KARMØY KOMMUNE

Datatilsynet

Postboks 458 Sentrum

0105 OSLO

Dato: 27.04.2023

Dokumentnummer: 23/3146-2
Deres referanse: 23/01323-1
Saksbehandler: Beathe Andreassen

Svar - Brevkontroll - tilsyn med etterlevelsen av personvernforordningen

Viser til brev datert 30.03.2023 «Brevkontroll – Pålegg om å sende informasjon».

Formålet med tilsynsarbeidet er å kontrollere kommunenes systematikk for tekniske og organisatoriske tiltak for å ivareta personvern og personopplysningssikkerhet, herunder kommunenes gjeldende retningslinjer, jf. personvernforordningen artikkel 24 nr. 1 og 2, jf. artikkel 32.

Krav om redegjørelse

Vedlagt følger Karmøy kommunes redegjørelse på tilsynet.

4.1 Kommunens behandlingsprotokoll, jf. personvernforordningen artikkel 30

Svar: Karmøy kommune bruker verktøyet Draftit for å kartlegge kommunens behandlingsaktiviteter, ref Beskrivelse av kommunens overordnede styringssystem og verktøy (vedlegg 4.3).
Vedlegg 4.1 – Behandlingsprotokoll, viser kommunens behandlingsprotokoll fordelt i fire ulike skjema.

4.2 Oversikt over kommunens organisering av ansvarsforhold knyttet til etterlevelse av personvernregelverket, jf. personvernforordningen artikkel 5 nr. 2

Svar: Ansvar og myndighet for informasjonssikkerhet og personvern følger det ordinære linjeansvaret i Karmøy kommune. Ledere som har ansvar for mål, arbeidsoppgaver og tjenester har også ansvaret for tilhørende informasjonsbehandling (herunder også behandling av personopplysninger), IKT-system og informasjonssikkerhet, ref Reglement - informasjonssikkerhet og personvern (vedlegg 4.4.a).

4.3 En kort beskrivelse av kommunens overordnede styringssystem (internkontroll) for etterlevelse av personvernregelverket, herunder hvilke verktøy som eventuelt brukes

Svar: Se vedlegg 4.3 - Beskrivelse av kommunens overordnede styringssystem og verktøy

4.4 Styrende retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser, jf. personvernforordningen artikkel 32.

Svar: Se vedlegg 4.4.a - Reglement - informasjonssikkerhet og personvern

4.4.b - Internkontroll personvern

4.5 Kommunens eventuelle overordnede sikkerhetsstrategi

Svar: Se vedlegg 4.5.a - Strategi for informasjonssikkerhet og personvern

4.5.b - Beredskapsplan for informasjonssystemer – *Unntatt offentlighet, jmf. Offl. § 24 tredje ledd første punktum*

4.5.c - Fysisk sikkerhet datasenter - *Unntatt offentlighet, jmf. Offl. § 24 tredje ledd første punktum*

4.6 Oversikt over eventuelle IKT-samarbeid med andre kommuner

Svar: Se vedlegg 4.6.a - Haugaland IKT oppgavefelleskap - Kommunestyrevedtak

4.6.b - Haugaland IKT oppgavefelleskap - samarbeidsavtale

4.7 Styrende retningslinjer for autentiseringsløsninger i kommunen

Svar: Se vedlegg 4.7 - Autentiseringsløsninger

4.8 Styrende retningslinjer for sikkerhetskopiering og gjenoppretting av systemer, jf. personvernforordningen artikkel 32.1.c)

Svar: Se vedlegg 4.8 - Driftsrutine - sikkerhetskopiering - *Unntatt offentlighet, jmf. Offl. § 24 tredje ledd første punktum*

4.9 Styrende retningslinjer/prosedyrer for sikkerhetsrevisjoner, jf. personvernforordningen artikkel 32.1.d)

Svar: Karmøy kommune tester regelmessige tekniske tiltak for å sikre behandling av personopplysninger. Eksisterende tiltak evalueres forløpende og endres etter behov. Eksisterende sikkerhetskopierings rutiner vurderes, testes og eventuelt endres fortløpende etter behov. Rutinene inngår i beredskapsplan for informasjonssystemer i Karmøy kommune.
IT styringssystemer oppdateres fortløpende i henhold for å sikre at disse har sist tilgjengelig sikkerhetsoppdatering. Klient utstyr (PC, nettbrett, mobile enheter og tynn klienter) oppdateres fortløpende i henhold til leverandørenes sikkerhets patcher og release datoer.
Tilgangsstyring gjennomgås og forbedres for å ivareta at riktige personer har tilgang til riktige data og at andre ikke får tilgang.
Som et resultat av regelmessig gjennomgang av tekniske tiltak har kommunen tatt i bruk en helhetlig sikkerhetsløsning fra Cisco (Cisco Secure Endpoint og Cisco Umbrella) for å ivareta sikkerhet ved behandling av persondata. Løsningen er felles for hele kommunen, har bedre endepunkt sikkerhet med raskere respons ved sikkerhetsbrudd og gir effektiv beskyttelse av brukere, data og applikasjoner i skyen uavhengig av arbeidssted.
Tilgang til, og sikring av datasenter/datarom med persondata er beskrevet i "Fysisk sikkerhet datasenter" (vedlegg 4.5.c) som er en del av Beredskapsplan for informasjonssystemer i Karmøy kommune (vedlegg 4.5.b) .
Beredskapsplanen inneholder også klassifisering av kommunens systemer i henhold til beskyttelsesbehov (konfidensialitet, integritet, tilgjengelighet og robusthet) med tilhørende organisatoriske og andre tiltak for å ivareta sikker behandling av personopplysninger.
Beredskapsplanene inneholder i tillegg tiltakskort for kjente sårbarheter og trusler.
Beredskapsplanen for informasjonssystemer med tilhørende vedlegg revideres regelmessig.
Eksisterende tiltak vurderes og endres etter behov for å ivareta sikkerheten ved behandling av personopplysninger

4.10 Lenke til kommunens personvernerklæring

Svar: https://www.karmoy.kommune.no/personvernerklaering/

Merk: 31.05.2023 skal Karmøy kommune lansere nye nettsider. Dette kan påvirke lenken til personvernerklæringen. Ta kontakt med kommunens kontaktperson ved behov.

4.11 Informasjon om kommunens personvernombud, herunder:

- **Navn, telefonnummer og e-postadresse til personvernombudet i kommunen**
  Svar: Gisle Stødle
  e-post: gisle.stodle@haugesund.kommune.no
  Tlf: 52 74 31 34/ 47 64 70 35
- **Kort beskrivelse av organiseringen av personvernombudsfunksjonen; herunder hvor stor del av full stilling vedkommende skal kunne bruke på utøvelsen av rollen.**
  Svar: Det er inngått samarbeidsavtale med Haugesund kommune om personvernombud.
  Se vedlegg 4.11.a - Prosedyre for personvernombud
  4.11.b - avtale PVO
- **Lenke til kommunens nettside som inneholder informasjon om personvernombudet**
  Svar: https://www.karmoy.kommune.no/personvernombud/

  Merk: 31.05.2023 skal Karmøy kommune lansere nye nettsider. Dette kan påvirke lenken. Ta kontakt med kommunens kontaktperson ved behov.

Med hilsen

Beathe Andreassen
rådgiver

Dokumentet er godkjent elektronisk.

Vedlegg:
4.1 - Behandlingsprotokoll
4.3 - Beskrivelse av kommunens overordnede styringssystem og verktøy
4.4.a - Reglement - informasjonssikkerhet og personvern
4.4.b - Internkontroll personvern
4.5.a - Strategi for informasjonssikkerhet og personvern
4.5.b - Beredskapsplan for informasjonssystemer - U.OFF
4.5.c - Fysisk sikkerhet datasenter - U.OFF
4.6.a - Haugaland IKT oppgavefelleskap - Kommunestyrevedtak
4.6.b - Haugaland IKT oppgavefelleskap - samarbeidsavtale
4.7 - Autentiseringsløsninger
4.8 - Driftsrutine - sikkerhetskopiering - U.OFF
4.11.a - Prosedyre for personvernombud
4.11.b - avtale PVO