Riksrevisjonen

Revisjonsrapport for 2017 om informasjonssikkerhet i forskningssystemer

Mottaker: Kunnskapsdepartementet

Revisjonen er en del av Riksrevisjonens kontroll av disposisjoner i henhold til *lov om Riksrevisjonen* § 9 første ledd og *instruks om Riksrevisjonens virksomhet* § 3b. Revisjonen er gjennomført i samsvar med ISSAI 400 /4000, INTOSAIs internasjonale prinsipper og standarder for etterlevelsesrevisjon.

Forsideillustrasjon: Colourbox

Innhold

1 Sammendrag

Forskning er en viktig del av virksomhetene i universitets- og høgskolesektoren (UH-sektoren). Når et forskningsprosjekt behandler personopplysninger, må kravene i *lov om behandling av personopplysninger* (personopplysningsloven) følges. Personopplysningsloven og tilhørende forskrift skal beskytte den enkelte fra å få personvernet sitt krenket. Det følger av lovens § 13 at det skal etableres tilfredsstillende informasjonssikkerhet gjennom planlagte systematiske tiltak ved behandling av personopplysninger. Systemet og tiltakene skal dokumenteres.

Virksomhetene kan bruke eksterne leverandører til å behandle og/eller lagre prosjektinformasjon, men er allikevel ansvarlige for at kravene i loven blir fulgt.

Mangelfull informasjonssikkerhet i forskningssystemer gir en risiko for at uautoriserte personer får tilgang til sensitiv informasjon, tap av tillit og omdømme, forskningsjuks og brudd på lover og regler. Å etterleve personopplysningsloven § 13 er prinsipielt vesentlig for tilliten til den offentlige forvaltningen, og å sikre sensitiv informasjon er vesentlig for personvernet til alle de berørte partene.

Målet med revisjonen er å kontrollere om utvalgte universiteter/høgskoler har dokumenterte styringssystemer som skal sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter, i samsvar med kravene i personopplysningsloven og personopplysningsforskriften.

Utvalget i revisjonen består av tre virksomheter fra UH-sektoren, og kontrollen er gjennomført ved dokumentanalyse og intervju.

Det er mangler ved dokumentasjonen av sentrale elementer i styringssystemet for informasjonssikkerhet ved alle de tre kontrollerte universitetene/høgskolene, som viser at virksomhetene ikke etterlever flere av kravene i personopplysningsloven § 13 og personopplysningsforskriften kapittel 2. I 2018 får Norge nye personvernregler, som gir virksomhetene ytterligere ansvar for å behandle personopplysninger korrekt.

2 Innledning

I 2017 besto UH-sektoren av 8 universiteter og 13 høgskoler med statlig eierskap. Forskning er en stor og viktig del av oppgavene til universitetene/høgskolene. Dersom et forskningsprosjekt skal behandle personopplysninger, må prosjektet meldes til Datatilsynet og/eller personvernombudet[1] i virksomheten, i tillegg til at kravene i personopplysningsloven må være oppfylt. Personopplysningsloven skal beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger. I tillegg skal loven bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, herunder behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.[2]

Personopplysningsloven § 13 viser til at det er den behandlingsansvarlige[3] som er ansvarlig for informasjonssikkerheten. Hvis en databehandler[4] utfører oppdrag i tilknytning til informasjonssikkerhet, er det likevel den behandlingsansvarlige som er ansvarlig for at kravene til informasjonssikkerhet er oppfylt. I denne revisjonen er de utvalgte universitetene/høgskolene behandlingsansvarlige for personopplysninger i forskningsvirksomheten.

Virksomhetene kan ha egne systemer for sikker lagring og behandling av forskningsdata, men de kan også bruke eksterne tjenesteleverandører, datasentraler eller driftsoperatører for å drifte deler av forskningssystemene sine og sikker lagring av forskningsdata.

Tjenester for Sensitive Data (TSD) ved Universitetets senter for informasjonsteknologi ved Universitetet i Oslo leverer lagringstjenester for sensitive forsknings- og persondata og vil etter lovens definisjon være databehandler. I tillegg til å lagre dataene kan brukerne også samle inn, dele og gjøre beregninger på sensitive data innenfor et

[1] *Personvernombudets plikter – vedtaket.* <https://www.datatilsynet.no/regelverk-og-skjema/personvernombud/personvernombudets-plikter---vedtaket/>
[2] Personopplysningsloven § 1.
[3] «Behandlingsansvarlige»: den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal brukes, jf. personopplysningsloven § 2 punkt 4.
[4] «Databehandler»: den som behandler personopplysninger på vegne av den behandlingsansvarlige, jf. personopplysningsloven § 2 punkt 5.

lukket miljø. Når prosjektet avsluttes, blir tilgangen stengt for brukerne. I denne revisjonen har vi kun sett på virksomheter som bruker TSD.

Den behandlingsansvarlige og databehandleren inngår egne avtaler som regulerer partenes rettigheter og plikter, databehandlerens bruk av personopplysninger og ivaretakelse av sikkerhet i samsvar med personopplysningsloven og personopplysningsforskriften.

Mangelfull informasjonssikkerhet i forskningssystemer gir en risiko for at uautoriserte personer får tilgang til sensitiv informasjon, tap av tillit og omdømme, forskningsjuks og brudd på lover og regler.

Å etterleve personopplysningsloven § 13, jf. §§ 14 og 15 er prinsipielt vesentlighet for tilliten til den offentlige forvaltningen, og å sikre sensitiv informasjon er vesentlig for personvernet til alle de berørte partene.

3 Revisjonens mål og problemstillinger

Målet med revisjonen er å kontrollere om utvalgte universiteter/høgskoler har dokumenterte styringssystemer som skal sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter, i samsvar med kravene i personopplysningsloven og personopplysningsforskriften. I tillegg vil kravene i *lov om medisinsk og helsefaglig* forskning (helseforskningsloven), *lov om helseregistre og behandling av* helseopplysninger (helseregisterloven) og *forskrift om organisering av medisinsk og helsefaglig forskning* være aktuelle for medisinsk og helsefaglig forskning på helseopplysninger.

Ut fra dette er målet med revisjonen å undersøke følgende problemstillinger:

Problemstilling 1:
Har virksomhetene dokumentert et styringssystem for informasjonssikkerhet som gir grunnlag for å etablere sikkerhetstiltak som tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i de enkelte forskningsprosjekter?

Problemstilling 2:
Følger virksomhetene opp om sikkerhetsstrategien og -tiltak gir tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter jf. personopplysningsloven § 13 og personopplysningsforskriften kapittel 2?

3.1. Avgrensning

Revisjonen er rettet mot utvalgte virksomheter og de underliggende forskningsmiljøene i UH-sektoren, og er basert på et utvalg av tre universiteter/høgskoler som har inngått avtaler med TSD.

Kontrollen er avgrenset til de tre utvalgte universitetenes/høgskolenes styringssystem for å ivareta informasjonssikkerheten ved behandling av personopplysninger i forskningsprosjekter i 2017 og hvordan ansvaret for informasjonssikkerheten er (avtalt) regulert mellom virksomhetene og TSD. Revisjonen omfatter kun enkelte deler av styringssystemet til virksomhetene. Tekniske løsninger for å sikre informasjonssikkerheten er ikke kontrollert, og det er ikke kontrollert hva som er gjort i de enkelte forskningsprosjektene for å sikre tilfredsstillende informasjonssikkerhet.

4 Metoder

Utvalget i denne revisjonen består av tre av totalt 21 virksomheter i UH-sektoren. Virksomhetene er av forskjellig størrelse: ett universitet, én stor høgskole og én mindre høgskole.

Metodene som er brukt i denne revisjonen, er dokumentanalyse og intervju med de tre utvalgte virksomhetene. Det er hentet inn dokumentasjon både i forkant og etterkant av intervjuene. Dokumentene er analysert og sett i sammenheng med intervjuene. Virksomhetene har verifisert referatene fra intervjuene.

4.1. Problemstilling 1

Har virksomhetene dokumentert et styringssystem for informasjonssikkerhet som gir grunnlag for å etablere sikkerhetstiltak som bidrar til tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i de enkelte forskningsprosjekter?

Revisjonen har analysert dokumenter i virksomhetenes styringssystemer, for eksempel: sikkerhetsmål, sikkerhetsstrategi, rollekort og tilleggsdokumentasjon som blant annet retningslinjer for behandling av personopplysninger, policy og prinsipper for informasjonssikkerhet og IT-reglement. I tillegg har revisjonen vurdert risikovurderinger og databehandleravtaler med virksomhetene og TSD. Avtaler med vedlegg er innhentet fra TSD.

Tema i intervjuene med de tre virksomhetene har vært følgende:

- definerte sikkerhetsmål og sikkerhetsstrategi for forskningsprosjekter
- databehandleravtalen med TSD
- oversikt over hvilke personopplysninger som behandles i virksomhetens forskningsprosjekter
- risikovurderinger av sikkerhetsbrudd i forskningsprosjekter og om det er lagt til rette for risikovurderinger i de enkelte prosjektene
- skriftlig dokumentert ansvarsforhold for behandling av persondata i forskningsprosjekter og skriftlige rutiner for å behandle sikkerhetsbrudd og andre avvik fra fastlagte rutiner

4.2. Problemstilling 2

Følger virksomhetene opp om sikkerhetsstrategien og -tiltak gir tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter, jf. personopplysningsloven § 13 og personopplysningsforskriften kapittel 2?

Revisjonen har ved intervju og dokumentgjennomgang (dokumentasjon på gjennomgang av sikkerhetsstrategi) kontrollert om virksomhetene følger opp sikkerhetsstrategi og tiltak, oppfølging av databehandler og sikkerhetsrevisjoner, ved behandling av personopplysninger i forskningsprosjekter.

Revisjonen har ved intervju med de utvalgte virksomhetene undersøkt følgende:

- sikkerhetsrevisjoner av organisering, sikkerhetstiltak og bruk av leverandører i egen virksomhet
- oppfølging av TSD
- gjennomgang av sikkerhetsstrategien

I etterkant av intervjuene har revisjonen fått tilsendt dokumentasjon på sikkerhetsgjennomgang fra én virksomhet.

5 Revisjonskriterier

Personopplysningsloven med tilhørende forskrift er sentrale kilder til revisjonskriterier. Sentrale kilder til kriterier for medisinsk og helsefaglig forskning på helseopplysninger er helseforskningsloven, helseregisterloven og forskrift om organisering av helseforskning.

5.1. Felles for begge problemstillingene

Personopplysningsloven § 13 viser til at den behandlingsansvarlige og databehandleren gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger. Den behandlingsansvarlige er ansvarlig dette. Informasjonssystemet og sikkerhetstiltakene skal dokumenteres. Lovens § 14 omhandler internkontroll og viser til at den behandlingsansvarlige skal etablere og vedlikeholde planlagte og systematiske tiltak som er nødvendige, og at tiltakene skal dokumenteres og være tilgjengelige.

Nærmere regler om internkontroll går fram av *forskrift om behandling av personopplysninger* (personopplysningsforskriften) § 3-1. De systematiske tiltakene skal tilpasses virksomhetens art, aktiviteter og størrelse i det omfang som er nødvendig for å etterleve kravene gitt i eller i medhold av personopplysningsloven, med særlig vekt på bestemmelser gitt i medhold av personopplysningsloven § 13. Tiltakene skal også sikre kvalitet på personopplysningene.

5.2. Problemstilling 1

Har virksomhetene dokumentert et styringssystem for informasjonssikkerhet som gir grunnlag for å etablere sikkerhetstiltak som bidrar til tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i de enkelte forskningsprosjekter?

Av personopplysningsloven § 15 går det fram at databehandlerens behandling av personopplysninger skal avtalefestes. I første ledd stilles det krav om at en databehandler ikke kan behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Videre sier andre ledd at det i avtalen med den behandlingsansvarlige skal gå fram at databehandleren plikter å gjennomføre sikringstiltak som følger av § 13 *Informasjonssikkerhet*.

Nærmere regler om organisatoriske og tekniske sikkerhetstiltak går fram av personopplysningsforskriften kapittel 2, som omhandler blant annet krav knyttet til sikkerhetsledelse, risikovurderinger, avvikshåndtering og organisering. Formålet med behandlingen av personopplysninger skal beskrives i et sikkerhetsmål, og valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi, jf. personopplysningsforskriften § 2-3 andre og tredje ledd.

I henhold til personopplysningsforskriften § 2-6 skal bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd behandles som avvik. Det skal jf. forskriftens § 2-7 være etablert klare ansvars- og myndighetsforhold for bruk av informasjonssystemet, og det skal i henhold til forskriftens § 2-4 første ledd føres oversikt over hva slags personopplysninger som behandles.

I personopplysningsforskriftens § 2-4 andre og tredje ledd vises det til at den behandlingsansvarlige skal gjennomføre risikovurderinger for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd, og at resultatet av risikovurderingen skal sammenlignes med de fastlagte kriteriene for akseptabel risiko ved behandling av personopplysninger.

5.3. Problemstilling 2

Følger virksomhetene opp om sikkerhetsstrategien og -tiltak gir tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter, jf. personopplysningsloven § 13 og personopplysningsforskriften kapittel 2?

Personopplysningsloven § 13 tredje ledd viser til at der den behandlingsansvarlige lar databehandleren få tilgang til personopplysninger, vil den behandlingsansvarlige ha det overordnede ansvaret for at informasjonssikkerheten er tilfredsstillende. Personopplysningsforskriften § 2-15 viser til at den behandlingsansvarlige skal etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører, og at dette forholdet skal beskrives i en særskilt avtale. Videre skal den behandlingsansvarlige ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.

Virksomhetene skal gjennomføre sikkerhetsrevisjoner av organisering, sikkerhetstiltak og bruk av leverandører jevnlig, og resultatet av revisjonen skal dokumenteres. Dette er regulert i forskriftens § 2-5. Bruk av informasjonssystemet skal gjennomgås jevnlig for å klarlegge om den er hensiktsmessig i forhold til virksomhetens behov og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat, jf. forskrift § 2-3.

6 Funn

Funnene i revisjonen er oppsummert i en tabell, hvor virksomhetene i revisjonen er omtalt som A, B og C. Grønn farge vil si at dokumentasjon er på plass. Gult vil si at virksomhetene delvis har dokumentasjon på plass, men at det mangler noe. Rødt vil si at det foreligger betydelige mangler i dokumentasjonen.

6.1. Problemstilling 1

Har virksomhetene dokumentert et styringssystem for informasjonssikkerhet som gir grunnlag for å etablere sikkerhetstiltak som bidrar til tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i de enkelte forskningsprosjekter?

Tabellen under oppsummerer funnene i problemstilling 1.

	Virksomhet A	Virksomhet B	Virksomhet C
Definert sikkerhetsmål og sikkerhetsstrategi for forskningsprosjekter			
Databehandleravtale med TSD			
Oversikt over hvilke personopplysninger som behandles i virksomhetens forskningsprosjekter			
Risikovurderinger av sikkerhetsbrudd i forskningsprosjekter, og om det er det lagt til rette for risikovurderinger i de enkelte prosjektene			
Skriftlig dokumentert ansvarsforhold for behandling av persondata i forskningsprosjekter og skriftlige rutiner for å behandle sikkerhetsbrudd og andre avvik fra fastlagte rutiner			

Tabell 1 Funn problemstilling 1

Sikkerhetsmål og -strategi

Formålet med å behandle personopplysninger skal beskrives i et sikkerhetsmål. Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi.[5]

Revisjonen har gjennom intervjuer[6] og dokumentanalyse kontrollert styringssystemet for informasjonssikkerheten ved virksomhetene. Virksomhet B har et felles styringssystem for sikkerhet, som inkluderer informasjonssikkerhet for forskningsprosjekter på et overordnet nivå. Virksomhet C har et eget styringssystem for informasjonssikkerheten. Denne ble sist revidert i 2015. Begge styringssystemene inneholder sikkerhetsmål som blant annet omtaler formålet med behandling av personopplysninger. Hvordan virksomhetene skal oppnå sikkerhetsmålene, er omtalt i sikkerhetsstrategien.

Virksomhet A har utarbeidet en rekke frittstående dokumenter og retningslinjer som omhandler rutiner for behandling av personopplysninger i forskningsprosjekter. Dokumentene fremstår som spredt og er ikke i tilstrekkelig grad samlet på en systematisk måte. Enkelte dokumenter er 7–12 år gamle og er ikke oppdatert. Dokumentene «Prinsipper for informasjonssikkerhet» og «Policy for informasjonssikkerhet» er fra 2010, og «IT-reglementet» er fra 2005. Samlet spesifiserer og klargjør dokumentene en rekke sider ved og krav til informasjonssikkerhet i forskningsvirksomheten og omfatter generelt sikkerhetsmål og sikkerhetsstrategi.

Databehandleravtalen

Databehandlerens behandling av personopplysninger skal avtalefestes.[7] Videre fastslår loven at databehandleren ikke kan behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige, og at det i avtalen med den behandlingsansvarlige skal gå fram at databehandleren plikter å gjennomføre lovfestede sikringstiltak.[8]

Datatilsynet har utarbeidet en veileder[9] med noen punkter som er å anse som minimumskrav for hva en databehandleravtale bør inneholde:

[5] Jf. personopplysningsforskriften § 2-3 andre og tredje ledd.
[6] Intervju med de utvalgte virksomhetene.
[7] Jf. personopplysningsloven § 15.
[8] Jf. personopplysningsloven § 13.
[9] https://www.datatilsynet.no/regelverk-og-skjema/veiledere/databehandleravtale/

- Angi formålet med behandlingen
- Beskrive hvordan personopplysningene skal behandles
- Bruk av underleverandør skal reguleres i avtalen
- Ivareta den registrertes rettigheter
- Pålegge databehandleren tilfredsstillende informasjonssikkerhet
- Avtalens varighet

Revisjonen viser ved intervju[10] og gjennomgang av avtalene, med vedlegg, at alle de tre kontrollerte virksomhetene har inngått en standard databehandleravtale (rammeavtale) med TSD om behandling av personopplysninger og lagring av forskningsdata. Avtalene inneholder to vedlegg. Vedlegg 1 er en beskrivelse av teknisk løsning[11] og risikoanalyser fra TSD. Vedlegg 2 er mal for informasjon som skal sendes inn til TSD ved opprettelse av enkeltprosjekter i TSD.

Hvert forskningsprosjekt som skal bruke TSD, må utarbeide vedlegg til avtalen.[12] Vedlegget skal blant annet opplyse om sluttdato for prosjektet og gi en kort beskrivelse av de sensitive dataene som skal lagres. Det understrekes at TSD ikke under noen omstendigheter vil levere ut data til andre enn prosjektets registrerte medlemmer/brukere.

Formålet med avtalen[13] er å regulere rettigheter og plikter etter helseregisterloven og personopplysningsloven og tilhørende forskrift. TSD tilbyr lagringstjenester til forskere i Norge som forsker på personsensitive data, inkludert helsedata. Avtalene regulerer TSDs behandling og sikring av person- og helseopplysninger som den behandlingsansvarlige har gjort tilgjengelig. Virksomhet A og B inngikk avtale med TSD i 2016, mens virksomhet C inngikk avtale i november 2017.

Det går fram av avtalen[14] at databehandler (TSD) bare kan behandle personopplysninger i henhold til de formål den behandlingsansvarlige (virksomheten) har bestemt, og i samsvar med vilkårene i avtalen. Punkt 11 i avtalen omhandler bruk av underleverandører, og punkt 12 omhandler overdragelse av rettigheter og plikter.

Avtalen omhandler krav til informasjonssikkerhet[15]:

> *«Begge parter skal til enhver tid tilfredsstille krav til informasjonssikkerhet og internkontroll, samt tilgangskontroll, etter bestemmelsene i helseregisterloven, personopplysningsloven og personopplysningsforskriften. Databehandleren skal sikre at all behandling av helse- og personopplysninger som er omfattet av denne avtalen utføres i samsvar med akseptabel risikonivå definert av Behandlingsansvarlig. Som en del av dette skal Databehandler legge fram risikovurderinger av egen sikkerhet. Det forutsettes at databehandler har definert sikkerhetsmål, - strategi, - organisering og ansvar i samsvar med helseregisterloven, personopplysningsloven og personopplysningsforskriften og at dette følges opp med nødvendig internkontrollsystem.»*

I tillegg omhandler avtalens punkt 6 følgende:

- Sikkerhetsbrudd eller mistanke om sikkerhetsbrudd skal rapporteres til behandlingsansvarlige umiddelbart.
- Databehandleren skal ha klare rutiner for logg av feil og avvik i systemet.
- Avvik skal varsles senest innen 24 timer, og det skal igangsettes tiltak med en gang.
- Den behandlingsansvarlige kan til enhver tid kreve dokumentasjon for å forsikre seg om at databehandleren overholder krav til informasjonssikkerheten.
- Databehandleren skal framvise gode rutiner knyttet til informasjonssikkerhet.

<u>Oversikt over hvilke personopplysninger som behandles</u>

[10] Intervju med de utvalgte virksomhetene.
[11] Whitepaper TSD v4.4.
[12] Vedlegg 2 til avtalen.
[13] Punkt 2 i avtalen.
[14] Punkt 4 i avtalen.
[15] Punkt 6 i avtalen.

Det skal føres oversikt over personopplysninger som behandles.[16] Oversikt over hvilke personopplysninger som behandles er nødvendig for at virksomheten skal kunne ivareta pliktene sine og danner også grunnlag for utarbeidelse av virksomhetens sikkerhetsmål og sikkerhetsstrategi, i tillegg til at den vil være nødvendig ved risikovurderinger.[17]

Alle de utvalgte virksomhetene har i intervjuene opplyst at de ikke har utarbeidet en egen fullstendig oversikt over personopplysninger som behandles i forskningsprosjektene. Virksomhetene har videre opplyst at de kan hente ut oversikt over prosjektene fra databehandleren. I noen tilfeller kan virksomhetene hente ut dokumentasjon i sine egne saksbehandlingssystemer. Alle virksomhetene benytter Norsk senter for forskningsdata (NSD) som personvernombud. For prosjekter som omfattes av tjenesten til NSD, kan virksomhetene hente inn oversikt over hvilke personopplysninger som behandles i forskningsprosjekter gjennom et meldingsarkiv. Virksomhet B har opplyst at de har rutine på arkivering av dokumenter i saksbehandlingssystemet P360 og i tillegg en excel-oversikt som viser hvilke type personopplysninger som behandles, for prosjekter som ikke omfattes av tjenesten til NSD. Virksomhet B har også opplyst at de arbeider med å få satt opp en «egen» forskningsdatabase der alle forskningsprosjekter blir registrert og som vil gi nødvendige oversikter. For de to øvrige virksomhetene er det ikke dokumentert en oversikt over hvilke personopplysninger som behandles der prosjektet ikke er meldt inn til tjenesten til NSD.

Risikovurderinger – overordnet

Den behandlingsansvarlige skal gjennomføre risikovurderinger for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd, og ny risikovurdering skal gjennomføres etter endringer som har betydning for informasjonssikkerheten. Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriteriene for akseptabel risiko forbundet med behandling av personopplysninger.[18]

Revisjonen viser ved intervju[19] og dokumentanalyse av risikovurderinger at virksomhetene i varierende grad kan dokumentere at de har gjennomført risikovurderinger for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd i forskningsprosjekter. Ingen av virksomhetene har gjennomført risikovurderinger etter at de har tatt i bruk TSD.

Virksomhet B har dokumentert at det i juni 2015 ble gjennomført risikovurderinger av informasjonssikkerheten i forskningsvirksomheten, som også inneholder anbefalte nødvendige tiltak. Formålet var å identifisere, vurdere og anbefale tiltak mot hendelser som kan føre til brudd på informasjonssikkerheten til forskningsdata, og i tillegg se på hendelser som kan føre til mangelfull etterlevelse av krav som for eksempel personopplysningsloven, helseforskningsloven og helseregisterloven. Revisjonen har ikke gått videre og sett om tiltakene er iverksatt. I intervju med virksomheten har det kommet fram at det i etterkant av risikovurderingen har vært mye oppfølging i sikkerhetsarbeidet; blant annet innføringen av lagringsløsningen TSD 2.0, og at de i 2017 har satset på utvikling og bruk av nettsiden «sikresiden.no». Sikresiden.no er et nettsted som tilbyr opplæring og veiledning i hva man skal gjøre i en krisesituasjon, og i forebyggende arbeid. Løsningen er spesielt tilpasset studenter og ansatte ved universiteter og høgskoler.

Virksomhet C har opplyst i intervju at de gjennomfører helhetlige risiko- og sårbarhetsanalyser på et overordnet nivå (ROS), og at uønskede hendelser i forskningssammenheng har vært et tema i ROS. Revisjonen har mottatt dokumentasjon på ROS fra 2016 og 2017, men hendelser i forskningssammenheng har ikke vært et tema i disse ROS-analysene.

Virksomhet A har opplyst at de per i dag ikke har noen systematisk oversikt som dokumenterer risikovurdering på dette området, men at overordnede dokumenter i virksomheten sier at de skal ha en risikobasert tilnærming ved behandling av personopplysninger.

Virksomhet B og C har opplyst at de har lagt til rette for risikovurderinger i de enkelte prosjektene, og viser til dokumenter som retningslinjer, FOU-håndbok, styringssystemet og nettsider. Virksomhet C påpeker at forskningsprosjektene i mindre grad vil kunne legge fram skriftlige risikovurderinger. Ingen av virksomhetene kan dokumentere at de har oversikt over hvilke risikovurderinger som gjennomføres på prosjektnivå.

[16] I henhold til personopplysningsforskriften § 2-4.
[17] Datatilsynet - En veiledning om internkontroll og informasjonssikkerhet (2009)
[18] Personopplysningsforskriftens § 2-4 andre og tredje ledd.
[19] Intervju med de utvalgte virksomhetene.

Ansvarsforhold og rutiner for å behandle sikkerhetsbrudd og andre avvik
Det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemet.[20] Bruk av informasjonssystemet som er i strid med fastlagte rutiner, og sikkerhetsbrudd skal behandles som avvik.[21]

Revisjonen viser gjennom intervju[22] og dokumentanalyse at alle virksomhetene har formalisert at det er fordelt ansvarsforhold ved behandling av persondata i forskningsprosjekter. Det er også dokumentert at det er etablert rutiner for å behandle sikkerhetsbrudd og andre avvik.

Virksomhet A har i dokumentene «Roller og ansvar for behandling av personopplysninger» og «Retningslinjer for behandling av personopplysninger i forvaltning og forskning» beskrevet ansvarsforhold for behandling av persondata. «Retningslinjer for behandling av personopplysninger i forvaltning og forskning» omhandler også behandling av avvik.

Virksomhet B har opplyst og dokumentert at det i styringssystemet, rollekortet[23] og FOU-håndboken er beskrevet ansvarsforhold for behandling av persondata. I tillegg ligger det informasjon på nettsider om den forskningsansvarliges rolle og oppgave. Styringssystemet, rollekortet og flere nettsider omhandler også uønskede hendelser, avvik og håndtering av hendelser. Virksomheten har også opplyst at de har retningslinjer for mottak av meldinger og behandling av enkeltsaker knyttet til vitenskapelig uredelighet ved virksomheten.

Virksomhet C har gjennom styringssystemet beskrevet roller, ansvar og arbeidsoppgaver de ulike rollene i sikkerhetsorganisasjonen er pålagt å ivareta. Rektoratet er forskningsansvarlig og har det overordnede ansvaret for informasjonssikkerheten i forskningsprosjekter. Ansvaret er videre delegert til faglig ledelse (dekan) på avdelingene, som har oversikt over forskningsprosjekter og sørger for at vedtatte sikkerhetsmål, kriterier for akseptabel risiko og sikkerhetsstrategi blir fulgt opp. Styringssystemet omtaler også avviksmelding og håndtering. Virksomhet C har i tillegg prosedyrer for å følge opp avvik fra forskningsetikk, gitt i institusjonens forskningsetiske retningslinjer (før og etter en publisering). I gjennomgangen av styringssystemet har virksomhet C dokumentert hvordan et sikkerhetsbrudd i 2017 ble oppdaget, og hvordan saken ble behandlet i etterkant.

6.2. Problemstilling 2

Følger virksomhetene opp om sikkerhetsstrategien og -tiltak gir tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter, jf. personopplysningsloven § 13 og personopplysningsforskriften kapittel 2?

Tabellen under oppsummerer funnene i problemstilling 2.

	Virksomhet A	Virksomhet B	Virksomhet C
Sikkerhetsrevisjoner av organisering, sikkerhetstiltak og bruk av leverandører i egen virksomhet			
Oppfølging av TSD			I/A
Gjennomgang av sikkerhetsstrategien			

Tabell 2 Funn problemstilling 2

Sikkerhetsrevisjoner
Virksomhetene skal gjennomføre sikkerhetsrevisjoner av organisering, sikkerhetstiltak og bruk av leverandører jevnlig, og resultatet av revisjonen skal dokumenteres.[24]

Revisjonen viser gjennom intervju[25] og dokumentanalyse mangler vedrørende sikkerhetsrevisjoner for alle de utvalgte virksomhetene. De kontrollerte virksomhetene har ikke lagt fram dokumentasjon som viser at det er gjennomført sikkerhetsrevisjoner av organisering, sikkerhetstiltak og bruk av leverandører.

[20] Jf. personopplysningsforskriften § 2-7.
[21] Jf. personopplysningsforskriften § 2-6.
[22] Intervju med de utvalgte virksomhetene.
[23] Rollekortet inngår i styringssystemet.
[24] Jf. personopplysningsforskriften § 2-5.
[25] Intervju med de utvalgte virksomhetene.

Virksomhet B har dokumentert at det ble gjennomført en sikkerhetsgjennomgang i 2015 i forbindelse med utarbeidelse av styringssystemet. I etterkant av denne gjennomgangen har virksomheten satset på sikresiden.no.

Virksomhet C har opplyst at de gjennomfører sikkerhetsrevisjoner årlig på utvalgte områder.

Oppfølging av tjenesteleverandør

Den behandlingsansvarlige har ansvaret for tilfredsstillende informasjonssikkerhet. Der den behandlingsansvarlige lar databehandleren få tilgang til personopplysninger, vil den behandlingsansvarlige ha det overordnede ansvaret for at informasjonssikkerhet er tilfredsstillende.[26] Videre skal den behandlingsansvarlige etablere klare ansvars- og myndighetsforhold overfor kommunikasjonspartnere og leverandører.[27] Dette forholdet skal beskrives i en særskilt avtale. Videre skal den behandlingsansvarlige ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet. Datatilsynets veileder[28] viser til at virksomhetene skal kontrollere at rutinene for håndtering av personopplysninger og informasjonssikkerhetstiltak fungerer etter hensikten. Videre skal leverandør og virksomhet samarbeide om de sikkerhetsbrudd som kan tilskrives leverandøren. Datatilsynet anbefaler at det som ledd i virksomhetens årlige egenkontroll, bør være et møte for å gjennomgå leverandørens organisatoriske og tekniske sikkerhetstiltak.

Revisjonen viser gjennom intervju[29] og dokumentanalyse at virksomhet A og B har hatt rammeavtale med TSD siden 2016. Virksomhet C skrev under rammeavtale med TSD i november 2017 og hadde på revisjonstidspunktet ikke inngått avtaler på prosjektnivå. I intervjuene kommer det fram at ingen av de to virksomhetene som hadde avtale med TSD gjennom 2017, har hatt oppfølging av TSD etter at databehandleravtalen ble inngått, verken i form av revisjon eller andre kontrolltiltak. Virksomhet A påpeker at prosjektlederen følger opp med vedlegg til rammeavtalen, og at det ikke er rutine for videre oppfølging. Virksomhet B påpeker at databehandleravtalen følges opp ved endringer. Når de inngår rammeavtale med TSD, mottar virksomhetene risikoanalyse og beskrivelse av teknisk løsning. Ingen av virksomhetene har gitt informasjon som tilsier at det er rutine for å innhente dokumentasjon fra TSD som sikkerhetsrevisjoner, sikkerhetsstrategi, rapporter og lignende.

Gjennomgang av sikkerhetsstrategi

Bruk av informasjonssystemet skal gjennomgås jevnlig for å klarlegge om den er hensiktsmessig for virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet.[30] Resultatet fra gjennomgangen skal dokumenteres og brukes som grunnlag for eventuell endring av sikkerhetsmål og strategi.

Revisjonen viser gjennom intervju[31] og dokumentanalyse mangler ved oppfølgingen av sikkerhetsstrategien for to av virksomhetene. Virksomhet C har i intervju opplyst at de gjennomgår sikkerhetsstrategien årlig. Revisjonen har mottatt møtereferat fra gjennomgang av strategien fra 2017. Virksomhet B har opplyst i intervju[32] at strategien ble gjennomgått sammen med resten av styringssystemet på et halvdagsmøte mellom direktør for digitalisering og infrastruktur og sikkerhetsleder/fagleder i januar i 2017, men at det ikke er arkivert noen dokumentasjon fra møtet. Virksomhet A opplyser i intervju at de er i gang med å utarbeide ett nytt styringssystem, hvor det skal bli tatt inn krav om at sikkerhetsstrategien skal gjennomgås hvert andre år. Virksomhet A kan ikke dokumentere gjennomgang av sikkerhetsstrategi.

7 Konklusjoner

Formålet med personopplysningsloven er å beskytte den enkelte fra å få personvernet sitt krenket gjennom behandling av personopplysninger. Forskningsmiljøene i UH-sektoren bruker ofte eksterne tjenesteleverandører i forbindelse med behandling eller lagring av forskningsdata. Det er den behandlingsansvarlige som er ansvarlig for at kravene til informasjonssikkerheten er oppfylt, uavhengig av om en databehandler utfører oppdrag i tilknytning til informasjonssikkerheten, jf. personopplysningsloven § 13.

[26] Jf. personopplysningsloven § 13 tredje ledd.
[27] Jf. personopplysningsforskriften § 2-15.
[28] Datatilsynets: En veiledning om internkontroll og informasjonssikkerhet
[29] Intervju med de utvalgte virksomhetene.
[30] jf. personopplysningsforskriften § 2-3.
[31] Intervju med de utvalgte virksomhetene.
[32] Intervju med de utvalgte virksomhetene.

Mangelfull informasjonssikkerhet i forskningssystemer kan blant annet gi en risiko for at uautoriserte personer får tilgang til sensitiv informasjon. Å etterleve personopplysningsloven er vesentlig for tilliten til den offentlige forvaltningen. I tillegg er sikring av sensitiv informasjon vesentlig for personvernet til alle de berørte partene.

7.1. Problemstilling 1

De kontrollerte virksomhetene har i varierende grad dokumentert et styringssystem for informasjonssikkerhet som gir grunnlag for å etablere sikkerhetstiltak som gir tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter.

To av de kontrollerte virksomhetene har styringssystem for sikkerhet som inkluderer informasjonssikkerhet for forskningsprosjekter på et overordnet nivå, slik loven krever. Én virksomhet har kun utarbeidet en rekke frittstående dokumenter og retningslinjer, hvor enkelte dokumenter er 7–12 år gamle og ikke oppdatert. Kravet om å beskrive sikkerhetsmål og -strategi i personopplysningsforskriften § 2-3 andre og tredje ledd vurderer revisjonen at er delvis etterlevd for denne virksomheten og etterlevd i de to andre virksomhetene.

Det foreligger rammeavtaler mellom TSD og de tre kontrollerte virksomhetene. Avtalene er i overensstemmelse med kravene i personopplysningsloven § 15 og punktene i Datatilsynets veileder. Alle de utvalgte virksomhetene har dokumentert at ansvarsforholdet for behandling av persondata i forskningsprosjekter er formalisert, og at det foreligger skriftlige rutiner for å behandle sikkerhetsbrudd og andre avvik.

Ingen av de kontrollerte virksomhetene har utarbeidet en egen fullstendig oversikt over hvor mange prosjekter som behandler personopplysninger, hvilke typer personopplysninger som behandles eller hvordan prosjektene sikrer nødvendig konfidensialitet, tilgjengelighet og integritet for opplysningene. For å få oversikt over hvilke personopplysninger som behandles i prosjekter meldt inn til NSD, må virksomhetene hente inn informasjon fra meldingsarkivet. To av virksomhetene har ikke dokumentert oversikt over prosjekter som ikke er meldt inn til meldingsarkivet. Kravet i personopplysningsforskriften § 2-4 første ledd er kun delvis etterlevd.

De kontrollerte virksomhetene kan i varierende grad dokumentere at det er gjennomført risikovurderinger for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd i forskningsprosjekter. Én virksomhet har dokumentert at det ble gjennomført risikovurdering av forskningsvirksomheten i 2015. De to andre virksomhetene kan ikke dokumentere risikovurderinger på dette området. Ingen av virksomhetene har oversikt over hvilke risikovurderinger som blir gjennomført på prosjektnivå. Kravet i personopplysningsforskriften § 2-4 andre og tredje ledd er kun delvis etterlevd.

7.2. Problemstilling 2

Virksomhetene følger i mindre grad opp at sikkerhetsstrategien og -tiltak gir tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter, jf. personopplysningsloven § 13.

Ingen av virksomhetene kan dokumentere sikkerhetsrevisjoner av organisering, sikkerhetstiltak og bruk av leverandører og etterlever ikke kravet i personopplysningsforskriften § 2-5. Ingen av de to virksomhetene som hadde rammeavtale med TSD gjennom 2017, har hatt noen form for oppfølging av TSD etter at avtalen ble inngått. Virksomhetene har ikke tatt initiativ til handlinger for å forsikre seg om at TSD etterlever sin del av avtalen. Avtalene følges kun opp ved endringer. Kravet i personopplysningsloven § 13 tredje ledd er ikke etterlevd. Én virksomhet kan dokumentere gjennomgang av sikkerhetsstrategien i 2017. De to andre virksomhetene kan ikke dokumentere gjennomgang av sikkerhetsstrategien. Kravet i personopplysningsforskriften § 2-3 fjerde ledd er ikke etterlevd for de to virksomhetene.

7.3. Hovedkonklusjon

Målet med revisjonen er å kontrollere om utvalgte universiteter/høgskoler har dokumenterte styringssystemer som skal sørge for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i forskningsprosjekter, i samsvar med kravene i personopplysningsloven og personopplysningsforskriften.

Det er mangler ved dokumentasjonen av sentrale elementer i styringssystemet for informasjonssikkerhet ved alle de tre kontrollerte universitetene/høgskolene, som viser at virksomhetene ikke etterlever flere av kravene som følger av personopplysningsloven § 13 og personopplysningsforskriften kapittel 2.