Krav til informasjonssikkerhet

Formål
Dokumentet er en informasjon til potensielle leverandører av informasjonssystemer til RegionData og omhandler krav til informasjonssikkerhet som leverandørene er pålagt gjennom lovgivningen og RegionDatas sikkerhetsregelverk.

RegionData
RegionData er et interkommunalt selskap som eies av kommunene Skjåk, Lesja, Sel, Vågå, Lom og Dovre. RegionDatas oppgave er å serve IKT-systemer for eierkommunene som basis for samarbeid om tjenesteproduksjon mellom kommunene. Dette omfatter IKT-struktur, drift, service, sikkerhet, innføring av felles fagsystemer samt strategiutvikling.

Lover- og forskriftskrav
For RegionDatas informasjonssikkerhet gjelder en rekke lover og bestemmelser som bl.a. tar sikte på å hindre at noen uten lovlig hjemmel får tilgang til personopplysninger, herunder opplysninger om er underlagt meldeplikt eller øvrige informasjoner som er unntatt offentlighet.

RegionData har således et lovpålagt krav om å etablere systemer for informasjonssikkerhet og internkontroll som er tilpasset behov for og krav til å sikre informasjon for kommunene. Dette følger blant annet av personopplysningsforskriftens (POF) § 2-15 (sikkerhet hos andre virksomheter) og § 2-16 (dokumentasjon – rutiner for bruk av informasjonssystemet og annen informasjon med betydning for informasjonssikkerheten). Personopplysningsforskriftens bestemmelser om informasjonssikkerhet må ses i sammenheng med andre lover og forskrifter som gjelder for RegionData og dets eierkommuner, blant annet helseregisterloven, pasientrettighetsloven og helsepersonelloven.

Med hensyn til de begrepene som benyttes bl.a. i forskriftene til *Personopplysningsloven* (POL) er RegionData ***behandlingsansvarlig*** virksomhet som interkommunalt selskap. Systemleverandører som, gjennom sine leveranser (installasjon, testing, oppgraderinger eller support), kan få tilgang til personopplysninger for at den behandlingsansvarlige kan gjennomføre sine arbeidsrettslige plikter eller rettigheter, er å betrakte som ***databehandler***.

Lovpålagte krav til leverandører
POF, kapittel 3 – Internkontroll: Databehandlere som behandler personopplysninger på oppdrag fra behandlingsansvarlige, skal behandle opplysningene i samsvar med de rutinene den behandlingsansvarlige har oppstilt (se nedenfor).

Leverandører som gjennomfører sikkerhetstiltak, eller gjør annen bruk av informasjonssystemet på den behandlingsansvarliges vegne, skal tilfredsstille kravene i personopplysningsforskriftens kapittel 2 - Informasjonssikkerhet.

RegionData er pålagt å etablere klare ansvars- og myndighetsforhold overfor sine kommunikasjonspartnere og leverandører. Ansvars- og myndighetsforhold skal framgå av særskilt avtale.

RegionData skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.

RegionDatas sikkerhetsregelverk
Regiondata har etablert et sikkerhetsregelverk som oppfyller kravene til informasjonssikkerhet som er fastsatt gjennom særlovgivning og kontraktmessige forpliktelser til eierkommunene.

Sikkerhetssystemet er bygd opp på følgende måte:
1. Sikkerhetssystemet – systemoversikt:
   Forholdet til kommunene, sikkerhetspolitikk, lover og forskrifter, sikkerhetsorganisasjon
2. Sikkerhetsprosedyrer:
   Fysiske, systemtekniske og organisatoriske sikkerhetsprosedyrer.
3. Støtteprosedyrer og systemutvikling:
   Sikre at systemet er hensiktsmessig og virker effektivt i forhold til lovverk, kontrakter, brukerkrav og interne mål.

Leverandører skal:
1. Imøtekomme kravene i personopplysningsforskriftens kapittel 2 (se ovenfor)
2. Dokumentere sin sikkerhetsstrategi/-politikk (følger av punkt 1).
3. Behandle personopplysninger i samsvar med gjeldende retningslinjer i RegionDatas sikkerhetssystem. Vesentlige punkter i denne sammenhengen er:
   - Regulerte ansvars- og myndighetsforhold mellom partene.
   - Gjeldende prosedyrer for autorisasjon og tilgangsrettigheter ved oppgradering, endring eller feilretting.
   - Gjeldende prosedyrer for sikkerhetstesting og kontroll ved installasjon eller oppgradering.
   - Sikkerhetserklæringer for personale hos leverandøren som gjennomfører sikkerhetstiltak eller gjør annen bruk av informasjonssystemet på vegne av RegionData.
   - Rapportering om eventuelle svakheter i IT-system som leverandøren observerer eller har mistanke om. Leverandørene må ikke forsøke å bekrefte mistanker om svakheter. Dette kan tolkes som mulig misbruk av systemet. I tillegg kan det medføre utilsiktet skade og resultere i juridisk ansvar for den personen som foretar testingen.
   - Krav til at leverandøren har sikringstiltak som skal sikre tilgang på nøkkelkompetanse ved behov.