

VEDLEGG 6 DEFINISJONER OG NASJONALE RESSURSER

Definisjoner

Definisjoner er i hovedsak hentet fra eller anvendt som utgangspunkt [Datatilsynets ordliste](#), samt [Digitaliseringsdirektoratets ordliste for internkontroll med informasjonssikkerhet](#).

Avvik	Hendelse eller situasjon som bryter med gjeldende regler eller interne retningslinjer. Et avvik kaller også en uønsket hendelse. Avvik, eller brudd, knyttet til personopplysningssikkerhet skal meldes til Datatilsynet innen 72 timer, med mindre avviket sannsynligvis ikke vil medføre en risiko for fysiske personers rettigheter og friheter.
Behandling av personopplysninger	All bruk av personopplysninger, slik som innsamling, registrering, sammenstilling, lagring og utlevering, eller en kombinasjon av slike bruksmåter.
Behandlingsansvarlig	Den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes. Dette er vanligvis en virksomhet.
Behandlingsgrunnlag	Rettslig grunnlag for å behandle personopplysninger. Dette kan for eksempel være samtykke eller lov.
Behandlingsprotokoll	Oversikt over alle behandlinger av personopplysninger i virksomheten. Må inneholde informasjon som er opplistet i GDPR artikkel 30.
Brudd på personopplysningssikkerhet	Et brudd på sikkerheten som fører til utilsiktet eller ulovlig tilintetgjøring, tap, endring, ulovlig spredning av eller tilgang til personopplysninger som er overført, lagret eller på annen måte behandlet.
Databehandler	Den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. Dette er vanligvis en virksomhet.
Databehandleravtale	En avtale mellom databehandler og behandlingsansvarlig om hvordan personopplysninger skal behandles.

Etableringsaktivitet	Etableringsaktiviteter er aktiviteter som bør gjennomføres når en virksomhet første gang skal etablere systematisk internkontroll på informasjonssikkerhetsområdet. De kan også være aktuelle ved behov for oppdatering eller vesentlig forbedring av ulike deler i det grunnleggende arbeidet.
Iboende risiko	Den risiko som ligger naturlig i virksomheten, på bakgrunn av drift og bransje, eller risikoen som ligger naturlig i produktet mv.
IKT-system	IKT-systemer er et fellesbegrep for informasjons- og kommunikasjonssystemer, dvs. systemer som samler inn, behandler, overfører, lagrer og presenterer informasjon. Begrepet inkluderer her også infrastruktur og nettverk som er knyttet til IKT-systemet.
Informasjonssikkerhet	Sikring av opplysninger ved å bruke prinsippene om konfidensialitet, integritet og tilgjengelighet. Det betyr å sikre informasjonssystemene som benyttes for å behandle informasjon – inkludert sikkerhet i alle IKT-systemer, IKT-tjenester og IKT-komponenter som inngår i systemene.
Informasjonssikkerhetsbrudd	Informasjonssikkerhetsbrudd er brudd på konfidensialitet, integritet og/eller tilgjengelighet. Bruddet kan ha store, små eller ingen konsekvenser.
Informasjonssystem (se også «IKT-system»)	Et informasjonssystem er et system for innsamling, lagring, behandling, overføring og presentasjon av informasjon.
Informasjonsverdi	Informasjonsverdi, eller bare verdi i en informasjonssikkerhetssammenheng, er et samlebegrep. Begrepet inkluderer både informasjon og tilhørende støtteverdier som IKT-system, digitale tjenester, datautstyr av ulike varianter mv. Støtteverdiene er «noe» som benyttes i behandlingen av informasjonen.
Integritet	Prinsipp om at opplysninger skal være sikret mot utilsiktet eller uautorisert endring eller sletting.
Internkontroll	Planlagt og systematisk styringssystem som virksomheter etablerer for å oppdage brudd på gjeldende regler.

Konfidensialitet	Prinsipp om at opplysninger må være sikret mot at uvedkommende får tilgang til dem.
OT-system	Operativ teknologi (OT) referer til maskinvare- og programvaresystemer som brukes til å overvåke, kontrollere og administrere fysiske prosesser i ulike bransjer og kritisk infrastruktur.
Personopplysning	Opplysning eller vurdering som kan knyttes direkte eller indirekte til en enkeltperson.
Personopplysningsloven	Personvernforordningen inngår i personopplysningsloven. Personopplysningsloven består i tillegg av særnorske regler.
Personvernforordningen	EUs forordning (regelverk) for personvern og en del av personopplysningsloven. På engelsk: the General Data Protection Regulation (GDPR).
Personvernkonsekvensvurdering (DPIA)	En prosess som skal bidra til å håndtere de risikoene behandlingen medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastlegge risikoreduserende tiltak. DPIA er en forkortelse for Data Protection Impact Assessment, en vurdering av personvernkonsekvenser.
Personvernombud	En person som er utpekt av en behandlingsansvarlig. Personen har som oppgave å bidra til at den behandlingsansvarlige følger personopplysningsloven.
Risiko	Hypotese om hvilken fare en hendelse representerer eller sannsynlighet kombinert med konsekvens.
Risikostyring	Risikostyring er et sett av aktiviteter for å styre og kontrollere risiko. De kalles ofte «risikostyringsprosessen», men aktivitetene er ikke nødvendigvis sekvensielle. De ulike aktivitetene kan i hovedsak være foranlediget av hvilken som helst av de andre aktivitetene.
Sikkerhetsavtale	Avtale etter sikkerhetsloven som skal regulere sikkerheten ved gjennomføre en sikkerhetsgradert anskaffelse som gir leverandøren tilgang til sikkerhetsgradert informasjon, skjermingsverdige objekter eller skjermingsverdig infrastruktur uten oppsyn av en representant fra kommunen.

Sikkerhetstiltak	Når det snakkes om sikkerhetstiltak menes alt som gjøres for å redusere risikoer på informasjonssikkerhets- og personvernområde. I personvernforordningen er sikkerhetstiltakene kategorisert som tekniske og organisatoriske.
Skjermingsverdig verdi	Skjermingsverdige verdier er skjermingsverdig informasjon, informasjonssystem, infrastruktur eller objekter. Med skjermingsverdig menes at f.eks. informasjon er skjermingsverdig om det kan skade nasjonale sikkerhetsinteresser om den blir kjent for uvedkommende, går tapt, blir endret eller blir utilgjengelig.
Styringssystem	Betegnelse brukt for det sett av prosesser, tiltak mv. som må etableres og fungere for at en virksomhet skal ha tilstrekkelig intern styring og kontroll.
Særlig kategori av personopplysning	Også kalt sensitive personopplysninger. Dette er opplysninger som krever ekstra vern, slik som opplysninger om rasemessig eller etnisk opprinnelse, religion, helseopplysninger, seksuell orientering med mer.
Tilgjengelighet	Prinsippet om at opplysninger skal være tilgjengelig for det formålet de er tiltenkt.
Tiltak	Dette veiledningsmateriellet benytter begrepet tiltak på alt som gjøres både for å redusere risikoer på det som er i fokus, i vårt tilfelle informasjonssikkerhet, og det som gjøres for å gjøre internkontrollprosessene bedre.
Tjenestenivåavtaler	Avtale mellom leverandør av en tjeneste og kunden. Tjenestene det er snakk om er typisk IT-tjenester. På engelsk blir slike avtaler omtalt som <i>Service level agreement (SLA)</i> .
Tjenesteutsetting	Det å sette ut arbeidsoppgaver og/eller funksjoner til eksterne leverandører og tjenesteytere. Tjenesteutsetting blir også kalt utkontraktering eller konkurranseutsetting. På engelsk heter det Outsourcing.
Trusler eller trusselaktører/-kilde	Begrepet trusler brukes her som synonym til trusselkilder. Begrepet benyttes om både aktører for villedte handlinger og farekilder.

Verdivurdering	En kartlegging av informasjonsverdier (også kalt verdivurdering) innebærer å få en tilstrekkelig oversikt over informasjonsverdier som er omfattet av regelverk for ivaretagelse av informasjonssikkerhet og personvern, eller som er av så vesentlig betydning for virksomhetens mål for informasjonssikkerhet at de bør omfattes av risikovurderinger.
----------------	--

Lover og forskrifter:

eForvaltningsforskriften	Forskrift om elektronisk kommunikasjon med og i forvaltningen	Forskrift om elektronisk kommunikasjon med og i forvaltningen (eForvaltningsforskriften) - Lovdata
Digitalsikkerhetsloven	Lov om digital sikkerhet	Lov om digital sikkerhet (digitalsikkerhetsloven) - Lovdata
Kommuneloven	Lov om kommuner og fylkeskommuner	Lov om kommuner og fylkeskommuner (kommuneloven) - Lovdata
Personopplysningsloven	Lov om behandling om personopplysninger	Lov om behandling av personopplysninger (personopplysningsloven) - Lovdata
Sikkerhetsloven	Lov om nasjonal sikkerhet	Lov om nasjonal sikkerhet (sikkerhetsloven) - Lovdata

Nasjonale ressurser på personvern og informasjonssikkerhet

I Norge har vi flere myndigheter og ekspertmiljøer på personvern og informasjonssikkerhet. Nedenfor følger en liste over nasjonale ressurser og hva de kan tilby:

Datatilsynet

[Datatilsynet](#) er et uavhengig forvaltningsorgan som skal bidra til bedre personvern i hele Norge. Det fører tilsyn med virksomheters etterlevelse av personvernforordningen, har en ombudsrolle overfor publikum og gir råd om personvernforordningen.

Datatilsynets nettsider inneholder mye relevant informasjon for kommunal sektor. Her finnes blant annet veiledere for hvordan virksomheter skal etterleve regelverket. Datatilsynet har også en egen veiledningstelefon.

Nyttige lenker:

<https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/>

<https://www.datatilsynet.no/rettigheter-og-plikter/personvernprinsippene/>

Nasjonal sikkerhetsmyndighet (NSM)

[Nasjonal sikkerhetsmyndighet](#) er Norges ekspertorgan for informasjons- og objektsikkerhet, samt det nasjonale fagmiljøet for IKT-sikkerhet. NSM gir råd, informasjon og veiledning om forebyggende sikkerhetsarbeid, og kravene i sikkerhetsloven.

NSM har mange relevante veiledere og håndbøker for etterlevelse av sikkerhetsloven. I tillegg har de flere veiledere som gir god informasjon om sikkerhetsarbeid som faller utenfor sikkerhetsloven.

Nyttige lenker:

<https://nsm.no/regelverk-og-hjelp/veiledere-og-handboker-til-sikkerhetsloven/>

<https://nsm.no/fagomrader/digital-sikkerhet/rad-og-anbefalinger-innenfor-digital-sikkerhet/grunnprinsipper-ikt>

Digitaliseringsdirektoratet (Digdir)

[Digitaliseringsdirektoratet](#) (Digdir) er statens organ for digitalisering. Direktoratet har blant annet som oppgave å gi anbefalinger for internkontroll på området informasjonssikkerhet. Dette ansvaret gjelder overfor både statlig og kommunal sektor. Direktoratet har utarbeidet veiledere for internkontroll for informasjonssikkerhet som er relevant for alle kommuner. På direktoratets nettsider finnes det også guide til topplederens arbeid med informasjonssikkerhet og e-læringskurs for ledere.

Nyttige lenker:

<https://www.digdir.no/informasjonssikkerhet/informasjonssikkerhet/882>

<https://www.digdir.no/informasjonssikkerhet/helhetlig-styring-og-kontroll-av-informasjonssikkerhet/2284>

<https://laeringsplattformen.dfo.no/kursoversikt/er-det-sikkert-informasjonssikkerhet-ledere>

Direktoratet for forvaltning og økonomistyring (DFØ)

[Direktoratet for forvaltning og økonomistyring](#) er statens fagorgan for offentlige innkjøp. DFØ eier nettstedet www.anskaffelser.no, der du finner informasjon om hvordan offentlig anskaffelser bør gjennomføres, og oversikt over regelverk som skal følges. Her finnes i tillegg relevant informasjon om personvern og informasjonssikkerhet ved anskaffelser.

Nyttige lenker:

<https://www.anskaffelser.no/avtaler-og-regelverk/sikkerhetsloven-og-offentlige-anskaffelser>

<https://www.anskaffelser.no/verktoy/kontrakter-og-avtaler/databehandleravtale-og-sjekklister>

Helse- og KommuneCert

Cybersikkerhetssenter for Helse- og kommunesektor. Skal bidra til å øke motstandsdyktigheten mot ikt-sikkerhetshendelser i helse- og kommunesektoren, inkludert fylkeskommuner – sektorvis responsmiljø for både helse- og kommunesektor.

Nyttige lenker:

<https://www.nhn.no/tjenester/helsecert>

eHelse / Normen

[Normen](#) er en bransjenorm for informasjonssikkerhet og personvern og utarbeidet og forvaltet av organisasjoner og virksomheter i helsesektoren.

- Hva er eHelse /Normen.
- Hva innebærer eHelse og Normen for kommunen
- Velferdsteknologi?

Nyttige lenker:

<https://www.ehelse.no/normen/>

Norsk Senter for Informasjonssikring (NorSIS)

[NorSIS](#) er en del av regjeringens helhetlige satsing på informasjonssikkerhet i Norge. Målgruppen for NorSIS' aktivitet er norske virksomheter i privat og offentlig sektor. NorSIS skal så langt som mulig også imøtekomme innbyggernes behov, og alle samfunnsgrupper skal kunne dra nytte av NorSIS tjenester. NorSIS opptre som en nøytral informasjonssikkerhetsinstans, og skal samarbeide med virksomheter for gjennomføring av informasjonssikkerhetstiltak.

Nyttige lenker:

<https://norsis.no/>

Foreningen Kommunal Informasjonssikkerhet (KiNS)

Formålet med [KiNS](#) er å bidra til økt informasjonssikkerhet i kommuner og fylkeskommuner. KiNS arrangerer en stor årlig konferanse der medlemmer møtes for nettverksbygging og faglig påfyll. KiNS arrangerer kurs innenfor ISO 2700x, teknisk informasjonssikkerhet og GDPR i tillegg til lokale/regionale seminarer.

Nyttige lenker:

<https://kins.no/verktoykasse/>

Pågående og kommende prosjekter/aktiviteter/lov- og regelverksendringer

Digitaliseringsloven / NIS og kommende NIS2

I desember 2023 vedtok Stortinget en ny lov om digital sikkerhet (Digitaliseringsloven). Loven med forskrift(er) skal implementere EUs NIS-direktiv fra 2016 i norsk rett, og det er forventet at loven vil tre i kraft i 2024.

Digitaliseringsloven bygger på Europaparlaments- og rådsdirektiv (EU) 2016/1148 av 6. juli 2016 om tiltak for å sikre et høyt felles nivå for sikkerhet i nettverks- og informasjonssystemer i hele Unionen (NIS-direktivet). Lov om digital sikkerhet er ment å være i samsvar med NIS-direktivet og øvrige sammenlignbare lands nasjonale lovgivning på området. Loven skal forplikte virksomheter som har en særlig viktig rolle for å opprettholde kritisk samfunnsmessig og økonomisk aktivitet, til å overholde digitale sikkerhetskrav og varsle om alvorlige digitale hendelser. Loven skal også bidra med forebyggende sikkerhetstiltak som gjør en virksomhet bedre rustet til å stå imot angrep mot nettverks- og informasjonssystemer de er avhengige av. Videre skal loven sikre planer for håndtering av uønskede hendelser.

Tidlig i 2023 kom det et oppdatert NIS 2-direktiv i EU. De nye reglene skal være implementert i nasjonal rett i EU-landene i oktober 2024. I Norge pågår det utredning av NIS 2 og CER-direktivene, og det er forventet at det norske regelverket vil bli oppdatert iht. NIS 2 så snart som mulig.

Nyttige lenker:

Digitaliseringsloven - <https://lovdata.no/dokument/LTI/lov/2023-12-20-108>

Regjeringen - NIS2 direktivet - <https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2021/feb/nis2-direktivet/id2846097/>

NIS2 direktivet - <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>

KI forordningen (EU AI-act)

KI-forordningen (AI Act) ble godkjent i EU i mars 2024, og er forventet å tre i kraft i sin helhet i løpet av 2026. Regelverket er verdens første juridiske rammeverk som spesifikt regulerer kunstig intelligens.

KI-forordningen tar en risikobasert tilnærming til reguleringen av KI. Dette innebærer at kravene et system må oppfylle vil avhenge av hvor stor risiko systemet utgjør. Det er i utgangspunktet to risikonivåer; uakseptabel risiko og høyrisiko. I tillegg er det noen sporadiske krav som gjør seg gjeldende for systemer som faller utenfor disse kategoriene, som noen ganger omtales som systemer med minimal risiko.

I Norge har det vært bred politisk enighet om at vi skal tilpasse oss KI-forordningen, og noen sektorer er i gang allerede. Et eksempel er helsesektoren hvor arbeidet med å forberede helse- og omsorgstjenesten på KI-forordningen er godt i gang, med fokus på risikohåndtering, tillitsrammeverk og datahåndtering. Helsedirektoratet har også engasjert helsesektoren i relevant standardiseringsarbeid for KI.

Nyttige lenker:

[Ny forordning for kunstig intelligens | Digdir](#)

KS SkoleSec

I prosjektet «[SkoleSec](https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/)» har kommuner og fylkeskommuner gått sammen om å styrke arbeidet med personvern og informasjonssikkerhet knyttet til digitalt læringsmiljø.

Det er blant annet gjennomført en overordnet vurdering av personvernkonsekvenser av Google Workspace for Education som kommunene som bruker denne plattformen kan ta utgangspunkt i sitt eget arbeid.

Prosjektet har lagt planer for å gjøre det samme med Microsoft 365 i 2025.

Nyttige lenker:

<https://www.ks.no/fagomrader/digitalisering/felleslosninger/skolesec/>

Samordning av veiledningsaktører for informasjonssikkerhet og personvern

Digitaliseringsdirektoratet (Digdir) har etablert et nettverk for veiledningsaktører som fokuserer på styring og kontroll av informasjonssikkerhet. Dette nettverket skal arbeide for mer samarbeid og dialog mellom veiledningsaktørene, og bidra til en helhetlig tilnærming innen informasjonssikkerhet.

Nyttig lenke:

[Veiledningsaktører innen styring og kontroll | Digdir](#)

