



Til organisasjonsdirektør  
Elin Rognes Solbu

Vår saksbehandler  
Børge Sundli

Vår ref.  
20/69363  
oppgis ved alle henv.

Deres ref.

Dato  
19.05.2021

## Etterlevelseskontroll av lagring av regnskapsinformasjon

### 1. Innledning

I forbindelse med ny kommunelov er regnskapsrevisor gitt en ny oppgave fra 2019, benevnt som forenklet etterlevelseskontroll med økonomiforvaltningen. Kontrollen skal skje i forlengelsen av revisjonen av regnskapet og skal rette seg mot de delene av økonomiforvaltningen som går utover å uttale seg om årsregnskapet.

Loven forutsetter en egen uttalelse om utført arbeid med såkalt moderat sikkerhet. Kravene til denne kontrollen er definert gjennom god kommunal revisjonsskikk<sup>1</sup>. RSK 301" Forenklet etterlevelseskontroll med økonomiforvaltningen" er en ny standard gjeldende fra 2020.

Trondheim kommunerevisjon har gjennomført en forenklet etterlevelsesrevisjon av lagring av regnskapsmateriale og personopplysninger knyttet til regnskapsmateriale. Formålet med en forenklet etterlevelseskontroll etter kommuneloven, er å forebygge svakheter og bidra til å sikre at kommunen følger sentrale bestemmelser og vedtak på økonomiområdet.

I denne revisjonen har vi undersøkt om pliktig regnskapsrapportering og personopplysninger lagres i henhold til lov og forskrift.

Vi har i den sammenheng valgt ut noen vesentlige IT-systemer der vi har undersøkt om pliktig regnskapsrapportering og personopplysninger fra disse systemene lagres i henhold til bokføringsloven med forskrift og personopplysningsloven (GDPR). Vi har særlig hatt fokus på hvor dataene lagres.

Etterlevelseskontrollen formaliseres gjennom en revisoruttalelse til kontrollutvalget.

### 2. Problemstilling

Oppbevarer leverandørene til Trondheim kommune pliktig regnskapsrapportering og personopplysninger i henhold til lov og forskrift?

---

<sup>1</sup> Med god kommunal revisjonsskikk menes at revisjonen skal utføres i samsvar med den oppfatning av etiske og revisjonstekniske prinsipper for revisjon av kommuner som til enhver tid er alminnelig anerkjent og praktisert av dyktige og ansvarsbevisste utøvere av yrket.

## Kriterier:

1. Bokføringsloven med forskrift skal etterleves ved oppbevaring av pliktig regnskapsmateriale hos leverandørene.
2. Personopplysninger i tilknytning til regnskapsmateriale oppbevares i henhold til kravene i Personopplysningsloven - GDPR.

Kravet i bokføringslovens §13 er at oppbevaringspliktig regnskapsmateriale skal oppbevares i **Norge** i fem år etter regnskapsårets slutt. Oppbevaringspliktig regnskapsmateriale skal oppbevares ordnet og være betryggende sikret mot ødeleggelse, tap og endring. Regnskapsmaterialet skal kunne fremlegges for offentlig kontrollmyndighet i hele oppbevaringstiden i en form som muliggjør etterkontroll. Det skal være tilgjengelig i lesbar form og skal kunne skrives ut på papir i hele oppbevaringsperioden.

Personopplysningsloven og personvernforordningen (GDPR) gjelder ved behandling av personopplysninger. Alle virksomheter som benytter seg av en underleverandør ved databehandling har i henhold til personvernforordningen (GDPR artikkel 289 **plikt til å ha en databehandleravtale med leverandøren**. Databehandleravtalen skal sikre at personopplysninger blir behandlet i samsvar med regelverket og setter en klar ramme for hvordan databehandleren<sup>2</sup> kan behandle opplysninger. En databehandleravtale er en avtale mellom databehandler og behandlingsansvarlig<sup>3</sup> om hvordan personopplysninger skal behandles.

### 3. Metode

Metodisk baserer undersøkelsen seg på dokumentgjennomgang, intervjuer og spørreskjema. IT-systemene som inngår i undersøkelsen er valgt ut på grunnlag av vesentlighet i tallstørrelser i regnskapet og omfanget av transaksjoner.

Undersøkelsen er rettet mot flere forhold omkring lagring av regnskapsmateriale og har et særlig fokus på om hvorvidt fysisk lagringssted er innenfor lovbestemmelsene. Vi har gjennomført analyse av dokumenter i forkant av møter med kontaktpersoner, oppnevnt av Trondheim kommune. I møtet med kontaktpersonene presenterte vi problemstillinger og kriterier. Vi informerte også om etterlevelsesrevisjon generelt og de forskjellige trinnene i undersøkelsen, samt denne undersøkelsen spesifikt. Vi har også bedt kontaktpersonene om innspill til det videre arbeidet.

For å videre kartlegge situasjonen har vi sendt ut spørreskjema til tjenesteforvalterne<sup>4</sup> for de systemene som inngår i undersøkelsen. Spørsmålene som er stilt, danner hovedinndelingene i neste kapittel vedrørende gjennomføringen.

Vi har også stilt noen spørsmål til IT-tjenesten i kommunen, disse er besvart av IT-sjefen.

### 4. Gjennomføring

Med bakgrunn i dokumentgjennomgangen og svarene som er mottatt på spørreskjemaene, oppsummerer vi resultatet av gjennomføringen i dette kapitlet.

---

<sup>2</sup> Databehandler: Den som behandler personopplysninger på oppdrag fra den behandlingsansvarlige. (IT-selskap)

<sup>3</sup> Behandlingsansvarlige er "den som bestemmer formålet med behandlingen" i denne sammenheng Trondheim kommune.

<sup>4</sup> Tjenesteforvalter er en fagperson i Trondheim kommune som har ansvaret for den daglige driften av IT-systemene. Tjenesteforvalter er et bindeledd mellom leverandør og Trondheim kommune.

De ni utvalgte systemene i denne undersøkelsen er:

Systemnavn	IT-systemets oppgaver i kommunen	Regnskapsmateriale	Systemleverandør	Systemet driftes av	Hvor data lagres
LIFT	Kommunens IT-system for innkjøp, finans, regnskap og økonomi.	Kommunens regnskap og regnskapsdokumentasjon.	TietoEvry AS	TietoEvry AS	TietoEvry AS
Bluegarden (PAGA/PARF)	Kommunens lønns og HR-system.	Dokumentasjon av kommunens lønnsutbetalinger.	Visma	Visma	Digiplex skylagring
Acos	IT-system for saksbehandling og økonomi innen barnevern. Utbetaling av utgiftsdekning til oppdragstakere <sup>5</sup> i barnevernet.	Dokumentasjon av utbetaling av utgift til oppdragstakere innen barnevernet.	ACOS AS, oppkjøpt av DIPS	Sopra Steria	Digiplex skylagring
Boei	Husleiesystem for utleie av kommunale boliger. Utfakturering av husleie.	Fakturering av husleie for kommunale boliger. Reskontro for leietakerne.	Arnett AS	Sopra Steria	Digiplex skylagring
Escali	Porteføljesystem for verdipapirer og lån.	Kommunens portefølje av verdipapirer.	Escali	Escali	Microsoft Azure Nettsky
Gerica	Pasientjournalsystem for pleie-, rehabiliterings- og omsorgstjenesten. Fakturering av egenandeler til mottakere av helsetjenester i kommunen.	Fakturagrunnlag egenandeler for helse og velferdstjenester.	TietoEvry AS	Sopra Steria	Digiplex skylagring
Tilskuddsbasen	Behandling og godkjenning av vedtak om tilskudd fra kommunen til organisasjoner.	Vedtak om tilskudd fra kommunen.	Bouvet via underlev. Visolit	Sopra Steria	Digiplex skylagring
Velferd	IT-system for utbetalinger av økonomisk sosialhjelp. Saksbehandling og integrasjon mot økonomi- og lønnsystem.	Dokumentasjon av utbetalt økonomisk sosialhjelp.	Visma	Sopra Steria	Digiplex skylagring
Vigilo	IT-system for administrasjon og kommunikasjon barnehage og SFO. Utfakturering av kontingent og kostpenger barnehage og SFO.	Grunnlag for utfakturering av kontingent og kostpenger barnehage og SFO.	Vigilo	Vigilo	Microsoft Azure Nettsky

<sup>5</sup> Oppdragstakere i Trondheim kommune innen barnevern: fosterforeldre, besøkshjem, husverter og tilsynspersoner.

## 4.1 Oppbevarers kommunens regnskapsmateriale i henhold til kravene i bokføringsloven?

Bokføringsloven med forskrift gir bokføringspliktige adgang til å oppbevare elektronisk regnskapsmateriale i andre EØS-stater. En forutsetning er at avtale eller overenskomst med det aktuelle landet sikrer norske skatte- og avgiftsmyndigheter tilfredsstillende adgang til regnskapsinformasjonen for kontrollformål i oppbevaringstiden, og at slik oppbevaring ikke vil være til hinder for effektiv norsk politietterforskning. Regnskapsmaterialet skal være tilgjengelig i lesbar form og skal kunne skrives ut på papir fra terminal eller lignende i Norge i hele oppbevaringsperioden. Den bokføringspliktige skal skriftlig informere Skattedirektoratet om hvilket regnskapsmateriale som oppbevares i utlandet, hvor regnskapsmaterialet oppbevares, og hvordan kontrollmyndighetene til enhver tid kan få adgang til regnskapsmaterialet. Oppbevaringstiden skal som et minimum følge bokføringsloven § 13 annet ledd og reglene i denne forskrift selv om oppbevaringstiden er en annen etter det aktuelle lands lovgivning. Skattedirektoratet fastsetter forskrift om hvilke EØS-land som til enhver tid oppfyller vilkårene etter lovens krav. Ved lagring i utlandet må de bokførte opplysningene være tilgjengelig gjennom terminal eller lignende i Norge.

De fleste vesentlige IT-systemene som Trondheim kommune benytter i tjenesteproduksjonen har den senere tiden i stor grad blitt flyttet fra lokal drift og lagring, over til såkalte skyløsninger<sup>6</sup>. I praksis innebærer dette at man overlater drift av systemer og lagring av data til eksterne aktører, som igjen har ulike løsninger for driftsmiljø og datalagring. For å sikre lovmessig drift av systemer og lagring av data, er det avgjørende at overholdelse av lovkrav avklares med den eksterne tjenesteleverandøren og sikres gjennom gode avtaler som er tilpasset Trondheim kommunes løpende behov.

Gjennomgangen vår viser at systemene vi har undersøkt har mer eller mindre forskjellig løsning når det gjelder driftsarkitektur. Vi ser også at data for alle de undersøkte systemene lagres hos eksterne leverandører. Avtalene som er inngått varierer imidlertid når det gjelder lagringssted, løsninger og arkitektur.

Resultatet av dokumentanalyse og spørreundersøkelse viser at "fysisk lagringssted" består av flere forskjellige skylagringssteder for de undersøkte systemene, hvor Digiplex skylagring fremhever seg som vesentlig.

### **LIFT**

Tjenesteforvalter for LIFT i kommunen og leverandøren TietoEvry AS opplyser at det er sikret at kommunens regnskapsdata lagres i Norge. Dette er spesifisert nærmere i avtalen mellom kommunen og leverandøren i sikkerhetsdokumentet "ASP/SAAS Unit4 ERP". Regnskapsdataene fra LIFT lagres hos TietoEvry AS i to datahaller på samme geografiske lokasjon i Gjøvik. Disse to datahallene er uavhengige av hverandre og kan dermed betraktes som to geografisk adskilte lokasjoner. Dette utgjør en ekstra sikkerhet. TietoEvrys driftssenter på Gjøvik består totalt av tre separate bygg; der to av disse byggene er inne i fjell.

### **Bluegarden, Acos, Boei, Gerica, Tilskuddsbasen og Velferd**

Seks av de ni systemene som inngår i denne undersøkelsen, har sine data lagret på servere hos skylagringselskapet Digiplex. Digiplex er et av de største skylagringsstedene som har datasentre i Norden, beliggende i Oslo, Stockholm og København. Digiplex har også inngått en avtale med skylagringselskapet Megaport som har base i Australia, og som har lokasjoner over hele verden. Bluegarden ble kjøpt opp av Visma fra Evry (nå TietoEvry AS), mens datalagringen for systemet fortsatt er hos TietoEvry AS på Fet i Norge. TietoEvry AS benytter Digiplex som skylagringssted blant annet for Bluegarden.

---

<sup>6</sup> Skyløsninger: Skylagring er en tjeneste der du lagrer data ved å overføre dem over Internett eller et annet nettverk til et eksternt lagringssystem som vedlikeholdes av en tredjepart.

Systemene Acos, Boei, Gerica, Tilskuddsbasen og Velferd driftes for kommunen av IT-selskapet Sopra Steria. Dataene fra disse fire systemene lagres i to kopier i to adskilte datasentre hos Sopra Steria i Oslo. Sopra Steria leier plass til serverne de benytter, i datasentrene til skylagringselskapet Digiplex. For Tilskuddsbasen lagres også noe data i Trondheim i Tungaveien.

#### **Escali og Vigilo**

Microsoft Azure Nettsky er et annet skylagringssted der data fra Trondheim kommune lagres. Data fra systemene Escali og Vigilo lagres i denne nettskyen.

**Escali:** Data i form av elektroniske dokumenter og elektroniske bilag oppbevares i Norge. Ekstra backup av data oppbevares på Bønes utenfor Bergen. Selve datasystemet lagres i Nederland.

**Vigilo:** Vigilo lagres også i Microsoft Azure Nettsky. De serverne som benyttes for Vigilo er lokalisert hos Sysco AS på Stord i Norge.

#### **Konklusjon:**

Undersøkelsen av lagring av regnskapsmateriale for de ni utvalgte IT-systemene viser at Trondheim kommune for disse systemene overholder Bokføringslovens krav til lagring av regnskapsinformasjon i Norge.

Digiplex sin størrelse og globale tilknytning gjør at kommunen bør ha fokus på at kommunens data beskyttes tilstrekkelig og ikke eksponeres på en slik måte at det utgjør en risiko for kommunens tjenesteproduksjon. Det er samtidig viktig å sikre at valg av lokasjon for lagring av data ikke fører til lovbrudd. Et lovbrudd her kan være at lovkrav til sted for fysisk oppbevaring av elektronisk regnskapsmateriale ikke overholdes ved at det lagres utenfor EØS-stater.

## **4.2 Inneholder avtalen med systemleverandører bestemmelser om lagring av kommunens data dersom systemet avsluttes eller leverandøren blir kjøpt opp eller inngår samarbeide med andre leverandører?**

I henhold til bokføringslovens §13 skal oppbevaringspliktig regnskapsmateriale oppbevares i Norge i fem år etter regnskapsårets slutt. Det er derfor viktig at kommunen sikrer at regnskapsmateriale lagres i henhold til bokføringsloven krav de første fem årene etter at systemet avsluttes.

Når det gjelder oppbevaring av regnskapsdata har vi innhentet informasjon fra kommunens IT-tjeneste. Ansvaret for bevaring av regnskapsdata i de enkelte IT-systemene ligger hos kommunens tjenesteforvalter for det enkelte systemet. Driftsavtalen for systemene legger til rette for dette med bestemmelser knyttet til deponering av data og bistand rundt dette. Det som har en bevaringsverdi, herunder regnskapsmateriale overleveres Byarkivet for deponering. Dette er altså noe som tjenesteforvalter i kommunen for IT-systemet har ansvar for å bestille, driftsleverandøren har ikke ansvar for å passe på dette.

#### **LIFT**

Avtalen mellom systemleverandøren TietoEvry AS og kommunen omtaler eiendomsretten til kommunens data. Trondheim kommune beholder eiendomsretten til alle data som overlates til systemleverandøren for behandling og lagring. TietoEvry AS har tilgang til data kun i den utstrekning som er nødvendig for at de skal kunne oppfylle sine forpliktelser i henhold til avtalen. Leverandøren har ikke under noen omstendighet rett til å utøve tilbakeholdsrett i kundens data.

#### **Bluegarden**

Ved avslutning av avtalen mellom kommunen og leverandøren Bluegarden, uansett årsak, skal leverandøren stille nødvendige tjenester til rådighet for kommunen i avviklingsperioden. Bluegarden skal

også bistå kommunen i forbindelse med forberedelsene til inngåelse av avtale med ny systemleverandør og levere den informasjon som er nødvendig i forbindelse med slik forberedelse. Leverandøren er også forpliktet til å bidra med kompetanseoverføring til ny vedlikeholdsorganisasjon. Detaljert beskrivelse av leverandørens forpliktelser er gitt i avtaletekst.

### **Acos og Boei**

Revisjonen har etterspurt men ikke mottatt informasjon om kommunen har avtale med systemleverandøren Acos/ Dipps og Arnett for Boei, som inneholder bestemmelser om lagring av kommunens data dersom systemene avsluttes eller leverandøren blir kjøpt opp eller inngår samarbeide med andre leverandører. Disse to systemene driftes imidlertid av Sopra Steria for Trondheim kommune og data fra disse systeme lagres der. I avtalen mellom kommunen og Sopra Steria er det krav om at Sopra Steria skal tilby langtidslagring av data fra de ulike systemene de drifter for kommunen.

### **ESCALI**

For Escali har vi fått opplyst at alle backup'er for systemet slettes umiddelbart etter at kunden har avsluttet kundeforholdet. Kunden kan be om backup av databasen før kundeforholdet avsluttes. Ifølge avtalen mellom kommunen og Escali har kommunen eiendomsretten til dataene, mens Escali eier programvaren. Alle data behandles konfidensielt. Avtalen med Escali har ingen punkter som vedrører oppkjøp eller samarbeid med andre leverandører.

### **Gerica**

Avtalen mellom kommunen og systemleverandør av Gerica har bestemmelser om opphør av avtale, uansett årsak. Leverandør er forpliktet til å bistå ved overgang eller avslutning av systemet eller kundeforholdet. Avtalen med Sopra Steria som drifter Gerica inneholder bestemmelser om tilgjengelighet/kopi av database. Tjenesteforvalter har ikke svart på hva som skjer ved et eventuelt oppkjøp av systemet.

### **Tilskuddsbasen**

Tjenesteforvalter for systemet Tilskuddsbasen i kommunen oppgir at oppkjøp av leverandør eller samarbeid med andre leverandører ikke skal påvirke avtaleforholdet de har med systemleverandøren i dag. Det er tjenesteforvalter i kommunen som har ansvar for å bestille deponering av systemet og arkivering av arkivverdige opplysninger. Alle arkivverdige opplysninger fra Tilskuddsbasen arkiveres også fortløpende automatisk i TKSak7 og er dermed tilgjengelig for kommunen der. Tilskuddsbasen driftes av Sopra Steria og i avtalen mellom kommunen og Sopra Steria er det krav om at Sopra Steria skal tilby langtidslagring av data fra de ulike systemene de drifter for kommunen.

### **Velferd**

Tjenesteforvalter for systemet Velferd i kommunen opplyser at for Visma Velferd og Visma VSA<sup>8</sup> vil data ved opphør eller oppkjøp av system ligge i to databaser (Velferd og VSA Noark 5). Disse databasene vil være tilgjengelig, eventuelt bli tilgjengelig i arkiveringskopi eller ved deponering av data. Det foreligger ikke noen avtale på dette mot leverandøren Visma i og med at systemleverandøren ikke disponerer kommunens data. Lagring av data inngår i driftsavtalen med Sopra Steria.

### **Vigilo**

Avtalen mellom kommunen og systemleverandøren Vigilo omhandler partenes plikter i avslutningsperioden. Leverandøren Vigilo har plikt til å legge til rette for at kommunens data blir overført til kommunen, eller til tredjepart utpekt av kommunen.

Avtalen mellom kommunen og Vigilo omhandler også overdragelse av rettigheter og plikter. Leverandøren kan bare overdra sine rettigheter og plikter etter avtalen med skriftlig samtykke fra kunden. Dette gjelder

---

<sup>7</sup> Kommunens saksbehandlings- og arkivsystem

<sup>8</sup> Visma Samhandling Arkiv, sikker digital arkivering av personsensitiv informasjon

også hvis leverandøren deles i flere selskaper, eller hvis overdragelsen skjer til et datterselskap eller annet selskap i samme konsern, men ikke dersom leverandøren slås sammen med et annet selskap. Samtykke kan ikke nektes uten saklig grunn. Retten til overdragelse i avsnittet over gjelder kun hvis den nye leverandøren oppfyller de opprinnelige kvalifikasjonskravene, det ikke foretas andre vesentlige endringer i kontrakten og overdragelse ikke skjer for å omgå regelverket om offentlige anskaffelser.

**Konklusjon:****Avslutning av systemet**

For systemene Acos og Boei har revisjonen etterspurt, men ikke mottatt informasjon om kommunen har avtale med systemleverandørene som inneholder bestemmelser om lagring av kommunens data dersom disse systemene avsluttes. Dette dekkes imidlertid av driftsavtalen mellom Sopra Steria og Trondheim kommune.

De øvrige sju undersøkte systemene har alle avtaler som sikrer kommunen eiendomsretten til egne data ved avvikling av systemløsningen. Det er imidlertid ulik beskrivelse av avslutningsprosedyrene. Geric, Tilskuddsbasen og Velferd driftes av Sopra Steria og i avtalen mellom kommunen og Sopra Steria er det krav om at Sopra Steria skal tilby langtidslagring av data fra disse systemene.

**Oppkjøp av leverandør eller leverandøren inngår samarbeid med andre leverandører**

Det er for ingen av de ni systemene som er med i denne undersøkelsen besvart om avtalene med systemleverandøren inneholder informasjon om sikring av kommunens data dersom systemleverandøren kjøpes opp av et annet firma eller inngår samarbeid med annen leverandør.

### 4.3 Oppbevares personopplysninger i tilknytning til regnskapsmaterialet i henhold til kravene i personopplysningsloven - GDPR?

Alle virksomheter som benytter seg av en underleverandør ved databehandling har i henhold til personvernforordningen (GDPR artikkel 28) plikt til å ha en databehandleravtale med leverandøren. Databehandleravtalen skal sikre at personopplysninger blir behandlet og lagret i samsvar med regelverket. EUs personvernforordning GDPR gjelder for EØS-området. Det inkluderer alle EU-land, Island, Liechtenstein og Norge. Alle landene innenfor EU/EØS-området har gjennomført personvernforordningen og slik sikret at personopplysninger behandles forsvarlig. Derfor kan man fritt overføre personopplysninger til disse statene forutsatt at personopplysningslovens øvrige vilkår er oppfylt.

Kommunen må undersøke om databehandler som skal behandle personopplysninger oppfyller kravene i personopplysningsloven (GDPR personvernforordningen) og at de har etablert tilfredsstillende sikkerhetstiltak. I dette inngår også om databehandler har tilstrekkelig dybdekunnskap om personvernregelverket, er pålitelig og har tilstrekkelige ressurser til å sikre en forsvarlig behandling av bedriftens personopplysninger. Det er bare "tillatt" å benytte databehandlere som gir "tilstrekkelige garantier" for at personopplysningene vil bli behandlet forsvarlig og i henhold til kravene i GDPR. Dette betyr at bedriften må vurdere databehandlers egnethet før løsningen tas i bruk og før personopplysningene kan overføres til databehandlers systemer. Kommunen må inngå databehandleravtaler som oppfyller kravene i GDPR. Databehandler skal også inngå databehandleravtale med alle sine underleverandører (underdatabehandlere).

Det er sju av de ni systemene vi har sett på i denne undersøkelsen hvor det det lagres personopplysninger. Disse systemene er Lift, Bluegarden, Acos, Geric, Tilskuddsbasen, Velferd og Vigilo. Vi har stilt tjenesteforvalterne spørsmål om databehandlerne for disse systemene oppfyller Personopplysningslovens krav med hensyn til lagring av data.

**LIFT**

Trondheim kommune har inngått databehandleravtale med systemleverandøren Tieto Evry AS i 2019. Gjeldende lovverk og råd fra tilsynsmyndigheter er lagt til grunn for avtalen mellom leverandøren Tieto Evry og Trondheim kommune. Personvernforordningen GDPR er spesifikt nevnt som lovgrunnlag.

I driftsavtalen mellom TietoEvro og kommunen er det et sikkerhetsdokument med et punkt om internkontroll iht Personopplysningsloven. Det kreves i avtalen at alle ansatte fra TietoEVRY og underleverandører undertegner taushetserklæring ved ansettelse. Sikkerhetsdokument for LIFT slår fast at hovedregelen for personopplysninger er at disse ikke skal lagres eller behandles utenfor EU/EØS-området uten særskilt dataeksportavtale.

**Bluegarden**

Det er inngått en databehandleravtale mellom kommune og systemleverandøren Visma i 2018, med et endringstillegg fra 2019. Gjeldende lovverk og råd fra tilsynsmyndigheter er lagt til grunn for avtalen. Personvernforordningen GDPR er spesifikt nevnt som lovgrunnlag.

Ifølge inngått avtale kan databehandler Visma/Bluegarden ikke la behandling og lagring av personopplysninger foregå utenfor EU/EØS uten skriftlig samtykke fra behandlingsansvarlig, som er Trondheim kommune.

**Acos, Geric, Tilskuddsbasen og Velferd**

Sopra Steria er databehandler for og drifter systemene Acos, Geric, Tilskuddsbasen og Velferd for Trondheim kommune. Kommunen har inngått databehandleravtale med Sopra Steria i 2021. Kommunens IT-tjeneste forvalter avtalen med driftsselskapet Sopra Steria. IT-tjenesten opplyser at driftsavtalen og databehandleravtalen med Sopra Steria ivaretar kravene til sikkerhet i henhold til personopplysningsloven og GDPR.

IT-sjefen i Trondheim kommune har opplyst at alle systemene som driftes gjennom avtalen med Sopra Steria skal tilfredsstillere kravene til:

- sikkerhetstiltak med tanke på teknisk sikkerhet og prosessikkerhet.
- dybdekunnskap om personvernregelverket hos leverandøren.
- leverandøren har både pålitelig og nok ressurser for å sikre forsvarlig behandling av alle type opplysninger.

Ved gjennomgang av databehandleravtalen med Sopra Steria går det frem at data lagres i Norge, mens tilgang, overvåking, support og vedlikehold utføres fra annet EØS-land.

**Vigilo**

Kommunen har inngått en databehandleravtale med systemleverandøren Vigilo. I denne avtalen står det spesifisert at lagring av data fra Vigilo skal skje innenfor EU/ EØS - området. Databehandleravtalen skal sikre at data behandles i henhold til personopplysningsloven og GDPR.

**Konklusjon:**

Det er inngått databehandleravtaler med tjenesteleverandørene som lagrer personopplysninger for de sju IT-systemene som inngår i denne undersøkelsen.

**LIFT**

Vi mener at databehandleravtalen mellom kommunen og TietoEvry oppfyller kravene i Personopplysningsloven. Det er avtalt tilfredsstillende sikkerhetstiltak, kunnskap om personvernregelverket og tilstrekkelige ressurser til å sikre en forsvarlig behandling av Trondheim kommunes personopplysninger.



**Bluegarden**

Revisjonen mener at databehandleravtalen mellom kommunen og Visma oppfyller kravene i Personopplysningsloven. Det er avtalt tilfredsstillende sikkerhetstiltak, kunnskap om personvernregelverket og tilstrekkelige ressurser til å sikre en forsvarlig behandling av Trondheim kommunes personopplysninger for Bluegarden.

**For Acos, Gerica, Tilskuddsbasen og Velferd** som driftes av Sopra Steria, mener vi også at databehandler oppfyller kravene i Personopplysningsloven og at avtalene tilfredsstillende sikkerhetstiltak, kunnskap om personvernregelverket og tilstrekkelige ressurser til å sikre en forsvarlig behandling av Trondheim kommunes personopplysninger.

**For Vigilo** har kommune inngått databehandleravtale med systemleverandøren og det er spesifisert at lagring av data fra Vigilo skal skje innenfor EU/ EØS - området i henhold til kravene i personopplysningsloven og GDPR.

Vi ber om tilsvarende innen 27. mai. Revisorsuttalelsen skal til behandling i Kontrollutvalget 7. juni 2021.

Med hilsen

Per Olav Nilsen  
revisjonsdirektør

Børge Sundli  
revisor/CISA

*Elektronisk dokumentert godkjenning uten underskrift*

Kopimottaker: Postmottak Organisasjonsdirektøren  
Tove Tveråmo  
Ole Bjørn Nordland  
Unn Elisabeth Huse