Sikkerhetshåndbok Gjesdal kommune

Vedtatt i KLT den

Innhold

1. Informasjonssikkerhet og personvern

Informasjonssikkerhet handler om å håndtere risiko relatert til kommunens informasjonsverdier og behandling av personopplysninger. Vi skal sikre at informasjon ikke er tilgjengelig uten autorisasjon (*konfidensialitet*), at informasjon ikke uautorisert endres eller ødelegges (*integritet*), at informasjon er til stede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (*tilgjengelighet*), og at organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser(*robusthet*).

Personvern handler om den registrerte sin rett til et privatliv og rett til å bestemme over egne personopplysninger.

Aktuelt lovverk og forskrifter:

EUs forordning for personvern, The General Data Protection Regulation (GDPR), ble norsk lov i 2018. Forordningen erstattet da gjeldende norsk personvernlovgivning som er bygget på EUs personverndirektiv fra 1995.

Gjesdal kommune arbeider kontinuerlig med å oppdatere styringsdokumenter, instrukser og rutiner for å kunne etterleve det nye regelverket.

I Gjesdal kommune følger vi Norm for informasjonssikkerhet i helse og omsorgssektoren (Normen) for alle som benytter Norsk Helsenett. Normen er juridisk bindende for Gjesdal kommune gjennom signert avtale for tilknytning til Norsk Helsenett.

Normen stiller krav som detaljerer og supplerer gjeldende regelverk, først og fremst personvern- og helselovgivningens krav til å etablere tilfredsstillende informasjonssikkerhet for systemer som behandler helse- og personopplysninger.

Formål og omfang

Denne håndboka for informasjonssikkerhet er et verktøy for ledere og ansatte i Gjesdal kommune for å ivareta tilfredsstillende informasjonssikkerhet og personvern. 120

Håndboken gjelder all informasjonsbehandling som skjer internt i Gjesdal kommune og som kommunen har ansvaret for eksternt. Dette omfatter all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt. All bruk av IKT-løsninger er også inkludert.

Definisjoner

Definisjon av sentrale begreper som benyttes i dokumentasjon av kommunens informasjonssikkerhet og personvern er beskrevet på Datatilsynet sine sider: https://www.datatilsynet.no/regelverk-og-verktoy/ordliste/

Lovgrunnlag og kildehenvisninger

Sikkerhetshåndboka, samt gjeldende rutiner og instrukser, er en del av kommunens internkontroll for informasjonssikkerhet. Følgende regelverk og kilder ligger til grunn:

FL	Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)
eFF	Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften)
SL	Lov om nasjonal sikkerhet
VSF	Forskrift om virksomheters arbeid med forebyggende sikkerhet
POL	Lov om behandling av personopplysninger (personopplysningsloven)
POF	Forskrift om behandling av personopplysninger (personopplysningsforskriften)
HOL	Lov om kommunale helse- og omsorgstjenester m.m. (helse- og omsorgstjenesteloven)
HPL	Lov om helsepersonell mv. (helsepersonelloven)
HRL	Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)
PBL	Lov om pasient- og brukerrettigheter (pasient- og brukerrettighetsloven)

- Norm for informasjonssikkerhet i helse- og omsorgssektoren (Normen)
- Organisasjonskart – Gjesdal kommune
- Personvernprinsippene (Datatilsynet)
- Veileder: Internkontroll og informasjonssikkerhet (Datatilsynet)
- Veileder: Internkontroll i praksis - informasjonssikkerhet (Digdir)
- NSM grunnprinsipper

2. Personvernprinsippene

Gjesdal kommune behandler personopplysninger i samsvar med de grunnleggende personvernprinsippene, jf. personvernforordningens artikkel 5. Her følger en kort beskrivelse av prinsippene. For mer utfyllende informasjon se veileder fra Datatilsynet.

Lovlig, rettferdig og gjennomsiktig
Respekter de registrertes interesser og forventninger. Informer på en forståelig måte.

Formålsbegrensning
Opplysningene skal brukes til uttrykkelig angitte og legitime formål, og ikke (senere) til uforenelige formål.

Dataminimering
Personopplysningene skal være tilstrekkelige, relevante og begrenset til hva som er nødvendig.

Riktighet
Ukorrekte eller utdaterte personopplysninger skal rettes eller slettes.

Lagringsbegrensning
Det skal ikke være mulig å identifisere de registrerte lenger enn hva som er nødvendig for formålet.

Integritet og fortrolighet
Personopplysninger sikres mot uautorisert tilgang og mot tap, ødeleggelse eller skade.

Ansvarlighet
Gjesdal kommune har ansvar for etterlevelse og må kunne dokumentere etterlevelsen.

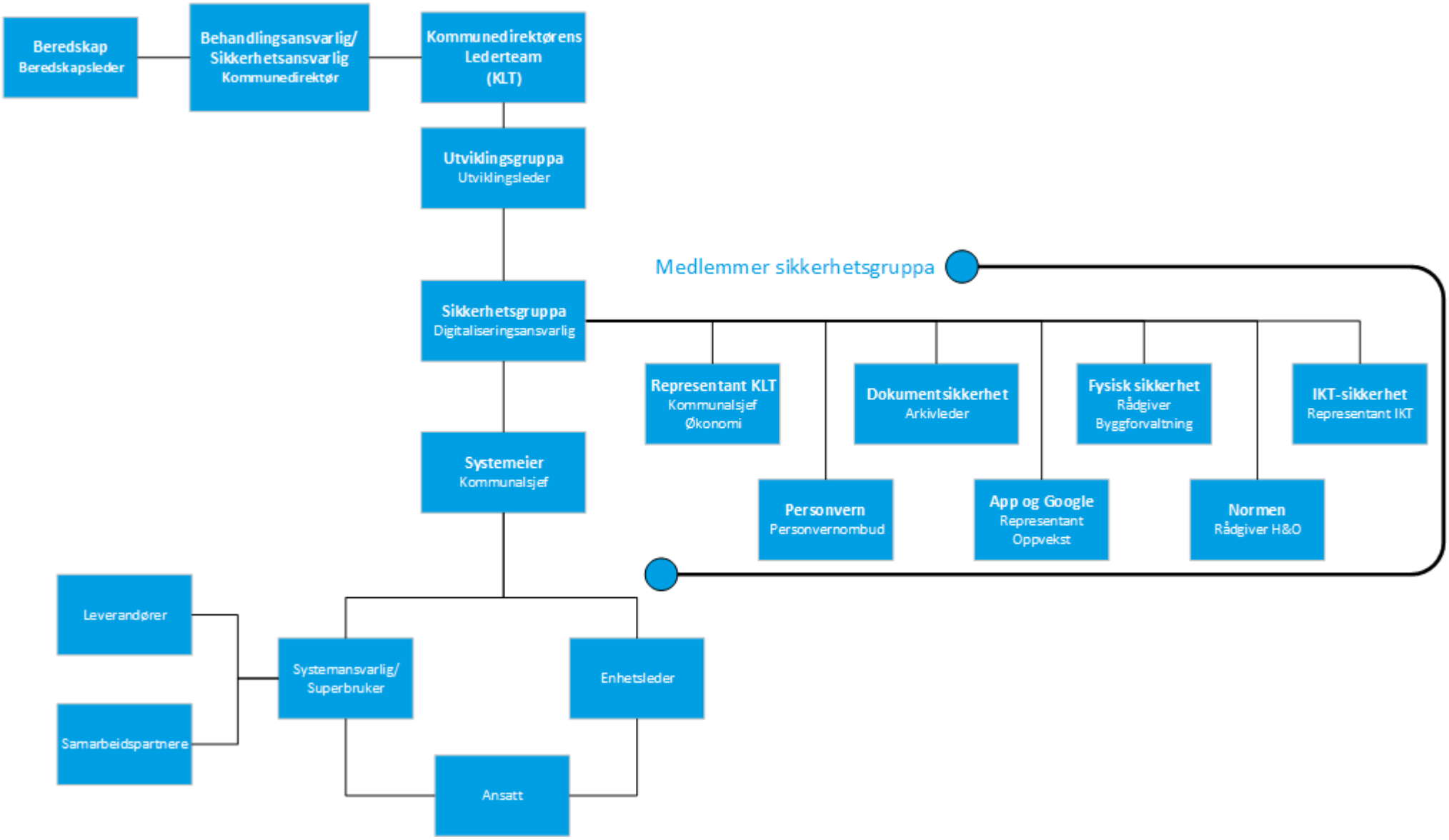
3. Sikkerhetsorganisasjon og ansvarsfordeling

Som overordnet ansvarlig er kommunedirektøren behandlingsansvarlig i Gjesdal kommune. Sikkerhetsorganisasjonen illustrert i figur 3.1 er etablert for å ivareta kommunedirektørens ansvar knyttet til informasjonssikkerhetsarbeid og personvern

Sikkerhetsgruppa i Gjesdal består av:

- Digitaliseringsansvarlig (Leder)
- Kommunalsjef Økonomi
- Personvernombud
- Arkivleder
- Representant fra Oppvekst
- Representant fra Kultur og Samfunn
- Representant fra Helse og Velferd
- Representant fra IKT

Figur 3.1 Sikkerhetsorganisasjon Gjesdal kommune



4. Sikkerhetsmål og sikkerhetsstrategi

Gjesdal kommunes sikkerhetsmål og sikkerhetsstrategi gjelder all informasjonsbehandling som skjer internt i Gjesdal kommune og som kommunen har ansvaret for eksternt. Dette omfatter all behandling, lagring og kommunikasjon av informasjon både muntlig, på papir og digitalt. All bruk av IKT-løsninger er også inkludert. Gjesdal kommune vil bruke NSM sine grunnprinsipper som mal for god sikkerhet.

Formålet med informasjonsbehandling i Gjesdal kommune er å understøtte våre oppgaver og tjenester slik at vi kan nå våre mål og realisere vår visjon. Kommunens mål og prioriteringer framkommer i vår overordnede strategi og økonomiplan.

En informasjonsbehandling som er målorientert, effektiv, lovlig og til å stole på er avgjørende for at kommunen skal lykkes. Tilstrekkelig og balansert informasjonssikkerhet er en kritisk faktor for å understøtte dette.

Mål for informasjonssikkerhet

Vår behandling av informasjon er i samsvar med lover, regler og avtaler, og bidrar på en formåls- og kostnadseffektiv måte til best mulig realisering av kommunens samlede mål.

Konfidensialitet

Bare personer med innsynsrett og ansatte med tjenstlig behov får kjennskap til taushetspliktig informasjon. Bare personer med innsynsrett og de ansatte som ledelsen har bestemt, får kjennskap til informasjon som kommunen har unntatt offentlighet av andre grunner enn taushetsplikt.

Brannmurer, fysisk kontroll og opplæring sikrer tilgang bare for autoriserte brukere. Lagring av personopplysninger hvor konfidensialitet er nødvendig skal bare skje på kommunens egne datasystemer og lagringsmedier. Sensitive personopplysninger skal utelukkende behandles i sikre soner og relevante fagsystem. Ansatte skal ikke laste ned filer med sensitive data/persondata til mobile enheter (eksempelvis fra Altinn og Public 360°).

Integritet

Informasjon som kommunen har ansvaret for blir bare produsert og endret av ansatte eller eksterne som har fullmakt til dette. Informasjon blir ikke endret utilsiktet. Informasjonen skal være fullstendig, oppdatert og korrekt.

Autorisert personell får kun tilgang til datasystemet gjennom innlogging med personlig passord eller kode og aktiviteten kan spores. Kommunen har etablert antivirusløsning slik at ødeleggende programvare ikke skal kunne endre lagrede personopplysninger.

Tilgjengelighet

Relevant informasjon og hensiktsmessige IKT-løsninger er tilgjengelig på en effektiv måte for ansatte, innbyggere og næringslivet.

Sikre at systemene er operative til enhver tid.

Robusthet
At organisasjonen og systemene er motstandsdyktige, og evner å gjenopprette normaltilstand ved hendelser

Sentral backup-løsning sikrer at informasjon som er lagret på kommunens servere kan gjenopprettes. Alternative manuelle prosedyrer sikrer tilgjengelighet for informasjon som er viktig for liv og helse når IKT-løsningene er utilgjengelige.

Strategi for informasjonssikkerhet

Det er etablert en sikkerhetsorganisasjon med klare ansvars. Og myndighetsforhold, jf. Figur i kapittel 3.

Det skal gjennomføres tilfredsstillende opplæring, internkontroll, avvikshåndtering, ROS-analyser, sikkerhetsrevisjoner og ledelsens årlige gjennomgang.

Alle ansatte skal ha et bevisst forhold til å overholde kommunens instruks for informasjonssikkerhet.

4. Oversikt over behandling av personopplysninger

POL art. 30 Hver behandlingsansvarlig og, dersom det er relevant, den behandlingsansvarliges representant skal føre en protokoll over behandlingsaktiviteter som utføres under deres ansvar

Gjesdal kommune skal til enhver tid ha en oppdatert oversikt over hvilke behandlinger av personopplysninger som foretas på papir og digitalt, og hvilke personopplysninger som inngår i disse.

Oversikten er nødvendig for at vi skal kunne ivareta våre plikter. Oversikten danner også grunnlag for utarbeidelse av sikkerhetsmål og sikkerhetsstrategi, og vil være grunnlag ved risikovurderinger og klassifisering av IKT-løsninger.

Oversikten, som skal føres i kommunens digitale register, omfatter *blant annet* følgende:

- Hvilke opplysninger som lagres og formålet med behandlingen,
- Hjemmelsgrunnlag for behandlingen
- Omfanget av behandlingen
- Hvor og hvor lenge opplysningene lagres
- Bruk av databehandlere (selve avtalen skal lagres i arkivsystem)

Ansvar
Kommunedirektør har ansvar for at det dokumenteres hvilke personopplysninger som behandles i kommunen.

Sikkerhetsleder skal påse at oversikt vedlikeholdes.

Kommunalsjef har ansvar for at avdelingen utarbeider og vedlikeholder oversikt.

Personvernombud skal bidra til å få oversikt over behandlingene.

Ansatte skal delta i utarbeiding og vedlikehold av oversikt.

Dokumentreferanse

Personvernerklæring

5. Risikovurderinger

(og vurdering av personvernkonsekvenser, DPIA)

POL Art. 32.2 Ved vurderingen av egnet sikkerhetsnivå skal det særlig tas hensyn til risikoene forbundet med behandlingen, særlig som følge av utilsiktet eller ulovlig tilintetgjøring, tap, endring eller ikke-autorisert utlevering av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.

Risikovurdering skal gjennomføres før iverksettelse av ny behandling av personopplysninger eller ved endringer i behandlingen som har betydning for informasjonssikkerheten. Slike endringer kan være endring i type opplysninger som behandles, organisasjonsendringer eller tekniske og bygningsmessige endringer. Grundighet og omfang av risikovurderingen bestemmes ut fra den enkelte situasjon som skal vurderes.

En risikovurdering består av fem hoveddeler:

- Kartlegge risiko: *Oversikt identifiserte trusler, hva kan gå galt?*
- Vurdere risiko: *Sannsynlighet og konsekvens, hvor galt kan det gå?*
- Dokumentere tiltak: *Hva er gjort for å unngå at det går galt?*
- Vurdere tiltak: *Er det nok til å redusere risiko til et akseptabelt nivå?*
- Følge opp tiltak: *Skal vi endre eller etablere kontrolltiltak?*

Nivå for akseptabel risiko skal fastsettes før behandling av personopplysninger startes og før risikovurderinger gjennomføres. Overordnet nivå for akseptabel risiko i Gjesdal kommune er at behandlinger med høy og middels risiko ikke kan iverksettes før det er gjennomført tiltak som begrenser risikoen. Dersom risikonivå fortsatt er middels eller høyt må behandlingen vurderes av sikkerhetsgruppa.

Som hovedregel skal alle, gjennomførte risikovurderinger dokumenteres i kommunens arkivsystem og kommunens kvalitetssystem. Dersom gradert informasjon inngår i risikovurderingen skal den bare arkiveres unntatt offentlighet i kommunens arkivsystem.

En risikovurdering av informasjonssikkerhet vurderer sannsynligheten for brudd på sikring av konfidensialitet, integritet og tilgjengelighet. Dersom det er sannsynlig at behandlingen vil medføre høy risiko for en persons rettigheter og friheter, skal det gjennomføres en vurdering av konsekvenser for personvernet (Data Protection Impact Assessment – DPIA) jf. GDPR artikkel 35.
Personvernombudet skal delta på DPIA. Eksempler hvor vi må gjennomføre DPIA kan være ved:

- systematisk og omfattende vurdering av personlige forhold når opplysningene brukes til automatiserte avgjørelser
- behandling av sensitive personopplysninger i stort omfang

- systematisk overvåking av offentlig område i stort omfang

Ved høy risiko for personvernet, som ikke kan begrenses, skal personvernombudet involvere Datatilsynet i forhåndsdrøftelser.

Ansvar

Kommunedirektør fastsetter nivå for akseptabel risiko.

Kommunalsjef er ansvarlig for at det gjennomføres risikovurderinger i sin avdeling i henhold til gjeldende rutiner.

Dokumentreferanse

Gjeldende overordnet nivå for akseptabel risiko (kommer)
Rutine for gjennomføring av risikovurdering (kommer)

Veileder om risikostyring i informasjonssikkerhet og personvern

6. Sikkerhetsrevisjon

POL art 24 *Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.*

Introduksjon

For å sikre våre digitale løsninger er det viktig at Kommunedirektørens lederteam har oversikt over system (herunder skytjeneste, programvare, infrastruktur, applikasjon), GDPR, ROS-analyser, sikkerhetsorganisasjon, mulige sikkerhetstrusler i nærmeste fremtid og kostnadsbildet.

For å dekke disse punktene, skal Sikkerhetsgruppa årlig levere en rapport som gjennomgås med KLT. Etter behandling skal det vedtas én Must win battle for året som kommer. Denne saken og andre punkter som det er naturlig å følge opp, skal føres i en handlingsplan som Sikkerhetsgruppa følger opp.

Roller

For å sikre god rapportering, er det viktig å definere noen roller rundt systemadministrasjon, jf. Sikkerhetsorganisasjonen i kapittel 3.

Kommunedirektøren er behandlingsansvarlig og har det overordnede ansvaret for kommunen.

Kommunedirektøren har delegert dette ansvaret til Sikkerhetsansvarlig som er økonomisjef i kommunen.

Sikkerhetsansvarlig støtter seg igjen på IKT-leder, som har ansvar for sikker drift, og Sikkerhetsgruppa som skal arbeide etter sitt mandat.

IKT-leder kan ikke ha oversikt over alle system, derfor skal hvert system ha disse to rollene definert: Systemeier og Systemansvarlig.

- Systemeier er alltid kommunalsjef for tjenesteområdet systemet hører til.
- Systemansvarlig er den ansatte som er operativt ansvarlig for systemet.

Hva skal rapporteres?

1. Dagens status for kommunens behandlingsprotokoll/Draftit (Jf. Personvernforordningen artikkel 30)
    a. Hvilke system er lagt inn og godkjent
    b. Hvilke system er lagt inn, men har mangler
    c. Hvilke system mangler
2. Kommunens organisering av ansvarsforhold knyttet til etterlevelse av personvernregelverket. (Jf. Personvernforordningen artikkel 5 nr. 2)
    a. Se kapittel om Sikkerhetsorganisasjon
3. En kort beskrivelse av kommunens overordnede styringssystem (interkontroll) for etterlevelse av personvernregelverket, herunder hvilke verktøy som eventuelt brukes.
    a. Orden i eget hus/internkontroll H&V
4. Styrende retningslinjer for gjennomføring av risiko- og sårbarhetsanalyser. (Jf. Personvernforordningen artikkel 32)
    a. Se ROS-analyse mal
5. Revidert sikkerhetshåndbok
    a. Se denne boka
6. Oversikt over IKT-samarbeid med andre kommuner
    a. Barnevern – Sandnes
    b. IKT-ledermøter med Jærkommunene
    c. DigiRogaland og ulike faggrupper
    d. Noen flere?
7. Styrende retningslinjer for autentiseringsløsninger i kommunen
    a. MFA og lignende
8. Styrende retningslinjer for sikkerhetskopiering og gjenoppretting av systemer. (Jf. Personvernforordningen artikkel 32.1.c)
    a. Finnes i Compilo
9. Styrende retningslinjer/prosedyrer for sikkerhetsrevisjoner (Jf. Personvernforordningen artikkel 32.1.d)
    a. Denne gjennomgangen
    b. Orden i eget hus
10. Kommunens personvernerklæring
    a. Se nettside
11. Kontaktinformasjon til kommunens personvernombud.
    a. Navn, telefonnummer og e-post
    b. Kort beskrivelse av organisering av personvernombudfunksjonen; herunder hvor stor del av full stilling vedkommende skal kunne bruke på utøvelsen av rollen.
12. Hvilke alvorlige sikkerhetsbrudd har vært i år.
13. Hvilke alvorlige sikkerhetstrusler ser Sikkerhetsgruppa og IKT-leder på som de mest sannsynlige i nær fremtid.
14. Hvilke opplæringstilbud er tilgjengelig for ansatte, er opplæringen tilstrekkelig og blir den fulgt opp.

15. Hvor mye koster IT-sikkerhet kommunen i året.
16. Når trengs neste eksternkontroll.

Rapporten skal leveres til KLT senest to uker før dato for gjennomgang. Rapporten skal stå ferdig innen 31. mars slik at rapporten kan føre til konkrete handlingsmål i god tid før Handlings- og økonomiplanen.

Selve gjennomgangen i KLT skal ledes av leder for Sikkerhetsgruppa. KLT, IKT-leder, beredskapsansvarlig, representant for hovedtillitsvalgte, representant for verneombud og Sikkerhetsgruppa skal inviteres.

Ansvar

Sikkerhetsgruppa har ansvar for å utarbeid rapporten i samarbeid med IKT-leder. Det er leder for Sikkerhetsgruppa som skal sette i gang arbeidet.

Systemeier har ansvar for at alle system er registrert i behandlingsprotokoll. Hver enkelt systemansvarlig bør stå for selve registreringen.

7. Konfigurasjon (arkitektur)

Med *konfigurasjon* menes informasjonssystemets utforming, det vil si utstyr og program, samt integrasjoner mellom disse.

Kommunen skal til enhver tid ha oversikt og kontroll over IKT-utstyr og programvare som benyttes i virksomheten. Kommunens informasjonssystem skal konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås i henhold til kommunens sikkerhetsstrategi, risikovurderinger og beslutninger om sikkerhetstiltak.

Konfigurasjonskontroll omfatter all programvare, servere, nettverksutstyr, interne og eksterne kommunikasjonsforbindelser m.m. som eies / disponeres av kommunen.

Følgende gjelder:

- Kommunens informasjonssystem er inndelt i soner som gjenspeiler skillet mellom behandling av sensitive (sikker sone) og "ikke-sensitive personopplysninger"(åpen sone).

- Denne soneinndelte konfigurasjonen sikrer også at ansatte (brukere) skilles med tanke på nettverkstilgang for kun å nå opplysninger som de er autorisert for.

- De deler av informasjonssystemet hvor sensitive personopplysninger behandles, er videre inndelt i samsvar med formålet med behandlingen av personopplysninger / tjenester kommunen leverer.

- Sikker sone er adskilt fra eksterne nett med minst to sikkerhetsbarrierer. Data kan ikke flyttes fra sikker sone til åpen sone.

- Tilgang til kommunens systemer gis via sikker oppkobling og gis ved konkret behov. Løsningen skal sikre at uautoriserte personer ikke får tilgang til kommunens informasjonssystem.

- Kommunens informasjonssystem skal være konfigurert i samsvar med kart over infrastruktur.

- Endringer i informasjonssystemets konfigurasjon skal utføres planmessig og systematisk og sikre at
    - *Alle konfigurasjonsendringer er i samsvar med besluttet sikkerhetsstrategi og digitaliserimgsstrategi.*
    - *Informasjonssystemet fungerer som forutsatt også etter at endringen er gjennomført.*

Ansvar

IKT-leder har ansvar for utforming og vedlikehold av konfigurasjonene og tilhørende dokumentasjon knyttet til informasjonssystemenes infrastruktur og driftstekniske forhold.

Systemeiere / Systemansvarlige / Superbrukere har ansvar for vedlikehold av konfigurasjonene og tilhørende dokumentasjon knyttet til fagsystemene.

Systemeier er ansvarlig for at det foreligger nødvendige avtaler (Service Level Agreement, databehandleravtaler) ved outsourcing av hele eller deler av kommunens IKT-driftstjenester eller når kommunen selv er databehandler for andre.

8. Avvik og avvikshåndtering

POL Art 33 og 34 Melding til tilsynsmyndigheten om brudd på personopplysningssikkerhet. Underretning av den registrerte om brudd på personopplysningsloven.

Avvik innen informasjonssikkerhet og personvern er brudd på etablert regelverk og prosedyrer som skal sikre konfidensialitet, integritet og tilgjengelighet.

Systematisk håndtering av avvik skal bidra til at brudd på lover, forskrifter, instrukser og rutiner rapporteres til ansvarlig person og sikre mulighet for læring og forbedring. Dersom det ikke er samsvar mellom fastlagte instrukser eller rutiner og hvordan informasjonssystemet faktisk benyttes, skal resultatet fra avvikshåndteringen benyttes som grunnlag ved eventuelle endringer.

Den enkelte medarbeider har ansvar for å rapportere avvik. Kommunens kvalitetssystem og gjeldende avviksrutiner skal benyttes. Det er viktig at man ikke bruker navn eller andre opplysninger som kan identifisere enkeltpersoner når man registrerer avvik.

Eksempler på situasjoner som gjør det nødvendig å iverksette rapportering og avvikshåndtering:

- Utilsiktet utlevering av personopplysninger, eller ved mistanke om slik utlevering.
- Medarbeidere som benytter informasjonssystem uten autorisasjon.
- Feil i utstyr eller program som kan ha innvirkning på informasjonssikkerheten eller driften av informasjonssystemet
- Brudd på taushetsplikten

Ved avvik som trolig vil medføre en risiko for personers rettigheter og friheter skal Datatilsynet varsles, jf. GDPR Artikkel 33. Dette skal skje uten ugrunnet opphold og senest 72 timer etter at avviket ble avdekket. Ved høy risiko skal den behandlingsansvarlige uten ugrunnet opphold underrette den registrerte om bruddet, jf. GDPR Artikkel 34.

Ansvar

Ansatte er ansvarlig for å rapportere avvik.

Avdelingsleder er ansvarlig for å følge opp rapporterte avvik og melde til Datatilsynet.

Sikkerhetsleder er ansvarlig for å påse at rutine for innmelding av avvik følges.

Personvernombud bistår ved behov.

Dokumentreferanse
Rutine for å melde avvik

9. Partnere og leverandører

POL art 28-3 *Behandling utført av en databehandler skal være underlagt en avtale eller et annet rettslig dokument i henhold til unionsretten eller medlemsstatenes nasjonale rett som er bindende for databehandleren med hensyn til den behandlingsansvarlige, og der gjenstanden for og varigheten av behandlingen, behandlingens art og formål, typen personopplysninger og kategorier av registrerte samt den behandlingsansvarliges rettigheter og plikter er fastsatt.*

Når eksterne partnere / leverandører behandler personopplysninger på vegne av Gjesdal kommune skal det alltid foreligge en skriftlig avtale som regulerer denne behandlingen, såkalt databehandleravtale.

- Databehandleravtalen skal være signert av begge parter før behandlingen iverksettes.
- Databehandleravtalen skal være i tråd med de til enhver tid gjeldende lovkrav, og signeres av systemeier med mindre det er felles for hele organisasjonen, da skal kommunedirektør signere. Alle databehandleravtaler arkiveres i kommunens sak-/arkivsystem.
- Ansatte hos partnere eller leverandører som gis adgang til kommunens datautstyr eller programmer skal underskrive taushetserklæring før adgang gis.
- Det er i utgangspunktet ikke tillatt å gi ansatte hos partnere og leverandører tilgang til kommunens IKT-løsninger med fjernstyringsverktøy, som for eks. Teamviewer, med mindre dette er godkjent av IKT-avdelingen.
- Alle konsulenter som kobler seg opp, skal ha undertegnet taushetserklæring, som en del av databehandleravtalen. Dersom dette ikke er en del av databehandleravtalen, må den enkelte konsulent undertegne dette før tilgang blir gitt.
- Alle som kobler seg opp til kommunens informasjonssystem ved bruk av slike fjernstyringsverktøy, skal informere om formål med oppkoblingen før denne tillates. De skal også gi tilbakemelding de ikke lenger har behov for tilkoblingen, og hva de har gjort mens de var koblet opp.
- Denne type fjerntilgang tillates kun så lenge det er nødvendig for den aktuelle oppgaven, og skal stenges umiddelbart når behovet opphører. Den som aktiverer fjerntilkoblingen, plikter å loggføre hendelsen.

- For prosess for å installere nye program, se digitaliseringsstrategien.

Ansvar
Ansatte som aktiverer fjerntilkobling plikter å loggføre hendelsen.

Avdelingsleder skal påse at eksternt personell signerer taushetserklæring ved behov.

Systemeier er ansvarlig for at det foreligger en signert databehandleravtale ved behov.

Dokumentreferanse
Mal databehandleravtale
Taushetserklæring
Leverandøroversikt

Må oppdateres!

10. Kompetanse

God sikkerhet forutsetter god opplæring og tilstrekkelig kompetanse hos de ansatte. Det er viktig å gjøre informasjonssikkerhet og personvern til en del av de ansattes daglige oppgaver – som en integrert del av kommunens internkontroll.

- Alle ansatte skal gis nødvendig opplæring i informasjonssikkerhet og personvern. Dette skal som minimum omfatte:
    - Instruks - Bruk av kommunens IKT-løsninger
    - Kurs - Informasjonssikkerhet for ansatte
    - Overordnede rutiner og instrukser.
    - Avdelingsspesifikke rutiner og instrukser.
    - Håndbok for informasjonssikkerhet

- Avdelingsleder er ansvarlig for at slik opplæring blir gitt til ansatte i sin avdeling.

- Krav til opplæring i informasjonssikkerhet og personvern samt tilhørende rutiner er samlet i en egen opplæringsplan (se lenke under). I tillegg til de ansatte omfatter planen også aktuelle opplæringstiltak for ledere, systemansvarlige, superbruker o.a. med spesielle roller i forhold til bruk og administrasjon av kommunens informasjonssystem.

- Dokumentasjon av de til enhver tid gjeldende rutiner og instrukser skal være tilgjengelig for alle ansatte på kommunens intranett og i kommunens avvikshåndteringssystem.

Det tilbys ulike former for opplæring innen informasjonssikkerhet og personvern, alt etter behov. Du finner mer informasjon om dette på kommunens interne nettsider.

Ansvar

Sikkerhetsleder fastsetter minimumskrav til ansattes kompetanse innen informasjonssikkerhet og personvern.

Avdelingsleder er ansvarlig for at nødvendig opplæring blir gitt til ansatte i sin avdeling.

Ansatte har selv ansvar for å følge opp og praktisere vedtatte regler og sikringstiltak. Dette innebærer årvåkenhet i det daglige arbeidet. Alle avvik som oppdages skal meldes nærmeste overordnede ved bruk av kommunens avvikshåndteringssystem.

Dokumentreferanse
Opplæringsplan – informasjonssikkerhet og personvern (kommer)
Taushetserklæring

Må oppdateres!

11. Autorisasjon

POL art 24 Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.

Med autorisasjon menes at en person, i et ansettelsesforhold, i en bestemt rolle, gis en bestemt rettighet til: Lesing av tekst og bilder, registrering, redigering, retting, sletting og/eller sperring av opplysninger.

Autorisasjon er personlig og skal registreres i et autorisasjonsregister.

Noen ansatte vil kunne ha utvidede systemrettigheter og/eller arkivtilgang, som superbrukere, systemansvarlige, arkivpersonell og ikt-personell. For disse påhviler det et særskilt ansvar i utøvelsen av sine rettigheter.

Det skal bare gis adgang til områder og utstyr, manuelle eller digitale informasjonssystemer, i den grad det er nødvendig for å utføre pålagte oppgaver. Alle typer autorisasjon som gis skal være i henhold til kommunens gjeldende sikkerhetsstrategi.

- Avdelingsleder er autorisasjonsansvarlig for manuelle og elektroniske behandlinger av personopplysninger i sin avdeling, og skal:
    - *Sørge for at alle nye ansatte, vikarer og periodisk personell får tilgang til aktuelle informasjonssystemer ved tilsetting i henhold til tjenstlige behov.*
    - *Skriftlig informere aktuelle instanser (Avdelingsleder/systemansvarlige o.l.) om endringer i behov for tilgang til informasjonssystemene.*
    - *Avslutte autorisasjoner når ansatte slutter eller ikke lenger har tjenstlig behov for autorisasjonen. Ved endringer i arbeidsforhold eller ansvar skal den ansattes tilganger i kommunens informasjonssystemer vurderes.*
    - *Årlig gjennomgå brukertilganger i egen avdeling.*

- Personer med periodisk arbeid for kommunens, f.eks. konsulenter, håndverkere, studenter og praktikanter, skal underskrive taushetserklæring, og være underlagt klare regler å forholde seg til når det gjelder:
    - *Hva de kan gjøre og ikke kan gjøre,*
    - *Hvor de kan oppholde seg,*
    - *Hvilke informasjoner de kan få tilgang til,*
    - *Hvilke konsekvenser eventuelle sikkerhetsbrudd kan få.*

- Ved sikkerhetsbrudd skal tilgangsstyringen for det aktuelle informasjonsområdet kontrolleres. Alle avvik registreres og behandles i henhold til gjeldende rutiner i kommunens kvalitetssystem.

For ethvert informasjonssystem hvor det kreves passord, skal passordet være i tråd med anbefalingene fra Nasjonal Sikkerhetsmyndighet:

De tre viktigste punktene er:

- Bruk unike passord
- Innfør to-faktor autentisering
- Ha lange passord:
    - Eks: Sikkerhetsgruppa-bestAar-av-8-gysla-fine-folk

Ansvar

Avdelingsleder er autorisasjonsansvarlig for elektroniske og manuelle behandlinger av personopplysninger i sin avdeling, og er ansvarlig for at taushetserklæring undertegnes.

Ansatte har selv et ansvar for sikkerheten på eget kontor/arbeidsplass, herunder å bidra til at uvedkommende ikke får tilgang til lagrede elektroniske opplysninger eller informasjon i papirform på arbeidsplassen.

IKT-avdelingen/systemansvarlige/superbrukere har ansvar for tildeling, endring og tilbaketrekking av autorisasjon til kommunens IKT-løsninger i henhold til melding fra autorisasjonsansvarlig (Avdelingsleder).

Dokumentreferanse

Taushetserklæring	Må oppdateres

Normen for informasjonssikkerhet og personvern i helse og omsorgssektoren- Autorisering

12. Fysisk sikkerhet

Tilfredsstillende fysisk sikkerhet er viktig for å hindre at uvedkommende får tilgang til opplysninger. Det er et samspill mellom tiltak for fysisk sikring og tiltak for elektronisk sikring. Tiltakene er gjensidig avhengig av hverandre for at tilfredsstillende sikkerhet skal oppnås.

Trusler som kan utløses ved for dårlig fysisk sikring kan bl.a. være:

- *At uvedkommende får tilgang til utstyr hvor kommunens informasjon behandles.*
- *Tyveri av datautstyr eller sikkerhetskopier.*
- *Sabotasje og hærverk mot vitale deler av informasjonssystemet.*

Risikovurderinger
Det skal gjennomføres risikovurderinger for alle fysiske arealer som skal sikres mot uautorisert adgang. Dette gjelder både på overordnet nivå og internt i hver avdeling.

Adgangskontroll
Adgang til kommunens lokaler skal kontrolleres.

Leder for byggforvaltning har ansvar for «skallsikring» av kommunens lokaler og administrasjon av adgangskontroll.

Avdelingsleder skal sørge for at lokaler og utstyr i sin avdeling er forsvarlig sikret. Det skal legges spesiell vekt på å sikre områder / rom hvor det det behandles gradert informasjon. Det tilstrebes at alle slike områder kontrolleres av digitalt adgangskontrollsystem.

Byggforvaltning skal føre oversikt over hvem som har tjenstlig behov for adgang til ulike områder og rom. Avdelingsleder er ansvarlig for å melde fra skriftlig til byggforvaltning om behov for og endringer i adgang.

Adgang til dedikerte rom med driftsutstyr (f.eks. serverrom) skal kun gis til personell med absolutte behov for tilgang. Generelt skal adgang i størst mulig grad begrenses.

Det er i dag varierende grad av besøkskontroll i de ulike avdelingene. Det skal tilstrebes at besøkende i størst mulig grad alltid følges av ansatt ved opphold i kommunens lokaler.

Fysisk sikring av utstyr utenfor kommunens lokaler
Utstyr som benyttes utenfor kommunens lokaler, f.eks. hjemmekontor/reise, skal sikres.

Ansvar

Avdelingsleder skal sørge for at lokale og utstyr i sin avdeling er forsvarlig fysisk sikret. Avdelingsleder har også ansvar for å melde inn endringer i adgangskontroll til byggforvaltning.

Ansatte skal følge regler for fysisk sikring av eget kontor/arbeidsplass.

Leder for byggforvaltning har ansvar for «skallsikring» av kommunens lokaler, samt overordnet administrasjon av adgangskontroll.

Dokumentreferanse
Instruks for innmelding av adgangskort

Tilgangsskjema

13. Dokumentsikkerhet

Dokumentsikkerhet omfatter sikker håndtering og oppbevaring av dokumenter i alle former. Det vil si alt fra tradisjonelt papirformat til all informasjon som kan leses, lyttes til, fremføres eller overføres, ved hjelp av maskinelt utstyr.

Sentrale momenter innenfor dokumentsikkerhet:

- Merking
- Journalføring
- Forsendelse, intern ombringelse og på reise

- Utlån, mangfoldiggjøring og annen spredning
- Tilintetgjøring, evakuering og rekonstruksjon
- Kontroll og rapportering
- Tilgjengelighet

Ansvar

Arkivleder har ansvar for å utarbeide og vedlikeholde overordnede rutiner og instrukser for dokumentsikkerhet i de digitale og fysiske arkivene.
Sikkerhetsgruppa har ansvar for at det utarbeides og vedlikeholdes overordnede rutiner og instrukser for dokumentsikkerhet i øvrige system.
Avdelingsleder har ansvar for å ivareta tilfredsstillende dokumentsikkerhet i egen avdeling.
Ansatte har selv et ansvar for å ivareta tilfredsstillende dokumentsikkerhet.

Dokumentreferanse
Arkivplan Gjesdal kommune

14. Internkontroll (dette kapittelet er under arbeid på grunn av nye retningslinjer fra Datatilsynet)

POL art 24 *Idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, samt risikoene av varierende sannsynlighets- og alvorlighetsgrad for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning. Nevnte tiltak skal gjennomgås på nytt og skal oppdateres ved behov.*

Internkontroll for informasjonssikkerhet i Gjesdal kommune skal bidra til

- helhetlig styring og riktig utvikling.
- kvalitet og effektivitet i tjenestene.
- godt omdømme og legitimitet.
- etterlevelse av politiske vedtak, rutiner, instrukser, lover og forskrifter.

Sjekkliste for internkontroll er hentet fra Datatilsynets sjekkliste for kommunens internkontroll.

Regelverket inneholder en rekke krav og påbud. I sjekklisten er regelkravene omsatt til påstander som kommunen svarer" ja" eller" nei" på. I første kolonne i tabellen blir dette visuelt fremvist som grønt (ja) og rødt (nei).

Ideelt sett skal vi kunne svare ja på alle spørsmål i sjekklista. Det betyr at kommunen etterlever personopplysningsloven på en god måte. For alle spørsmål der svaret er nei, må det sørges for å innføre tiltak, sikre dokumentasjon, eller bygge opp systemer for å sikre at vi etterlever loven.

Sjekklisten er delt inn i fire hoveddeler:

- Styrende del – Overordnet fokus, hovedsakelig rettet mot ledelsen.

- Gjennomførende del – Praktisk fokus, rutiner som sikrer at ansatte følger regelverket.
- Kontrollerende del – Kontrollrutiner som sikrer at kommunen etterlever regelverket.
- Andre forhold – Andre viktige elementer som taushetsplikt og forhold til andre virksomheter.

Aktører beskrevet i tabellen er ansvarlig (A), kontrollør (K) og utfører (U). Referansen gir en henvisning til gjeldende dokumentasjon, instruks eller rutine.

15. Passord for bruker i Office365

Hver bruker skal ha et unikt passord. Passordet skal bestå av minst 16 tegn og er gyldig i ett år med mindre det kommer på avveie. Tegnene kan ikke være ÆØÅ eller mellomrom.

16. Godkjenningsløp for program

Dersom ansatte i kommunen skal installere et nytt program på sin enhet, skal den først godkjennes av sikkerhetsgruppa. For å melde inn nye program til Sikkerhetsgruppa, fyller ansatt ut dette skjema og så blir det behandlet på neste møte.

Link til skjema: https://forms.office.com/e/nUTHe91Z44
Oversikt over allerede godkjente program ligger i Helpdesk-systemet.

17. Bruk av generativ KI

Denne teksten beskriver generativ kunstig intelligens (KI). For annen bruk av KI må det lages nye retningslinjer før bruk.

Generativ KI letter arbeidsbyrden i mange prosesser, men det må samtidig brukes med varsomhet. Nedenfor følger retningslinjer for bruk av generativ KI i Gjesdal kommune. Retningslinjene bygger på anbefaling fra Digitaliseringsdirektoratet som en finner her: Bruk av generativ kunstig intelligens i offentlig sektor | Digdir

Hva er generativ KI?

Med generativ KI menes kunstig intelligens som brukes til å genere tekst, bilder, musikk, video eller lignende. En generativ KI-modell for tekst vil for eksempel være trent på en enormt stor mengde tekst slik at den kan lage «ny» tekst når en bruker ønsker det.

Det genererte svaret lages ved at brukeren sender inn en ledetekst som beskriver ønsket resultat. KI-modellen analyserer så ledeteksten og skriver et svar den tror passer.

Retningslinjer

Nedenfor beskrives flere retningslinjer for bruk av generativ KI. De viktigste er oppsummert her:

- Bruk Copilot Edge eller egen KI-plattform for skole.
- Aldri del sensitive opplysninger med KI.
- Vær kritisk til det du får tilbake. Datagrunnlaget til modellen, modellens oppsett og leverandørens verdier påvirker resultatet.
- Opplys alltid om det dersom du publiserer KI-generert tekst, bilde eller lignende.
    - Skriv “Teksten er generert ved hjelp av KI og godkjent av forfatter”

- Du er til syvende og sist ansvarlig for alt du generer fra KI dersom du bruker det videre. Alltid sjekk at det som er generert ikke inneholder faktafeil, er diskriminerende eller plagierer eksisterende tekster.

Alltid bruk Copilot Edge for tekstgenerering (eller egen KI-plattform for skole)

Copilot Edge er Gjesdal kommunes primære kunstige intelligens. For ansatte i skole finnes det en egen KI-plattform. I Copilot Edge og KI-plattformen for skole kan både bilder og tekst genereres og ledetekstene blir ikke analysert videre av leverandøren. Det er likevel viktig å ikke dele sensitiv informasjon.

Andre KI-tjenester er mulig å bruke, men ikke anbefalt fra Gjesdal kommune. Bruker en KI-tjenester utenfor de anbefalt av Gjesdal kommune er vi ikke sikret hvordan informasjonen vi skriver inn brukes videre. Det er derfor imperativt at det ikke skrives inn noe sensitive opplysninger her.

Riktig opplæring for brukere

Brukere av generativ KI skal ha tilstrekkelig opplæring og forståelse for å bruke teknologien ansvarlig og effektivt. Dette inkluderer kunnskap om risikoer, samt beste praksis for bruk.

Ikke bruk sensitiv informasjon i ledetekster

Personopplysninger, taushetsbelagt informasjon, gradert informasjon, informasjon unntatt offentlighet, sikkerhetssensitiv informasjon eller immaterialrettslig vernet informasjon skal ikke brukes til å gi instruksjoner til generative KI-verktøy. Som utgangspunkt må det legges til grunn at informasjonen i en ledetekst blir sendt til selskapet bak verktøyet og vil bli lagret og brukt til videre trening av den underliggende maskinlæringsmodellen.

Tidskritiske prosesser

De generative KI-systemene har tidvis vært ustabile. Det skyldes blant annet svært høy trafikk til deres servere. Generativ kunstig intelligens bør derfor ikke brukes for tidskritiske prosesser.

Vær kritisk til modellens datagrunnlag

Generative KI-modeller er trent på enormt store mengder data. Når en trenger så store mengder data, vil det forekomme datasett med innebygde skjevheter basert på tanker fra tida forskningen ble gjort. Det er også vanlig at selskapene som gir ut modellene har lagt til begrensninger eller retningslinjer for modellens svar. Dette betyr også at en generativ KI-modell ikke bør brukes som et oppslagsverk.

Vær varsom ved bruk av språkmodeller som faktabasert oppslagsverk

KI-språkmodeller er laget for å gi brukeren et svar som virker fornuftig, men om svaret er rett eller galt er ofte sekundært. Dette fører til at språkmodeller ikke nødvendigvis er gode oppslagsverk når det gjelder fakta, selv om det kan virke slik. Det språkmodeller derimot er gode på er sammenhenger i og mellom språk. Det vil si at språkmodeller er veldig gode på å oversette, språkvask av tekst og genere programmeringskode.

KI finner sammenhenger selv om det kanskje ikke finnes noen

Som annen kunstig intelligens, finner generativ KI sammenhenger mellom ulike faktorer i en stor mengde data. Store språkmodeller forstår sammenhenger i språk. En sammenheng betyr imidlertid ikke at det er et årsak-virkning-forhold. Ved bruk av generativ kunstig må en ha et bevisst forhold at det er tilsynelatende sammenhenger som presenteres. Hvorfor presenteres akkurat denne tilsynelatende sammenhengen, og bør en være kritisk til denne? Dette gjelder særlig der en eventuell

tilsynelatende sammenheng er knyttet til faktorer som kan lede til diskriminering eller ulovlig forskjellsbehandling.

Innenfor statistikk kalles dette korrelasjon (tilsynelatende sammenheng), ikke kausalitet (årsak-virkning-forhold). Et eksempel kan være at KI vil tolke to ting som ofte skjer samtidig som tilsynelatende sammenhengende, som for eksempel, iskremsalg og at folk blir solbrent. Den klarer dermed ikke å forstå at det er noe annet, sol og varme, som er årsaken til begge to.

Bruk ytterligere verktøy som kan identifisere plagiat

Det finnes flere verktøy som kan bidra til å vurdere om tekstmaterialet som er produsert av en stor språkmodell kan være plagiat. Eksempelvis har enkelte skrivebehandlingsverktøy en «redaktør-funksjon» som kan bidra til å vurdere om tekstmaterialet er plagiert.

Opplys om at innholdet er KI-generert

Alt innhold som er generert av KI skal også informere om at det er generert av KI. Dette er spesielt viktig ved generering av realistiske bilder da det kan være vanskelig å skille KI-genererte bilder fra ekte bilder.

Skriv “Teksten er generert ved hjelp av KI og godkjent av forfatter”.

Kvalitetssikre alltid innhold fra store språkmodeller

I tillegg til å påse at materialet ikke er plagiert, bør du alltid lese over og kvalitetssikre. Ikke bruk materialet direkte. Det er du som til slutt er avsender av teksten og skal stå inne for innholdet.

18. Hente ut informasjon fra personlig e-post/dokumentområde

OneDrive og e-post er personlige. Det vil si at arbeidsgiver ikke skal ha innsyn i disse områdene. Det kan likevel forekomme at arbeidsgiver trenger informasjon som er kritisk for å sikre drift fra et personlig område etter at en ansatt slutter, er sykemeldt over lengre tid eller lignende.

Datatilsynet sier følgende om slike situasjoner:
Det er ikke tilstrekkelig at innsynet er praktisk og enkelt å gjennomføre av hensyn til den daglige driften. Det er kun tillatt å gjøre innsyn i e-post eller private filer dersom det ikke finnes andre mindre inngripende måter å oppnå det samme på.

Det kan være nyttig å forestille seg arbeidsgiverens berettigede interesser og den ansattes interesser på en skala. Arbeidsgiverens berettigede interesser kan variere fra nokså ubetydelige til tungtveiende. Innvirkningene på den ansatte kan også variere fra begrenset til meget alvorlig. Dersom arbeidsgiverens berettigede interesser er av mindre betydning, går de kun foran arbeidstakers interesser når disse er enda mer ubetydelige.

Rutinen for å hente ut informasjon fra personlig område er derfor som følger:

- Leder tar opp saken med kommunalsjef som igjen tar saken opp i Sikkerhetsgruppa og presenterer grunnlaget for hvorfor de trenger å hente ut filer og hvilke andre alternativ de har vurdert. Sikkerhetsgruppa må så vedta om det er god nok grunn eller ikke.

- Leder/kommunalsjef informerer tidligere ansatt hvilke filer som skal hentes fra personlig område og hvorfor. Tidligere ansatt inviteres med for å være med på uthentingen, men det er ikke et krav at hen er til stede.

- Når punktene ovenfor er utført og dokumentert, så kan IKT gå inn og hente fil(ene), men da med tillitsvalgt til stede som passer på at alt går rett for seg.

19. Utviklingsgruppa og sikkerhetsgruppa

Utviklingsgruppa er et internt organ som blant annet koordinerer anskaffelser av IKT-løsninger. Sikkerhetsgruppa arbeider med informasjonssikkerhet og personvern:

Utviklingsgruppa:

- *Anskaffelse, integrasjon og koordinering*
  Faggruppen skal sørge for at all anskaffelse eller større oppgradering av IKT-løsninger skal skje i tråd med kommunens digitaliseringsstrategi.

Sikkerhetsgruppa:

- Sikkerhetsgruppa skal være et ansvarliggjort og myndiggjort organ som har mandat til å fatte vedtak i pågående sikkerhetssaker.
- I noen saker vil det være mest hensiktsmessig å drøfte saken i andre organ som for eksempel i utviklingsgruppa eller kommunedirektørens ledergruppe eller sende forslaget ut på høring før det fattes et endelig vedtak.
- Gruppa skal påse at kravene til arkivtjeneste, informasjonssikkerhet og personvern er ivaretatt før sak fremmes til utviklingsgruppa eller kommunedirektørens ledergruppe for avgjørelse.

Utviklingsgruppa består av representanter fra hvert tjenesteområde, representant fra KLT, hovedtillitsvalgt, IKT-leder, digitaliseringsansvarlig og ledes av utviklingsleder. Ved større beslutninger gir Utviklingsgruppa råd til KLT.

Sikkerhetsgruppa består av representanter fra hvert tjenesteområde, representant fra KLT, representant fra IKT, personvernombud og ledes av Digitaliseringsansvarlig. Gruppa er ei undergruppe av Utviklingsgruppa. Mer informasjon og mandat finnes her: https://gjesdalkommune.sharepoint.com/sites/GK/SitePages/Utviklingsgruppa.aspx

20. Personvernombud

POL Art. 37 ***Utpeking av en personvernrådgiver (utdrag):*** *Den behandlingsansvarlige skal utpeke en personvernrådgiver når behandlingen utføres av en offentlig myndighet.*

Som offentlig virksomhet er Gjesdal kommune pålagt å ha personvernombud, jf. POL Art. 37

Personvernombud i Gjesdal kommune:

Bertha Johanne Fjelde Sivertsen
Personvernombud

e-post: personvernombud@Gjesdal.kommune.no
Telefon: 95988745

Kontaktinformasjon til ombudet finnes på kommunens hjemmesider.

Et personvernombud er en formelt oppnevnt kontakt for personvern og informasjonssikkerhet internt i organisasjonen mot ledelse/ansatte og eksternt mot Datatilsynet/den registrerte. Ombudet skal håndtere henvendelser fra de ulike aktørene og kan være et bindeledd mellom disse. Ombudet skal være en ressursperson som har kunnskap om virksomheten og behandlingen av personopplysninger.

Det juridiske ansvaret for at behandlingen av personopplysninger skjer i tråd med regelverket ligger hos behandlingsansvarlig (Kommunedirektøren). Personvernombudet har som oppgave å gi råd og veiledning om hvordan Gjesdal kommune best mulig kan ivareta personverninteressene. Dette innebærer blant annet å:

- Informere og gi råd om de forpliktelsene kommunen har etter personvernlovgivningen
- Kontrollere overholdelsen av personvernregelverket
- Gi råd om vurdering av personvernkonsekvenser
- Samarbeide og rådføre med Datatilsynet
- Bidra til å få oversikt over behandlingene
- Ta imot henvendelser fra de registrerte om personvernspørsmål

Personvernombudet skal tidlig involveres i alle saker som handler om behandling av personopplysninger i kommunen. Personvernombudet rapporterer til høyeste ledelsesnivå.

Dokumentreferanse
Kontaktinformasjon personvernombud