INNFØRING AV BEHANDLINGSPROTOKOLLER
- ARBEID MED INNFØRING AV FELLES STYRINGSSYSTEM FOR IKT AGDER KOMMUNENE
- KOMPETANSEHEVENDE TILTAK

MOTTAKSAPPARAT

- ALLE KOMMUNENE HAR EN INFORMASJONSSIKKERHETSANSVARLIG / GDPR KONTAKT OG FUNGERER SOM UNDERTEGNEDE, IKT AGDER OG PERSONVERNOMBUDETS «MOTTAKSAPPARAT».
- HVA SKAL INFORMASJONSSIKKERHET OG GDPR KONTAKT GJØRE?
  - KONTAKTPERSON FOR INFORMASJONSSIKKERHETSAVVIK OG PERSONVERNSAKER I IKT AGDER SAMARBEIDET
  - FØLGE OPP HENVENDELSER, AVVIK, RISIKOVURDERINGER OG PERSONVERNSKONSEKVENSVURDERINGER (BÅDE EKSTERNT (FELLESARBEID) OG INTERNT)
  - SIKRE FORANKRING INTERNT
  - GJENNOMFØRING AV LEDELSENS GJENNOMGANG
  - BIDRA TIL IMPLEMENTERING AV RUTINER, RETNINGSLINJER OG POLICYER I EGEN ORGANISASJON
  - BIDRA TIL LOKAL OPPLÆRING OG VEILEDNING
  - RÅDGIVER TIL TOPPLEDELSEN