Datainstruks

for IKT Agder-kommunene

Vedtatt i rådmannsutvalget 13.03.2019

Gjeldende fra 13.03.2019

08.02.2019

Innhold

Revisjon

Første versjon er utarbeidet av IKT Agder sikkerhetsforum 08.02.2019.

1. Formål og innhold

Formålet er å tilrettelegge for god, sikker og lovlig bruk av kommunenes dataverktøy. I den grad instruksen er relevant for andre virksomheter kan den også benyttes av disse.

2. Bruker ID – passord

Hver bruker har en personlig identifikasjon gjennom eget brukernavn og passord. Det skal velges passord som ikke lett lar seg knekke av uvedkommende. Passord er personlig og skal ikke deles til andre.

Dersom du har mistanke om at passordet har blitt kjent av uvedkommende, skal passordet byttes og hendelsen rapporteres som avvik.

3. Lås skjerm

For å hindre at uvedkommende /andre får tilgang til din datamaskin når du selv ikke bruker den/ ikke er på arbeidsplassen, skal maskinen enten slås av eller skjermen låses.

4. Bærbare pc-er – oppdateringer

Alle som har bærbar pc må jevnlig – og minst en gang pr. måned - logge maskinen på kommunens nettverk slik at nødvendige oppdateringer av programvare kan finne sted.

5. Sikkerhetstiltak

Alle ansatte er forpliktet til å følge de retningslinjer for IKT-sikkerhet arbeidsgiver iverksetter.

Lagringsmedier som inneholder personopplysninger/taushetsbelagte opplysninger skal håndteres og oppbevares på en måte som gjør at opplysningene ikke kommer på avveie. Papirutskrifter som inneholder personopplysninger den ansatte ikke lenger har behov for skal makuleres. Nærmere informasjon om dette gis av nærmeste leder og/eller kommunens informasjonssikkerhetsansvarlig samt finnes i kommunens overordnede sikkerhetsdokumentasjon. Personopplysninger skal kun lagres i systemer som er beregnet for dette formålet.

Ettersom nøkkel/nøkkelkort er et sentralt punkt for å skjerme informasjon så må medarbeidere umiddelbart fra til arbeidsgiver ved tap av disse.

- Den som mottar besøkende, er ansvarlig for at gjesten ikke får tilgang til konfidensiell informasjon

6. Privat bruk av arbeidsgivers utstyr

Arbeidsgivers datautstyr er stilt til disposisjon for bruk som arbeidsverktøy. Den enkelte ansatte kan bare bruke dette til private oppgaver i begrenset omfang. All privat bruk skal skje innenfor denne instruksen. Det er ikke adgang til å låne kommunens datautstyr til andre familiemedlemmer eller uvedkommende. Det er heller ikke adgang til å bruke kommunens datautstyr i egen næringsvirksomhet. Arbeidsgiver fraskriver seg alt ansvar for tap av private data, ved uhell eller vedlikehold/service på maskin/server/enheter.

Arbeidsgivers datautstyr skal ikke brukes til å lagre eller spre materiale som er pornografisk eller på annen måte fremstår som støtende, jfr. etiske retningslinjer i virksomheten.

7. Lagring av – og tilgang til data

Som hovedregel skal alle data lagres i kommunens sak- og arkivsystem eller de fagsystemer saken hører hjemme i. Lagring av andre kommunale data og arbeidsdokumenter skal skje i henhold til gjeldende retningslinjer for lagring.

Den ansatte skal foreta fortløpende rydding på sine områder.

Personopplysninger og annen beskyttelsesverdig informasjon som behandles skal være beskyttet mot uautorisert tilgang.

Data som inneholder personopplysninger skal lagres slik at de kun er tilgjengelig for medarbeidere som har behov for opplysningene i sitt arbeid. Sensitive personopplysninger skal kun lagres i områder og mapper med spesielle begrensninger. Alle data som inneholder helseopplysninger skal kun lagres i definerte fagapplikasjoner eller området med spesielle begrensninger på sensitiv sone.

Arbeidsgiver har i utgangspunktet ikke adgang til å gå inn på den enkelte ansattes personlige område og e-postboks. Innsyn i ansattes personlige områder og e-postboks må følge forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale.

8. Særlig om e-post

Arbeidsgivers e-post er opprettet som et arbeidsverktøy. Systemet tillates i begrenset grad brukt til private formål.

E-postsystemet er ikke et saksbehandlerprogram. E-post som inngår som del av saksbehandlingen skal legges inn i vedkommende saksbehandlersystem. Hva som er arkivverdig fremkommer av arkivplanen.

Utover det angitte foran gjelder følgende regler ved bruk av e-post:

- E-post skal ikke brukes når det er konfidensiell eller sensitiv informasjon uten at innholdet er kryptert eller anonymisert. Ved forsendelse av personopplysninger gjelder personopplysningsloven. En huskeregel er å vurdere hvilke konsekvenser en feilsending kan få.
- Dersom en ansatt er forhindret fra å lese e-post i flere arbeidsdager bør fraværsassistenten / automatiske svar brukes.
- Kjedebrev eller lignende tillates ikke videresendt eller distribuert.

Når arbeidstaker slutter blir vedkommendes epostkasse avsluttet. Den ansatte har ansvar for å videreformidle nødvendige data til rette vedkommende før arbeidsforholdet avsluttes.

9. Installasjon av utstyr og programvare på arbeidsgivers datamaskin

Enhver installasjon utover det som utgjør arbeidsgivers IT-plattform skal være faglig begrunnet, og ved tvil skal informasjonssikkerhetsansvarlig godkjenne installasjonen. Den ansatte er selv ansvarlig for konsekvensene ved egen installasjon. Ved egen installasjon forutsettes at det foreligger brukerlisens. Kopiering av lisensiert programvare er forbudt.

Arbeidsgiver kan uten varsel fjerne programvare som er lagt inn i strid med foranstående, eller programvare som ikke følger norsk lov. Det er ikke tillatt å koble privat eller fremmed IT-utstyr opp mot arbeidsgivers kablede nettverk uten skriftlig godkjenning fra informasjonssikkerhetsansvarlig.

10. Bruk av datautstyr utenfor arbeidsgivers nettverk

Ved oppkobling av kommunale PC-er og andre digitale enheter, mot eksterne datanettverk må brukeren utvise særskilt aktsomhet.

Dersom ansatte skal medbringe slikt utstyr til land som kan utgjøre en sikkerhetsrisiko, må dette avklares med sikkerhetsansvarlig.

11. Internettbruk

Det anses som brudd på arbeidskontrakt å laste ned eller dele ulovlig materiale. Under ingen omstendighet tillates nedlasting av ulovlig materiale som rammes av straffelovens §§ 317 (pornografi) og 311 (seksuelle overgrep mot barn).

12. Innlevering ved avsluttet arbeidsforhold

Ansatte som har bærbar PC, iPad, mobiltelefon, annet utstyr, eller autorisasjoner for fjerntilgang, skal levere dette tilbake senest siste arbeidsdag. Annet tidspunkt kan avtales mellom arbeidsgiver og arbeidstaker.

13. Rapportering og avvik

Dersom det oppdages sikkerhetsbrudd eller hendelser som kan ha betydning for sikkerheten skal kommunens avvikshåndteringssystem benyttes. Avhengig av type hendelse og tidsperspektiv må det meldes fra til nærmeste leder og sikkerhetsansvarlig. Se også "plan for informasjonssikkerhet, personvern og internkontroll i IKT Agder-kommunene''.

Dersom det oppdages virus eller annen skadelig programvare, dataangrep eller annet unormal aktivitet på datautstyr eller telefoner, skal IKT Agder varsles umiddelbart.

14. Oppdatering/revisjon

Mindre endringer gjøres av sikkerhetsforum. Større endringer forelegges rådmannsutvalget for godkjenning.

15. Signatur fra ansatt på lest og forstått

Jeg bekrefter at jeg har gjort meg kjent med gjeldende datainstruks, og forplikter meg til å holde meg oppdatert om endringer i instruksen.

Gjeldende instruks skal til enhver tid være tilgjengelig på ansattportalen.

_____ _____

Sted Dato

_____

Stilling og navn på ansatt - enhet/ arbeidssted

(Undertegnet datainstruks skannes inn i vedkommende personalmappe)

Plan for informasjonssikkerhet, personvern og internkontroll i IKT Agder-kommunene

Herunder bestemmelser for Sikkerhetsforum

29.03.2019

Revisjon

Denne planen revideres årlig i henhold til årshjul for sikkerhetsforum. Mindre endringer gjøres av sikkerhetsforum. Større endringer vedtas av rådmannsutvalget.

Dato	Godkjent / revisjon	Hvem
25.05.18	Første versjon - forslag til mandat for sikkerhetsforum	GDPR-prosjektet
07.12.18	Andre versjon - utkast til plan med mandat og endret navn på dokument	IKT Agder sikkerhetsforum
08.02.19	Endelig forslag til plan	IKT Agder sikkerhetsforum
13.03.19	Behandling	Rådmannsutvalget
29.03.19	Justert forslag til plan	Arbeidsgruppe fra IKT Agder sikkerhetforum og rådmannsutvalget
11.04.19	Godkjent	Rådmannsutvalget

1 Innledning

Kommunene i IKT Agder-samarbeidet har behandlingsansvar for personopplysninger om sine innbyggere og ansatte, samt en del felles databehandlingsløsninger. Sikkerhetsforum er derfor etablert for å samordne arbeidet med informasjonssikkerhet og personvern i IKT Agder-samarbeidet.

Endringer i dette dokumentet vedtas av rådmannsutvalget etter innspill fra sikkerhetsforum når dette gjør det nødvendig for å oppfylle kommunenes ansvar for informasjonssikkerheten.

Dette dokument er ikke uttømmende, ettersom lov og forskrift er særdeles detaljert på dette området. Det er ikke hensiktsmessig å løse alle detaljer i sikkerhetsforum, men gjennom forumets videre samarbeid ønsker en å finne hvilke fremtidige utfordringer som forumet/kommunene må ta tak i. EU-direktiv 2016/679 av 27. april 2016, General Data Protection Regulation (heretter Personvernforordningen) trådte i kraft i EU 25. mai 2018 og erstatter EU sitt personverndirektiv fra 1995. Ny personvernlovgivning i Norge trådte i kraft juli 2018.

2 Definisjoner og begrepsavklaringer

Informasjonssikkerhet:
: Handler om tiltak for sikring av konfidensialitet, integritet og tilgjengelighet på informasjon

Behandlingsansvarlig:
: Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes

Databehandleransvarlig:
: Den som behandler personopplysninger på vegne av den behandlingsansvarlige

Sikkerhetsansvarlig (ledelse):
: Den som er delegert ansvaret for den daglige ledelsen på vegne av virksomheten som den behandlingsansvarlige driver

Systemansvarlig (forvalter):
: Den person som behandlingsansvarlig (systemeier) har pekt ut som operativt ansvarlig for et informasjon/fagsystem på vegne av virksomheten (systemeier)

Internkontroll:
: Den interne styringen og kontrollen i virksomheten

Informasjonssystem:
: Et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon

Data Protection Impact Assessment (DPIA):

En vurdering av personvernkonsekvenser

General Data Protection Regulation (GDPR):

En forordning som skal styrke og harmonisere personvernet ved behandling av personopplysninger i EU

(I Norge avløser denne personverndirektivet)

Personvern:

Retten til privatliv og retten til å bestemme over egne personopplysninger

Personopplysninger:

Opplysninger og vurderinger som kan knyttes til en enkeltperson

Personvernombud:

Er virksomhetens personvernekspert og skal være bindeleddet mellom ledelsen, de registrerte og Datatilsynet

Sikkerhetsforum:

Faglig nettverkssamarbeid for IKT Agder kommunene/fylkeskommunen

Avklaring: Når det henvises til kommune eller kommunene, menes alle medlemskommunene i IKT Agder samarbeidet, inkludert fylkeskommunen.

3 Lovgrunnlag og formål

Personopplysningslovens (Pol.) kapittel 1 har slik ordlyd:

> *§ 1. Gjennomføring av personvernforordningen*
> EØS-avtalen vedlegg XI nr. 5e (forordning (EU) 2016/679) om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt oppheving av direktiv 95/46/EF (generell personvernforordning) gjelder som lov med de tilpasningene som følger av vedlegg XI, protokoll 1 og avtalen for øvrig.

https://lovdata.no/dokument/NL/lov/2018-06-15-38

Den nye personopplysningsloven med EUs personvernforordning har slik ordlyd:

> *Artikkel 1.Formål og mål*
>
> 1. Denne forordning fastsetter regler om vern av fysiske personer i forbindelse med behandling av personopplysninger samt regler om fri utveksling av personopplysninger.
>
> 2. Denne forordning sikrer vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger.
>
> 3. Fri utveksling av personopplysninger i Unionen skal verken begrenses eller forbys av årsaker knyttet til vern av fysiske personer i forbindelse med behandling av personopplysninger.

https://lovdata.no/lov/2018-06-15-38/gdpr/a1

Sikkerhetslovens formålsbestemmelse har slik ordlyd:

> Formålet med denne lov er å
> a. Legge forholdene til rette for effektiv å kinne motvirke trusler mot rikets selvstendighet og sikkerhet og andre vitale nasjonale interesser,
> b. Ivareta den enkeltes rettsikkerhet, og
> c. Trygge tilliten til og forenkle grunnlaget for kontroll med forebyggende sikkerhetstjeneste

https://lovdata.no/dokument/NL/lov/1998-03-20-10

Forvaltningsforskriften:

> Forskriftens formål er å legge til rette for sikker og effektiv bruk av elektronisk kommunikasjon med og i forvaltningen. Den skal fremme forutsigbarhet og fleksibilitet og legge til rette for samordning av sikre og hensiktsmessige tekniske løsninger. Forskriften skal legge til rette for at enhver på en enkel måte kan utøve sine rettigheter og oppfylle sine plikter overfor det offentlige.
> Forskriften gjelder for elektronisk kommunikasjon med forvaltningen og for elektronisk saksbehandling og kommunikasjon i forvaltningen når ikke annet er bestemt i lov eller i medhold av lov.
> Denne forskrift gir ikke grunnlag for å gjøre unntak fra de alminnelige reglene om forsvarlig saksbehandling i forvaltningsloven.

https://lovdata.no/dokument/SF/forskrift/2004-06-25-988

4 Mål og ansvarsfordeling for sikkerhetsarbeidet i kommunene

4.1 Mål

Kommunens overordnede mål for arbeidet med informasjonssikkerhet og sikkerhet for personopplysninger er å sikre at korrekt og nødvendig informasjon er tilgjengelig for at kommunen skal kunne utøve sine tjenester, og samtidig sikre at den enkelte innbyggers personvern ivaretas.

Felles strategi og samordnet arbeid med personvern og informasjonssikkerhet i kommunene skal over tid gi gevinst i form av bedre sikkerhet rundt opplysninger i alle kommunens tjenester, bedre personvern, bedre personopplysningssikkerhet, færre avvik ved tilsyn og ingen saker som får juridiske konsekvenser for kommunene. Arbeidet med informasjonssikkerhet og personvern er en del av internkontrollen og det øvrige kvalitetsarbeidet i kommunen.

4.2 Ansvarsfordeling

Det skal sørges for tilfredsstillende håndtering av informasjonssikkerhet på følgende måte:

- Rådmannen har det overordnede ansvaret for informasjonssikkerheten og defineres som behandlingsansvarlig.
- Rådmannen har ansvaret for å organisere, koordinere og styre arbeidet med informasjonssikkerhet og personvern i kommunen, iverksette internkontroll, gjennomføre forbedringsprosesser samt følge opp at sikkerheten vedlikeholdes i alle ledd.
- Rådmannen har ansvaret for å oppnevne kommunens medlem til sikkerhetsforum. Vedkommende har myndighet og ansvar til å kunne gjennomføre oppgavene i forumet. Ansvar innebærer å organisere, koordinere og styre sikkerhetsarbeidet, evt. utarbeide retningslinjer, iverksette internkontroll, gjennomføre forbedringsprosesser, samt følge opp at sikkerheten vedlikeholdes i alle ledd.
- Medlemmet rapporterer til rådmannen i forbindelse med ledelsens årlige gjennomgang.
- Ledere er ansvarlig for informasjonssikkerheten og sikkerhet for personopplysninger i sin enhet / sektor. Ved brudd, skal dette meldes i henhold til avviksprosedyren i den enkelte kommune. Vedlegg til dette dokumentet kan benyttes.

5 Spesielt om informasjonssikkerhet

Informasjonssikkerhet handler om tiltak for sikring av konfidensialitet, integritet og tilgjengelighet (KIT) på informasjon.

5.1 Gjennomgående elementer i all behandling av informasjon og opplysninger

- Konfidensialitet - uvedkommende får ikke tilgang på opplysningene.
- Integritet - opplysningene endres ikke uautorisert eller utilsiktet.
- Tilgjengelighet - opplysningene er tilgjengelige når det er behov for dem.

5.2 Sikkerhetsmål

1) Kommunen skal sikre at informasjon behandles kun i henhold til relevante lover, forskrifter og andre retningslinjer som vil gjelde for kommunen. For eksempel godkjente adferdsnormer (bransjenormer) og sertifiseringer.
2) Sikkerheten i kommunen skal ha forankring i kommunens øverste administrative ledelse og skal ivaretas som en integrert del av hele kommunens organisasjon.
3) Den fysiske sikkerhet skal hindre at uautoriserte får adgang til kommunens lokaler der personopplysninger og andre opplysninger kan være lagret og behandlet.
4) Tilgang til systemer og informasjon gis kun til medarbeidere etter behov («Need to Know») og tilgang til systemer og informasjon for uvedkommende skal forhindres.
5) Kommunen skal sikre at informasjonsbehandling er korrekt og at informasjon ikke forandres uten lovlig tilgang.
6) Kommunen skal sikre tilgjengelighet til systemer, tjenester og informasjon til rett tid for de personer som er autorisert.
7) Det skal være tatt i bruk rutiner for å håndtere uønskede hendelser og det skal være mulig å spore slike uønskede hendelser.
8) Det skal være tatt i bruk systematiske læreprosesser ved uønskede hendelser slik at sannsynlighet for tilsvarende eller gjentatte hendelser reduseres.
9) Det skal forhindres at personer eller systemer hos kommunen bevisst eller ubevisst er årsak til sikkerhetsmessig uønskede hendelser mot egen eller andre virksomheter eller fysiske personer.
10) Kommunen skal sikre at medarbeidere som bruker kommunens informasjonssystemer og behandler personopplysninger har en tilstrekkelig kompetanse for å ivareta kommunens sikkerhetsbehov/krav.

Sikkerhetsmål skal regelmessig gjennomgås og endres etter kommunens virksomhet, rammevilkår og trusselbilde. Bakgrunnsmateriale for gjennomgangen vil være:

- resultater og hovedkonklusjoner fra risikoanalyser og internkontroll
- endringer i offentlige sikkerhetskrav, som kan medføre vesentlig endringer for kommunen
- vurderinger om tilstrekkelige ressurser er tilgjengelige for å ivareta internkontroll og informasjonssikkerhet

6 Spesielt om personvern

Personvern er retten til et privatliv og til å bestemme over egne opplysninger. Utøvelse av godt personvern omhandler behandlers plikter i kombinasjon med den registrertes rettigheter.

Overlapping av personvern og informasjonssikkerhet: konfidensialitet, integritet og tilgjengelighet (KIT) for personopplysninger.

Prinsipper for behandling av personopplysninger

Følgende prinsipper skal være styrende for behandling av personopplysninger i kommunen:

1) **Lovlig behandling.** All behandling av personopplysninger i kommunen skal skje på en lovlig, rettferdig og transparent måte. Transparens skal allikevel vike dersom dette prinsippet kommer i strid med prinsippene om konfidensialitet eller kan være en risiko for personvernet til enkelte.
2) **Formålsbegrensning**. Det skal kun behandles personopplysninger med et klart formål og innenfor formålet. Personopplysninger skal ikke brukes til andre formål enn de er samlet inn for.
3) **Registrertes rettigheter**. Det skal sørges for at de registrertes rettigheter kan håndheves etter lovverket.
4) **Dataminimering**. De personopplysninger som behandles skal være adekvate, relevante og begrenset til det som er nødvendig for formålene personopplysningene behandles for.
5) **Krav til it-systemer**. De it-systemer og løsninger som kommunen benytter seg av skal understøtte pliktene etter lovverket, og skal ikke forhindre etterlevelse av lovverket eller de registrertes rettigheter.
6) **Riktighet.** Opplysningene skal sikres riktighet, og skal rettes på oppfordring eller når det avdekkes at opplysningene ikke er korrekte eller oppdaterte.
7) **Begrensning i behandlingstid.** Personopplysninger skal slettes når formålet for behandlingen er opphørt, eller når de kreves slettet av de registrerte. Hvis oppbevaring er påkrevd i henhold til arkivloven eller annen lovgivning, skal

imidlertid personopplysningene oppbevares i samsvar med gjeldende lovbestemmelser.

8) **Integritet og fortrolighet.** Det skal iverksettes tilstrekkelige tiltak for å sikre personopplysninger mot uautorisert eller ulovlig behandling og mot utilsiktet tap, ødeleggelse eller skade, ved bruk av egnede tekniske eller organisatoriske tiltak.
9) **Ansvarlighet.** Kommunen skal opptre ansvarlig for behandling av personopplysninger når kommunen er behandlingsansvarlig, og skal påse at databehandlere kommunen benytter gir de tilstrekkelige garantier og sørger for lovlig og sikker behandling.

7 Internkontrollrutiner for kommunene

Internkontroll på informasjonssikkerhets- og personvernfeltet tilsvarer forbedring av kontroll og styring. Økt kontroll og styring gir igjen bedre omstillingsevne.

7.1 Årlig ledergjennomgang og internkontroll

Den årlige ledergjennomgangen av informasjonssikkerhet og personvern er også når den årlige internkontrollen for dette arbeidet i kommunen gjennomføres. Det er avgjørende å dokumentere hva som blir gjennomgått og bestemt i ledergjennomgangen/internkontrollen.

Den årlige ledergjennomgangen/internkontrollen skal bestå av følgende:

- Gjennomgang av overordnede sikkerhetsdokumenter
- Risikovurdering: revidere ROS for informasjonssikkerhet
- Gjennomgang av innrapporterte avvik på feltet siste år
- Risikohåndtering: bli enige om de viktigste fokusområdene og foreslå tiltak
    - Internkontrollen skal resultere i en fremdriftsplan (forpliktende dokument) for året for informasjonssikkerhet- og personvernarbeidet. Her skal det fastsettes fokusområder basert på ROS og tidligere avvik. Fremdriftsplanen skal fordele ansvar og oppgaver for oppfølging i ledergruppen, og minne om kontinuerlige oppgaver i den kommunale driften.
    - Fremdriftsplanen tas opp igjen i ledergjennomgangen/internkontrollen påfølgende år og det rapporteres til målene som ble satt. Videre revideres fremdriftsplanen for et nytt år.

8 Avvikshåndtering

Avvik som setter informasjonssikkerheten og personvernet i fare skal fortløpende rapporteres i henhold til fastlagt avviksprosedyre. Avvikshåndteringen skal skje i tråd med vedlagt mal (vedlegg 1), eller gjennom annet tilsvarende system – på en slik måte at dokumentasjonen blir tilstrekkelig for etterprøving og rapportering i den årlige ledergjennomgangen/internkontrollen.

Avviket skal behandles sammen med de personer som er relevante for slik behandling og beslutte eventuelle rutinemessige eller tekniske tiltak for å forhindre at avvik gjentar seg.

Et avvik er enhver hendelse eller tilstand som bryter med kommunens internkontroll.

8.1 Avvik kan defineres inn i følgende kategorier:

- Avvik fra gjeldende rutiner
- Hendelser som kan ha sikkerhetsmessig konsekvens
- Utført av ansatte, som brudd på sikkerhetsbestemmelser
- Utført av eksterne, som fysisk innbrudd, elektroniske angrep
- Beredskapshendelser

Ansatte som oppdager uønskede hendelser skal snarest rapportere om dette til nærmeste overordnede eller annen bestemt ansvarlig.

8.2 Rapportering til Datatilsynet

Foreligger det brudd på personopplysningssikkerheten skal kommunen uten ugrunnet opphold og når det er mulig, senest 72 timer etter å ha fått kjennskap til det, melde bruddet til Datatilsynet, med mindre det er lite trolig at bruddet vil medføre en risiko for fysiske personers rettigheter og friheter. Meldes ikke bruddet til Datatilsynet innen 72 timer, skal årsakene til forsinkelsen oppgis.

Det er rådmannen som er ansvarlig for at brudd på personopplysningssikkerheten meldes, og skal selv sørge for at dette blir utført. Dersom det kan være aktuelt å melde til Datatilsynet, skal alltid rådmann vurdere dette, i samråd med informasjonssikkerhets/personvernansvarlig.

Meldingen til Datatilsynet skal minimum angi:

- Beskrivelse av arten av bruddet på personopplysningssikkerheten, herunder, når det er mulig, kategoriene av og omtrentlig antall registrerte som er berørt, og kategoriene av og omtrentlig antall personopplysningsposter som er berørt,
- navnet på og kontaktopplysningene til personvernombud eller et annet kontaktpunkt der mer informasjon kan innhentes,
- beskrivelse av de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten,
- beskrivelse de tiltak som er truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Er det ikke mulig å gi all informasjon samtidig, kan den gis trinnvis uten ytterligere ugrunnet opphold til Datatilsynet. Er det sannsynlig at bruddet på personopplysningssikkerheten vil medføre en høy risiko for de registrertes rettigheter og friheter, skal de registrerte varsles om bruddet uten ugrunnet opphold.

Varslet til de registrerte skal inneholde en klar og tydelig beskrivelse av arten av bruddet på personopplysningssikkerheten og skal minst inneholde følgende:

- Navnet på og kontaktopplysningene til personvernombudet eller et annet kontaktpunkt der mer informasjon kan innhentes.
- Beskrivelse av de sannsynlige konsekvensene av bruddet på personopplysningssikkerheten.
- Beskrivelse av de tiltak som den behandlingsansvarlige har truffet eller foreslår å treffe for å håndtere bruddet på personopplysningssikkerheten, herunder, dersom det er relevant, tiltak for å redusere eventuelle skadevirkninger som følge av bruddet.

Varsling av de registrerte er ikke nødvendig dersom noen av følgende vilkår er oppfylt:

- Det er gjennomført egnede tekniske og organisatoriske sikkerhetstiltak, og disse tiltakene er blitt anvendt på personopplysningene som er berørt av bruddet på personopplysningssikkerheten, særlig tiltak som gjør personopplysningene uleselige for enhver person som ikke har autorisert tilgang til dem, f.eks. kryptering.
- Kommunen har truffet etterfølgende tiltak som sikrer at det er lite trolig at den høye risikoen for de registrertes rettigheter og friheter vil oppstå.
- Det vil innebære en uforholdsmessig stor innsats å varsle de registrerte. Dersom dette er tilfellet, skal allmennheten isteden underrettes, eller det skal treffes et lignende tiltak som sikrer at de registrerte underrettes på en like effektiv måte.

8.3 Avviksliste og rapportering

Alle avvik skal dokumenteres som nevnt og oppbevares samlet i passende system (internkontrollsystem el.) slik at informasjonen kan anvendes og er tilstrekkelig sikret.

Det skal føres avviksliste som er løpende oppdatert i kommunens internkontrollsystem.

I ledelsens årlige gjennomgang/internkontroll, skal det fremlegges en oversikt over avvikene som er registrert det siste året. Fremgangsmåten for denne prosessen kan planlegges i Sikkerhetsforum.

9 Håndtering av innsynsbegjæringer

Rutine for håndtering av innsynsbegjæringer etter Offentlighetsloven eller Forvaltningsloven finnes i kommunens arkivplan under kapittel for innsyn.

Den enkelte kommune skal ha rutiner for håndtering av begjæringer om innsyn i egne personopplysninger, etter Personopplysningsloven.

Se også personvernerklæringer for innbyggere og for ansatte.

For innsynsforespørsler innen enkelte fagområder kan ytterligere regler gjelde.

10 Mandat for Sikkerhetsforum

Sikkerhetsforum skal være et rådgivende forum for

- deling av erfaringer og kunnskap om effektiv og praktisk håndtering av informasjonssikkerhet
- koordinering og samordning av kommunenes arbeid med oppfølging av Personvernforordningen og Personopplysningsloven
- utvikling og vedlikehold av felles strategier, maler, prosedyrer og annet verktøy for slik oppfølging

Sikkerhetsforum skal bistå kommunene med å tilrettelegge, gi anbefalinger og koordinere arbeidet som må gjøres i hver enkelt kommune for å ivareta kravene som er nedfelt i Personvernforordningen og personopplysningsloven til personvern og informasjonssikkerhet for innbyggerne og virksomhetens plikter og ansvar.

10.1 Sikkerhetsforum skal ha følgende oppgaver

- Utvikle, følge opp og vedlikeholde årshjul for arbeidet med informasjonssikkerhet og personvern.
- Holde oversikt over relevante prosedyrer, rutiner og maler for å ivareta riktig håndtering av informasjonssikkerhet og personvern i kommunene.
- Bidra til arbeidet med opplysning og informasjon ut i kommunene om hva personvern og informasjonssikkerhet er, og hva personopplysningslovverket innebærer for hver enkelt ansatt og innbygger.
- Bistå kommunene med å holde oversikt om hvilke personopplysninger kommunene behandler og behandlingsgrunnlaget for dette. Den enkelte kommunen må sørge for at denne oversikten vedlikeholdes og revideres årlig.
- Ha god oversikt over de felles digitale løsningene som behandler personopplysninger, leverandørene av disse og inngåtte databehandleravtaler.
- Følge opp endringer i lovverket og implementere nødvendige endringer i oversikter, prosedyrer og maler som følge av nye eller endrede krav.
- Vurdere og dele løsninger og metodikk for effektiv opplæring av ansatte i personopplysningslovgivningen og kommunenes relaterte rutiner.
- Vurdere verktøy som finnes på markedet for å hjelpe kommunene i personvern-arbeidet.
- Videreutvikle og følge opp de aktiviteter, oversikter og verktøy som er etablert gjennom og overlevert fra GDPR-prosjektet, ref. (oversikt/innholdsliste i vedlegg til dette dokumentet).

Det er gjennom GDPR-prosjektet i IKT Agder-samarbeidet utarbeidet et sett med oversikter, prosedyrer og maler for håndtering av personvernet. Disse skal videreutvikles og vedlikeholdes av sikkerhetsforumet.

10.2 Oversikt over behandlinger og informasjonssystemer

Det er utarbeidet en behandlingsoversikt som dokumenterer kommunenes behandlinger av personopplysninger. Oversikten inkluderer blant annet informasjonssystemer med angitt type/funksjon, ansvarsforhold (for eksempel systemansvarlig) og relevante forhold som behandlingsgrunnlag og lovhjemler.

Behandlingsoversikten revideres årlig, eller ved behov, og skal til enhver tid være oppdatert og tilgjengelig på sikkerhetsforums område som beskrevet.

10.3 Relevant dokumentasjon i den enkelte kommune

Den enkelte kommune må selv vedlikeholde en rekke dokumentasjon som gjelder informasjonssikkerhet. Sikkerhetsforum kan bidra til anbefalinger og forslag til utarbeidelse av felles maler.

Nedenfor er det listet opp eksempler på relevant dokumentasjon (ikke uttømmende):

- Datainstruks eller tilsvarende
- Arkivplan
- Sletterutiner / kassasjonsplan (kan inngå i arkivplan)
- Rutine for håndtering av ustrukturerte data
- Rutine for personvernbrudd (varsling/avviksprosedyre)
- Rutine for personvernkonsekvensanalyser (DPIA)
- Rutine for å etterkomme innsynsbegjæring
- Rutine for kameraovervåkning (dersom aktuelt)
- Rutine for håndtering av bilder, film, sosiale medier etc.
- Prosedyre for oppdatering og vedlikehold av behandlingsoversikt
- Veileder for innkjøp av systemer som behandler personopplysninger
- Oppfølging av prosjekt- og anskaffelsesmetodikk – ivaretakelse av personvern
- Veileder for systemansvarlige

10.4 Økonomi

Sikkerhetsforum har ikke budsjett eller rammer for å gjøre innkjøp eller andre økonomiske forpliktelser på vegne av kommunene. Sikkerhetsforum skal overlevere anbefalinger og tiltaksplaner som følges opp i den enkelte kommune.

10.5 Dette følges opp i den enkelte kommune

Sikkerhetsforum kan ikke ta ansvar for utførelse eller etterlevelse av informasjonssikkerhet og personopplysningslovgivningen i den enkelte kommune. Det skal være klare ansvars- og myndighetsforhold for dette i hver enkelt kommune, og ved oppnevning av ansvar på de forskjellige nivåer skal en sikre informasjonssikkerhet og personvern i hele organisasjonen. Ledere for enheter/sektorer har et særlig ansvar for informasjonssikkerhet og personvern.

Forumet skal ikke ivareta forespørsler om endringer i fagsystemer, men skal ha oversikt over felles fagsystemer som til enhver tid håndterer personopplysninger.

11 Årshjul og rutiner for Sikkerhetsforum

11.1 Årshjul

Sikkerhetsforum møtes normalt 4-6 ganger i året. Frekvens vurderes fortløpende. Sikkerhetsforum skal utarbeide et årshjul som skal beskrive møtedatoer og faste agendapunkter for de planlagte møtene. Utover de faste aktivitetene i årshjulet bestemmes agenda for neste møte fortløpende etter behov.

11.2 Kommunikasjon i Sikkerhetsforum

Sikkerhetsforum skal dele informasjon, dokumenter, planer og aktiviteter på felles arbeidsområde. Utarbeidede prosedyrer, rutiner og malverk skal ligge på felles lagringsområde. Arkivverdig informasjon som utarbeides i Sikkerhetsforum er det den enkelte kommunes medlem sitt ansvar å arkivere i egen kommunes sak-/arkivsystem.

Sikkerhetsforum skal utarbeide og dokumentere som følger:

- Møtereferat
- Årsberetning
    - Evaluere utført arbeid og resultater
    - Anbefalinger om videre arbeid og organisering
    - Revisjon av felles maler og prosedyrer
    - Statistikker (avvik, innsynsbegjæringer og lignende)
    - Gevinster av samarbeidet
- Mangel på oppfølging av foreslåtte tiltaksplaner, rutiner og prosedyrer, mulige konsekvenser av dette

11.3 Rapportering i egen kommune

Kommunens medlem i sikkerhetsforum rapporterer direkte til rådmann (eller rådmannens utnevnte) som avtalt.

Ledelsen i hver kommune anbefales i tilknytning til årsberetningen å verifisere at mål og strategi for, samt organisering av, sikkerhetsforum er tilstrekkelig for å ivareta kommunens behov og lovpålagte krav. Resultatene fra gjennomførte risikovurderinger, sikkerhetsrevisjoner og de viktigste meldte avvik bør være en del av slik gjennomgang.

12 Organisering av Sikkerhetsforum

Oppdragsgiver

Sikkerhetsforums mandat er forankret hos og iverksatt av rådmannen i hver kommune.

Leder

Sikkerhetsforum konstituerer seg selv, og blir enige om ansvar for koordinering og innkalling. Formen for dette evalueres underveis.

Medlemmer

Sikkerhetsforums medlemmer pr. 08.02.2019

- Arendal kommune, Rune Olsen
- Aust-Agder fylkeskommune, Martin Zeiffert
- Froland kommune, Reidun Brinchmann
- Gjerstad kommune, Lasse Fosse
- Grimstad kommune, Marit Fagernes
- Risør kommune, Geir Steen-Tveit
- Tvedestrand kommune, Elias Lien
- Vegårshei kommune, Anne-Grete Glemming
- Åmli kommune, Trine Krossbekk Agersborg
- IKT Agder, Olve Sveen

13 Personvernombud

Kommunene har felles personvernombud, stedsplassert i Arendal kommune. Aust-Agder og Vest-Agder fylkeskommuner har felles personvernombud.

Personvernombudet inviteres med som rådgiver i sikkerhetsforumet. Personvernombudets og sikkerhetsforumets roller og oppgaver må nærmere avklares og defineres etter evaluering når begge organene har fungert en stund.

Konto*	Beskrivelse*	År	Kredit	disponert 2019	disponert 2020	
25199067	1207 - ØSTRE AGDER - KOMPETANSEUTVIKLING SKOLE	2019	-1 027 704	1 027 704		DEKOM brukes f
25199068	1207 - ØSTRE AGDER - SAMHANDLINGSREFORM	2019	-2 741 692	180 000	180 000	felles ressurs utv
25199069	1207 - ØSTRE AGDER - FOU HELSE	2019	-319 631			
25199226	1207 - ØSTRE AGDER KØH	2019	-2 967 724	2967724		Refundert driftsr
25199556	1207 - SAMHANDLINGSREFORMEN - KOMM. ØYEBL. HJELP	2019	-2 801 882	750 000		telemedisinsk se
25199561	1207 - ØSTRE AGDER FOU - HELSE	2019	-1 748 406	310 000	315 000	PHD helse Tvede
25199898	1207 - STRATEGISK NÆRINGSPLAN - ØSTRE AGDER	2019	-559 529			
25199899	1207 - FELLES VEILYSPROSJEKT ØSTRE AGDER	2019	-284 172			Forprosjekt vedr
25199925	1207 - ØSTRE AGDER 2015	2019	-837 914			
			-13 288 654	5 235 428	495 000	-7 558 226

ortløpende
iklingssykehjem Grimstad

midler til kommunene
ntral TELMA
strand

ørende total overgang til LED-veilys

Østre Agder regionråd

Saksfremlegg

Saksbehandler/Tittel	Saksgang	Saksnummer	Møtedato
Ole Jørgen Etholm, sekretariatsleder	Rådmannsutvalget i Østre Agder regionråd	Sak 21/19	11.04.19

Anbefaling for framtidig organisering av NAV i kommunene Arendal, Froland, Gjerstad, Risør, Tvedestrand, Vegårshei og Åmli

Forslag til vedtak:

Kommunestyret/bystyret i ……. Kommune gir sin tilslutning til en organisatorisk sammenslåing av NAV kontorene i Arendal, Froland, Gjerstad, Risør, Tvedestrand, Vegårshei og Åmli på følgende premisser:

- Alle kontorstedene skal bestå og levere daglige tjenester til innbyggerne lokalt, herunder også ivareta det lokale, tverrfaglige samarbeidet med kommunene forøvrig.
- Det skal etableres et nytt, felles NAV - kontor med 7 virksomhetssteder og en vertskommune.
- Utforming av arbeidsmetodikk og organisering i ny modell skal skje med alle ansatte involvert i henhold til lov og avtaleverk, og med sikte på, så langt det er mulig, å benytte beste praksis ved de eksisterende kontorene.
- Som navn på det nye samarbeidet foreslås «NAV Østre Agder» med Arendal som vertskommune.

Kommunestyret/bystyret forutsetter at det utarbeides et forslag til samarbeidsavtalen for NAV Østre Agder som avklare økonomiske forpliktelser knyttet til den nye virksomheten. Vedtaket bygger på at hver kommune skal dekke kostnader til sosiale ytelser til egne innbyggere. De administrative kostnadene hver enkelt kommune i dag dekker til den kommunale delen av NAV skal ikke økes for den enkelte kommune som deltar i det nye NAV Østre Agder.

Samarbeidsavtalen legges fram for kommunestyrer og bystyrer for godkjenning før den nye virksomheten kan etableres. NAV Østre Agder etableres som en vertskommunesamarbeid etter §20-2 i kommuneloven.

Dokument i saken:

1. Utredningsrapport for fremtidig organisering av NAV-kontorene i Risør, Gjerstad, Vegårshei, Tvedestrand, Froland, Åmli og Arendal kommune – vedlegg 1.
2. Anbefaling fra møte i styringsgruppen for utredning av framtidig organisering av NAV i kommunene Arendal, Froland, Gjerstad, Risør, Tvedestrand, Vegårshei og Åmli – vedlegg 2.

Anbefaling fra styret i Østre Agder regionråd:

Flertallet styret i Østre Agder - styremedlemmene fra Arendal (2), Risør, Gjerstad og Åmli, anbefaler kommunene å fatte beslutning om en organisatorisk sammenslåing av NAV kontorene i Arendal, Froland, Gjerstad, Risør, Tvedestrand, Vegårshei og Åmli.

Styrets mindretall, styremedlemmene fra Froland og Vegårshei, anbefaler kommunene å fatte beslutning om en organisatorisk sammenslåing av NAV kontorene i Froland, Gjerstad, Risør, Tvedestrand, Vegårshei og Åmli.

Vedtaket bygger på følgende premisser:

- Alle kontorstedene skal bestå og levere daglige tjenester til innbyggerne lokalt, herunder også ivareta det lokale, tverrfaglige samarbeidet med kommunene forøvrig.
- Det skal etableres et nytt, felles NAV - kontor med 7 virksomhetssteder og en vertskommune.
- Utforming av arbeidsmetodikk og organisering i ny modell skal skje med alle ansatte involvert i henhold til lov og avtaleverk, og med sikte på, så langt det er mulig, å benytte beste praksis ved de eksisterende kontorene.
- Som navn på det nye samarbeidet foreslås «NAV Østre Agder» med Arendal som vertskommune.

Et samlet styret gir sin tilslutning til hovedbegrunnelsen fra styringsgruppa som i sin anbefaling erkjenner at for å løse våre felles utfordringer med levekår og sysselsetting øst i det nye Agder så trenger regionen å stå samlet i et partnerskap med NAV for sammen å kunne benytte alle tilgjengelige ressurser i vårt felles bo- og arbeidsmarked.

Et samlet styret anbefaler at ny NAV-organisering skjer fra 1/1-2020. Det utarbeides en samarbeidsavtale for virksomheten basert på premissene i dette vedtak. Videre skal samarbeidsavtalen avklare økonomiske forpliktelser knyttet til den nye virksomheten. Avtalen legges fram for kommunestyrer og bystyrer for godkjenning før den nye virksomheten etableres.

Bakgrunn for saken:

Styret drøftet i sak 47/18 Orientering om organisatoriske endringer i NAV Agder og ved lokale Nav-kontor. Der ga leder for NAV Agder Elisabeth Blørstad og leder ved NAV Aust-Agder fram til 31.desember 2018 Hilde Høynes en orientering om planlagte endringer NAV Agder fra årsskiftet. Herunder hvilke behov for endring dette medføre ved lokale NAV-kontor. I møtet opplyste sekretariatsleder at rådmennene i Østre Agder hadde anmodet NAV-leder i de åtte kommunene om å utrede hvilke strukturelle endringer som kan være aktuelle i Østre Agder. De redegjorde også for grunnlaget for disse endringene som bygger på stortingets vedtak av Stortingsmelding 33«NAV i en ny tid – for arbeid og aktivitet».

Styret stilte seg bak rådmennenes ønske om å gjennomføre en utredning av hensiktsmessige organisatoriske grep i Østre Agder med sikte på å kunne løse nye oppgaver ved lokale NAV-kontor når det blir aktuelt å flytte oppgaver fra regionalt NAV.

Alle kommunestyrer/bystyrer fikk informasjon om det planlagte utredningsarbeidet. Noen ble saken formelt behandlet.

Når utredningen foreligger så var forutsetningen at den skulle legges fram for styret i Østre Agder regionråd. Etter at styret har gitt sin anbefaling oversendes saken til kommunene til beslutning.

Organisering av utredningen og mandatet for utredningsarbeidet ble vedtatt i styret 16. november sak 77/18. Til dette møtet var det avklart at Grimstad kommune skulle ta del i en utredning for kommunene Grimstad, Lillesand og Birkenes.

Til å styre utredningsarbeidet ble det nedsatt en gruppe med rådmennene i de deltakende kommuner, direktør og ass. direktør i NAV Agder og to tillitsvalgte. Det ble etablert en utredningsgruppen med en rådmann(Bo Andre Longum – Froland), NAV-lederne i de syv kommunene og to tillitsvalgte. NAV Agder og Østre Agder regionråd har vært sekretariat for utredningsgruppen.

I samsvar med framdriftsplanen for utredningsarbeidet avga utredningsgruppen sin rapport 7.mars til styringsgruppen. Denne følger som vedlegg. Styringsgruppen drøftet denne i sitt møte 11.mars og 18.mars. Styringsgruppen anbefaler at det etableres en ny felles NAV-organisasjon. Det er listet opp forutsetninger knyttet til vedtaket som ligger til grunn for at styringsgruppen har samlet seg om denne anbefalingen.

Rådmennenes felles vurdering i saken:

Som det framgår av forslaget til vedtak er hovedbegrunnelsen for styringsgruppas anbefaling er erkjennelsen av at for å løse våre felles utfordringer med levekår og sysselsetting øst i det nye Agder trenger partnerskapet i NAV å benytte alle tilgjengelige ressurser i vårt felles bolig- og arbeidsmarked.

NAV er et partnerskapssamarbeid der stat og kommune i fellesskap har lederansvar. Under drøftingen som har pågått i styringsgruppen har ledelsen ved NAV Agder lagt vekt på at de ønsker og tror det blir viktig å ha en organisering av NAV i Østre del av Agder som gir tyngde inn mot det nye Agder. Det er helt nødvendig at den løsning som anbefales er forankret hos begge eierne. Ledelsen av NAV Agder er tydelige i sin anbefaling om å velge alternativet der 7 kommuner inngår, dvs. et samarbeid som inkluderer Arendal kommune. Etter rådmennenes vurdering, er dette et viktig signal for kommunenes valg.

For rådmennene er det viktig å oppnå maksimal kompetanse og kapasitet innenfor NAV for at den enkelte innbygger som trenger bistand fra denne sentrale velferdsdistributøren får optimal hjelp.

For rådmennene har det ikke vært viktig hvor ledelsen skulle legges, men fra dere side ligger det til grunn at vertskommunen må ha kapasitet og kompetanse som sikrer ivaretakelse av de medarbeidere som vil omfattes av ny organisering. Rådmennene står derfor samlet bak at Arendal kommune velges som vertskommune.

Som det framgår av rapporten, ligger det an til at det i nåværende Vest-Agder vil bli 3 store NAV-kontor (etter vertskommunemodellen). Rådmennene er av den oppfatning at dette er et viktig argument for at vi i østre del av det nye Agder bør gjøre det samme slik at vi framstår som likeverdige og konkurransedyktige i forhold til tilsvarende virksomhet i vest.

Rådmennene er opptatt av at ledelsen av nye NAV Østre Agder må få handlingsrom til å kunne videreutvikle virksomheten ut fra virksomheten behov i dag og i framtiden. Innenfor rammen at de forutsetninger forslaget til vedtak bygger på så skal ledelse og medarbeidere i virksomheten kunne bidra til valg av gode løsninger.

Rådmennene anbefaler at ny NAV-organisering trer i kraft fra 1/1-2020. Til grunn for organiseringen av NAV Østre Agder skal det ligge en samarbeidsavtale. Denne utarbeides av sekretariatet i Østre Agder i dialog med de syv NAV-lederne og med støtte av jusnettverket i Arendal kommune.

En forutsetning for rådmennenes anbefaling er at hver kommune skal være ansvarlig for utbetalingen av økonomisk sosialhjelp og eventuelle andre kommunale støtteordninger innenfor NAV sitt ansvarsfelt. Vertskommunen har ansvar for de direkte utgiftene med driften av felles Nav-kontor (lønn alle ansatte, reisekostnader, opplæring, IKT og annet kontorteknisk utstyr).

En detaljert framstilling av økonomiske rettigheter og plikter for hver enkelt kommune skal foreligge sammen med utkast til samarbeidsavtalen. Utgiftsfordelingen skal bygge på at hver deltakende kommune i NAV Østre Agder ikke skal få økte administrative kostnader. Betalingsmodell må bygge på denne forutsetningen. Skal NAV Østre Agder klare forutsetningen om like høye eller lavere administrative kostnader så forutsettes det at ny leder rekrutteres blant ledere ved ett av dagens seks kontor (Åmli har ikke lokal NAV-leder fordi NAV-leder i Froland ivaretar denne rollen). Ambisjonen ved en nyorganisering skal være å nytte stordriftsfordeler og nye IKT-løsninger slik at administrasjonsutgiftene på arbeidsfeltet over tid kan reduseres.

Rådmennene ser at det ligger en utfordring knyttet overhead på 4% knyttet til vertskommunens drift av nytt NAV Agder. For å klare denne utgiften så må samarbeidskommunenes utgifter til slikt som IKT og lønn reduseres tilsvarende.

Rådmannen i xxx kommune sin særlige vurdering i forhold til kommunens særlige behov og ønsker knyttet til den foreslåtte løsningen:

nn