UNIVERSITETET I BERGEN

Dato: 22.01.2016

Arkivsaksnr: 2011/12877

Styre: Universitetsstyret
Styresak: 15/16
Møtedato: 11.02.2016

Internrevisjon, rapporter

Henvisning til bakgrunnsdokumenter

- Sak 99/14: Internrevisjon, revisjonsplan for 2014/2015: http://www.uib.no/sites/w3.uib.no/files/attachments/2014-099.pdf
- Sak 66/15, Internrevisjon, rapport om digital eksamen
- Sak 93/15, Internrevisjon, rapporter om sidegjøremål og forskningsbevillinger: http://www.uib.no/sites/w3.uib.no/files/attachments/us2015-093.pdf
- Sak om organisering av internrevisjon i samme møte, 11.2.2016

Saken gjelder:

Vedlagt ligger rapport om internrevisjonsprosjektene om: Behandling og oppbevaring av personopplysninger og Gjennomgang Paga WEB.

Begge rapportene viser tilfredsstillende internkontroll, men det er identifisert forbedringspotensiale.

PwC vil presentere rapportene i styremøtet 11. februar 2016.

vedtak:
Universitetsstyret tar rapporten om Behandling og oppbevaring av personopplysninger og rapporten om Paga Web til etterretning.

Kjell Bernstrøm
universitetsdirektør

22.01.2016/Silje Christine Nerheim

Vedlegg:
1. Saksframstilling
2. Rapport, Delprosjekt Nr 2015/03: Behandling og oppbevaring av personopplysninger
3. Rapport, Delprosjekt Nr 2015/04: Gjennomgang Paga WEB

Saksframstilling

Styre:	Styresak:	Møtedato:	Arkivsaksnr:
Universitetsstyret	15/16	11.02.2016	2011/12877

Internrevisjon, rapporter

Rapport om behandling og oppbevaring av personopplysninger
Internrevisjonen har gjennomgått rutiner og prosesser for håndtering av personopplysninger ved Det medisinsk-odontologiske fakultet og Det psykologiske fakultet. Revisjonen er avgrenset til større forskningsprosjekter.

Revisjonen har fokusert på:
- Redegjøre kort for juridiske føringer og rammer for håndtering av personopplysninger
- Kartlegge og vurdere om det er etablert tilstrekkelige rutiner og retningslinjer for behandling av personopplysninger
- Teste gjennomføring og etterlevelse av rutinene ved UiB på utvalgte institutter.

UiB har to internkontrollsystemer for forskning, ett for forskning etter personopplysningsloven og ett felles system med Helse Bergen for forskning regulert av helseforskningsloven. Behandling av personopplysninger er et linjeansvar.

Internrevisjonen har sett indikasjoner på at instituttene ikke har tydelige dokumenterte rutiner for etterlevelse av fakultetets og universitetets retningslinjer. På den annen side peker internrevisjonen på at instituttledere og prosjektledere er svært bevisste og kompetente i håndteringen av personopplysninger og det er ikke avdekket brudd på lovverk.

Internrevisjonen har observert at samarbeid med regional etisk komité (REK) og Norsk Samfunnsvitenskapelig Datatjeneste (NSD) fungerer svært godt og medvirker til at forskningsprosjekter blir planlagt og gjennomført i samsvar med etiske standarder og gjeldende lov og forskrifter.

Internrevisjonen peker videre på at UiB har hatt en lite ensartet teknisk løsning for lagring og behandling av persondata. Det arbeides med en ny sikker løsning kalt SAFE. Revisjonen påpeker at SAFE fremstår som tilfredsstillende etter de standarder som kreves av tekniske løsninger for behandling og oppbevaring av persondata.

Internrevisjonen anbefaler flere tiltak for forbedringer, blant annet mer presise maler og veiledninger, faste ressurspersoner som er tilgjengelige for instituttene og at SAFE bør gjøres tilgjengelig for samtlige institutt som driver forskning som innebærer behandling av persondata.

Rapport om Paga Web
Internrevisjonen har gjennomført en revisjon med følgende hovedformål:

- kartlegge og vurdere om det er etablert gode rutiner for registrering av faste og variable lønnsdata i PagaWeb som bidrar til å sikre korrekt registrering av lønn og relaterte kostnader.
- Teste at rutinene etterleves i praksis
- Gjennomgå brukertilganger for å vurdere om de gir grunnlag for god arbeidsdeling
- Vurdere om det kun er brukere som har behov for tilgang til PagaWeb, som har tilgang til løsningen.

Revisjonens hovedinntrykk er at UiB har fått på plass nødvendige rutiner og retningslinjer for lønnsoppgaver som utføres på fakultets-/instituttnivå og at disse i hovedsak etterleves. Det pekes på at det er etablert formelle rutiner og retningslinjer for lønnsområdet som er lett tilgjengelige.

Det er videre etablert god kommunikasjon mellom lønnskontoret og fakultet/institutt. På den annen side viser rapporten noen konkrete områder med rom for forbedring knyttet til våre rutiner og til funksjonalitet i Paga.

Internrevisjonen har testet etterlevelse av retningslinjene for reiseregninger gjennom dialog og undersøkelser ved noen utvalgte enheter. Hovedinntrykket er at det stort sett fungerer bra, men at det er noen forbedringsområder.

Universitetsdirektøren sine kommentarer:

Behandling og oppbevaring av personopplysninger
Det er svært viktig at behandling av personopplysninger i forskning skjer i henhold til regelverket. De som deltar i forskningsprosjekter må ikke være i tvil om at personopplysningene blir behandlet forsvarlig og i samsvar med de gjeldende lover og forskrifter.

Internrevisjonsrapporten gir viktige innspill til vårt pågående arbeid med å styrke kompetansen og rutinene knyttet til personvern i forskning.

Ledelsen ved UiB har behandlingsansvar for personopplysninger. Oppgavene knyttet til dette ansvaret er delegert til fakultets- og instituttnivå. Det er viktig at ledelsen ved UiB legger til rette for at behandlingen av personopplysninger på instituttnivå i de enkelte forskningsprosjektene blir god og skjer i overensstemmelse med lov og regelverk.

Det er satt i gang flere prosjekter for å styrke arbeidet med personvern i forskning ved UiB. I avvikssaken som ble meldt til Datatilsynet, omtalt i styresak 76/15, ble det avdekket mangler ved opplæring av prosjektledere og andre som jobber med forskning på personopplysninger. Det jobbes med å forbedre rutinene knyttet til opplæring.

Internkontrollsystemene for forskning skal rutinemessig revideres i løpet av 2016 og dette arbeidet er påbegynt.

Det er utviklet en løsning for sikker behandling av sensitive personopplysninger i forskningsdata, SAFE (Sikker Adgang til Forskningsdata og E-infrastruktur). Løsningen lanseres og rulles ut i organisasjonen våren 2016.

Internrevisjonen peker på at universitetet bør ha faste ressurspersoner og kompetanse innenfor håndtering av personopplysninger og helseforskning som er tilgjengelig for instituttene. UiB har styrket kompetansen på dette området, slik at bistanden til forskningsmiljøene blir bedre og lettere tilgjengelig.

Internrevisjonsrapporten gir en rekke detaljerte og nyttige innspill og forslag til tiltak som vi tar med i det videre arbeidet.

PagaWeb
Økonomiavdelingen har hatt og har fortsatt stor fokus på å etablere tilstrekkelig internkontroll for å sikre rett lønn til rett tid. Dette gjøres blant annet gjennom utarbeiding av rutiner og prosessbeskrivelser for lønnsområdet, gjennom oppsett og arbeidsflyt i Paga Web og gjennom opplæring, kompetanseutvikling og dialog med de som har en funksjon/rolle i lønnsprosessen. Rutinene er gjort tilgjengelig på UiBs ansattsider.

Internrevisjonsrapporten peker på noen forbedringsområder som lønnskontoret allerede har iverksatt tiltak for å videreutvikle.

Det er etablert dialog med leverandør av lønnstjenestene med sikte på å lukke de punktene knyttet til roller og brukertilganger i lønnssystemet. Dette er i stor grad på plass.

Internrevisjonsrapporten peker på noen områder der funksjonalitet og prosessflyt virker tungvint. Økonomiavdelingen har kontinuerlig fokus på å effektivisere alle sine økonomiprosesser og tiltakene foreslått i rapporten vil bli hensynstatt. Noen endringsforslag er allerede meldt til leverandøren. Reiseregningsprosessen er en av arbeidsprosessene som vil bli gjennomgått.

Internrevisjonsrapporten har gitt nyttige innspill til vårt arbeid for å videreutvikle og forbedre lønnsprosessene.

22.01.2016/Silje Nerheim/Kirsti Aarøen/Tone Elin Skaugvold

Revisjonsprosjekt
Behandling og oppbevaring av personopplysninger
Nr. 2015/03

Utkast rapport: 20.10.2015

Endelig rapport: 09.11.2015

Til: Universitetet i Bergen
v/ Kollegiesekreteriatet

Kopi til: Universitetsdirektøren
ved Universitetet i Bergen

Fra: Jan Roger Hånes,
PricewaterhouseCoopers AS

Sign: 

pwc

Innholdsfortegnelse

1 Introduksjon

Bakgrunn

PricewaterhouseCoopers (PwC) har gjennomført en internrevisjon vedrørende håndtering av personopplysninger. Gjennomgangen er basert på årsplan for internrevisjonen og planleggingsmemo godkjent av UiB.

Formål og omfang

Formål og omfang er definert i årsplan vedtatt av styret for 2014-2015.

Formålet med revisjonen er å gjennomgå rutiner og prosesser for håndtering av personopplysninger ved Medisinsk- odontologisk fakultet og Psykologisk fakultet, og resultatene vil kunne gjelde for øvrige deler av Universitetet.

Revisjonen er avgrenset i gjennomgangen til å gjelder for større forskningsprosjekter.

Revisjonen har fokusert på

- Redegjøre kort for gjeldende juridiske føringer og rammer for håndtering av personopplysninger
- Kartlegge og vurdere om det er etablert tilstrekkelige rutiner og retningslinjer for behandling av personopplysninger
- Teste gjennomføring og etterlevelse av rutinene ved UiB på utvalgte institutter

Revisjonsperiode

Internrevisjonsprosjektet ble gjennomført i august-oktober 2015.

Gjennomført arbeid

Revisjonens tilnærming har vært todelt. I første omgang har PwC gjennomgått instrukser og policyer som universitetet har utarbeidet for vurdere hvor godt de samsvarer med juridiske føringer. I andre omgang har PwC gjennomgått instituttenes prosess for håndtering av personopplysninger i forbindelse med større forskningsprosjekt, for å vurdere om de har tilstrekkelige rutiner, systemer og kompetanse for å etterleve universitetets instrukser. Vi har hatt intervjuer med følgende avdelinger (deltakerlisten er ikke komplett):

Avdeling	Navn	
Klinisk Institutt 2	Per Bakke Julie Stavnes	Roland Jonson Siv Johnsen Eggereide
Institutt for Samfunnspsykologi	Normann Andersen Anita Lill Hansen Hege Høivik Bye Ståle Einarsen	Jørn Hetland Terje Manger Bjørn Sætrevik Nora Wiium
Institutt for Global Helse og Samfunnsmedisin	Rolv Terje Lie Tone Bjørge Kari Juul	Stein Emil Vollset Siri-Smith Giske Grethe Tell
UiB IT avdeling	Jan Kristian Walde Johnsen Tore Burheim (*Innspill på foreløpig rapport*)	Tore Linde

Revisjonsteam

Følgende personer har deltatt i revisjonen fra PwC:
Jan Roger Hånes, Øistein Jensen, Bård Strøm, Marius Mjelde og Mari Strøm.

2 Oppsummering

Risikovurdering: Middels	**Vurdering av internkontroll:**		**Trend: Ikke aktuelt**

Oppsummering av observasjoner:

Ved Universitetet i Bergen behandles personopplysninger i universitetets administrative systemer og i forskning. Personopplysningsloven med forskrift stiller krav til hvordan slike opplysninger skal behandles. Medisinsk og helsefaglig forskning reguleres i tilleg av helseforskningsloven.

I samsvar med forskrift til personopplysningsloven § 2-3 er universitetsledelsen behandlingsansvarlig for behandling av personopplysninger i forskning ved Universitetet i Bergen. Rektor og universitetsdirektøren har delegert behandlingsoppgaver til lederne for de organisatoriske enhetene. Behandling av personopplysninger i forskningssammenheng er et linjeansvar.

Universitetet har utarbeidet et kvalitetssystem for behandling av personopplysninger, som angir retningslinjer for håndtering av personopplysninger i forskning. I tillegg har Universitetet i samarbeid med Helse Bergen utarbeidet retningslinjer for medisinsk og helsefaglig forskning. Medisinsk- odontologisk fakultet har videre utarbeidet retningslinjer for oppfølging av UiBs kvalitetessystem og behandling av personopplysninger i forskning. Dette inkluderer roller, ansvar og oppgaver for alle prosjekter som omhandler persondata, der det er tatt hensyn til dagens internkontrollsystem og delegasjonsvedtak fra rektor.

I faktultetets retningslinjer står det at instituttleder har ansvar for at nødvendige prosedyrer og rutiner er på plass ved egen institutt, samt at disse er iverksatt og oppdatert. Internrevisjonen har gjennom intervjuer og gjennomgang av øvrig dokumentasjon sett indikasjoner på at instituttene ikke har tydelige dokumenterte rutiner for etterlevelse av fakultetets og Universitetets retningslinjer. Dette inkluderer manglende standardisering og tilpasning av maler og dokumentasjon, manglende rutiner for tilgangsstyring, lagring og sletting og manglende sjekklister og erklæringer ved oppstart og avslutning av prosjekt. Likevel er det viktig å bemerke at instituttleder og prosjektledere er svært bevisste og kompetente i håndteringen av personopplysninger, og internrevisjonen har ikke avdekket brudd på lovverk. Internrevisjonens observasjoner er i hovedsak basert på de fremstillinger som er gitt i intervju med avdelingene gjengitt over, og dette medfører at internrevisjonen ikke kan utelukke at det kan foreligge brudd som ikke er avdekket.

Videre har internrevisjonen observert at dialog og samarbeid med regional etisk komite (REK) og Norsk samfunnsvitenskapelig datatjeneste (NSD) fungerer svært godt, og medvirker til at forskningsprosjekter blir planlagt og gjennomført i tråd med etiske standarder og gjeldende lover og forskrifter.

Det fremstår som at Universitetet har hatt en lite ensartet teknisk løsning for lagring og behandling av persondata. Arbeidet med implementering av en ny sikker løsning, kalt SAFE er imidlertid i gang. SAFE fremstår som tilfredsstillende etter de standarder som kreves av tekniske løsninger for lagring og behandling av persondata.

Oppsummering av tiltak:

For å imøtese de krav som stilles i forhold til håndering av personopplysningsloven, foreslås følgende tiltak:

- Det bør utarbeides mer presise maler og veiledninger. De enkelte institutt bør vurdere om det er hensiktsmessig for de å utarbeide egne maler til søknader og samtykkeerklæringer som er tilpasset instituttets behov, for å forenkle søknadsprosess overfor REK og NSD. I forbindelse med søknadsprosessen bør det opprettes sjekklister over hvilke aktiveter som må utføres før forskningsprosjektene kan settes i gang.

- Før søknad til REK/NSD sendes, bør det være en intern godkjenningsprosess. Dette kan løses ved å opprette en etikkomite, som foreslått av enkelte av forskerne. I tillegg bør instituttleder orienteres om prosjekter før søknad evt. sendes til REK/NSD. Instituttleder bør ha en komplett oversikt over alle pågående prosjekt ved instituttet. I en slik oversikt bør det minimum registeres godkjenningsdato, dato for eventelle godkjente endringer, publiserings- og/eller avslutningsdato samt dato for når persondata må slettes. Prosjektleder bør således orientere instituttleder både i forkant av oppstart, og ved publisering/innsending av sluttmelding til REK.

- For bedre å kunne bistå instituttene med juridiske avklaringer der det er tvil om tolkningen av lovmessige krav, vil det være en fordel om universitetet har faste ressurspersoner/kompetanse innenfor håndtering av personopplysninger og helseforskning som er tilgjengelig for instituttene.

- Hvert institutt bør utforme klare retningslinjer for hvordan data skal lagres, både fysiske og elektroniske. Retningslinjene må ivareta de spesifikke utfordringene knyttet til instituttet, slik som hvorvidt forskerne deler kontor, om det finnes muligheter for et felles arkivrom mv. Retningslinjene bør være tydelige, og konkretisere hvilke opplysninger som må låses inne.

- Det bør innføres en rutine for at prosjektleder kontrollerer at endringsmelding er sendt før det bes om ny systemtilgang eller informasjon blir delt.

- Det bør etableres rutiner for håndtering av krav om innsyn. I denne forbindelse bør det utarbeides et standarddokument som beskriver de sikkerhetstiltakene som er på plass for håndtering av personopplysninger slik at dette kan kommuniseres til forskningsdeltaker uten å kompromittere sikkerhetstiltakene. Prosjektleder må ha en oversikt over de personopplysninger som er lagret, slik at disse er enkle å samle dersom det stilles krav fra forskningsdeltaker om innsyn eller sletting/utlevering.

- Løsningen kalt SAFE for lagring og håndtering av persondata som er implementert ved Institutt for Global Helse og Samfunnsmedin, bør gjøres tilgjengelig for samtlige institutt som bedriver forskning som innebærer behandling av persondata. Dette inkluderer tilfeller hvor det kun benyttes indirekte identifiserbare personopplysninger. I tillegg anbefales at risikovurderingen knyttet til SAFE oppdateres, og at det utarbeides rutiner som innebærer oppdatert risikovurdering årlig, eller ved vesentlige endringer.

3 Revisjonskriterie

3.1 Definisjoner

«**Personopplysning**»: Det følger av personopplysningsloven § 2 nr. 1) at personopplysning er «*opplysninger og vurderinger som kan knyttes til en enkeltperson*». Dette innebærer at både direkte og indirekte tilknytning til person omfattes. En opplysning er indirekte knyttet til en person når flere opplysninger må undersøkes før persontilknytningen kan bringes på det rene. Det foreligger en «personopplysning» selv om det er flere ledd mellom opplysningen og personen. Likevel må det skjønnsmessig trekkes en grense mht. hvor stor innsats som kreves for å knytte en opplysning til en person. I fortalen nr. 26 til personverndirektivet (95/46/EF), er det uttalt at spørsmålet skal bedømmes ut i fra «*alle* hjelpemidler [...] som det er *rimelig* å ta i bruk for å identifisere vedkommende, enten av den behandlingsansvarlige eller av en annen person.» Dersom det kreves stor arbeidsinnsats og/eller kostnad å knytte opplysningen til en person, kan dette derfor tale for at en ikke anser opplysningen for å være «personopplysning». Tilsvarende dersom det er usikkerhet mht. hvilken person en opplysning er knyttet til. Det er ikke mulig å generelt angi hvor stor usikkerheten må være for at en opplysning ikke er å anse som «personopplysning». Det kan imidlertid antas at det vil bli godtatt større usikkerhet dersom de aktuelle personene tilhører samme hushold/familie enn dersom det ikke er slik tilknytning, jf. formålsbestemmelsen i popplyl § 1 annet ledd og beskyttelsen av privatlivets fred. Generelt må kravet om tilknytning til enkeltperson vurderes i relasjon til formålsbestemmelsen. Jo mer alvorlig de mulige personvernkrenkelsene er, jo større ressursinnsats og/eller usikkerhet kan være knyttet til identifiseringen av personer, uten at opplysningen av den grunn faller utenfor begrepet «personopplysning».

«Sensitiv personopplysning»: sensitive personopplysninger er definert i personopplysningsloven § 2 nr. 8) som opplysninger om enten:
(1) rasemessig eller etnisk bakgrunn, eller politisk, filosofisk eller religiøs oppfatning,
(2) at en person har vært mistenkt, siktet, tiltalt eller dømt for en straffbar handling,
(3) helseforhold,
(4) seksuelle forhold,
(5) medlemskap i fagforeninger

Behandling av sensitive personopplysninger stiller strengere krav til hjemmelsgrunnlag for behandling, herunder samtykke. I tillegg krever behandling av sensitive personopplysninger i utgangspunktet konsesjon fra Datatilsynet. Det er et viktig unntak fra konsesjonsplikten i forskrift om behandling av personopplysninger § 7-27 for forskningsprosjekter som er tilrådd av personvernombud. For medisinsk og helsefaglig forskning er det i tillegg krav om tilråding fra en regional forskningsetisk komité.

«**Helseopplysning**»: Det følger av helseforskningsloven § 4, bokstav d) at helseopplysninger er «*taushetsbelagte opplysninger i henhold til helsepersonelloven § 21 og andre opplysninger og vurderinger om helseforhold eller som er av betydning for helseforhold, som kan knyttes til en enkeltperson*». Det skilles i loven og i forarbeidene mellom personentydige helseopplysninger som er direkte personidentifiserbare (åpne helseopplysninger), og personentydige helseopplysninger som er indirekte personidentifiserbare (skjulte/krypterte e.l.). Begge disse typer opplysninger er likevel å anse som helseopplysninger.

«**Indirekte identifiserbare helseopplysninger**»: Begrepet er definert i helseregisterloven som «*helseopplysninger der navn, fødselsnummer og andre personentydige kjennetegn er fjernet, men hvor opplysningene likevel kan knyttes til en enkeltperson*». Begrepet er nytt i ny helseregisterlov, og erstatter tidligere benyttede begreper «avidentifiserte helseopplysninger» og «pseudonyme helseopplysninger». Det fremgår av forarbeidene til loven at dersom opplysningene ikke kan knyttes til et enkelt individ via en nøkkel, men det likevel kan være mulig å finne frem til individet på bakgrunn av variablene som inngår, vil datasettet være indirekte

identifiserbart. Dette kan tenkes dersom man i utgangspunktet har avidentifiserte opplysninger, hvor kun alder, kjønn, nasjonalitet og bostedskommune fremgår. At man har helseopplysninger om en norsk mann på 42 år som bor i Oslo innebærer at man faller utenfor definisjon på helseopplysning, da dette ikke kan knyttes til enkeltpersoner. Dette vil stille seg annerledes dersom man har helseopplysninger eksempelvis om en kvinne på 87 år fra San Marino som bor i Utsira kommune. I sistnevnte tilfelle vil man falle innenfor begrepet «indirekte identifiserbare helseopplysninger». Opplysningene vil da anses som helseopplysninger, og dermed være underlagt de restriksjoner som settes i lovgivningen.

Også personopplysninger som ikke er helseopplysninger kan være indirekte identifiserbare, og dermed være underlagt restriksjonene i personopplysningsloven. Dette følger direkte av definisjonen i personopplysningsloven § 2 nr. 1), «knyttes til en enkeltperson».

«**Anonyme opplysninger**»: Anonyme opplysninger kan ikke knyttes til en enkeltperson. Det er et strengt krav om at identifikasjon ikke skal være mulig, verken direkte eller indirekte, for at kravet til anonymitet skal være oppfylt. Dersom en opplysning anses som anonym faller den utenfor reguleringen etter personopplysningsloven, helseregisterloven og helseforskningsloven med tilhørende forskrifter.

3.2 Juridiske føringer

Rekkevidde av ansvar: Ansvaret tilligger i utgangspunktet den institusjonen som har tillatelsen til å behandle personopplysninger. Det innebærer at dersom UiB mottar opplysninger fra andre forskningsinstitusjoner som de har tillatelse til å behandle, er det i utgangspunktet utenfor UiBs ansvar å kontrollere hvorvidt disse forskningsinstitusjonene har nødvendige tillatelser til å dele denne informasjonen.

I tilfeller hvor det er forskere ved UiB som har tillatelsen til å behandle personopplysningene, er det strenge krav i forhold til deling/utlevering av disse opplysningene. Dersom opplysningene skal utleveres til andre enn de som opprinnelig har mottatt tilgang, må dette søkes om. Deling av personopplysninger innenfor EU/EØS, er regulert av personverndirektivet. For deling, både inn og ut av Norge, med land utenfor EU/EØS stilles det strenge krav etter personopplysningsloven § 29 og § 30, samt helseforskningsloven § 37. Det fremgår av forarbeidene til sistnevnte lov, Ot.prp. nr. 74 (2006-2007), kapittel 9.3.3.2, at:

«Ved store multinasjonale forskningsprosjekter, kan det være naturlig å anse den delen av prosjektet som den forskningsansvarlige er ansvarlig for, som et eget prosjekt. Det er ikke meningen at lovens virkeområde skal tolkes slik at ethvert samarbeid med utlandet tilsier at norske regler skal gjelde for forskningen som primært har tilknytning til andre land. […]

Det må […] forutsettes at der forskningsansvarlig er etablert i en stat innenfor EØS-området, vil helseopplysninger bli behandlet på en forsvarlig måte i tråd med direktivet. Der forskningsansvarlig er etablert i en stat utenfor EØS-området, og benytter hjelpemidler i Norge til å forske, må reglene i denne lov følges.»

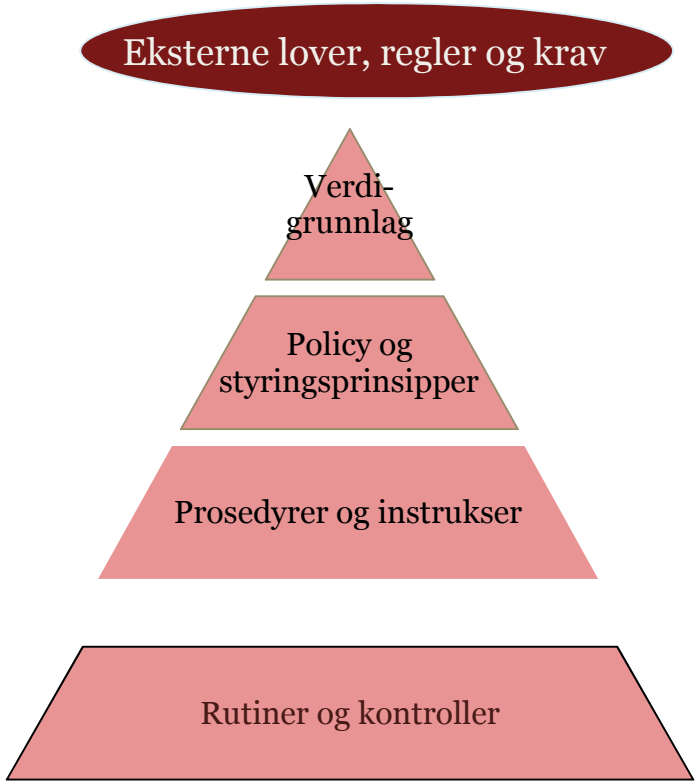
Dette innebærer at spesielt i tilfeller hvor det samarbeides med forskningsinstitusjoner utenfor EU/EØS-området bør det undersøkes nærmere hvorvidt tilfellet er regulert etter norsk rett, om behandlingen innebærer krav til godkjenning fra Rek mv.

Hvilke krav stilles til tekniske løsninger for lagring av personopplysninger?
Det følger av personopplysningsloven § 13 at den behandlingsansvarlige plikter å sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger. Videre oppstiller bestemmelsen en forskriftshjemmel, som blant annet kan regulere tekniske sikkerhetstiltak knyttet til behandling av personopplysninger.

I personopplysningsforskriften kapittel 2 er det gitt en del krav, se blant annet § 2-11 som fastslår at for «personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig». Forskriftshjemmelen gir imidlertid kun kompetanse til å fastsette bestemmelser innenfor rammene av bestemmelsene i loven. Lovens krav om at informasjonssikkerheten skal være «tilfredsstillende», forutsetter at det må gjøres en konkret vurdering av hvilke sikringstiltak som er påkrevet.

4 Internkontroll

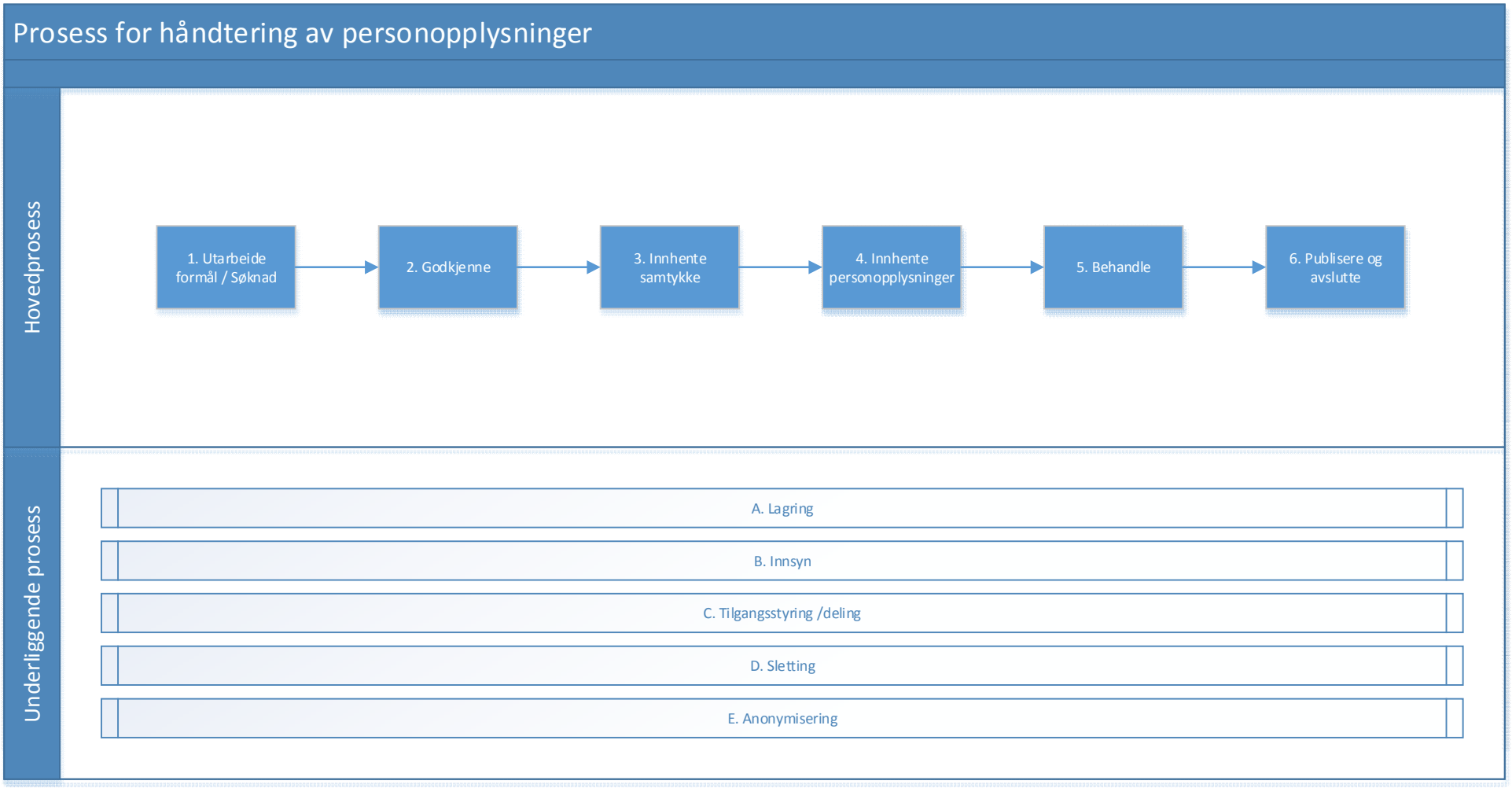
Helseforsikringsloven krever at det skal føres internkontroll i forskningsprosjekter og at det er prosjektleder/forskeren sitt ansvar å påse at det er et system for dette. Med internkontroll defineres det i «Veileder for personvern og informasjonssikkerhet» at det er planlagte og systematiske tiltak som skal sikre at virkshomhetens aktiviteter plalegges, organiseres, utføres og vedlikeholdes i samsvar med krav fastsatt i eller i medhold av lovgivningen. For forskningsprosjekter ved UiB vil internkontroll-rammeverket være en del av universitetets styringssystemer. Internkontroll handler om et helhetlig system som bidrar til å redusere risiko for brudd med eksterne og interne retningslinjer og som bidrar til å at universitetet når de mål som er satt. Internkontrollsystemet er ikke bare sjekklister og rutiner, men også etikk, verdigrunnlag og hvilken policy og ledelsesføringer som er gitt samt hvilken styrings- og kontrollstruktur som er etablert for å bidra til måloppnåelse og redusere sannsynlighet for at uheldige hendelser oppstår. Internkontrollsystemet bør være risikodrevet, slik at der risikoen er høyest stiller det høyere krav til internkontrollsystemet og omfanget av det. Dette kan illustreres med følgende figur.



Dokumentasjon og system

- Nivå 1
  - Verdigrunnlag og etiske retningslinjer
  - Beskrivelse av virksomhetens styringsmodell - plattformen for "Management Governance"
- Nivå 2
  - Fullmakter, og myndighet (rolle/ansvarsfordeling)
  - Styringsprinsipper/policies angir rammene og prinsippene som skal etterleves i utøvelsen av forretningsvirksomhet
- Nivå 3
  - Prosedyrer angir retningslinjene som skal sikre implementering av styringsprinsippene/policies
  - Reglement, forskrifter, instrukser, o.l. som ikke er definert som del av modellen for styringsdokumenter
- Kontrollhandlinger
  - Kontrollfunksjon for å ivareta kvalitet i operasjonelle- og finansielle prosesser, samt compliance i forhold til relevant regelverk
  - Overvåking av kontroller samt system for og dokumentasjon

Internrevisjonen har i samarbeid med instituttene utarbeidet et generisk prosesskart for å visualisere og strukturere prosessen for håndtering av personopplysninger.



5 Observasjoner

#	*Aktivitet*	*Observasjon*	*Konsekvens*	*Anbefalinger*
1	**Utarbeide forsknings-design og søknad**	Mal for søknad og samtykkeerklæringer finnes på REK og NSD sine nettsider, og forskerne oppgir at de hovedsakelig benytter disse. Universitetet har ikke egne maler for prosjekter, heller ikke i tilfeller hvor det ikke er påkrevd å søke REK eller NSD. Det utelukkes ikke at enkelte forskere kan ha utarbeidet sine egne maler.	Det er opp til den enkelte forsker selv å identifisere hvorvidt prosjekter krever REK godkjenning, noe som kan resultere i manglende godkjenningsprosess. Manglende ensartede maler der REK ikke er involvert kan resultere i manglende kvalitetssikring av prosjekter.	Instituttene bør vurdere å lage standardiserte maler for søknader bedre tilpasset eget institutt og forskning. Dette vil sikre at det ikke går med unødig mye tid til å tilpasse REK-maler, samt at det blir lettere å kvalitetssikre malene som benyttes, slik at behandlingstiden hos REK blir redusert. Det anbefales at det opprettes sjekklister pr. institutt for hvilke aktiviteter som må gjennomføres før forskniningsprosjektene starter, i henhold til UiB og Helse Bergens retningslinjer for medisinsk og helsefaglig forskning. http://www.helse-bergen.no/no/FagOgSamarbeid/forsking/Documents/401A%20Oppstart%20av%20forskningsprosjekter%20-%20rutine.pdf

2	**Godkjennings -prosess**	Godkjenning hos REK er en interaktiv prosess, med tett dialog og forskerne opplever at man kommer frem til felles, gode løsninger. PwC har ikke observert at det foreligger en beskrevet intern godkjenningsprosess. Forskerne trenger ikke søke eller melde instituttleder om nye forskningsprosjekt. Enkelte institutt melder om nyopprettede systemer med egenerklæringsskjema, som benyttes for innrapportering av pågående prosjekt. Planen er at alle forskere skal sende slik egenmelding til instituttet en gang i året. Dette er imidlertid ikke noe som er pålagt sentralt, og det er derfor store forskjeller mellom hvert institutt for hvordan/hvorvidt dette praktiseres. Praksis er at forskerne alltid søker godkjenning hos REK eller NSD, selv om han/hun er sikker på at prosjektet ikke er meldepliktig. Dette gjøres fordi forskerne i publikasjonen kan henvise til at prosjektet er unntatt meldeplikten i henhold til veiledning fra NSD. Enkelte forskere har meldt om at de ikke opplever at det er tilstrekkelig juridisk kompetanse internt, til å kunne motta hjelp ved komplekse problemstillinger som kan oppstå i søknadsprosessen. Det er mange lover og forskrifter å forholde seg til, og det er ofte behov for bistand til hvordan de ulike kravene skal forstås og håndteres.	Manglende innmelding av prosjekter til instituttleder gjør at det ikke foreligger en kontroll for å sikre at alle prosjekter blir meldt til REK/NSD der det er påkrevd. Ettersom det er oppstilt unntak fra konsesjonsplikt for forskningsprosjekt som er tilrådd av personvernombud (NSD) eller REK i personopplysningsforskriften § 7-27, vil manglende søknad kunne innebære brudd på krav til å innhente konsesjon for forskningsprosjekt som innebærer behandling av sensitive personopplysninger. Bruk av egenerklæring til å ha en årlig innrapportering av pågående prosjekter viser en klar forbedring på området. En årlig innrapportering vil likevel ikke nødvendigvis avdekke på et tidlig nok tidspunkt hvorvidt et prosjekt skulle ha være meldt til REK eller NSD. Manglende juridisk bistand fra UiB gjør at forskerne må henvende seg til andre institusjoner for bistand. Dette kan resultere i uensartet praksis og forståelse av regelverket. Dette kan også forlenge søknadsprosessen, da det ikke kan forventes at alle forskerne/forskningsledere har tilgang til den juridiske kompetansen de har bruk for utenfor UiB.	Instituttleder bør involveres på et tidligere tidspunkt i godkjenningsprosessen. Instituttleder bør ha en oversikt over alle forskningsprosjekter som pågår ved eget institutt, slik at disse kan kontrolleres mot REK og NSD sine oversikter over godkjente prosjekter. På den måten vil instituttleder ha kontroll på at prosjekter blir meldt eller søkt til hhv. NSD og REK dersom det er påkrevd. For bedre å kunne bistå instituttene med juridiske avklaringer der det er tvil om tolkningen av lovmessige krav, vil det være en fordel om universitetet har faste ressurspersoner/kompetanse innenfor håndtering av personopplysninger og helseforskning som er tilgjengelig for instituttene. Det ble fremmet forslag om at instituttene burde hatt en egen etikkomite, som vurderer alle påtenkte prosjekter. Dette skal i så fall fungere som et supplement til REK/NSD.

3	**Innhente samtykke**	Forskerne henter mal for samtykkeerklæring fra REK sin nettside. Denne må deretter tilpasses til det enkelte prosjekt. Forskerne melder om at utfordringene med samtykkeerklæringene er først og fremst balansen mellom at den må inneholde nok informasjon til å oppfylle lovkrav, men samtidig ikke bli så omfattende at pasienten rent faktisk ikke evner å sette seg inn i hva de gir sitt samtykke til. Det finnes eksempler på at samtykke er gitt i henhold til juridisk krav, men hvor det i ettertid tydelig har fremkommet at pasienten ikke var klar over hva han/hun hadde samtykket til. Forskerne vil over tid benytte sine egne maler, som de mener balansere disse hensynene best. For klinisk forskning melder forskerne om at det tidvis er utfordrende å innhente samtykke knyttet til forskning med patologisk materiale, der samtykker er avdødd. I tillegg har forskerne bare tillatelse å purre på samtykkeerklæringer en gang.	Det reduserer effektivitet at alle forskerne må tilpasse REK-malene til eget bruk. Enkelte forskere kan over tid utarbeide ganske gode maler, mens andre må bruke vesentlig tid på dette. I tillegg er det en risiko for at forskerne benytter maler som ikke er kvalitetssikret eller er uforståelig for den som samtykker. Begrensningen i at man kun kan purre på samtykkeerklæringer en gang kan medføre utfordringer knyttet til å få bredt nok referansegrunnlag til undersøkelser. Det vil derfor være viktig at man utarbeider maler og avgrensninger som sikrer at man mottar flest mulig samtykkeerklæringer.	Instituttene bør vurdere å lage standardiserte maler for samtykkeerklæringer bedre tilpasset eget institutt og forskning, se punkt 1. Instituttene er ansvarlig for dette, og må vurdere om det er hensiktsmessig å lage en egen sjekkliste som er best tilpasset de, eller om noe kan gjøres felles. Samtykkeerklæringene bør hensynta balansegangen mellom nåværende og framtidig forskningsbehov, samt tydelighet for forskningsdeltakeren og lovmessige krav til informert samtykke. I tillegg bør forskningsdeltaker føle seg trygg på at informasjonen ikke blir anvendt på måter som de ikke har samtykket til.
4	**Innhente person-opplysninger**	Forskerne kan innhente personopplysninger fra flere kilder: **Direkte henvendelser:** Forskerne sender ut spørreskjema eller lignende som respondenter svarer på. Resultatene må deretter manuelt registreres i datasystemet som brukes. Ofte settes forskningsassistenter til dette arbeidet, og de er en risiko for at de ikke er kjent med gjeldende instrukser for håndtering av personopplysninger. Det er ikke generelle krav om signering av taushetserklæringer e.l. i denne	**Direkte henvendelse:** Manuell registrering av data kan være et omfattende arbeid ved store undersøkelser. I mange tilfeller vil det være flere forskningsassistenter som er med i dette arbeidet og det vil være utfordrende å sikre riktig håndtering av personopplysninger. **Andre institusjoner** Det mangler klare rutiner for innhenting av kliniske data fra samarbeidende	Det er viktig at instituttene utarbeider egne rutiner for håndtering av personopplysninger ved registrering av store datamengder. I tilfeller der det er mange personer involvert i databehandlingen er det viktig at rutinene er kjent og detaljer tilpasset de enkelte aktivitetene slik at

		forbindelse. Forskerne kan sende ut én purring til respondenten dersom vedkommende ikke har svart. **Andre institusjoner:** Data blir innhentet fra andre institusjoner, bl.a. helseinstitusjoner. For norske institusjoner blir det etterspurt REK-nummer for prosjektet. For institusjoner utenfor Norden er det andre krav som gjelder, men forskerne melder om at det ikke er fastsatte rutiner for hvordan denne prosessen er. I enkelte tilfeller får UiB mer data enn de etterspør og dette må da slettes manuelt. Som en generell regel vil personopplysninger som UiB samler inn være underlagt norsk lov, selv om forskningsprosjektet er en del av et større internasjonalt forskningsprosjekt. **Andre register:** En rekke register benytter egne retningslinjer for å godkjenne bruk av deres opplysninger. Dette gjør at selv om et prosjekt er REK-godkjent, så vil andre registre sette ytterligere, og til tider motstridende krav til hvordan opplysningene håndteres og anvendes. Enkelte forskere melder om at det er manglende juridisk bistand i UiB for å håndtere gråsonetilfeller ved utforming av forskningsdesign. Forskerne melder at registrene i de fleste tilfeller sender anonymiserte data, men dersom dette ikke er tilfelle sendes data på en kryptert USB-minnepenn og passord sendes separat.	institusjoner. Andre institusjoner vil kreve et REK-nummer før de utleverer data til UiB, noe som sikrer at UiB må ha en godkjenning fra REK. Likevel er det ingen kontroll med at innholdet i REK-godkjenningen samsvarer med de dataene som UiB etterspør. Manglende samsvar kan medføre risiko for at opplysningene ikke kan benyttes og må slettes. **Andre Register** Problemstillingen knyttet til at flere eksterne register har ulike retningslinjer og krav for utlevering av informasjon gjør at enkelte forskere opplever det som utfordrende å innfri alle krav, inkludert de regulatoriske. Det er ingen entydig rolle for juridisk bistand innen personopplysningsloven, som medfører at forskerne tar kontakt med andre institusjoner for å få en juridisk avklaring. I tillegg risikeres det at forskerne med delt stilling hos andre forskningsinstitusjoner kan velge å legge prosjektet sitt hos den andre institusjonen, dersom de kan tilby bedre bistand i søknadsprosessen, og dermed redusere behandlingstid.	risiko for feil håndtering blir redusert. Det kan også være hensiktsmessig å utarbeide rutiner for å sikre at data blir slettet dersom det ikke er behov for dem, og at taushetserklæringer blir signert av alle involverte parter. Det er viktig at det blir formidlet hvilken juridisk kompetanse som besittes innenfor UiB, eventuelt styrke den juridiske kompetansen knyttet til sentrale problemstillinger for håndtering av personopplysninger.

5	**Gjennomføre forsknings-prosjekt**	Forskerne gjennomfører forskningsprosjekt i henhold til godkjenning som er gitt fra REK eller NSD. Eventuelle endringer blir meldt til REK/NSD fortløpende. Det virker som om forskerne er bevisst på at endringsmeldinger skal sendes dersom det er endringer i den opprinnelige søknaden. Dette gjelder både ved endring av formål, samarbeidsparter og forskningsteam. Det er imidlertid en del gråsoner knyttet til hva som er endring av formål i forhold til den opprinnelige godkjenningen. Det ble reist spørsmål om hver mindre endring utgjorde krav til endringsmelding, for eksempel dersom man hadde foretatt en studie på vitamin As påvirkning på hjerte- og karsykdommer, utgjør det en endring å studere vitamin K? Det ble uttalt at forskerne sender endringsmeldinger for sikkerhets skyld, i tilfeller hvor de er usikre på om endringen er meldepliktig eller ikke.	Likevel er det få formaliserte rutiner eller sjekklister som sikrer at alle endringer blir meldt og godkjent, samt at instituttleder har lite oppsyn med at forskerne arbeider innenfor rammene av godkjenningen. Ettersom det ikke foreligger klare retningslinjer for hva som utgjør en endring i forhold til den opprinnelige godkjenningen, utgjør dette en risiko for at det ikke sendes endringsmeldinger i tilfeller hvor det foreligger meldeplikt.	Det bør utarbeides tydelige instrukser og eventuelt rutiner for når det skal sendes endringsmeldinger til NSD eller REK.
6	**Publisere**	Helseforskning kan ikke publiseres uten et REK-nummer. REK-nummer blir tildelt når prosjektet er godkjent av REK. Godkjenning må foreligge før prosjektet blir startet.	Prosess for REK-godkjenning er et kraftfullt virkemiddel for å sikre at alle forskningsprosjekter er REK-godkjent før de påbegynnes. Likevel er det ingen formalisert system for å sikre at forskningsprosjektet har blitt gjennomført i henhold til godkjent søknad, men dette vil kunne bli avdekket etter publikasjonen. Forskerne vil kunne risikere å måtte trekke publikasjonen dersom det viser seg at prosjektet ble gjennomført uten tilstrekkelig godkjenning.	Prosjektleder bør melde til instituttleder når resultatene fra prosjektet publiseres. Dette for at instituttleder skal ha en komplett oversikt over pågående og avsluttete prosjekter.
A	**Prosess for lagring**	**Fysisk lagring** Det synes å være varierende praksis knyttet til hvordan forskerne håndterer fysiske dokumenter som inneholder personopplysninger. Hvorvidt dokumenter låses	**Fysisk lagring** Manglende rutiner for håndtering av fysiske dokumenter, samt manglende ensartet praksis for låsing av og adgang til kontor, gjør at det er en risiko for at	Instituttene bør etablere rutiner for oppbevaring og lagring av fysiske dokumenter spesifikt tilpasset lokasjonen. Det varierer blant annet

	Prosess for lagring (Forts.)	inn på kontor, i skap eller brannskap, samt å ta med seg dokumenter hjem, avhenger av rutinene til den enkelte forsker. Det er også varierende hvorvidt flere har nøkkeltilgang til hverandres kontorer eller om kontorer kan låses i det hele tatt. Det er ingen felles rutiner på instituttnivå som beskriver hvordan dokumenter skal oppbevares. Det ble også reist spørsmål om arkivskapene som benyttes for fysisk lagring er tilstrekkelig sikre **Elektronisk lagring** UiB har for tiden et pilotprosjekt for lagring og håndtering av sensitive personopplysninger, som er kalt SAFE. Dette eksisterer som en pilotløsning for Institutt for Global Helse, og forventes å være andvendbar for resten av Universitetet i Bergen for oppbevaring av sensistive personopplysninger eller sensitiv informasjon for øvrig i løpet av desember 2015. Med pilotprosjektet menes her en fullverdig løsning, som blir testet ut på IGS før det blir allmenngjort overfor øvrige institutt, etter eventuelle korrigeringer. SAFE innebærer at det kreves en totrinns pålogging. Den ansatte må først logge på via sin UiB-konto, og deretter vil han/hun motta en sms på sin registrerte konto. Det er ikke mulig for den enkelte ansatte å selv legge inn hvilket telefonnr engangspassordet skal sendes til. For å hente ut informasjon som er lagret i SAFE, må denne hentes ut via såkalte sluser. Informasjonen som hentes ut blir kryptert, og krypteringsnøkkelen blir sendt forskeren separat. Inne i selve systemet logges hvem som har logget inn/ut til hvilke tidspunkt, og det logges hvilken informasjon som er ført gjennom slusene. Det er	dokumenter ikke blir lagret på en forsvarlig måte. **Elektronisk lagring** Det må skilles mellom SAFE løsningen som er underveis, og som er er i pilot ved Insitutt for Global Helse og samfunnsmedisin, og øvrige metoder for lagring av personopplysninger. SAFE ser ut til å tilfredstille de krav som stilles til sikker lagring av personsensitive data. Utenfor SAFE er det ingen ensartede tekniske løsninger for å lagre personsensitive data. Selv om det finnes måter å løse dette på utenfor den nye løsningen, har tilbakemeldingene fra de ulike instituttene vært at dataene lagres på usikre lagringsmedium, og at det ikke var vært kommunisert noen rutiner eller systemer for å håndtere dette. Den eksisterende praksis med å lagre etter ad-hoc prinsipp, utgjør en stor risiko for at personopplysningslovgivningen brytes, hva gjelder oppbevaring av sensitive personopplysninger.	hvorvidt forskere har egne kontorer, hvorvidt disse kan låses etc. Rutinene bør inkludere instrukser i forhold til innlåsing av skap, oppbevaring og låsing av kontor, arkivering, mv. I tillegg bør det opprettes en liste pr. prosjekt som angir hva som blir lagret og hvor dette oppbevares. Samtlige institutt bør inkluderes i den nye løsningen for sikker lagring av sensitive persondata, slik at det opprettes en klar og ensartet rutine for lagring av personopplysninger. Basert på gjennomgang av prinsippskisse, samt forklaring rundt hvordan løsningen er utformet og beskrevet forvaltet, virker SAFE løsningen for å være en fullgod tjeneste for oppbevaring av sensitiv persondata. Vi anbefaler likevel at risikovurdering for løsningen fra 2013 oppdateres, og settes i system i henhold til Normen for Informasjonssikkerhet, som forventer oppdaterte risikovurderinger per vesentlige endring eller minimum årlig. I tillegg bør retningslinjer for etterlevelse av

	Prosess for lagring	ikke mulig å kopiere i systemet, eller å hente ut informasjon uten å gå via slusene. Ettersom SAFE ikke er lanseringsklar før desember d.å., lagres sensiv informasjon i tilknytning til de fleste forskningsprosjekt etter ad-hoc prinsipp, enten gjennom tradisjonell fillagring på usikre servere, eller egne oppsatte datalagringsenheter. For disse forskningsprosjene er det ikke observert en entydig måte å forvalte og sikre informasjon på, og sikkerheten er i stor grad basert på ansattes skjønn og forsiktighet. For forskningsprosjekt som ikke er omfattet av SAFE, har en av metodene for å sikre tilgangsstyring og informasjonssikkerhet vært at forskningsprosjektet kun foregår på datamaskinger som er totalt frakoblet internett, og på et fysisk avgrenset område. Det er fokus på dette fra sentralt hold i Universitetet, og ressurser fra IT-avdelingen har både holdt kurs/foredrag om emnet på IT-forum, samt vært i møter med sentrale personer fra enkelte av instituttene som anses å ha nytte av SAFE. Dette er gjort for å øke bevisstgjøring rundt problemstillingene. PwC har ikke observert en klar ensartet praksis ved UiB for hvordan de enkelte instituttene skal håndere personopplysninger.		Universitete i Bergen sitt styringssystem for informasjonssikkerhet styrkes, som kontinuerlig forvalter risikobildet, påser at rutiner for informasjonssikkerhet er oppdatert, og påser at sikkerhetsnivået møter et tilstrekkelig nivå av kvalitet. Dersom Universitetet i Bergen ikke har et slikt styringssystem i praksis, anbefales det at UiB på sentralt hold etablerer dette. For mer informasjon, se DIFI sine retningslinjer for styringssystem for informasjonsikkerhet: https://www.difi.no/artikkel/2014/05/veiledning-styringssystem-informasjonssikkerhet

B	**Prosess for innsyn**	Instituttene melder om at det er svært sjeldent at en respondent ønsker innsyn i sine opplysninger. Det foreligger derfor ingen rutiner for dette, men det er prosjektleders ansvar å sikre at dette blir gjort hvis påkrevd.	Det foreligger ingen konkrete rutiner eller sjekklister for å sikre at en person får innsyn i alle data om vedkommende. Data kan være lagret på flere forskjellige steder, både fysisk og elektronisk og det er en risiko at instituttene ikke er i stand til å gi en komplett oversikt. Forskningsdeltakeren har også rett til å få innsyn i sikkerhetstiltak ved behandlingen av opplysningene. PwC observerer ar forskerne ikke er kjent med at det foreligger en oversikt over sikkerhetstiltak og de vurderingene som skal ligge til grunn for at dette skal utleveres jfr. §40 i helseforskningsloven.	Det bør etableres rutiner for håndtering av krav om innsyn. Dette bør inkludere et dokument som beskriver de sikkerhetstiltakene som er på plass for håndtering av personopplysninger slik at dette kan kommuniseres til forskningsdeltaker på en lettfattelig måte. Prosjektledere bør ha en oversikt over personopplysninger som er lagret, slik at de enkelt kan slettes eller opplyses om.
C	**Prosess for tilgangs-styring og deling**	Prosjektleder gir forskere og forskningsassistenter tilgang til data og filområder basert på den enkeltes behov for data. Prosjektleder sender da en henvendelse til IT-avdelingen som deretter gir tilganger til de enkelte filområdene. Dette gjelder også ved IGH der prosjektleder sender en henvendelse til administrasjonen ved instituttet som deretter kontakter IT-avdelingen for å gi tilgang til sikker server. Endringsmelding til NSD eller REK blir ikke sjekket før tilganger blir gitt. Instituttene melder om at de i svært liten grad sender fra seg data, men i de tilfellene at dette skjer må det først søkes om godkjenning hos REK/NSD. Instituttene gjennomfører ingen kontroll med at mottaker er den de utgir seg for å være, dersom dette gjelder en forsker som er ansatt ved et tilsvarenede institutt eller forskningsinstitusjon.	Vi kan ikke se at det er formaliserte rutiner knyttet til tilgangsstyring, men det fremstår som at forskerne har utviklet egne rutiner spesielt i forhold til utdeling av tilgang. Vi kan imidlertid ikke se at det er fullt så innarbeidede rutiner knyttet til fjerning av tilganger, herunder ved avslutning av arbeidsforhold. Ettersom IT-tilganger blir gitt uten at det sjekkes at endringsmelding til NSD eller REK er sendt, er det en risiko for at innsyn til personopplysninger blir gitt uten at det er gitt forhåndsgodkjenning.	Det bør innføres en rutine for at prosjektleder kontrollerer at endringsmelding er sendt før det bes om ny systemtilgang eller informasjon blir delt. Instituttene melder om at det ved deling av informasjon bør det være en større grad av dialog og bekreftelse/kontroll på institusjonsnivå.
D	**Prosess for sletting**	**Sletting** Det er i dag ingen formaliserte rutiner knyttet til å identifisere de data som skal slettes ved utløp av godkjent lagringstid. Dersom det er ønskelig med forlengelse av lagringstiden skal dette søkes om, men det foreligger ikke noe system eller rutine som	Risiko for brudd: Det ble ikke avdekket faktiske brudd, men manglende rutiner knyttet til sletting etter utløp av godkjenningsperiode åpner for stor risiko for brudd på personopplysningsloven § 28 og helseforskningsloven § 38.	Det bør opprettes formaliserte rutiner og instrukser for sletting av personopplysninger. Instituttene bør ha en oversikt over lagrede

		sikrer at dette blir gjort. Forskerne mottar melding fra register når tid for avtalt lagring utløper. Likevel er det lite oppfølging med at dette faktisk blir gjort, spesielt i de tilfeller der forsker/prosjektleder har sluttet. I enkelte tilfeller vil det også være motstridende krav mellom godkjent lagringstid fra REK og pålagt lagringstid fra publiserende tidsskrift. Forskningsdeltaker kan kreve å få opplysningene om seg selv slettet. Forskerne oppfatter det som uklart hvorvidt det er tilstrekkelig å anonymisere dataene, eller om samtlige data må slettes. Dette kan blant annet være en utfordring hvor allerede innsamlet data inngår i en pågående analyse. Dersom forskerne velger å anonymisere dataene blir dette vanligvis gjort ved å slette personens oppføring i identifikatornøkkelen og eventuell annen informasjon som kan brukes til indirekte identifisering av forskningsdeltakeren.	Etter helseforskningsloven § 16 er utgangspunktet at ved tilbaketrekning av samtykke skal helseopplysningene slettes eller utleveres innen 30 dager. Det oppstilles et unntak fra hovedregelen om sletting/utlevering dersom opplysningene enten anonymiseres, inngår i et annet biologisk produkt eller dersom opplysningene inngår i allerede utførte analyser. Videre kan REK i spesielle tilfeller gi en videre tillaltelse til utsettelse av sletting, destruering eller utlevering mens forskningsprosjektet pågår.	personopplysninger, herunder hvor lenge det er godkjent lagring for disse, slik at de kan følges tettere opp og slettes når godkjent lagringstid utløper. Det bør også være en rutine som beskriver hvem som overtar ansvar for personopplysningene dersom prosjektleder skulle slutte.
E	**Prosess for anonym-isering av person-opplysninger**	Manglende entydige instrukser eller rutiner Forskerne opplever det som utfordrende å avgjøre når data er blitt tilstrekkelig anonymisert til å ikke lengre å være regnet som personopplysninger. Vurderingen hvorvidt er datasett kan knyttes til en enkelt person, og dermed være definert som indirekte identifiserbart, vurderes i hver enkelt situasjon. Data som mottas fra eksterne register vil i de fleste tilfellene være anonymisert.	Det er essensielt at forskeren og/eller forskningsleder har den nødvendige kunnskap til å skille mellom indirekte personopplysninger og anonyme opplysninger, da dette skillet er avgjørende for om opplysningene faller innenfor lovreguleringen i personopplysningsloven, helseregisterloven og helseforskningsloven. Dersom man feilaktig antar at opplysningene er tilstrekkelig anonymisert, og dermed ikke følger kravene og rutinene knyttet til behandling av personopplysninger, vil dette medføre klare brudd på personvernlovgivningen og resultere i nye bøter fra datatilsynet.	Det bør utarbeides tydelige retningslinjer for når data er tilstrekkelig anonymisert til ikke lengre å være regnet som personopplysninger. I de tilfellene der det fortsatt eksisterer en identifikator bør denne oppbevares i henhold til rutine for lagring av personopplysninger, se punkt A.

Vedlegg 1 – Symboler

Evaluering av internkontroll

Grad	Forklaring
	Tilfredsstillende. Internkontrollen møter generelt akseptable standarder.
	Tilfredsstillende – Internkontrollen møter generelt akseptable standarder, men det er identifisert noen forbedringsområder.
	Behov for forbedringer - Internkontrollen møter generelt akseptable standarder, men bør forbedres.
	Behov for forbedringer– Internkontrollen møter under tvil akseptable standarder og det er identifisert flere forbedringsområder.
	Ikke tilfredsstillende – Internkontrollen møter generelt ikke minimum akseptable standarder. Kritiske kontroller er ikke på plass og tap kan oppstå uten å bli oppdaget.

Risikovurdering

Risiko	Forklaring
Høy	Risikoen er klassifisert som lav, medium eller høy, og reflekterer områdets risiko for at UiB ikke skal nå sine mål
Medium	
Lav	

Utvikling

Utvikling	Forklaring
↗	Positiv trend siden forrige gjennomgang
→	Uendret trend siden forrige gjennomgang
↘	Negativ trend siden forrige gjennomgang

Prioritet

Prioritet	Forklaring
❶ Høy prioritet	Anbefalinger som bør gjennomføres umiddelbart. Anbefalingen har kritisk betydning for risikoen i revidert enhet.
❷ Medium prioritet	Anbefalinger som bør gjennomføres så snart som mulig. Anbefalingen har moderat betydning for risikoen i revidert enhet.
❸ Lav prioritet	Anbefalinger som bør gjennomføres, men det er ikke tidskritisk. Anbefalingen har i mindre grad betydning for risikoen i revidert enhet.

Revisjonsprosjekt

Delprosjekt Nr 2015/04:
Gjennomgang Paga WEB

Utkast rapport: 30.09.2015

Endelig rapport: 26.10.2015

Til:
Universitetsdirektøren
ved UiB

Kopi til:

Fra: Jan Roger Hånes,
PricewaterhouseCoopers AS

Sign:

pwc

Innholdsfortegnelse

1 Introduksjon

Bakgrunn

PricewaterhouseCoopers (PwC) har gjennomført en internrevisjon vedrørende Paga web. Gjennomgangen er basert på årsplan for internrevisjonen og planleggingsmemo godkjent av UiB.

Formål og omfang

Formål og omfang er definert i årsplan vedtatt av styret for 2014-2015.

Formålet med revisjonen har vært å;

- kartlegge og vurdere om det er etablert gode rutiner knyttet til registrering av faste og variable lønnsdata i Paga Web som bidrar til å sikre korrekt registrering av lønn og relaterte kostnader
- teste at rutinene etterleves i praksis

Vi vil i tillegg gjennomgå brukertilganger i løsningen for å vurdere;

- om brukertilgangene (rollene) bidrar til å sikre en god arbeidsdeling
- samt at det kun er brukere som har behov for å ha tilgang til Paga Web, som har tilgang til løsningen

Enheter som har deltatt i revisjonen

Revisjonen har dekket følgende fakulteter / institutter;

- Sentraladministrasjonen, POA (regelverk og rutiner)
- Det humanistiske fakultet
  - Institutt for første semester studier
  - Institutt for litteratur, lingvistiske og estetiske fag
  - Institutt for fremmedspråk
- Det matematisk-naturvitenskapelige fakultet,
  - Institutt for biologi
  - Institutt for fysikk og teknologi
- Det psykologiske fakultet

Avgrensning

Revisjonsprosjektet avgrenses til nevnte fakulteter og institutter. Vår revisjon har dekket gjennomgang og evaluering av UiBs rutiner knyttet til registrering av faste og variable lønnsdata i Paga Web samt testing av etterlevelse av disse for nevnte fakulteter og institutter.

Revisjonsperiode og revisjonsteam

Internrevisjonsprosjektet ble gjennomført i juni – oktober 2015.

Revisjonsteamet fra PwC har bestått av Jan Roger Hånes, Olav Høsøien og Tor Erik Tveit.

Gjennomført arbeid

Observasjoner med tilhørende anbefalinger er beskrevet i kapittel 3-8. Vår revisjon og vår rapport er basert på arbeidsmøter med representanter for de ulike enhetene samt gjennomgang av mottatt dokumentasjon. Tabellen nedenfor viser en oversikt over ansatte som har vært involvert i internrevisjonsprosjektet.

Avdeling	Navn
HR-avdelingen	Henrik Tøndel
Økonomiavdelingen	Kate Fauskanger Tone Skaugvold Berit Grimstad Berit Solsvik
Det humanistiske fakultet	Susanne Ostendorf Annhild Fetveit Arve Sennesvik
• Institutt for lingvistiske, litterære og estetiske studier	Siri Fredrikson Liv Mørch
• Institutt for filosofi og førsemesterstudier	Steinar Thunestveit Evy Halvorsen
• Institutt for fremmedspråk	Arve Kjell Uthaug Victoria Jensen Vigdis Westgård
Det matematisk-naturvitenskaplige fakultet	Astrid Breivik Elin K. Frigaard Eva Linde Rigmor Geithus Tine C. Overå
• Institutt for teknologi og fysikk	Grete Ersland Hanne Lilleskare Hammer
• Institutt for biologi	Anders Goksøyr Synnøve Myhre Linda Vagtskjold Solfrid Sture
Det psykologiske fakultet	Ove Borge Trine Knudsen Vala J. Hjort-Jenssen Inni M. Offerdal Hernadez

Rapport og rapportstruktur

Vi har i vår gjennomgang hatt fokus på å identifisere forbedringsområder, som vi mener vil kunne gi nyttige anbefalinger og innspill i den videre prosessen med å forbedre og videreutvikle UiBs intern kontroll på dette området. UiB må selv vurdere de foreslåtte anbefalingene med hensyn til kost/nytte-effekt.

Vår rapport er delt inn som følger

- oppsummering av hovedobservasjoner og konklusjon på totalnivå
- detaljrapport som viser detaljerte observasjoner og anbefalinger som gjelder alle enhetene

Vedlegg

Vedlegg 1 – Symboler
Vedlegg 2 - Tilgangsrettigheter – brukere som skulle vært slettet
Vedlegg 3 - Uoppgjorte reiseforskudd pr. 28.05.2015
Vedlegg 4 – Paga – brukere med administrasjonsrettigheter

2 Oppsummering

Risikovurdering: Middels	**Vurdering av internkontroll:**		**Trend:** ↗

Oppsummering:

HOVEDINNTRYKK
Det vårt hovedinntrykk at UiB har fått på plass nødvendige rutiner og retningslinjer for lønnsrealterte oppgaver som utføres lokalt på fakultets-/institutt-nivå, og at disse i hovedsak etterleves. Det er imidlertid fortsatt en del forbedringsområder.

Nedenfor følger en oppsummering av våre observasjoner med forslag til forbedringer fra vår revisjon. For mer detaljer henviser vi til kapittel 3 Observasjoner.

STERKE SIDER

- Det er utarbeidet formelle rutiner og retningslinjer for lønnsområdet; herunder rutiner for
  - Fastlønns-attestanter
  - Variabel-lønnsattestanter
  - Ledere
  - Rettledning for utfylling av reiseregninger

  Rutinene samt oppsett av arbeidsflyt i Paga Web bidrar til å sikre en god intern kontroll blant annet ved hjelp av god arbeidsdeling. Rutinene er videre lett tilgjengelige via UiBs intranett.

- Det er etablert opplegg for opplæring av lønnsmedarbeidere / ledere, herunder diverse kurs, fora i regi av UiB sentralt og underleverandører som f.eks. Infotjenester, herunder; HR Gruppen, HR forum, Variabel lønn forum. Dette er positivt og bidrar til å holde ansatte og ledere oppdatert på lover og regler på lønnsområdet.

- Det er etablert god kommunikasjon mellom lønnskontor og fakultet / institutt både via Issue tracker og muntlige forespørsler.

Dette er positivt og har bidratt til å forbedre UiBs intern kontroll på dette området.

Risikovurdering: Middels	Vurdering av internkontroll:		Trend: ↗

Oppsummering:

FORBEDRINGSOMRÅDER

Vår revisjon har også avdekket en del forbedringsområder;

Generelle observasjoner

- *Kontroll av reiseregninger*
  Reiseregning kontrolleres og anvises lokalt på institutt. I tillegg foretar lønnskontor rimelighetskontroll av beløp og TT-koder. UiB bør vurdere om dobbeltkontroll er nødvendig.

- *Registrering og kontroll av reiseforskudd*
  - Reiseforskudd registreres i Paga klient, men kan ikke trekkes automatisk fra på reiseregning
  - UiBs rutiner for kontroll og oppfølgning av reiseforskudd er mangelfulle. Det er en rekke reiseforskudd av eldre dato som ikke er oppgjort.

- *Bestilling og kostnadsføring av flybillett*
  I noen tilfeller sendes faktura for flybillett direkte til UiB. Denne kan medføre en risiko for dobbelbelastning ved at flybillett både kostnadsføres via reiseregning og via faktura fra reisebyrå.

- *Tjenestereiser*
  Det synes å være behov for å klargjøre begrepet tjenestereise / ikke tjenestereise, da utbetaling av visse tillegg som f.eks. kompensasjonstillegg kun utbetales dersom det er tjenestereise.

- *Registrering av oppsigelse fra ansatte*
  Rutine for registrering av oppsigelse er tungvint ved at institutt først må utarbeide sluttskjema som igjen må registreres i Paga av fastlønnsattestant ved fakultet.

Funksjonalitet i Paga

- *Vedlikehold faste lønnsopplysninger*
  Registrering av faste lønnsopplysninger synes tungvint som følge av manglende integrasjon mellom Paga og Ephorte og at data dermed kontrolleres to ganger.

- *Manglende svarfunksjon ved søknad om velferdspermisjon*
  Svar på søknad om f.eks. velferdspermisjon kan ikke sendes direkte fra Paga. Dette registreres i Ephorte, og svar må sendes som brev eller mail.

Risikovurdering: Middels	Vurdering av internkontroll:		Trend: ↗

Oppsummering:

- *Obligatoriske felt – må-felt*
  En del felt som er viktig i forbindelse med rapportering er ikke obligatoriske i Paga. Dette kan at viktig informasjon ikke registreres, noe som kan medføre ekstraarbeid blant annet i forbindelse med rapportering.

- *Rapporteringsfunksjon – Paga / Discoverer*
  Manglende og ufullstendige rapporter fra Paga / Dicoverer medfører en del ekstraarbeid ved at data må sammenstilles manuelt i f.eks. Excel.

Tilganger Paga WeB

- *Sletting av brukere*
  Vår revisjon av tilganger til Paga Web avdekket flere brukere som var sluttet / skiftet stilling ved UiB og som ikke var slettet i Paga.

- *Brukere med Admin-rettigheter i Paga*
  Veldig mange brukere har administrasjonsrettigheter i Paga. Dette gjelder både UiBs egne brukere samt brukere fra systemleverandør Bluegarden. UiB bør foreta en gjennomgang for å vurdere dette i forhold til reelt behov for denne type tilganger.

- *Manglende periodisk kontroll av tilganger*
  UiB har ikke etablert rutine for periodisk kontroll av tilganger i Paga.

- *Pålogging Paga Web*
  Slik vi forstår det, kan en bruker foreta ekstern pålogging til Paga Web via Feide fra hvilken som helst PC, f.eks. fra internett kafe, hjemme-PC, nettbrett osv.. UiB bør sjekke hvor mange påloggingsforsøk bruker har før vedkommende blir stengt ute.

TESTING

Vi har til sammen testet 66 reiseregninger fordelt på nedenforstående fakulteter/institutter. Vår hovedinntrykk er at rutiner knyttet til kontroll av reiseregninger stort sett fungerer bra, men det er noen unntak.

- *Testing HF*
  - To tilfeller der flybilletter ikke var vedlagt reiseregning.
  - Et tilfelle der flybillett var lagt ved reiseregning, men det var ikke krevd refusjon for denne.
  - 1 tilfelle der var gjort krav om diett der deler av reisen var av privat karakter.

Risikovurdering: Middels	**Vurdering av internkontroll:**		**Trend:** ↗

Oppsummering:

- 2 reiseregninger der taxiregning ikke var vedlagt.

- *Testing alle enheter*
  - Flere tilfeller der omregning fra utenlandsk valuta til NOK ikke var dokumentert.

- *Testing Psykologisk fakultet*
  - 1 tilfelle der taxiregning ikke var vedlagt reiseregning.
  - 1 tilfelle der utlegg ikke var dokumentert med originalbilag.

3 Generelle Observasjoner

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
3-1	❷ Medium prioritet	• *Reise-regninger*	**Kontroll av reiseregninger** Det er etablert gode rutiner for kontroll av reiseregninger. Den ansatte registrerer selv reiseregning i Paga Web eller fyller ut reiseregning på papir dersom vedkommende ikke har tilgang til Paga Web. Det gjelder i hovedsak eksterne. Variabel lønnsassistent kontrollerer reiseregning, herunder at; • alle utlegg er dokumentert • reiseregning er i henhold til UiBs retningslinjer samt gjeldende lover og regler. Reisebilag, hotellregninger osv. lagres lokalt. Dersom ok, sendes reiseregning på arbeidsflyt til leder som anviser den i Paga. Vi forstår det slik at den ansatte kan selv velge hvem reiseregning skal sendes til for kontroll. Dette kan medføre at reiseregning blir sendt til feil leder, noe som kan medføre ekstra arbeid samt at reiseregning ikke blir behandlet tidsriktig. Dersom ok, henter lønnskontor opp og overfører reiseregning til Paga klient. Lønnskontor foretar rimelighetskontroll av beløp og TT-koder.	**Kontroll av reiseregninger** Det bør vurderes om det er nødvendig at lønnskontor foretar rimelighetskontroll av beløp og TT-koder da reiseregning allerede er kontrollert og anvist ved fakultet / institutt. Videre bør det vurderes om det er nødvendig at den ansatte selv skal kunne velge hvem reiseregning skal sendes til for kontroll.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
3-2	❶ Høy prioritet	• *Registrering og oppfølgning av reiseforskudd*	**Registrering av reiseforskudd** Reiseforskudd registreres og utbetales i Paga klienten, og bokføres på egen konto i Oracle Financials. Det er ikke mulig å trekke reiseforskudd automatisk fra ved innlevering / registrering av reiseoppgjør. Dette kan medføre risiko for at reiseforskudd ikke blir gjort opp ved innlevering av reiseregning, se neste punkt. **Oppfølgning av reiseforskudd** Uoppgjorte reiseforskudd utgjorde pr. 28.05.205 kr. 5.956.009,- for UiB totalt, hvorav uoppgjorte reiseforskudd for fakultetene/ instituttene som inngikk i revisjonen utgjorde kr. 1.561.238,-, se vedlegg 3. Av disse var det en rekke uoppgjorte reiseforskudd av eldre dato, se vedlegg 3 UiB totalt, • 2013 og eldre kr. 986.871,-. • 2014-2015 kr. 829.343-. • 2015 kr 4.139.795,- Av dette utgjorde fakulteter /institutter som inngikk i revisjonen, eldre enn; • 2013 og eldre kr. 201.598,- • 2014-2015 kr. 325.813,- • 2015 kr. 1.037.856,-	**Registrering av reiseforskudd** UiB bør vurdere å ta opp med system-leverandør (Blue-garden) om det er mulig å trekke fra forskuddet på neste reiseregning i tillegg til at det vil være lettere å følge opp utestående reiseforskudd. **Oppfølgning av reiseforskudd** Vi anbefaler at det etableres faste rutiner for oppfølging av reiseforskudd, minimum månedlig oppfølgning. Dette innebærer at lønnskontoret må sende lister til fakultet/institutt (som i dag), eventuelt at det legges opp til at fakultet/ institutt selv kan skrive ut nødvendige lister. Det er videre viktig at variabellønnsattestant fakultet / institutt følger opp listene, og sørger uoppgjorte reiseforskudd blir oppgjort fortløpende. Dette vil bidra til at reiseforskudd blir fulgt opp og gjort opp tidsriktig samt redusere risikoen for at reiseforskudd ikke blir oppgjort.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
			Det er ifølge sentralt lønnskontor etablert fast rutine for utsendelse av lister over uoppgjorte reiseforskudd til fakultetene/instituttene, men listene følges ikke alltid opp fortløpende av disse. Dette kan i verste fall medføre at reiseforskudd ikke blir gjort opp som en del av reiseoppgjøret eller at det i verste fall ikke blir oppgjort i det hele tatt. Vår revisjon avdekket en del tilfeller; • et tilfelle på MatNat, Institutt for Fysikk og teknologi med dobbel utbetaling av reiseforskudd • der reiseforskudd ikke var oppgjort som følge av at den ansatte hadde sluttet. Øystein Djuvsland, kr 12.000. Dette er tapsført • Ansattes avdeling ikke var registrert på listen (25 forskudd), Se vedlegg 4.	
3-3	❸ Lav prioritet	• *Flybilletter*	**Bestilling og kostnadsføring av flybillett** I noen tilfeller blir flybillett bestilt og fakturert direkte til UiB. Flybillettfaktura fra reisebyrå blir da registrert og godkjent i Basware. Det er ingen link mellom Basware og reiseregning i Paga Web. Dette kan medføre en risiko for at flybillett	Flybillett bør alltid kostnadsføres som den del av reiseregningen. Dersom den ikke blir det, bør det være link fra faktura til reiseregning og omvendt.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
			belastes dobbelt dersom flybillett også kostnadsføres som en del av reiseregning. Faktura fra reisebyrået er stilet til den ansatte, UiB, Fakturamottak.	
3-4	❸ Lav prioritet	• *Tjeneste-reiser / ikke tjeneste-reiser*	**Tjenestereiser** Det synes å være behov for å klargjøre begrepet tjenestereise / ikke tjenestereise, da utbetaling av visse tillegg som f.eks. kompensasjonstillegg kun utbetales dersom det er tjenestereise. Uklarheter rundt dette kan medføre at tillegg blir urettmessig utbetalt. Det synes også å være noe ulikt hvordan dette praktiseres ved de ulike fakultetene / instituttene.	**Tjenestereiser** UiB bør klargjøre begrepet tjenestereise / ikke tjenestereise, slik at eventuelle misforståelser / feil unngås.
3-5	❷ Medium prioritet	• *Registrering av oppsig-else av arbeids-forhold i Paga*	**Registrering av oppsigelse** Ved oppsigelser registrerer fastlønns-attestant ved fakultet opplysninger i Paga basert på sluttskjema fra institutt. Dette innebærer slik vi forstår det at sluttskjema først fylles ut ved institutt og sendes til fastlønnsattestant ved fakultet for registrering i Paga. Dette synes tungvint da data registreres to ganger noe som er lite effektivt og som i tillegg kan medføre en økt risiko for feil.	**Registrering av oppsigelse** Vi anbefaler at registrering av slutt- skjema i Paga utføres av instituttet, f.eks. av personalleder/administrasjonssjef, og at skjema registreres direkte i Paga Web. Dette vil etter vår mening bidra til å gjøre prosessen mer effektiv (hindre dobbeltarbeid) samt redusere risikoen for feil. Dette innebærer videre at brukerne som skal uføre disse oppgavene ved instituttene må få nødvendige tilganger i Paga for å kunne utføre dette.

4 Funksjonalitet i Paga

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
4-1	❷ Medium prioritet	• *Kontroll / grensesnitt Paga / Ephorte*	**Vedlikehold faste lønnsopplysninger** Ved nyansettelser registreres og lagres arbeidskontrakt i Ephorte. Faste lønns-opplysninger registreres manuelt i Paga av fastlønnsattestant fakultet på grunnlag at arbeidskontrakt i Ephorte. Det er ikke grensesnitt mellom Ephorte og Paga. Etter registrering i Paga sendes skjemaet ''Administrasjon av arbeidsforhold'' til lønns-kontor som kontrollerer registrering i Paga mot arbeidskontrakt i Ephorte, herunder; • startdato, stillingskode, stillingsprosent, ansenitet, stopp dato dersom midlertid • samt kontering Dette synes noe tungvint og medfører at data kontrolleres to ganger.	**Vedlikehold faste lønnsopplysninger** UiB bør vurdere om det er nødvendig å utføre dobbeltkontroll av faste lønns- opplysninger. I tillegg bør det vurderes om det er mulig å etablere grensesnitt mellom Ephorte og Paga.
4-2	❷ Medium prioritet	• *Velferds-permisjon*	**Manglende svarfunksjon ved søknad om velferdspermisjon** Søknad om velferdspermisjon, ferie legges inn i Paga av den ansatte. Svar på søknad kan ikke sendes direkte fra Paga, men må registreres i Ephorte og sendes i brev /mail til den ansatte.	**Manglende svarfunksjon ved søknad om velferdspermisjon** UiB bør ta opp med systemleverandør om det er mulig å få på plass nødvendig funksjonalitet, slik at svar kan sendes automatisk direkte fra Paga.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
			Dette er både tungvint og kan medføre en risiko for at svar på søknad ikke blir sendt til den ansatte når søknad er ferdigbehandlet.	
4-3	❷ Medium prioritet	• *Obligatoriske felt i Paga*	**Obligatoriske felt – må-felt** Ved registrering i Paga er det en del felt som er merket med stjerne, dvs. disse må fylles ut for å komme videre. En del felter som burde vært obligatoriske, er ikke merket med stjerne slik vi forstår det. Eksempler på dette er: • Yrkeskode • Utdanningskode Dette kan medføre at viktig informasjon ikke blir registrert, noe som kan medføre unødvendig merarbeid og tap av tid.	**Obligatoriske felt – må-felt** Vi vil anbefale at UiB gjennomgår relevante felter i Paga og utarbeide en oversikt over felter som bør være obligatorisk, og at dette tas opp med systemleverandør slik at viktige felter kan gjøres obligatorisk. Dette vil kunne bedre datakvaliteten samt redusere omfanget av ekstraarbeid som følge av at viktig informasjon ikke blir registrert.
4-4	❷ Medium prioritet	• *Rapporter – Paga / Discoverer*	**Rapporteringsfunksjon – Paga / Discoverer** Paga inneholder en rekke standard-rapporter som benyttes. I tillegg benyttes rapportgeneratoren Discoverer. Det er systemgruppen som utvikler/ vedlikeholder rapporter i Discoverer. Tilbakemeldingen fra noen av enhetene er at; • det mangler en del rapporter • noen rapport er ufullstendige, dvs. inneholder ikke alle felter	**Rapporterings-funksjon – Paga / Discoverer** UiB bør gjennomgå og utarbeide en oversikt over rapporter som mangler / er ufullstendige og iverksette nødvendige tiltak slik at disse blir utarbeidet. Dette vil kunne forenkle en del arbeidsprosesser ved å f.eks. unngå unødvendig manuell innleggelse av data.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
			som trenges. • begrensning på antall linjer i rapport på maks 500 linjer medfører at data må overføres til f.eks. Excel og så settes sammen til 1 rapport. Dette er både tungvint og medføre en økt risiko for feil Eksempler på dette er: • personer med to stillinger, kommer kun frem 1 gang på rapport. • Statistikker: f.eks. turnover statistikk, mangler STYRK-kode som ligger i Paga klient, ikke Paga Web. • Statistikker som benyttes ved lønnsfastsettelse; får ikke fram lønnstrinn pr. ansatt. Må legges inn manuelt i Excel • Statistikker: f.eks. antall reiseregninger, timelønnede (antall skjema). Må telle manuelt. Manglende rapportfunksjonalitet kan medføre ekstraarbeid ved at data må legges inn manuelt f.eks. i Excel, noe som kan gå ut over andre viktige oppgaver. I følge systemgruppen finnes allerede noen av de nevnte rapportene som etterlyses; herunder:	Det er viktig at Økonomiavdelingen informerer om hvilke rapporter som er tilgjengelige samt tar dette med i opplæringen.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
			• STYRK-koder en nå få ut i rapporter • Statistikker vedr. lønnsfastsettelse kan tas ut i Discoverer Dette kan indikere at det er behov for mer informasjon om hvilke rapporter som finnes samt at dette tas opp i relevante fora.	

5 Tilganger Paga

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
5-1	❶ Høy prioritet	• *Sletting av brukere*	**Sletting av brukere** Vår gjennomgang av brukere i Paga Web for de enhetene som inngikk i revisjonen, avdekket flere brukere som skulle vært slettet / endret, (se vedlegg 2); • En bruker, variabel-lønnassistent ved Institutt for fysikk og teknologi som gikk over i ny stilling ved MI fra 22.6.2015 er fortsatt registrert som bruker i Paga. • En bruker, variabellønnassistent ved Institutt for fysikk og teknologi som sluttet 01.06.15 • En bruker ved Institutt for biologi har rollen Personal_lesetilgang. Hun jobber ikke lenger ved instituttet og burde således vært slettet som bruker. • En bruker ved Institutt for biologi har rollen Varlønn. Bruker må slettes, da hun jobber ikke lenger med økonomi. Manglende sletting av brukere kan medføre en risiko for feil og misligheter.	Ovenstående brukere anbefales slettet snarest. Vi anbefaler videre at; • det etableres rutiner som sikrer systemadministrator får beskjed når brukere slutter eller endrer stilling, slik at tilganger i Paga Web kan oppdateres tidsriktig. • det etableres rutine for periodisk kontroll av brukertilganger, se nedenfor. Dette vil bidra til at brukere som har sluttet / skiftet stilling blir slettet tidsriktig.
5-2	❶ Høy prioritet	• *Brukere med Admin-rettigheter*	**Brukere med Admin-rettigheter i Paga** Vår gjennomgang av tilganger i Paga avdekket at hele 58 brukere med Administrasjons-rettigheter, se vedlegg 4. De fleste av disse er fra Bluegarden, som er	Antall brukere med admin-rettigheter bør reduseres, slik at det kun er de som har behov for denne type rettigheter for å kunne utføre sin jobb, som har denne type tilganger. UiB bør derfor gjennomgå UiBs egne brukere som har Admin-rettigheter, for å

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
			systemleverandør for Paga. Dette medfører en risiko for feil – både bevisste og ubevisste - samt risiko at sensitiv informasjon om lønns- og ansettelses-data kan komme uvedkommende i hende.	verifisere at disse virkelig har behov for disse. I tillegg vil vi anbefale at UiB ber Bluegarden om å foreta en tilsvarende gjennom-gang sine brukere. Dette bør utføres halvårlig og ved større endringer. Dette vil etter vår mening redusere risikoen for feil.
5-3	❷ Medium prioritet	• *Periodisk kontroll av tilganger*	**Manglende periodisk kontroll av tilganger** Det er ikke etablert rutiner for periodisk gjennomgang av brukertilganger i Paga Web. Formålet med en slik gjennomgang vil være å få verifisert at; • det kun er autoriserte brukere som har tilgang til Paga Web • tilganger er fornuftig i forhold til vedkommendes stilling og funksjon. Manglende periodisk gjennomgang av brukertilganger kan medføre at brukere som er sluttet / flyttet til en annen avdeling ikke blir slettet, noe som vår gjennomgang av tilganger avdekket flere tilfeller av, se pkt 5.1. Dette kan medføre en risiko for feil – både bevisste og ubevisste samt at sensitiv informasjon om lønns- og ansettelsesforhold kommer uvedkommende i hende.	**Manglende periodisk kontroll av tilganger** Vi anbefaler UiB etablerer rutine for periodisk gjennomgang av brukere. Denne bør koordineres med periodisk gjennomgang av tilganger til andre løsninger. Videre vil vi anbefale UiB om å be Bluegarden om å gjennomføre periodisk gjennomgang av brukere som har tilgang til Paga, med spesiell fokus på brukere med admin-tilganger. Dette vil redusere risikoen for feil – både bevisste og ubevisste samt sørge for at UiB ikke betaler lisensavgifter for UiB-brukere som ikke trenger tilgang til løsningen. En slik gjennomgang bør foretas halvårlig og ved større endringer.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
5-4	❷ Medium prioritet	• *Pålogging Paga Web*	**Pålogging Paga Web** Slik vi forstår det, kan en bruker foreta ekstern pålogging til Paga Web via Feide fra hvilken som helst PC, f.eks. fra internett kafe, hjemme-PC, nettbrett osv.. Det er ikke etablert to-faktor autentisering ved pålogging. Det synes ikke å være klart hvor mange påloggingsforsøk bruker har før vedkommende blir stengt ute. Dersom det ikke er satt begrensning på antall påloggingsforsøk, kan dette medføre en sikkerhetsrisiko.	**Pålogging Paga Web** UiB bør sjekke hvor mange påloggings-forsøk bruker har før vedkommende blir stengt ute. Bruker bør ha maks 5 forsøk før vedkommende blir stengt ute. Dette vil redusere risiko for uautorisert tilgang til Paga Web.

Test av reiseregninger

Vi har som en del av revisjonen foretatt testing på stikkprøvebasis av reiseregninger. Testingen er basert på lister fra Paga. Nedenfor følger en oppsummering av testresultatene pr. fakultet/institutt.

Vi har i vår revisjon testet til sammen 66 reiseregninger fordelt på;

- 24 reiseregninger fordelt på Det humanistiske fakultet, Institutt for filosofi og førstesemesterstudier, Institutt for fremmed-språk og Institutt for litteratur, lingvistiske og estetiske fag
- 28 reiseregninger fordelt på Det matematisk-naturvitenskaplige fakultet, Institutt for fysikk og teknologi og institutt for biologi
- 14 reiseregninger for Det psykologiske fakultet

6 Testing – Det humanistiske fakultet

Vi har testet 24 reiseregninger.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
6-1	❷ Medium prioritet	• *Flybilletter - Institutt for filosofi og førstesemester studiet*	**Flybilletter ikke vedlagt reiseregning** For 2 reiser var flybillett ikke vedlagt reiseregningen. Det var heller ikke krevd fradrag for flybillettene. Dette gjelder følgende reiseregninger; • Reise 167141, reise til Oslo. • Reise 167140, reise til Mainz Tyskland Dette er reiser til lokasjoner der en normalt forventer å finne flybilletter eller annen transportdokumentasjon. Det fremgår ikke om flybillett er betalt av andre eller om flybillett er fakturert UiB direkte.	**Flybilletter ikke vedlagt reiseregning** Dersom flybillett er fakturert direkte til UiB, må det være referanse på reiseregning til faktura og omvendt. Flybillett må alltid legges ved reise-regning dersom flybillett kreves refundert.
6-2	❷ Medium prioritet	• *Flybilletter - Institutt for filosofi og førstesemester studiet*	**Flybillett ikke krev refundert** På reiseregning 132141 er flybillett vedlagt reiseregning som bilag, men ikke krevd refusjon for denne på reiseregningen.	**Flybillett ikke krev refundert** UiB bør sjekke om kostnad flybillett skulle vært refundert.
6-3	❷ Medium prioritet	• *Krav om diett – Institutt for fremmed-språk*	**Krav om diett** For reiseregning 167160 som gjelder reise til konferanse i Paris perioden 6.07-13.7 er det krevd diett for alle døgn på reisen i diett inklusiv 2 døgn (lørdag 11. og søndag	Dersom det er utbetalt diett for deler av reisen som må antas å være av privat karakter, bør denne tilbakebetales av den ansatte.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
			12. juli) som var av privat karakter. Dette er oppgitt på reiseregningen. Det er trukket ut måltider, hvorvidt dette gjelder den private delen av reisen er vi usikker på.	
6-4	❶ Høy prioritet	• *Manglende dokumenta-sjon – Det humanist-iske fakultet / Institutt for litteratur, lingvistiske og estetiske fag*	**Reiseregninger – manglende dokumentasjon** To reiseregninger, reise 167987 og reise 132141 manglet kvittering på krav om refusjon for taxikostnader for beløpene kr 318,- og kr 674,-.	Kostnader som ikke kan dokumenteres skal ikke refunderes.

7 Testing – Det matematisk-naturvitenskaplige fakultet

Vi har testet 28 reiseregninger. Det var ingen vesentlige avvik

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
7-1	❸ Lav prioritet	• *Valutakurs-omregning*	**Valutakursomregning** Det er flere reiseregninger hvor utlegg i valuta ikke er omregnet på skjema. Hvilken valutakurs som er benyttet er ikke vist på skjema. Det er flere tilfeller der benyttet valutakurs er dokumentert med kontoutskrift fra kredittkort eller privatbankkonto. Dette gjelder også de øvrige fakultetene / instituttene.	**Valutakurs-omregning** Det anbefales at kurs benyttet ved omregning fra valuta til NOK vises på reise-regningsskjema. Dette vil gjøre det lettere å kontrollere at det er benyttet korrekt kurs ved omregning

8 Testing – Det psykologiske fakultet

Vi har testet 14 reiseregninger.

#	Prioritet	Aktivitet	Observasjon	Anbefalte forbedringspunkter
4-1	❶ Høy prioritet	• *Manglende dokumentasjon*	**Manglende dokumentasjon** På reiseregning 160183, mangler bilag på kr 576 for taxi for refusjon av taxiutgifter. Reiseregning 156722; mangler original dokumentasjon på utlegg. Reiseregning 148195; er det feil omregnet taxi regning i DKK. Det er krevd fradrag for DKK 281 og ikke det omregnede beløpet i NOK	**Manglende dokumentasjon** Kostnader som ikke kan dokumenteres, bør ikke refunderes.

Vedlegg 1 – Symboler

Evaluering av internkontroll

Grad	Forklaring
	Tilfredsstillende. Internkontrollen møter generelt akseptable standarder.
	Tilfredsstillende – Internkontrollen møter generelt akseptable standarder, men det er identifisert noen forbedringsområder.
	Behov for forbedringer - Internkontrollen møter generelt akseptable standarder, men bør forbedres.
	Behov for forbedringer– Internkontrollen møter under tvil akseptable standarder og det er identifisert flere forbedringsområder.
	Ikke tilfredsstillende – Internkontrollen møter generelt ikke minimum akseptable standarder. Kritiske kontroller er ikke på plass og tap kan oppstå uten å bli oppdaget.

Risikovurdering

Risiko	Forklaring
Høy	Risikoen er klassifisert som lav, medium eller høy, og reflekterer områdets risiko for at UiB ikke skal nå sine mål
Medium	
Lav	

Utvikling

Utvikling	Forklaring
↗	Positiv trend siden forrige gjennomgang
→	Uendret trend siden forrige gjennomgang
↘	Negativ trend siden forrige gjennomgang

Prioritet

Prioritet	Forklaring
❶ Høy prioritet	Anbefalinger som bør gjennomføres umiddelbart. Anbefalingen har kritisk betydning for risikoen i revidert enhet.
❷ Medium prioritet	Anbefalinger som bør gjennomføres så snart som mulig. Anbefalingen har moderat betydning for risikoen i revidert enhet.
❸ Lav prioritet	Anbefalinger som bør gjennomføres, men det er ikke tidskritisk. Anbefalingen har i mindre grad betydning for risikoen i revidert enhet.