UNIVERSITETET I BERGEN

Styre: Universitetsstyret
Styresak: 120/17
Møtedato: 26.10.2017

Dato: 12.10.2017
Arkivsaksnr: 2016/11547

Internrevisjon, UiBs arbeid med personvernforordningen

Henvisning til bakgrunnsdokumenter

- Styresak 33/16: *Instruks for internrevisjonen ved Universitetet i Bergen*
  http://www.uib.no/sites/w3.uib.no/files/attachments/us2016-033.pdf
- Styresak 147/16: *Internrevisjon, revisjonsplan 2016/2017*
  http://www.uib.no/sites/w3.uib.no/files/attachments/us2016-147.pdf

Saken gjelder:

Internrevisjonen har, i samsvar med revisjonsplan 2016/2017, gått gjennom UiBs arbeid med å imøtekomme kravene i ny Personvernforordning. Ny personvernforordning trer i kraft i hele EU/EØS 25. mai 2018 og denne blir samtidig norsk rett ved innføring av ny personopplysningslov. Internrevisjonen har hatt fokus på å identifisere dagens status, identifisere hvordan regelverket medfører endringsbehov for UiB og foreslå tiltak og aktiviteter for å komme i samsvar med det nye regelverket innen mai 2018. Rapporten legges fram for universitetsstyret til orientering.

Hovedpunktene i rapporten:

Internrevisjonen har gjennomført en innledende GAP-analyse av UiBs arbeid med personvern og informasjonssikkerhet mot kravene i den nye Personvernforordningen. GAP - analysen viser at UiB i stor grad har på plass krav knyttet til dagens regelverk, men må gjøre en del tilpasninger for å imøtekomme kravene i nytt regelverk. Enkelte sentrale ressurser ved UiB har begynt å sette seg inn i forordningen, men det er internrevisjonens anbefaling at UiB etablerer et prosjekt med ansvaret for å identifisere områder med behov for justeringer og endringer.

Det anbefales at UiB jobber strukturert med:

- Skaffe en mer detaljert oversikt over samtlige behandlinger av personopplysninger i virksomheten, herunder bruk og dataflyt
- Sikre at opplysningene har gyldig hjemmel og kun behandles til det formålet det foreligger hjemmel for
- Gjennomføre DIPA (personvern konsekvensvurdering) for aktuelle behandlinger
- Sikre at god informasjonssikkerhet og internkontroll er ivaretatt og at det er tilstrekkelig sporbart
- Vurdere løsninger og rutiner for at de registrerte bedre kan å ivareta sine rettigheter
- Evaluere personvernombudsordningen for forskning og vurdere hvordan den også kan dekke øvrige behandlinger
- Summen av roller, ansvar og aktiviteter må vurderes opp mot dagens organisering, og eventuelt gjøre nødvendige endringer, samt sørge for at det gis nødvendig opplæring.

Universitetsdirektørens kommentarer

Ikrafttredelse av ny personopplysningslov/personvernforordningen innebærer en del endringer som UiB må forholde seg til. Blant annet vil de registrertes rettigheter bli styrket, melde- og konsesjonsplikten til Datatilsynet vil kunne falle bort og erstattes med en plikt til vurdering av personvernkonsekvenser og forhåndsdrøfting med tilsynsmyndigheten. Videre innføres det en plikt til å ha personvernrådgiver for offentlige myndigheter og det innføres vesentlig høyere overtredelsesgebyrer enn i dag.

UiB har startet arbeidet med forberedelsene for den nye forordningen og imøtekommelse av kravene den vil stille til oss. UiB har også avgitt høringsuttalelse til utkast til ny personopplysningslov.

Internrevisjonen anbefaler at det etableres et formelt prosjekt som bør eies av UiBs ledelse, for å komme i samsvar med den nye personvernforordningen. Internrevisjonens anbefaling vil bli fulgt opp ved at det settes ned en arbeidsgruppe som ledes fra Sekretariat for universitetsledelsen og som rapporterer løpende til universitetsledelsen. Arbeidsgruppen vil blant annet vurdere ulike løsninger for organisering av personvernombudsordningen ved UiB, både for forskning og administrative behandlinger.

Forslag til vedtak:

Universitetsstyret tar internrevisjonsrapporten «UiBs arbeid med personvernforordningen» til orientering.

Kjell Bernstrøm
universitetsdirektør

12.10.2017/Silje Nerheim/Arne Ramslien

Vedlegg:
Rapport, UiBs arbeid med Personvernforordningen

Revisjonsprosjekt
UiBs arbeid med Personvernforordningen
Nr. 2017/01

Utkast rapport: 27.4.17

Endelig rapport: 12.5.17

Til:	Universitetet i Bergen v/Sekretæriat for universitetsledelsen
Kopi til:	Universitetsdirektøren ved Universitetet i Bergen
Fra:	Jan Roger Hånes, PricewaterhouseCoopers AS
Sign:	

pwc

Innholdsfortegnelse

1 Introduksjon

Bakgrunn

PricewaterhouseCoopers (PwC) har gjennomført en internrevisjons gjennomgang av UiBs arbeid med å imøtekomme kravene i ny Personvernforordning. Gjennomgangen er basert på årsplan for internrevisjonen og planleggingsmemo godkjent av Universitetet i Bergen (UiB).

Formål og omfang

Det er et mål for Universitetet i Bergen å være i samsvar med gjeldene lover og regler. EU-parlamentet har nå vedtatt personvernforordningen. Det betyr at alle EU-land får ny og enhetlig personvernlovgivning fra 2018.
Personvernforordningen blir norsk rett og erstatter dagens Personopplysningslov med forskrift. Regelverket er svært omfattende og vil for mange kreve vesentlige endringer i internkontroll, teknologi og bruk av data. Internrevisjonen har fokusert på hvor UiB står i forhold til de endringer som vil komme i det nye regelverket med formål å bidra med innsikt til hvilke aktiviteter og tilpasninger UiB må gjennomføre for å imøtekomme nytt regelverk. Internrevisjonen har hatt fokus på følgende:

- Identifisere dagens status i arbeidet med Personvern
- Identifisere hvordan regelverket til medføre endringsbehov for UiB
- Foreslå tiltak og aktiviteter UiB må starte å arbeide med for å komme i samsvar med det nye regelverket fra Mai 2018.

Avgrensning

Revisjonsprosjektet har vært avgrenset til å gjennomgå dokumentasjon og gjennomføre intervjuer og arbeidsmøter med ressurspersoner hos UiB. Vi har ikke testet etterlevelse av gjeldende rutiner og krav.Det presiserer at gjennomgangen ikke nødvendigvis har dekket alle sentrale forhold i den nye personvernforordningen, og at UiB i sitt prosjekt bør sikre en fullstendig gjennomgang av regelverket i forhold til de behandlinger av personopplysninger UiB gjennomfører.

Revisjonsperiode

Internrevisjonsprosjektet ble gjennomført i perioden Desember 2016– Mars 2017.

Gjennomført arbeid

Som grunnlag for internrevisjonen har PwC gjennomført et arbeidsmøte med personell fra UiB, der vi har gjennomført en overordnet GAP analyse ved hjelp av et eget verktøy. Videre har vi gjennomgått eksisterende dokumentasjon knytt til personvern og informasjonssikkerhet. Det er også gjennomført intervjuer med enkelte ressurspersoner i etterkant av arbeidsmøtet. Hensikten har vært å identifisere dokumentasjon, og få oversikt over hvordan UIB jobber med etterlevelse av dagens krav for å identifisere forbedringer og endringsbehov i forhold til nytt personvernregelverk. Følgende ressurser og avdelinger fra UiB har vært involvert.

Avdeling/fakultet/institutt	Navn
Økonomiavdelingen	Ernst Pedersen
IT	Tore Burheim
Universitetsdirektørens kontor	Janecke Helene Veim
Innkjøp	Kitty Amlie Tverrå
Universitetsdirektørens kontor	Silje Nerheim

Utdrag av dokumentasjon og kilder

Mål og strategi i administrative system. Mål og strategi for helseforskning og behandling av personopplysninger i forskning. Overordnede rammer for helseforskning og behandling av personopplysninger ved UiB. Sikkerhetsmål og sikkerhetsstrategi i administrative system. Sikkerhetsmål og sikkerhetsstrategi i forskning. Retningslinjer for systemeiere. Datatilsynets veiledere og informasjon om GDPR. EUs GDPR dokument med tilhørende veiledere fra Artikkel 29-gruppen.

Revisjonsteam

Fra PwC; Jan Roger Hånes, Olav Høsøien og Nils Harald Børve.

2 Oppsummering

Risikovurdering: Høy	**Vurdering av prosjekt:**	Ikke relevant	**Trend:** Ikke relevant

Oppsummering av observasjoner:

Internrevisjonen har gjennomført en innlededene GAP analyse av UiBs arbeid med personvern og informasjonssikkerhet mot kravene i den nye Personvernforordningen. Formålet har vært å gi UiB inspill til hvilke aktiviteter UiB bør gjennomføre for å komme i samsvar med kommende personvernregelverk.

GAP analysen viser at UiB i stor grad har på plass krav knyttet til dagens regelverk, men må gjøre en del tilpasninger for å imøtekomme kravene i nytt regelverk. En vesentlig «fokusendring» i det nye regelverket, er at ansvaret for å kunne dokumentere etterlevelse av kravene i regelverket er blitt betydelig strengere. Dette betyr i praksis at regelverket stiller strengere krav til å kunne dokumentere og vise etterlevelse av kravene en tidligere, dette gjelder både på systemnivå, samt på policy og rutinenivå. Til gjengjeld er det slik vi forstår det, lagt opp til mindre kontrollvirksomhet fra myndighetene sin side i forhold til dagens regime. Det er verdt å merke seg at det nye regelverket har en større nedside i form av bøter dersom uregelmessigheter eller avvik fra kravene forekommer, samtidig kan det være en større oppside dersom samtykke for behandling av personoppllysninger fra den registrerte er gode, og nødvendig internkontroll er på plass.

UiB har ikke etablert eget formelt prosjekt eller andre formelle intiativer for å imøtekommer personvernforordningen på nåværende tidspunkt. Enkelte sentrale ressurse med koordinerende ansvar for administrative systemer og forskningsprosjekter, har likevel begynt å sette seg inn i forordningen. Det er internrevisjonens anbefaling at UiB etablerer et formelt prosjekt med riktig bemanning som får ansvaret for å identifisere endringer som må til for at UiB skal kunne få på plass løsninger som gjør at man har innrettet virksomheten på en slik måte at kravene i den nye personvernforordningen blir ivaretatt.

UiB har et rammeverk for etterlevelse av dagens personvernkrav, i tillegg er det gjennomført et arbeid med å forbedre UiBs rammeverk for informasjonssikkerhet. Ettersom flere av de mest sentrale kravene i den nye forordningen allerede er gjeldene i norsk rett, ser internrevisor disse intativene som verdifulle og en viktig forutsetning for å komme i samsvar med Personvernforordningen. Av områder som UiB må jobbe strukturert med er:

- Skaffe en mer detaljert oversikt over samtlige behandlinger av personopplysninger i virksomheten, herunder bruk og dataflyt
- Sikre at opplysningene har gyldig hjemmel og kun behandles til det formålet som det foreligger hjemmel for
- Gjennomføre DIPA (Personvern konsekvensvurdering) for aktuelle behandlinger
- Sikre at god informasjonssikkerhet og internkontroll er i varetatt, og at det er tilstrekkelig sporbart
- Vurdere og finne gode løsninger for å ivareta den registrertes rettigheter
- Evaluere personombudsordningen for forskning og vurdere hvordan den også kan dekke øvrige behandlinger
- Summen av roller, ansvar og aktiviteter må vurderes opp mot dagens organisering, og eventuelt gjøre nødvendige endringer, samt sørge for at det

Risikovurdering: Høy	**Vurdering av prosjekt:**	Ikke relevant	**Trend:** Ikke relevant

Oppsummering av observasjoner:

gis nødvendig opplæring

Anbefalingene innebærer at det vil være behov for å iverksette en prosess -med formål å skape bedre detaljkunnskap om de opplysninger som faktisk samles inn og behandles ved UiB. Videre må det gjennomføres oppdateringer av rutiner og policyer der hvor dette er aktuelt. De nye kravene medfører at det må gjennomføres en del ny aktiviteter, og UiB må sikre at alle plikter blir gjennomført, og at det blir dokumentert. Enkelte områder bør vurderes om skal løses i felleskap i sektoren, eventuelt sammen med NSD. I kapittel 2 har vi gjengitt våre observasjoner og anbefalinger. I kapittel 4 har vi foreslått en overordnet prosjektplan for hvordan UiB kan gå vider i arbeid med forordningen.

3 Observasjoner

#	Prioritet	Aktivitet	Observasjon	Relevant artikkel*	Anbefaling
1	❶ Høy prioritet	Organisering og forankring	UiB har ikke etablert et formelt arbeid med å komme i samsvar med den nye personvern-forordningen. Selv om regelverket er komplekst og det fortsatt er en del uklare områder i forordningen, bør UiB etablere et formelt arbeid for å imøtekomme kravene. Det er positivt at flere ressurspersoner har startet arbeidet med å sette seg inn i det nye regelverket, og således har startet arbeidet med å identifisere områder som krever endringer for å være i samsvar med det nye regelverket. Videre i denne rapporten tar Internrevisjonen opp særlige områder vi mener UiB bør jobbe videre med i et slikt arbeid.	I/A	Internrevisjonen anbefaler UiB å etablere et prosjekt, arbeidsgruppe eller annen sammensetning av ressurspersoner som kan: • Gjøre seg kjent med regelverket • Får oversikt over dagens praksis, mangler og forbedringer • Utrede og arbeide med relevante problemstillinger i denne rapporten. • Sikrer at nødvendige tiltak blir etablert. • Vurdere behov for samarbeid i sektoren Prosjektet bør eies og forankres av UiBs ledelse.
2	❷ Medium prioritet	Personvernombud	Det er etablert personvernombud for forskning gjennom samarbeidsavtale med NSD. Det er ikke etablert personvernombud for administrative behandlinger av personopplysninger. Offentlige virksomheter blir gjennom det nye regelverket pliktet til å etablere Personvernombud.	37-39	Internrevisjonen anbefaler at UiB evaluerer ordningen med Personvernombud, og vurdere ulike løsninger for hvordan de kan etablere Personvernombud som dekker hele virksomheten. Noen former som kan vurderes: • UiB etablerer en personvernombudsrolle i egen organisasjon med ansvar for samtlige behandlinger av personopplysninger. Herunder forskning og administrative behandlinger av personopplysninger. • UiB viderefører NSD som personvernombud for - forskning, men etablerer eget personvernombud for øvrige behandlinger. • UiB viderefører NSD som personvernombud og tilknytter seg et eksternt personvernombud også for øvirge behandlinger.

*Relevant artikkel i Personvernforordningen som beskriver forholdet

#	Prioritet	Aktivitet	Observasjon	Relevant artikkel*	Anbefaling
					Ved etablering av personvernombud er det en rekke forhold UiB bør vurdere, herunder uavhengighet. Det er utarbeidet egen veileder for Personvernombud – vi viser til følgende link for nærmere forhold som bør vurderes: http://ec.europa.eu/newsroom/document.cfm?doc_id=44100

3	❶ Høy prioritet	Oversikt over behandlinger	Virksomheten ved UiB innebærer informasjon og behandling av personopplysninger i mange ulike varianter og sammenhenger.
			
			Slik vi forstår det foreligger det foreløpige ingen komplett oversikt over hvilke personopplysninger UiB behandler, i hvilke systemer, til hvilke formål og til hvilke hjemmel.
			
			Oversikt over omfang og innhold i behandling av personopplysninger er en forutsetning for å kunne innrette seg etter kravene i gjeldene og kommende regelverk. Det er også et eksplisitt krav i forordningen å kunne dokumentere en skriftlig oversikt over alle behandlinger av personopplysninger. Det stilles også en del formkrav til denne oversikten.
				5.1e, 5.2, 24.1, 30	Internrevisjonen anbefaler at UiB utfører en kartlegging av alle behandlinger av personopplysninger, og følgende aktiviteter anbefales å gjennomføre:
					
					• Identifiser hvilke personopplysninger som behandles hvor, av hvem, og i hvilke prosesser og systemer
					• Sikre at UiB har oversikt over følgende:
					  ○ Navn og kontaktperson på den som har ansvar for databehandlingen ved UiB
					  ○ Navn og kontaktperson på eventuelle eksterne databehandlere
					  ○ Formålet med behandlingen
					  ○ Lovhjemmel for behandlingen
					  ○ Hvilke kategorier av personopplysninger som behandles
					  ○ Tidsplan for sletting av opplysninger
					  ○ Hvordan opplysningene er sikret*
					• Det bør utarbeides rutiner for hvordan registeret skal vedlikeholdes. Herunder av hvem, når og hvordan.
					
					Se artikkel 30 for utdypende beskrivelse av disse forholdene
					
					*En beskrivelse av tekniske og organisatoriske sikkerhetstiltak som er tatt.

#	Prioritet	Aktivitet	Observasjon	Relevant artikkel*	Anbefaling
4	❷ Medium prioritet	Hjemmelsgrunnlag	I det nye regelverket faller krav om melde om konsesjon for behandling av personopplysninger bort, samt at alle behandlinger av personopplysninger får «nye» hjemler. I de tilfeller hvor UiB har behandling av personopplysninger som i dag er underlagt konsesjon med tilhørende hjemmelsgrunnlag, er det behov for at UiB selv må fastsette ny lovhjemmel for dagens praksis for behandling av personopplysninger. I denne sammenheng, er det viktig å ta høyde for følgende forhold. Der samtykke er lagt til grunn som hjemmelsgrunnlag – kommer det skjerpede formkrav for utforming av samtykke, det kommer også krav om å kunne trekke tilbake samtykke.	5-11 24, 26, 28, 32, 33, 34	I forbindelse med kartlegging jf pkt 3 ovenfor, anbefaler Internrevisjonen at UiB bør gjennomgå sine behandlinger og vurdere hjemmel etter forordningen. Dette gjelder særskilt områder der konsesjon eller samtykke er hjemmelsgrunnlag. For forskningsprosjekter; anbefaler vi at UIB samarbeider med NSD, ettersom forskningsprosjekter er dekket særskilt i forordningen og prinsippene for hjemmel i stor grad vil være felles i sektoren. UiB bør også gjennomgå og sikre at alle samtykkeskjema er oppdatert iht. forordningens formkrav. Både for forskning og administrative behandlinger. For forskning bør dette med fordel gjennomføres i samarbeid med NSD. Noen forhold UiB bør merke seg knyttet til samtykke: • Samtykke bør være enkelt, kort og presist • Samtykke kan ikke være generelt, men må innhentes for hvert enkelt formål, gjerne en form for «flervalgs-funksjon» dersom det er aktuelt. • Det må fremgå at samtykke kan trekkes tilbake • Samtykke må være sporbart, UiB må kunne bevise at samtykke er innhentet • Dersom samtykke innhentes fra barn under 16 år, må UiB sikre at samtykke innhentes fra foresatte.
5	❷ Medium prioritet	Privacy by design	«Privacy by design» eller «innebygd personvern» er et nytt begrep i forordningen. Kravet går ut på at virksomheten ta hensyn til personvern i alle utviklingsfaser av et IKT-system. Dette innebærer bl.a. • Gjennomføre DIPA (jf. pkt 8) for å vurdere behandlingen før en starter	Art 25	Internrevisjonen anbefaler at UiB etablerer rutiner for hvordan godt personvern kan etableres som en standardinnstilling i samsvar med forordningens krav. Rutinene må implementeres i UiBs prosesser for utvikling, innføring og etablering av nye behandlinger av personopplysninger og IKT systemer.

#	Prioritet	Aktivitet	Observasjon	Relevant artikkel*	Anbefaling
			opp • Ha fokus på å ikke lagre/samle inn mer data en nødvendig • Vurdere om anonymisering eller avidentifisering kan benytte for å oppnå samme formål • Sikre at nødvendige tilganger o.a. er utformet etter behov for tilgang • At tilstrekkelige sikkerhetskontroller er etablert, fungerer og at en dokumentere etterlevelse • M.m.		Kravet bør også stilles til alle leverandører som levere programvare/tjenester til UiB. Datatilsynet har utarbeidet en veileder for dette som UiB kan ta utgangspunkt i. https://www.datatilsynet.no/Teknologi/Innebygd-personvern/
6	❷ Medium prioritet	Den behandledes rettigheter	I forordningen legges det stor vekt på den behandledes rettigheter. Dette innebærer en del endringer i forhold til dagens regelverk. Retten til å bli glemt - Dette innebærer at UiB må etablere rutiner som sikrer at alle opplysninger blir slettet på forespørsel, eller at det kan vises til annen hjemmel som hindrer UiB å slette data. Dette må kunne defineres på «opplysningsnivå». For å kunne imøtekomme kravet om å bli glemt, forutsetter det at UiB har komplett oversikt over alle data som samles inn jf. pkt 3. og hvor disse lagres. Dette gjelder både strukturerte og ustrukturerte data. Dataportabilitet – Dette innebærer at den registrerte skal på et enkelt maskinlesbart format kunne ta med seg opplysninger om seg selv. Gjerne i form av en selvbetjeningsløsning eller på forespørsel.	Art 12, 15-23	Internrevisjonen anbefaler at det etableres rutiner som sikrer at «Retten til å bli glemt» – rettigheten må kommuniseres til de registrerte (vha personvernerklæring jf. pkt 7). Videre anbefaler Internrevisjonen at det etableres gode rutiner for hvordan sletting skal gjennomføres og at man har løsninger som ivaretar følgende forhold: • Hvor kan den registrerte henvende seg? • Hvem skal gjøre vurderingen? • Fra hvor, av hvem, og hvordan skal en slette data og hvordan sikrer at en sletter alle data? Herunder sikkerhetskopi og andre kopier av data. • En må sikre at denne muligheten også ligger hos eventuelle underleverandører

#	Prioritet	Aktivitet	Observasjon	Relevant artikkel*	Anbefaling
7	❷ Medium prioritet	Personvernerklæring	I det nye regelverket er det skjerpede krav til å informere den registrerte i forhold til hva slags informasjon som skal innhentes og hva disse skal brukes til. Slik Internrevisjonen har forstått det, foreligger det i dag begrenset informasjon til de registrerte rundt dette, dette gjelder både Administrative (egne ansatte og studenter) og i forskningsprosjekter. Dette betyr at de skjerpede kravene vil kreve endringer i rutiner og praksis.	Art 12-14	For alle behandlinger jf. pkt 3 - bør UIB sikre at tilstrekkelig informasjon blir distribuert til de registrerte. Internrevisjonen vil også anbefale UiB å vurdere å etablere et register som gir god oversikt over samtlige behandlinger en person er involvert i. Dette kan bidra til å forenkle håndtering av forespørsel om innsyn, sletting og tilbaketrekking av samtykke. Det foreligger som nevnt noen nye forhold UiB bør merke seg knyttet til personvernerklæringer, og som vi anbefaler UiB å ta med seg i revisjon av disse rutinene og praksis: • Vurder den beste måten for hvordan informasjon kan formidles klart og tydelig til den registrerte • Vurder hvordan informasjon enklest mulig kan være maskinlesbart • Eksisterende informasjon om formål, informasjonssikkerhet, hjemmel, rettigheter osv. bør og videreføres eventuelt oppdateres.
8	❷ Medium prioritet	Personvernvurdering / DPIA	I eksisterende regelverk er det stort fokus på gjennomføring av risikovurderinger. I det nye regelverket er det større fokus på «Data Privacy Impact assessment» der man i en i større grad har fokus på Personvernet og hvilke konsekvenser en behandling kan få for den behandlede. For behandlinger der risiko blir identifisert som «høy», er man forpliktet til å føre dialog med Datatilsynet før behandling starter.	Art 35-36	Internrevisjonen anbefaler at UiBs rutiner for risikovurdering oppdateres i forhold til kravet om gjennomføring av DPIA. Rutinen bør beskrive når, av hvem, og hvordan en DPIA skal gjennomføres, samt hvordan dialog med Datatilsynet skal føres der høy risiko er identifisert. Artikkel 29 gruppen har utarbeidet utkast til en veileder for gjennomføring av DIPA: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137 Mrk: denne er et utkast som er på høring til 23.5.17 – og endringer kan komme på dette punktet.
9	❷ Medium	Avvikshåndtering	UiB har etablert rutiner for avvikshåndtering i samsvar med dagens regelverk. I det nye	Art 33-34	Internrevisjonen anbefaler at UiB foretar en revisjon av eksisterende rutine med formål å sikre seg at nye krav i

#	Prioritet	Aktivitet	Observasjon	Relevant artikkel*	Anbefaling
	prioritet		regelverket stilles det også krav til at en skal vurdere behov for å og eventuelt varsle det individet som det har vært uautorisert utlevering av personopplysninger om. Kravet om å ha et avviksregister, og melde dette til Datatilsynet vil fortsatt gjelde. Se for øvrig forordningen artikkel 33-34 for utfyllende detaljer rundt dette kravet.		forordningen blir ivaretatt i rutinene. Internrevisjonen anbefaler at minimum bør følgende vurderinger gjøres i denne forbindelse for å se om det er behov for endringer: • Vurder hvem og hvordan avvik skal meldes • Vurder hvem som skal vurdere avviket • Der Datatilsynet skal varsles, skal dette skje innen 72 timer • Der personopplysninger med «høy-risiko» (jf. DIPA) blir kompromittert, skal personene det gjelder varsles uten ugrunnet opphold. • Vurder hvilke aktiviteter og hvem som skal gjennomføre slik varsling • Vurder behovet for egne beredskapsplaner for - behandlinger som er definert som «høy-risiko» (jf. DIPA) • UiB må forsikre seg om at eventuelle underleverandører varsler i tide ved eventuelle hendelser. • Vurder hvordan UiB kan få komplett oversikt over alle relevante avvik i organisasjonen. Eks. gjennom et avviksregister
10	❷ Medium	Roller og ansvar	Roller og ansvar for personvern og informasjonssikkerhet er tydelig definert i UiBs styrende dokumenter. For forskning er arbeidet i stor grad desentralisert og ansvar for å sikre at plikter blir fulgt hviler på det enkelte forskningsprosjekt. For administrative systemer er det systemeier og systemforvalter som sikrer at pliktene blir fulgt. I tillegg har IT avdelingen et ansvar for at arbeidet med informasjonssikkerhet i IT systemer, og at løsninger blir håndtert jf. personopplysningsforskriften kap.2. Her blir	Art 24, 37-39	Internrevisjonen anbefaler at UiB oppdaterer roller og ansvar ifht de rutiner og oppgaver som blir etablert som følge av dette oppdateringsarbeidet. Internrevisjonen anbefaler videre at det gis opplæring til alle som har roller som har et vesentlig ansvar jf. pkt 11.

#	Prioritet	Aktivitet	Observasjon	Relevant artikkel*	Anbefaling
			ledelsen involvert gjennom årlige ledelsesgjennomganger. Som en følge av at forordningen gir en hel del mer detaljert plikter som vil kreve endringer i rutiner og oppgaver, må roller og ansvarsbeskrivelser oppdateres i forhold til disse.		
11	❷ Medium prioritet	Opplæring	Å kunne vise til, og dokumentere etterlevelse av kravene i forordningen blir et større fokus enn tidligere. Opplæring vil derfor bli et viktig virkemiddel for å sikre forståelse for, og kompetanse om hvilke oppgaver og aktiviteter som skal gjennomføres, og hvordan dette skal skje.	I/A	Internrevisjonen anbefaler at UiB etablerer en opplæringsplan for alle identifiserte roller, slik at en sikrer at nødvendige oppgaver blir tilstrekkelig utført.

4 Forslag til nærming

Under følger forslag til en overordnet tilnærming for hvordan UiB kan gjennomføre arbeidet med å komme i samsvar med Personvernforordningen

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.