Policy for informasjonssikkerhet og personvern i høyere utdanning og forskning

Fastsatt av Kunnskapsdepartementet i rundskriv F-04-20 1. oktober 2020

Følgende krav gjelder for arbeidet med informasjonssikkerhet og personvern hos Kunnskapsdepartementets underliggende virksomheter i høyere utdanning og forskning:

1. Virksomheten har et ledelsessystem for informasjonssikkerhet

Det er virksomhetens øverste ledelse som har ansvaret for at informasjonssikkerheten er tilfredsstillende. Virksomhetens øverste ledelse må derfor se til at arbeidet med informasjonssikkerhet skjer på en systematisk og planmessig måte. Dette gjøres ved at (i) det innføres et ledelsessystem for informasjonssikkerhet og (ii) informasjonssikkerhet inngår i den generelle virksomhetsstyringen.

a) Virksomheten innfører, vedlikeholder og forbedrer et ledelsessystem for informasjonssikkerhet tilpasset virksomhetens størrelse og behov. Ledelsessystemet bør basere seg på anerkjente internasjonale standarder, for eksempel ISO/IEC 27001.
b) Virksomhetens øverste ledelse stiller tydelige krav til arbeidet med informasjonssikkerhet. Virksomhetens øverste ledelse fastsetter sikkerhetsmål, sikkerhetsstrategi og kriterier for akseptabel risiko.
c) Virksomhetens øverste ledelse kan delegere sikkerhetsoppgaver og myndighet til andre ansatte i virksomheten. Dette beskrives i virksomhetens sikkerhetsorganisering.
d) Virksomhetens øverste ledelse ser til at arbeidet med informasjonssikkerhet tilføres tilstrekkelige ressurser.
e) Virksomhetens øverste ledelse forsikrer seg om at tilfredsstillende organisatoriske og tekniske sikringstiltak er etablert og holder seg orientert om sikkerhetstilstanden i virksomheten, for eksempel med utgangspunkt i NSMs grunnprinsipper for IKT-sikkerhet[1].
f) Virksomhetens øverste ledelse sørger for periodisk revisjon av arbeidet med informasjonssikkerhet og oppdatering av ledelsessystemet (ved behov).
g) Virksomhetens øverste styrende organ fører kontroll med arbeidet med informasjonssikkerhet.

2. Virksomheten har oversikt over informasjon og personopplysninger

For å kunne ivareta informasjonssikkerheten på en tilfredsstillende måte, må virksomheten først kjenne til hvilke typer informasjon og personopplysninger den forvalter. Den må også ha god oversikt over digitale systemer og tjenester, dataflyten mellom digitale løsninger og hvordan det lokale datanettverket er oppbygd. Slike oversikter fremskaffes gjennom å kartlegge og dokumentere informasjons- og personopplysningsbehandlingen i virksomheten.

a) Virksomheten har oversikt over digitale systemer eller tjenester hvor informasjon og personopplysninger behandles, hvilke informasjons- og opplysningstyper som behandles, dataflyten mellom systemene eller tjenestene og hvem som har tilgang til dem.

[1] Se NSMs Grunnprinsipper for IKT-sikkerhet 2.0

b) Virksomheten bør klassifisere sine informasjonsverdier i henhold til anbefalingene i UFS 136[2].
c) Virksomheten har oversikten over digitale systemer eller tjenester som leveres av eksterne tjenesteleverandører, for eksempel skytjenester.
d) Virksomheten sørger for at protokoller over behandlinger av personopplysninger utarbeides og vedlikeholdes.
e) Virksomheten har oversikt over eventuelle kunnskapsområder som reguleres av eksportkontroll-lovgivningen.[3]
f) Virksomheten varsler departementet om informasjon og informasjonssystemer som kan ha vesentlig betydning for grunnleggende nasjonale funksjoner (jf. sikkerhetslovens § 2-1).

3. Virksomheten gjennomfører risikovurderinger og etablerer sikringstiltak

Virksomheten har ansvaret for å forebygge hendelser som kan føre til brudd på informasjonssikkerheten, for eksempel tyveri av personopplysninger og forskningsresultater eller misbruk av lokale dataressurser. Dette gjøres gjennom å vurdere risikoen for slike og andre sikkerhetshendelser. Risikovurderinger kan gjennomføres for den enkelte systemløsning eller innenfor bestemte tjenesteområder (forskning, studieadministrasjon, bibliotek, HR, osv.). Det skal iverksettes organisatoriske og/eller tekniske sikringstiltak der hvor risikoen for brudd på informasjonssikkerheten vurderes å være større enn hva virksomhetens øverste ledelse kan godta.

a) Virksomheten vurderer risikoen for brudd på (i) sikkerheten til informasjon og personopplysninger og (ii) sikkerheten i digitale systemer, tjenester og datanettverk. Metodikk for vurdering av risiko og kriterier for akseptabel risiko er kjent i virksomheten.
b) Virksomheten gjennomfører risikovurderinger før digitale systemer eller tjenester tas i bruk. Nye risikovurderinger gjennomføres ved vesentlige tekniske endringer eller endringer i måten systemene eller tjenestene brukes på. Risikovurderingene revideres jevnlig.
c) Virksomheten etablerer tilfredsstillende organisatoriske og/eller tekniske tiltak for sikring av viktig informasjon, personopplysninger, digitale systemer, tjenester og datanettverk.
d) Viktig informasjon, for eksempel sensitive (særlig kategorier) personopplysninger eller store forskningsdatasett, sikres ekstra godt.

4. Virksomheten etablerer løsninger for hendelseshåndtering, lukking av avvik og kontinuitet

Det er ikke alltid mulig å forebygge alle hendelser som kan føre til brudd på informasjonssikkerheten. Det må derfor etableres hensiktsmessige løsninger for oppdagelse, varsling og håndtering av hendelser som det ikke har vært mulig å forebygge. Ved alvorlige brudd på informasjonssikkerheten må kritiske arbeidsoppgaver fortsatt kunne utføres. Vesentlige avvik fra interne rutiner for behandling av personopplysninger må også rapporteres og korrigeres.

a) Virksomheten etablerer tiltak/løsninger for å avdekke og håndtere brudd på informasjonssikkerheten, inkludert nettbaserte trusler/cyberangrep. Virksomheten identifiserer og eliminerer årsaken til sikkerhetsbruddet.
b) Virksomheten bør utpeke medarbeidere som har et særlig ansvar for håndtering av brudd på informasjonssikkerheten («incident response team»: IRT).

[2] UFS136: Veiledning i klassifisering av informasjon, UNINETT Fagspesifikasjon
[3] Se Utenriksdepartementets retningslinjer for kontroll med kunnskapsoverføring.

c) Virksomhetens IRT bør ha nødvendige fullmakter, rutiner og kompetanse til å beskytte informasjon og personopplysninger mot skade. Det samme gjelder for digitale systemer, tjenester og datanettverk.
d) Virksomhetens IRT deltar i samarbeidet med sektorvist responsmiljø (SRM), UNINETT CERT, og har varslingsrutiner for IKT-sikkerhetshendelser[4].
e) Virksomheten etablerer planer for hvordan kritiske arbeidsoppgaver kan utføres ved langvarig bortfall av viktige digitale systemer, tjenester eller datanettverk (kontinuitet).
f) Virksomheten øver på håndtering av alvorlige brudd på informasjonssikkerheten.
g) Virksomheten etablerer prosesser og rutiner for varsling av Datatilsynet og de registrerte personene ved brudd på personopplysningssikkerheten.
h) Virksomheten etablerer prosesser for intern varsling og håndtering av avvik fra egne rutiner for behandling av personopplysninger (avvikshåndtering).
i) Virksomhetens øverste ledelse fastsetter egne krav til kontinuitet og sikrer tilstrekkelige ressurser til dette arbeidet.

5. Virksomheten sørger for kontroll med tjenesteleverandører

Når drift av digitale systemer eller tjenester settes ut til eksterne tjenesteleverandører har virksomheten fortsatt ansvaret for at informasjonssikkerheten i tjenesteleveransen er tilfredsstillende. Tilsvarende gjelder for personvernet når tjenesteleveransen omfatter behandling av personopplysninger. Ansvaret for informasjonssikkerheten og personvernet omfatter hele leverandørkjeden, det vil si alle underleverandører som tjenesteleverandøren benytter, for eksempel tilbydere av datasentre, vedlikeholdstjenester eller brukerstøtte. Ansvaret omfatter også informasjon eller personopplysninger som tjenesteleverandøren overfører til datalokasjoner i utlandet.

a) Virksomheten forsikrer seg om at leverandører av digitale systemer eller tjenester ivaretar sikkerheten til informasjon og personopplysninger på en tilfredsstillende måte.
b) Virksomheten og leverandøren avtaler hvilke sikkerhetskrav og krav til behandling av personopplysninger som skal gjelde for tjenesteleveransen (for eksempel i databehandleravtaler og tjenestenivåavtaler).
c) Virksomheten forsikrer seg jevnlig om at avtalte krav til informasjonssikkerheten og vilkår for behandling av personopplysninger overholdes av tjenesteleverandøren.
d) Virksomheten forsikrer seg om at tjenesteleverandørens overføring av personopplysninger til land utenfor EU/EØS skjer på lovlig og sikker måte. Dette gjelder også når virksomheten selv overfører personopplysninger til mottakere (behandlingsansvarlige) i land utenfor EU/EØS.
e) Virksomheter som er databehandlere for andre virksomheter i eller utenfor universitets- og høyskolesektoren har kompetanse og kapasitet til å overholde de lovpålagte eller avtalefestede plikter som hører til denne rollen.

6. Virksomheten har internkontroll for behandling av personopplysninger

For at personvernet til de registrerte (studenter, medarbeidere, gjester eller deltakere i forskningsprosjekter) skal kunne ivaretas, må prosesser og rutiner for riktig og lovlig håndtering av personopplysninger integreres i den daglige driften og virksomhetsstyringen. Dette gjøres gjennom

[4] Se Rammeverk for håndtering av IKT-sikkerhetshendelser i UH-sektoren som er Units sektortilpasning av NSMs nasjonale rammeverk.

etablering av et system for internkontroll. Internkontrollen er forankret hos virksomhetens øverste ledelse og konkretiserer hvordan rettslige krav til behandling av personopplysninger skal etterleves i det daglige arbeidet. Ledelsessystem for informasjonssikkerhet inngår i internkontrollen.

a) Virksomheten har god kjennskap til reglene i personopplysningsloven og personvernforordningen (GDPR).
b) Virksomheten sørger for at det etableres prosesser og rutiner for overholdelse av sine plikter som behandlingsansvarlig, eventuelt også som databehandler.
c) Virksomheten sørger for å ha oversikt over egne behandlinger av personopplysninger (protokoll).
d) Virksomheten sørger for at grunnleggende prinsipper for behandling av personopplysninger overholdes, blant annet når det gjelder formål og formålsbegrensning, dataminimering, riktighet (datakvalitet) og lagringsbegrensning.
e) Virksomheten sørger for at den har behandlingsgrunnlag for behandlinger av alminnelige personopplysninger, særlige kategorier (sensitive) personopplysninger og opplysninger knyttet til straffedommer og straffbare forhold.
f) Virksomheten etterlever regler for bruk av eksterne tjenesteleverandører (databehandlere) og for overføringer av personopplysninger til tredjeland.
g) Virksomheten kjenner til og overholder de personvernplikter som følger av annen lovgivning, for eksempel forvaltningsloven, offentleglova, universitets- og høyskoleloven, helseforskningsloven eller arbeidsmiljøloven.
h) Virksomheten sørger for periodisk revisjon av arbeidet med personvern og behandling av personopplysninger.
i) Virksomhetens daglige ledelse og øverste styrende organ fører kontroll med arbeidet med personvern og behandling av personopplysninger.

7. Virksomheten ivaretar de registrertes rettigheter

Det er særlig viktig at internkontrollen for behandling av personopplysninger sørger for at rettighetene til de som opplysningene gjelder blir ivaretatt, for eksempel studenter, ansatte og deltakere i forskningsprosjekter. Rettighetene som følger av personopplysningsregelverket (GDPR og den norske personopplysningsloven) skal sikre at de registrerte (studenter, ansatte, osv.) får innsikt i og medinnflytelse over hvordan opplysninger om dem blir brukt.

a) Virksomheten sørger for at det etableres interne prosesser og rutiner for ivaretakelse av de registrertes personvernrettigheter, blant annet retten til informasjon, innsyn, retting og sletting av opplysninger.
b) Virksomheten forsikrer seg om at digitale systemer eller tjenester som utvikles internt eller driftes av eksterne leverandører inneholder funksjonalitet for ivaretakelse av de registrertes rettigheter, jf. punkt 10 nedenfor.

8. Virksomheten utnevner personvernombud

Personvernombudet er et annet viktig element i internkontrollen for behandling av personopplysninger. Offentlige virksomheter har plikt til å utnevne personvernombud. Personvernombudet skal blant annet gi råd om hvordan personopplysningsregelverket kan etterleves og føre kontroll med at all behandling av personopplysninger skjer på lovlig måte. Ombudet rapporterer sine funn og anbefalinger til virksomhetens øverste ledelse, men er ikke underlagt virksomhetens øverste ledelses instruksjonsmyndighet.

a) Virksomheten utnevner et personvernombud.
b) Virksomheten sikrer at personvernombudet har tilstrekkelige ressurser, nødvendig kompetanse og uavhengighet til å ivareta sine lovpålagte oppgaver.
c) Virksomheten rådfører seg med personvernombudet i spørsmål som gjelder behandling og sikring av personopplysninger.

9. Virksomheten gjennomfører vurderinger av personvernkonsekvenser (DPIA[5])

Før personopplysninger brukes på måter som kan utgjøre en høy risiko for den enkeltes rettigheter og friheter, spesielt retten til personvern, skal en personvernkonsekvensvurdering gjennomføres. Datatilsynet har laget en oversikt over når det er nødvendig å gjennomføre slike vurderinger.[6] Konsekvensvurderingen skal blant annet avdekke hva som må gjøres for at bruken av opplysningene skal være lovlig og forsvarlig. Dersom det er tvil om lovligheten og forsvarligheten, skal råd og anbefalinger innhentes fra Datatilsynet (forhåndsdrøftelser).

a) Virksomheten er kjent med lovpålagte krav og Datatilsynets oversikt over når vurdering av personvernkonsekvenser skal gjennomføres.
b) Virksomheten etablerer prosesser og rutiner for gjennomføring av personvernkonsekvensvurdering.
c) Virksomheten etablerer rutiner for forhåndsdrøftelser med Datatilsynet dersom personvernkonsekvensvurderingen viser at det er nødvendig.

10. Virksomheten sørger for innebygd personvern og informasjonssikkerhet

Innebygd personvern og informasjonssikkerhet innebærer at digitaliseringstiltak utformes slik at begge hensyn ivaretas gjennom hele digitaliseringsløpet (fra begynnelse til slutt). Hensikten er å unngå at problemstillinger knyttet til personvern og informasjonssikkerhet må løses ved hjelp av uhensiktsmessige eller ineffektive ad hoc-løsninger etter at digitaliseringstiltakene er ferdig utformet eller satt i drift.

a) Virksomheten stiller krav til at digitale systemer eller tjenester som behandler personopplysninger inneholder funksjonalitet som ivaretar personvernet, for eksempel innsynsløsninger eller muligheter for retting, sperring eller sletting av opplysninger.
b) Virksomheten stiller krav til at digitale systemer eller tjenester som behandler personopplysninger (eller annen viktig informasjon) inneholder funksjonalitet som ivaretar informasjonssikkerheten, for eksempel kryptering, sikkerhetskopiering, forsvarlig tilgangsstyring eller logging av hendelser i digitale systemer.

11. Virksomheten sørger for opplæring og kompetanseheving

For å kunne ha et fungerende informasjonssikkerhets- og personvernarbeid, er relevant opplæring og kompetanse avgjørende. Ledere, medarbeidere og (der hvor det er aktuelt) studenter må få informasjon om vanlige trusler mot personvernet og informasjonssikkerheten, for eksempel svindel-epost, og hvordan truslene best kan håndteres. Ledere og medarbeidere som har roller i ledelsessystemet for informasjonssikkerhet og internkontrollen for behandling av personopplysninger, må få opplæring i hvordan pålagte oppgaver kan utføres.

[5] Data Protection Impact Assessment
[6] Datatilsynets oversikt er tilgjengelig på tilsynets hjemmeside.

a) Virksomheten sørger for god bevisstheten om informasjonssikkerhet og personvern hos ledere, medarbeidere og (der hvor det er aktuelt) studenter.
b) Virksomheten sørger for at ledere og medarbeidere har god nok kompetanse til å ivareta sine informasjonssikkerhets- og personvernoppgaver på tilfredsstillende måter.
c) Virksomheten sørger for god bevissthet om IKT-trusselbildet.

12. Virksomheten dokumenterer arbeidet med informasjonssikkerhet og personvern

Dokumentasjon av arbeidet med informasjonssikkerhet og personvern gir bedre kontroll med egen innsats og muligheter for å lære av tidligere erfaringer. I tillegg vil dokumentasjonen være viktig som underlag ved periodiske revisjoner av arbeidet og ved tilsyn eller kontroller, for eksempel fra Datatilsynet eller Riksrevisjonen.

a) Virksomheten dokumenterer sitt ledelsessystem for informasjonssikkerhet og internkontroll for behandling av personopplysninger, jf. punkt 1 og 6 ovenfor.
b) Virksomheten dokumenterer at øvrige informasjonssikkerhets- og personvernoppgaver beskrevet i denne policyen er utført.

Vedlegg 1: Oversikt over relevante lovgivning og sentrale nasjonale føringer

Lover og forskrifter

Lov om arbeidsmiljø, arbeidstid og stillingsvern mv. (arbeidsmiljøloven)

Lov om arkiv (arkivlova)

Lov om behandling av personopplysninger (personopplysningsloven)

Lov om behandlingsmåten i forvaltningssaker (forvaltningsloven)

Lov om helseregistre og behandling av helseopplysninger (helseregisterloven)

Lov om kontroll med eksport av strategiske varer, tjenester og teknologi mv. (eksportkontrolloven)

Lov om medisin og helsefaglig forskning (helseforskningsloven)

Lov om rett til innsyn i dokument i offentleg verksemd (offentleglova)

Lov om universiteter og høyskoler (universitets- og høyskoleloven)

Forskrift om arbeidsgivers innsyn i e-postkasse og annet elektronisk lagret materiale

Forskrift om eksport av forsvarsmateriell, flerbruksvarer, teknologi og tjenester

Forskrift om elektronisk kommunikasjon med og i forvaltningen (e-forvaltningsforskriften)

Forskrift om kameraovervåkning i virksomhet

Forskrift om Nasjonal vitnemåls- og karakterportal

Forskrift om opptak til høgre utdanning (opptaksforskrifta)

Forskrift om organisering av medisinsk og helsefaglig forskning

Forskrift om register for utestengte studenter – RUST

Forskrift til forvaltningsloven (forvaltningslovsforskriften)

Reglement for økonomistyring i staten

Bestemmelser om økonomistyring i staten

Øvrige nasjonale føringer

Digitaliseringsstrategi for universitets- og høyskolesektoren (2017-2021)

Handlingsplan for digitalisering i høyere utdanning og forskning (2019-2021)

Nasjonal strategi for digital sikkerhet

Rammeverk for håndtering av IKT-sikkerhetshendelser

Styringsdokument for arbeid med samfunnssikkerhet i Kunnskapsdepartementets sektor (2019)

Tiltaksoversikt til nasjonal strategi for digital sikkerhet

Utenriksdepartementets retningslinjer om eksportkontroll i kunnskapssektoren