Styringssystem for informasjonssikkerheit og personvern

Aukra kommune

Aaslaug Søreide,
Servicesjef og informasjonsikkerheitsleiar

Litt bakgrunn

- Om kommunen
  - 3 500 innbyggjarar.
  - Ca. 500 årsverk.
  - Øy- og fastlandsperle på Romsdalskysten.
  - Er medlem i eit IKT-samarbeid saman med kommunane Molde, Rauma og Vestnes.

Vegen fram til etablering av styringssystemet

- Historikk:
  - Forvaltningsrevisjonsprosjekt i 2015
  - Kva hadde kommunen «på plass»?
    - Nesten ingenting.

1. oversikt over virksomhetens organisering, eksempelvis i form av organisasjonskart
2. styrende dokumenter for internkontroll og informasjonssikkerhet
3. oversikt over hvilke typer personopplysninger kommunen behandler
4. oversikt over informasjonssystemets utforming, eksempelvis i form av systemkart
5. risikovurderinger av informasjonssystemet
6. avviksrutiner
7. navn og funksjon på ansatte som har oppgaver knyttet til informasjonssikkerhet

Kva sa forvaltningsrevisjonen?

Anbefalinger
Med utgangspunkt i de funn som er gjort i denne undersøkelsen gir revisjonen følgende anbefalinger knyttet til informasjonssikkerhet:

1. Aukra kommune bør sikre at det utarbeides sikkerhetsmål og sikkerhetsstrategi for informasjonssikkerhet og implementere dette i egen organisasjon.

2. Aukra kommune bør klargjøre arbeidsdeling gjeldende informasjonssikkerhet med ROR-IKT.

3. Aukra kommune bør utarbeidet en enkel oversikt over de personopplysninger som behandles i kommunen. Oversikten bør gjøres kjent for de med ansvar for informasjonssikkerhet og aktuelle ansatte i organisasjonen.

4. Aukra kommune bør utarbeide rutiner for sikkerhetsrevisjon, og gjennomføre jevnlige sikkerhetsrevisjoner.

5. Aukra kommune bør utarbeide og implementere rutiner for melding av avvik fra bestemmelser om informasjonssikkerhet. Ledelsen bør formidle klare forventninger om at det meldes avvik knyttet til informasjonssikkerhet.

6. Aukra kommune bør utarbeide oppdatert organisasjonskartet i forhold til behandlingsansvaret etter personopplysningsloven, og gjennom dette tydeliggjør ansvarslinjene knyttet til informasjonssikkerhet.

7. Aukra kommune bør gjennomgå og revidere tiltak som er innført for å hindre uautorisert bruk av informasjonssystemene. Aukra kommune bør innføre system som sikrer at alle ansatte jevnlig går gjennom disse tiltakene.

8. Aukra kommune bør utarbeide dokument(er) som tydeliggjør tiltak som skal hindre uautorisert innsyn. Videre bør det utarbeides system som sikrer implementering og vedlikehold av slik kunnskap.

9. Aukra kommune bør gjennomgås og revideres tiltak som skal hindre uautorisert endring av personopplysninger. Aukra kommune bør innføre system som sikrer at alle ansatte jevnlig får vedlikeholde og oppdatere kunnskap om dette.

I kva ende skulle vi starte?

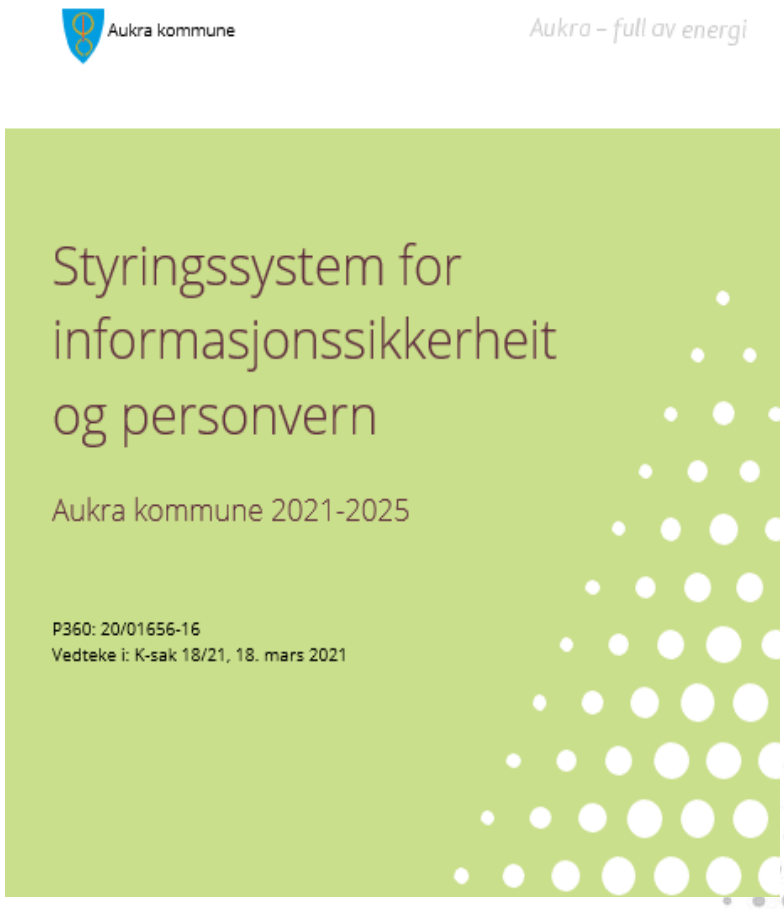
- Kommunestyret vedtok at kommunen skulle jobbe med avvika.
- Vi etablerte derfor eit prosjekt saman med Compilo:
  - Gjennomførte ROS-analysar for dagleg informasjonssikkerheit i einingane.
  - Fekk på plass prosedyrar for personvern, informasjonssikkerheit og fysisk sikring.
  - Opplæring av alle tilsette.
- Vi fekk også på plass planverk på dette området, samt rolla for informasjonssikkerheitsleiar.
- So vart det litt stille…

Så kom GDPR…

- Vanskeleg å få med resten av organisasjonen i starten.
- Mykje å sette seg inn i.
- Vi jobba mest på overordna nivå:
  - Deltok på fleire KiNS-kurs og NYPE-samlingar.
  - Oppdatering av alle prosedyrar.
  - Oppdatering av kvalitetssystemet Compilo.
  - Etablering av styringssystem.

Korleis fekk vi på plass eit styringssystem?

- Informasjossikkerheitsleiar deltok på kurs gjennom KiNS: *Etablering av styringssystem* (over 2 dagar).
  - Ei god stund etter kurset starta kommunen å jobbe fram eit styringssystem basert på kursmaterialet.
  - Fekk gode råd og støtte undervegs i prosessen av Trond og Roy Allan, og av tidlegare PVO.
  - Styringssystemet vart vedteke i kommunestyret i mars 2021.



Implementering

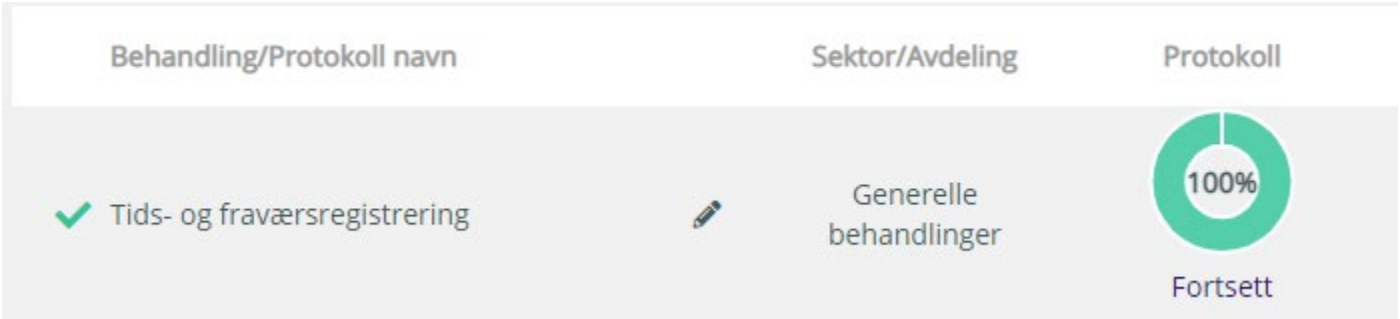
- Kommunedirektøren ga klarsignal til eit GDPR-prosjekt i 2021:
  - Opplæring av leiarguppa og andre nøkkelpersonar.
  - Opplæring av tilsette.
  - Gjennomføring av andre ulike oppgåver knytt til styringssystemet.

Opplæring

- **Leiargruppa og nøkkelpersonar:**
  - KiNS gjennomførte Grunnkurs i personvern og informasjonssikkerheit.
  - Andre kurs:
    - Behandlingsprotokoll (Samsvar)
    - DPIA (Samsvar)
    - ROS (Compilo)
    - Avvik (Compilo)
    - Gjennomgang av kommunen sine prosedyrar (Compilo)
- **Alle tilsette:**
  - Alle tilsette skal gjennomføre KiNS-kursa i KS læring.

Implementering forts.

- Revisjon av behandlingsprotokollane.
  - Protokollmalen vart revidert.
- Gjennomføre DPIA.
  - DPIA-malen vart revidert.
- Gjennomgang av databehandlaravtalar
  - Malen vart revidert
- Utarbeidde århjul
- Gjennomføre ROS-analyser
- Gjennomføre leiinga sin gjennomgang



Korleis jobbe vidare med implementering i 2022?

- Fokus på dei ulike emne i styringssystemet:
  - Revidere resten av protokollane.
  - Revidere delar av styringssystemet slik at det heng saman med IKT-samarbeidet sitt styringssystem.
  - Revidere matrise for sannsynlegheit og konsekvens for personvern og informasjonssikkerheit.
  - Revidere systemoversikta (samarbeid med arkiv og IKT).
  - Motivere leiarane til å gjennomføre ROS-analyser og DPIA.
  - Motivere leiarane til å jobbe meir med avvikskultur.