Universitetsledelsen
Arkivref: 2017/5560/INJ024
Dato: 08.11.2020

SAKSFRAMLEGG

Til:	Møtedato:	Sak:
Universitetsstyret		

Styrende del av ledelsessystem for informasjonssikkerhet – revidering og utvidelse til å omfatte personvern

Innstilling til vedtak:
Universitetsstyret vedtar de foreslåtte endringene til styrende del av ledelsessystemet for informasjonssikkerhet.

Ledelsessystemet endrer navn til «ledelsessystem for informasjonssikkerhet og personvern ved UiT Norges arktiske universitet»

Bakgrunn:

I 2015 godkjente Universitetsstyret «styringssystem for informasjonssikkerhet» i sak S 07/15.

Styringssystemet har senere blitt omdøpt til ledelsessystem for informasjonssikkerhet, samt undergått visse mindre strukturendringer. Deler av ledelsessystemet har også blitt revidert, eksempelvis gjennom vedtakelsen av ny strategi for informasjonssikkerhet (sak S 9/19) og ny retningslinje for klassifisering av informasjon (sak F 13/19).

Ledelsessystemet består av tre deler:

1. **Styrende del** (overordnet policy, herunder sikkerhetsstrategi og -mål, akseptabel risiko, klassifisering, roller og ansvar)
2. **Gjennomførende del** (konkrete retningslinjer og rutiner, risikovurderinger, opplæring mv.)
3. **Kontrollerende del** (internrevisjon, rapportering og håndtering av avvik, ledelsens gjennomgang/årsrapport).

Som hovedregel er det Universitetsstyret som vedtar endringer i den *styrende* del, mens Universitetsdirektøren vedtar endringer tilhørende *gjennomførende* og *kontrollerende* del.

Som nevnt omfatter ledelsessystemet i dag kun informasjonssikkerhet. Som forespeilet i årsrapport 2019 (sak S 10/20) er det ønskelig å utvide ledelsessystemet til å omfatte både informasjonssikkerhet og personvern. Dette fordi disse temaene henger nært sammen, selv om sentrale deler av personvern ikke omhandler informasjonssikkerhet (f.eks ivaretagelse av registrertes rettigheter, lovlig behandlingsgrunnlag mv) og vice versa (sikring av informasjonsverdier som ikke inneholder personopplysninger, eksempelvis byggdata, økonomiske

data, forskningsdata som ikke omhandler personer mv). Erfaring har vist at det ikke er hensiktsmessig å forsøke å skille feltene, og en mer enhetlig tilnærming er derfor ønsket.

Denne saken fremmes derfor Universitetsstyret for å få en beslutning på at ledelsessystemet skal bygges ut, samt foreta de nødvendige endringer i ledelsessystemets *styrende del.* De nødvendige endringer i *gjennomførende* og *kontrollerende del* vil deretter bli utarbeidet og fremmet Universitetsdirektøren for behandling.

I dag består *styrende del* av fire kapittel:

1. Innledning
2. Sikkerhetsstrategi (inkludert sikkerhetsmål) og akseptabel risiko
3. Klassifisering av informasjon
4. Roller, ansvar og oppgaver

I denne saken fremmer Universitetsdirektøren forslag til materielle endringer i kapittel 1 og 4. Kapittel 3 ønskes flyttet til *gjennomførende del* da tematikken som reguleres er mer passende der, fremfor i den overordnede, styrende delen av ledelsessystemet[1].

Det vil være viktig å revidere og utvide informasjonssikkerhetsstrategien (kapittel 2) til å også omfatte en strategi for UiTs arbeid med, og ivaretagelse av, personvern. Dette er imidlertid er omfattende arbeid som ikke vil bli klart før tidligst våren 2021. Universitetsdirektøren anser det derfor som hensiktsmessig å fremme de øvrige forslagene til endringer nå, slik at arbeidet med nødvendig revidering av resten av ledelsessystemet kan ta til. Inntil videre vil derfor kapittel 2 forbli uendret selv om ledelsessystemet skal omfatte både informasjonssikkerhet og personvern.

Kapittel 1 - innledning

I kapittel 1 er det foretatt en viss omstrukturering for å ta inn personvern, og det er lagt til tekst som beskriver UiTs ansvar for ivaretagelse av personvern.

Videre foreslår Universitetsdirektøren at kapittel 1.4 *«Behandlingsansvarlig og databehandlere»* tas ut. Dette underkapittelet forklarer primært hva som ligger i begrepene samt understreker at databehandleravtale alltid skal inngås før eksterne aktører behandler personopplysninger på vegne av UiT. Slik ledelsessystemet og øvrig regelverk ved UiT har utviklet seg etter hvert som det har blitt større modenhet på feltet fremstår det som unødvendig å ha dette med i *styrende del,* og innholdet kan bedre ivaretas direkte i egne retningslinjer.

Den siste foreslåtte endringen i kapittel 1 er at oppdelingen mellom kapittel 1.2 og 1.3 fjernes slik at disse slås sammen til ett underkapittel (1.2).

Kapittel 4 – roller, ansvar og oppgaver

De største endringene kommer i kapittel 4 *roller, ansvar og oppgaver.* Primært går dette på å ta inn eksisterende roller og strukturer på UiT innenfor personvern, slik at disse fremkommer på et overordnet nivå. Eksempelvis gjelder dette personvernombudet samt gruppen som gjennomgår utførte personvernkonsekvensvurderinger («DPIA-gruppen»).

[1] Kapittel tre (klassifisering av informasjon) blir da nytt kapittel fire, mens dagens kapittel fire (roller, ansvar og oppgaver) blir nytt kapittel tre. Kapittelnummer og henvisninger ajourføres dersom vedtatt som foreslått.

Ellers er det ønskelig at arbeidet med personvern legges opp slik at det følger den samme organiseringen og ansvarsfordeling som for informasjonssikkerhet, og de eksisterende rollene i dagens ledelsessystem er revidert slik at dette gjenspeiles.

Av andre endringer som kan trekkes frem her er at i nåværende utgave står det at *«Universitetsdirektøren er behandlingsansvarlig for alle personopplysninger, dette omfatter også å bestemme formålet med behandling av personopplysninger, samt å ha dokumentert oversikt over disse».*

Den *behandlingsansvarlige* er den som bestemmer formålet med behandling av personopplysninger og hvilke midler som skal benyttes, og er en svært sentral og viktig rolle i personvernforordningen (GDPR). Når det er tale om en organisasjon eller virksomhet som behandler personopplysninger vil den behandlingsansvarlige etter personvernforordningen typisk være virksomheten som sådan, og ikke en konkret rolle i virksomheten, selv om avgjørelser i det daglige naturligvis ofte vil være delegert til ulike posisjoner og roller.

Spørsmålet om hvem som formelt regnes som behandlingsansvarlig ("controller"), og hvorfor dette legges på organisasjonsnivå fremfor til konkrete roller eller posisjoner, omtales bl.a i boken *The EU General Data Protection Regulation (GDPR) A Commentary*[2]: "However, where an organised collective entity determines the purposes and means of processing, the point of departure is that the entity as such is the controller, rather than any particular individual natural/physical person who is part of that entity. In the words of WP29, this is due not just to 'the strategic perspective of allocating responsibilities', but also 'in order to provide data subjects with a more stable and reliable reference entity for the exercise of their rights'. Thus, for instance, in the case of a corporation, the controller will usually not be any of the members/employees of the corporation (e.g. Chief Executive Officer, Board Chairperson, Chief Financial Officer, Chief Privacy Officer etc.) who actually decide on the purposes and means of the processing, but the corporation as such.".

Det er slikt sett ikke helt treffende med den nåværende formuleringen. Universitetsdirektøren foreslår derfor at dette synliggjøres ved at det tas inn et nytt punkt under Universitetsstyrets ansvar, og nåværende punkt under Universitetsdirektørens ansvar omformuleres. Beskrivelsen av ansvaret vil da bli mer presist, og i tråd med de premisser som personvernforordningen setter.

I vedlegg én følger revidert forslag til *styrende del*. I vedlegg to følger samme forslag, men med «spor endringer» markert slik at de konkrete endringene lettere vises, mens i vedlegg tre er någjeldende utgave.

Jørgen Fossland
universitetsdirektør

Stig Ørsje
IT-direktør

Dokumentet er elektronisk godkjent og krever ikke signatur

Saksbehandler: Ingvild Stock-Jørgensen

Vedlegg
1 Revidert styrende del av ledelsessystemet (forslag)
2 Revidert styrende del av ledelsessystemet (forslag - med spor endring)
3 Gjeldende versjon av styrende del av ledelsessystemet
4 Grovskisse org.kart DPIA-gruppe og faggruppe for informasjonssikkerhet og personvern

[2] Lee A. Bygrave og Luca Tosoni, "Article 4(7), Controller" i The EU General Data Protection Regulation (GDPR) A Commentary, edited by Kuner, Bygrave, Docksey, 1st ed., 2020, Oxford University Press, s 149