



# Informasjonssikkerhet og personvern

## Definisjoner



**Gjelder for:** Alle ansatte

**Vedtatt av:** Rådmannen

**Dokumentansvarlig (Enhet):** Interne tjenester

**Revisjonsintervall:** Årlig

**Distribusjon:** Intranett, hjemmeside, QM+

**Merknad:** Vedlegg til «Håndbok for informasjonssikkerhet». Definisjon av sentrale begreper som benyttes i dokumentasjon av kommunens informasjonssikkerhet og personvern.

## DEFINISJONER

<b>Adgangskontroll</b>	Kontroll av medarbeideres adgang til områder eller utstyr, med retningslinjer for tildeling av adgang og bruk av fysiske innretninger.
<b>Akseptert risiko</b>	Se <a href="#">risiko</a> .
<b>Ansatt</b>	Fast og midlertidig ansatt, samt innleid personell (for eks. konsulent eller håndverker), studenter, praktikanter, mv.
<b>Arkivverdig informasjon</b>	I prinsippet alle typer av informasjon som skal bevares for ettertiden og som skal kunne gjenfinnes på et senere tidspunkt. Arkivverdighet er kanaluavhengig. <a href="#">Kommunens arkivreglement</a> gir nærmere opplysninger om hva som ligger i begrepet.
<b>Automatisert avgjørelse</b>	Avgjørelser med rettsvirkning, eller som på tilsvarende måte betydelig påvirker vedkommende, som foretas av dataprogrammer uten menneskelig innblanding eller påvirkning.
<b>Autorisasjon</b>	En person i en bestemt rolle gis bestemte rettigheter for tilgang til informasjon. Kan bare gis i den grad det er nødvending for vedkommendes arbeid, er begrunnet ut fra tjenstlig behov og er i henhold til bestemmelser om taushetsplikt.
<b>Avvik</b>	Hendelse eller tilstand som bryter med gjeldende lover og regler, samt Eigersund kommunes instruks og interne rutiner.
<b>Behandling av personopplysninger</b>	All bruk av personopplysninger, slik som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksområder. Både manuelt og ved bruk av digitale løsninger.
<b>Behandlingsansvarlig</b>	Virksomhetens leder, i Eigersund kommune representert ved Rådmannen, som har det juridiske ansvaret for at gjeldende personvernlovgivning følges.
<b>Brannmur</b>	Et system eller en gruppe system for tilgangskontroll mellom ulike nettverk og soner for ulike tjenester.
<b>Bruker</b>	Person som har tilgang til kommunens IKT-løsninger.
<b>Brukerkonto</b>	En brukers definerte tilgang til IKT-ressurser som datamaskiner, nettverk, fagsystemer m.m.
<b>Brukernavn</b>	En unik symbolsk betegnelse som identifiserer en bruker/brukerkonto med tilgang til en IKT-ressurs.
<b>Databehandler</b>	Den som behandler personopplysninger på vegne av den behandlingsansvarlige.

<b>Dataoverføring</b>	Elektronisk overføring av data i et informasjonssystem. Dataoverføring der overføringsmedium er utenfor kommunens kontroll betegnes eksternt dataoverføring.
<b>Demilitarisert sone (DMZ)</b>	En sone hvor eksterne kan gis tilgang, men hvor kommunen har en viss grad av sikkerhetsmessig kontroll. Demilitarisert sone (DMZ) er ofte en del av en brannmurløsning.
<b>Eksternt nettverk</b>	Fellesbegrep for nettverk med elektroniske tjenester som tilbys eller brukes av andre virksomheter enn kommunen selv.
<b>Elektronisk kommunikasjon</b>	All form for kommunikasjon ved bruk av elektroniske midler. Dette omfatter bla e-post, nettbaserte meldingstjenester, sosiale medier, telefaks, tekstmeldinger mv.
<b>Felles lagringsområde</b>	Lagringsområde på kommunens nettverk som er tilgjengelig for flere brukere, gjerne avgrenset til en enhet.
<b>Fødselsnummer</b>	Fødselsnummer (11 siffer) er et unikt identifiseringsnummer som staten tildeler alle mennesker som blir født eller bosetter seg i Norge. Nummeret regnes ikke som en sensitiv opplysning og er ikke taushetsbelagt. Det er allikevel skjermingsverdig og klare grenser mot publisering, offentliggjøring mv.
<b>GDPR</b>	General Data Protection Regulation, <a href="#">personvernforordningen</a> .
<b>Gradert informasjon</b>	I Eigersund kommune brukes benevnelsen gradert informasjon som en fellesbetegnelse om sensitive personopplysninger, taushetsbelagt informasjon og skjermingsverdig informasjon som fødselsnummer.
<b>Helseopplysninger</b>	Personopplysninger om en fysisk persons fysiske eller psykiske helse, herunder ytelse av helsetjenester som gir informasjon om vedkommende sin helsetilstand.
<b>Hjemmekontor</b>	Teknisk løsning som gjør at det er mulig å koble seg opp til kommunens sentrale IKT-systemer på en sikker måte fra eksterne lokasjoner (f.eks. hjemmefra, fra hytta).
<b>IKT</b>	Informasjons- og kommunikasjonsteknologi
<b>Informasjonssikkerhet</b>	Tiltak iverksatt for å sikre at informasjon ikke er tilgjengelig uten autorisasjon (konfidensialitet), at informasjon ikke uautorisert endres eller ødelegges (integritet) og å sikre at informasjon er tilstede og anvendelig for medarbeidere slik at pålagte oppgaver kan utføres (tilgjengelighet).
<b>Informasjonssystem</b>	Et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon. Et informasjonssystem er teknologinøytralt, det kan være helt manuelt eller en IKT-løsning.

<b>Instruks</b>	Veiledning, ordre, pålegg og regler for hvordan og hva som skal utføres. Vedtas av rådmann eller den som har fått delegert fullmakt til dette. Instruks vil i hovedsak kun gjelde internt i organisasjonen Eigersund kommune.
<b>Integritet</b>	Å sikre at informasjon og informasjonssystemer er korrekte, gyldige og fullstendige. Beskyttelse mot utilsiktet endring av opplysninger.
<b>Interessent</b>	Personer, grupper eller organisasjoner som kan påvirke, vil bli påvirket av, eller oppfatter at de vil bli påvirket av behandlingen.
<b>Intern sone</b>	Fellesbegrep for de ulike nettverk som finnes i kommunen til bruk for de ansatte. Intern sone må være forsvarlig sikret mot eksterne nettverk. Sensitive personopplysninger skal ikke lagres i intern sone.
<b>Internkontroll</b>	Kvalitetssystem med planlagte og systematiske tiltak for etterlevelse av regelverk.
<b>Konfidensialitet</b>	Å sikre at informasjon og informasjonssystemer bare er tilgjengelig for de som skal ha tilgang.
<b>Konfigurasjon</b>	Informasjonssystemets utforming, det vil utstyr og program samt sammenkoblinger mellom disse.
<b>Kryptering</b>	Prosess som gjør informasjon uforståelig for andre enn dem som er autorisert for tilgang. Det er egne krav til godkjent kryptering av informasjon.
<b>Lagringsmedia</b>	Et lager som inneholder informasjon i form av tekst, lyd eller bilde. Dette kan være fysisk som papir (tilsvarende) eller elektronisk som harddisk, minnepinne, minnekort mv..
<b>Lokal lagring</b>	Lagring av informasjon direkte på den enkelte brukers klientutstyr (f.eks. lokal disk på brukerens PC, nettbrett, mobiltelefon, minnepinne m.v.) Data lagret her omfattes ikke av kommunens sentrale backupløsning.
<b>Makulering</b>	Fysisk ødeleggelse av lagringsmedia i en slik grad at det ikke er mulig å rekonstruere informasjon på lagringsmediet, f.eks bruk av makuleringsmaskin, fysisk knusing av digitale lagringsmedier.
<b>Metadata</b>	Data om data, informasjon som beskriver annen informasjon, om en elektronisk fil (tekstdokument, bilde, film). Metadata kalles også "tagging". Så godt som alle dokumenttyper har, eller har mulighet for, slik metadata.
<b>Normen</b>	Norm for informasjonssikkerhet i helse og omsorgstjenesten (Normen) er et omforent sett av krav til informasjonssikkerhet basert på lovverket. Normen er først og fremst basert på personvern- og helselovgivningens krav til å etablere tilfredsstillende informasjonssikkerhet for systemer som behandler helse- og personopplysninger.

<b>Passord</b>	En sekvens av tegn som sammen med tilhørende brukernavn gir en autorisert bruker tilgang til en IKT-ressurs. Det er egne krav til utforming og oppbevaring av passord.
<b>Periferutstyr</b>	Utstyr som kan kobles til f.eks. en datamaskin. Eksempler på periferutstyr er skrivere, skannere, minnepinne mm.
<b>Personlig lagringsområde</b>	Lagringsområde på kommunens nettverk som ikke er tilgjengelig for andre enn den enkelte bruker.
<b>Personopplysning</b>	En opplysning eller vurdering som kan knyttes til deg som enkeltperson (den registrerte). For eksempel navn, adresse, kontaktinformasjon, IP-adresse, bilnummer, bilder, fingeravtrykk, hodeform, fødselsnummer, adferdsmønstre, mv.
<b>Personvern</b>	Retten til et privatliv og retten til å bestemme over egne personopplysninger
<b>Personvernombud</b>	En person som er utpekt av en behandlingsansvarlig og godkjent av Datatilsynet. Personen har som oppgave å bidra til at den behandlingsansvarlige følger personopplysningsloven med forskrift.
<b>PKI</b>	Public Key Infrastructure – infrastruktur for offentlig nøkkelkryptering. En teknologi for å utstede, administrere og bruke elektronisk ID og e-signatur basert på en standardisert krypteringsteknologi.
<b>Privat utstyr</b>	Alt utstyr som ikke er kjøpt eller eies av Eigersund kommune eller som kommunen ikke har stilt til disposisjon for den enkelte bruker.
<b>Registrert</b>	Den personen som en personopplysning kan knyttes til.
<b>Reglement</b>	Overordnede regler om hvordan noe skal utføres. Vedtas av politisk utvalg. Vil ofte også gjelde utover administrasjonen, f.eks politikere, publikum.
<b>Risiko</b>	Risiko betegner forholdet mellom sannsynligheten for at en uønsket hendelse vil inntreffe og konsekvenser av en slik hendelse. Akseptert risiko er ledelsens etablerte kriterier for hvilken risiko som aksepteres.
<b>Rolle</b>	Sammensetning av en eller flere funksjoner som gir ulike typer tilgang til en IKT-løsning. Rolle tildeles ut fra stilling, arbeidsoppgaver og plassering i organisasjonen. Enhetsleder gir autorisasjon til informasjonssystemet basert på rolle.
<b>Rutine</b>	Detaljert fremgangsmåte, ofte praktisk, på gjennomføring av ulike forhold. Vedtas av rådmann eller den som har fått delegert fullmakt til dette.

<b>Samtykke</b>	En frivillig, uttrykkelig og informert erklæring fra den registrerte om at han/hun godtar behandling av opplysninger om seg selv.
<b>Sensitive personopplysninger (særlige kategorier)</b>	Beskrives i <a href="#">personvernforordningen artikkel 9</a> . Personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering. Omfatter også personopplysninger om straffedommer og lovovertridelser som beskrevet i <a href="#">personvernforordningen artikkel 10</a> .
<b>Sikker sone</b>	En sone for behandling av sensitiv informasjon som er sikkerhetsmessig atskilt fra andre sikrede soner, intern sone og dobbelt sikret mot eksterne nettverk.
<b>Sikkerhetshendelse</b>	Enhver hendelse som kan kompromittere sikkerheten i et system eller en tjeneste og åpne denne for urettmessig tilgang.
<b>Skybaserte IKT-løsninger</b>	IKT-løsninger som ikke driftes av kommunen og der tilgang skjer via internett gjennom en standard nettleser. All informasjon lagres normalt utenfor kommunens nettverk.
<b>Sletting av informasjon</b>	Det skilles mellom:  <i>Sikker sletting:</i> Fjerning av informasjon uten å ødelegge lagringsmediet og der det i etterkant er umulig å rekonstruere informasjonen som har blitt slettet. Det er egne krav til godkjent bruk av sikker sletting.  <i>Usikker sletting:</i> Fjerning av informasjon men der informasjonen på en enkel måte kan rekonstrueres.
<b>Sone</b>	De deler av informasjonssystemet som kan kommunisere ved hjelp av dataoverføring. Soner opprettes etter analyse av behovet for tilgang og dataoverføring mellom enkelte enheter i informasjonssystemet.
<b>Sporbarhet</b>	Beskriver metoder som gjør det mulig å knytte enhver endring av informasjon til en identitet.
<b>System</b>	Se informasjonssystem.
<b>Taushetsplikt</b>	Taushetsplikt er en plikt til å hindre andre å få adgang eller kjennskap til bestemte opplysninger. Taushetsplikt kan følge av lov, instruks eller avtale.
<b>Tilgangskontroll</b>	Kontroll av tilgang til soner, data og program. Tilgangskontroll skjer i henhold til retningslinjer for tildeling av tilgang (autorisasjon) og bruk av informasjonssystemet.

**Tilgjengelighet**

Å sikre at informasjon og informasjonssystemer er tilgjengelig innenfor de tilgjengelighetskrav som er satt.

**Virksomhets sertifikat**

Sertifikat som identifiserer en registreringsenhet eller en underenhet i Enhetsregisteret.