Riksrevisjonen

Revisjonsrapport for 2017 om sikring av personopplysninger i Direktoratet for økonomistyring

Mottaker: Finansdepartementet (FIN)

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.

Forsidefoto: Blue Coat Photos/Flickr

Innhold

1 Sammendrag

Riksrevisjonen har gjennomført en revisjon av Direktoratet for økonomistyring (DFØ) der målet har vært å kontrollere om DFØ sørger for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i lønns- og personalsystemet SAP.

DFØ leverer lønnstjenester til et stort antall statlige virksomheter og i dette arbeidet behandler DFØ personopplysninger på vegne av virksomhetene. DFØ har satt ut driften av lønns- og personalsystemet til leverandøren Evry. Det er av vesentlig betydning, både for både for enkeltmennesker og for virksomhetene, at personopplysninger som blir samlet inn og behandlet blir sikret på best mulig måte. Dersom personopplysninger kommer på avveie eller blir misbrukt, kan det få store konsekvenser for den det gjelder, for eksempel i form av identitetstyveri eller innsyn i personlige forhold som kan oppleves som belastende.

Revisjonen viser at det er svakheter ved flere sider av DFØs arbeid med å sikre personopplysningene:

- DFØ har ikke dokumentert oversikt over det samlede risikobildet for behandlingen av personopplysninger.
- DFØs sikkerhetstiltak gir ikke tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i lønnssystemet SAP.
- DFØs oppfølging av iverksatte tiltak og oppfølgingen av leverandøren Evry er mangelfull.

Funnene fra revisjonen gjør at DFØ på flere områder vurderes å ikke etterleve relevante krav i personopplysningsloven og forskriften vedrørende sikring av personopplysningene i SAP. Dette øker risikoen for at personopplysninger kan komme på avveie eller misbrukes.

DFØ er en viktig tjenesteleverandør i norsk forvaltning og er ekspertorgan for økonomi- og virksomhetsstyring i staten. Det er av vesentlig betydning at DFØ, som leverandør av lønnstjenester til et stort antall statlige virksomheter, har innrettet arbeidet med informasjonssikkerhet på en slik måte at krav i personopplysningsregelverket etterleves. For DFØs kunder er det av avgjørende betydning at de kan føle seg trygge på at DFØ behandler og lagrer personopplysningene til deres ansatte på en sikker måte, og at behandlingen er i tråd med eksisterende og framtidig regelverk.

2 Innledning

Direktoratet for økonomistyring (DFØ) er statens ekspertorgan for økonomi og virksomhetsstyring, og utfører forvaltningsoppgaver for mange statlige virksomheter. DFØ skal levere fellestjenester på økonomiområdet som skal gi staten stordriftsfordeler.[1]

En viktig oppgave for DFØ er å levere gode lønnstjenester. Hver måned utfører DFØ lønnsutbetalinger for 79 000 ansatte i 171 statlige virksomheter.[2] DFØ må håndtere og behandle store mengder personopplysninger for at den enkelte arbeidstaker skal få utbetalt lønnen sin.

Personopplysninger er opplysninger og vurderinger som kan knyttes til en enkeltperson. På lønnsområdet behandler DFØ personopplysninger som navn, adresse, fødsels- og personnummer, kontonummer, lønn, lønnstrekk, skatteopplysninger og fagforeningstilhørighet.

Sikker ivaretakelse og behandling av personopplysninger er av vesentlig betydning for enkeltmenneskets personvern. Dersom personopplysninger kommer på avveie eller blir misbrukt, kan det få store konsekvenser for den det gjelder, for eksempel i form av identitetstyveri eller innsyn i personlige forhold som kan oppleves som

[1] Direktoratet for økonomistyring (2017) *Årsrapport 2016*.
[2] DFØ leverer lønnstjenester til 171 statlige virksomheter, jf. DFØs kundekartleggingsskjema for lønn per oktober 2017.

belastende. Personopplysninger på avveie kan dessuten medføre svekket omdømme og tap av tillit for virksomhetene som har mistet informasjonen.

Behandling av personopplysninger skjer ofte i ulike ikt-systemer. DFØ benytter datasystemet SAP til å beregne og utbetale lønn.[3] Driften av SAP er satt ut til leverandøren Evry, som igjen benytter IBM som underleverandør.[4] Ivaretakelsen av personopplysningene i SAP er dermed avhengig av informasjonssikkerheten hos DFØ, Evry og IBM.[5]

Riksrevisjonen har de siste årene gjennomført flere revisjoner av informasjonssikkerhet hvor det er avdekket vesentlige svakheter. I 2012 gjennomførte Riksrevisjonen en revisjon av informasjonssikkerheten i SAP i DFØ, som blant annet viste svakheter vedrørende sikkerhetsrevisjoner, risikovurderinger og brukertilganger.[6]

Stortingets kontroll- og konstitusjonskomité deler Riksrevisjonens bekymring for svakheter ved informasjonssikkerheten i statlige virksomheter og understreker at mangelfull styring og oppfølging av informasjonssikkerhet er svært alvorlig.[7] Nasjonal sikkerhetsmyndighets årlige undersøkelse av risiko og sårbarheter i Norge, viser at det er risiko forbundet med bruk av informasjonsteknologi på alle nivåer i samfunnet, og at risikoen er høy og økende.[8] En rekke mediesaker i 2017 viser at outsourcing av ikt-tjenester utgjør en risiko for at personopplysninger havner i feil hender.[9]

Utkast til revisjonrapport er forelagt Finansdepartementet i brev av 23. mars 2018. Departementet har i svar av 27. april 2018 gitt kommentarer til rapportutkastet. Som vedlegg til departementets svar følger brev av 24. april 2018 fra DFØ til Finansdepartementet med DFØs kommentarer til rapportutkastet. Det er foretatt enkelte endringer i rapportens kapittel 6 på grunnlag av tilbakemeldingene fra DFØ og departementet.

3 Revisjonens mål og problemstillinger

Målet med revisjonen er å kontrollere om DFØ sørger for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i lønns- og personalsystemet SAP, i henhold til krav i personopplysningsloven med forskrift og anbefalinger i anerkjente standarder.

Revisjonen har følgende problemstillinger:

1. *Har DFØ etablert et grunnlag for å planlegge sikkerhetstiltak som sørger for tilfredsstillende informasjonssikkerhet for personopplysninger i SAP?*

Problemstillingen omfatter DFØs arbeid med sikkerhetsmål og sikkerhetsstrategier, DFØs risikovurderinger av behandling av personopplysninger, avtaleverket som regulerer forholdet mellom DFØ og kundene og DFØ og leverandøren Evry, samt ansvars- og myndighetsforhold for sikkerhetsarbeidet og for lønnssystemet SAP.

2. *Har DFØ sikret at det gjennomføres systematiske tiltak som sørger for tilfredsstillende informasjonssikkerhet for personopplysninger i SAP?*

Problemstillingen omhandler tiltak som skal sikre personopplysningene i SAP og den underliggende infrastrukturen. Dette gjelder blant annet oppsett av systemet, autorisasjon og rettigheter, autentisering, systemoppdateringer og logging.

---

[3] SAP er modulbasert og leverer programvare, blant annet for regnskap og økonomi, inkludert lønn og personalhåndtering (SAP HR).
[4] Evry er Norges største IT-selskap. Selskapet leverer IT-tjenester til bank og finans, kommuner og statlig sektor, helse, olje og gass, samt prosessindustri og produksjon.
[5] Informasjonssikkerhet er en samlebetegnelse for krav til påliteligheten og sikkerheten som knyttes til overføring og lagring av informasjon. Kilde: https://snl.no/informasjonssikkerhet
[6] Riksrevisjonen (2012) *Sikkerhetsrevisjon av SAP*. Brev til DFØ 8. mars 2012.
[7] Innst.115 S (2017–2018) *Innstilling til Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2016*.
[8] Nasjonal sikkerhetsmyndighet (2017): *Risiko 2017 - Risiko og sårbarheter i en ny tid*.
[9] NRK, nettutgave (24.05.2017) Setter helse-utflagging på vent etter journalskandalen. <https://www.nrk.no/norge/rapport_-helse-sor-ost-mangler-kontroll-pa-pasientinformasjon-1.13530127> og NRK, nettutgave (24.07.2017) *Dette har skjedd i den svenske IT-skandalen*. <https://www.nrk.no/urix/dette-er-den-svenske-it-skandalen-1.13614666>

3. *Følger DFØ opp at sikkerhetsstrategi og iverksatte tiltak for informasjonssikkerhet i egen virksomhet og hos leverandøren Evry fungerer som forutsatt?*

Denne problemstillingen legger vekt på hvordan DFØ følger opp at sikkerhetstiltak som er besluttet, faktisk er satt i verk og fungerer etter hensikten. Videre vil vi se på hvordan DFØ følger opp leverandøren Evry og forsikrer seg om at Evry har en informasjonssikkerhet som verner om personopplysninger.

Avgrensning av revisjonen
Revisjonen er begrenset til hvordan DFØ sikrer behandlingen av personopplysninger i lønnssystemet SAP med underliggende infrastruktur, inkludert databaser, servere og filsystemet Opal_con.

Revisjonen tar utgangspunkt i gjeldende regelverk i 2017. EU-forordning 2016/679 (personvernforordningen/GDPR) trer i kraft i EU 25. mai 2018. Det er foreløpig ikke klart når den blir implementert i norsk lov.[10] Forordningen er en videreføring av tidligere regelverk, men den inneholder flere detaljreguleringer og innstramminger i tillegg til noen nye prinsipper for behandling av personopplysninger.

4 Metodisk tilnærming og gjennomføring

Problemstillingene er besvart gjennom dokumentanalyser, intervjuer og analyse av datauttrekk fra SAP og underliggende databaser og servere. Det ble avholdt et innledende kartleggingsmøte med DFØ 15. juni 2017 og et oppstartsmøte for revisjonen med DFØ og Finansdepartementet 15. september 2017. Videre ble det avholdt et oppsummeringsmøte med Finansdepartementet og DFØ 4. april 2018. Det er ikke utabeidet referater fra disse møtene.

4.1. Metode, problemstilling 1 og 3 – planlegging og oppfølging av sikkerhetstiltak

For å besvare problemstillingene er det gjennomført dokumentanalyser og intervju.

4.1.1. Dokumentanalyse

Formålet med dokumentanalysene er å undersøke DFØs gjennomføring og dokumentasjon av arbeidet med informasjonssikkerhet, inkludert utarbeidelse av sikkerhetsmål- og sikkerhetsstrategi, klassifisering og oversikt over personopplysninger, risikovurderinger, utarbeidelse og innhold i databehandleravtaler og ansvars- og myndighetsforhold for sikkerhetsarbeidet og lønnssystemet SAP. Følgende dokumenter er gjennomgått og analysert:

- styrende dokumenter
  - styringssystem for informasjonssikkerhet, datert 6. mai 2014
  - sikkerhetspolicy, datert 24. februar 2015
  - organisering av sikkerhets- og beredskapsarbeidet – roller og ansvar, datert 16. mai 2017
  - sikkerhetsstandard, datert 16. desember 2013
- klassifisering/oversikt over personopplysninger
  - informasjonsaktiva, datert 15. juni 2017
- risikovurderinger
  - halvårsrapport fra DFØ til FIN 2017
  - virksomhetsplan 2017 for lønnsavdelingen
  - Devoteam: «Vurdering av risiko forbundet med behandling av personopplysninger i DFØ» (2013)
- avtaler
  - driftsavtale mellom DFØ og Evry av 18. juni 2016, med bilag
  - driftsavtale (standardavtalen) mellom DFØ og kundene, med vedlegg

[10] Justis- og beredskapsdepartementet arbeider for tiden med å gjennomføre EUs personvernforordning (GDPR) i norsk rett og innlemme forordningen i EØS-avtalen, jf. Justis- og beredskapsdepartementet (06.03.2018) *Ny personopplysningslov og innlemmelse i EØS-avtalen*. <https://www.regjeringen.no/no/tema/lov-og-rett/innsikt/ny-personopplysningslov-og-innlemmelse-i-eos-avtalen/id2592984/>

- ansvars- og myndighetsforhold
    - DFØ: beslutningssak til ledergruppen – fordeling av systemroller, datert 7. mai 2017
    - DFØ: oversikt over systemer og systemroller, sist oppdatert 24. november 2017
- andre dokumenter
    - IT-styring, evaluering utført av KPMG, datert 7. juli 2017
    - DFØ: migreringsplan for HANA-prosjektet, mottatt 15. februar 2018
    - referat fra etatsstyringsmøter mellom departementet og DFØ våren og høsten 2017
    - DFØ: orienteringssak til ledergruppen – sikkerhetshendelser første halvår 2017, datert 30. august 2017

4.1.2. Intervju

Det ble avholdt intervju med DFØ 1. november 2017 for områdene omfattet av problemstilling 1 og 3. Formålet med intervjuet var å sikre korrekt forståelse av mottatt dokumentasjon, få utfyllende informasjon om tiltak og rutiner og foreta aktuelle avklaringer. Fra DFØ deltok representanter fra lønnsavdelingen, juridisk stab og sikkerhetsleder. Referatet fra intervjuet er verifisert av DFØ.

4.2. Metode, problemstilling 2 – gjennomføring av sikkerhetstiltak

For å besvare problemstillingen er det gjennomført dokumentanalyse, datauttrekk og -analyse samt intervjuer.

4.2.1. Dokumentanalyse

Formålet med dokumentanalysene er å undersøke om DFØ har dokumentert krav til gjennomføring av sikkerhetstiltak på områder omfattet av revisjonen. Følgende dokumenter er benyttet i denne problemstillingen:

- driftsavtale mellom DFØ og Evry av 18. juni 2016:
    - bilag 1 – kundens kravspesifikasjon
    - bilag 2 – leverandørens løsningsspesifikasjon
    - bilag 2 – vedlegg 1 – utfylt kravspesifikasjon
- IT-styring, evaluering av KPMG datert 7. juli 2017
- halvårsrapport fra DFØ til FIN 2017
- månedlig rapportering fra Evry til DFØ om bruk av upersonlige brukerkontoer
- rapporter fra SAP-systemet:
    - Earlywatch Alert (EWA)
    - SAP OS/DB Migration Check
    - SAP Security Optimization Service (SOS)
    - SMA-rapport (Solution Management Assessment)

4.2.2. Datauttrekk og -analyse

Formålene med datauttrekkene og analysene av dem er å se hvordan systemene benyttes, og undersøke om aktuelle sikkerhetstiltak er gjennomført og dokumentert i henhold til krav i regelverk og anbefalinger i anerkjente standarder.

Det er foretatt følgende datauttrekk:

- uttrekk av parametere for oppsett av SAP
- uttrekk av data fra Active Directory (håndtering av brukere, brukerrettigheter og ressurser)
- uttrekk av utstedte utviklernøkler for SAP
- uttrekk fra databasen SAP Hana
- uttrekk fra databaseserver
- uttrekk fra applikasjonsservere av programmer, administratorer, hva som logges osv.
- uttrekk fra databasen som brukes til administrasjon av web-brukere i Opal_con
- uttrekk av brukere med tilgang til Opal_con
- logg over hvem som har aksessert passordhvelv
- uttrekk fra klient-PC-er som brukes i DFØ

4.2.3. Intervjuer

Det ble avholdt intervju med DFØ 1. november 2017 og intervjuer med DFØ, Evry og IBM 1. og 14. desember 2017, for områdene som er omfattet av problemstilling 2. Formålet med intervjuene er å sikre forståelse av rutiner, datauttrekk og teknisk dokumentasjon. I intervjuene i desember deltok representanter fra DFØs leverandør av driftstjenester for SAP og deres underleverandør. Referatene fra intervjuene er verifisert av DFØ.

5 Revisjonskriterier

5.1. Kilder til revisjonskriterier

Lov og forskrift

Den sentrale kilden til revisjonskriterier i denne revisjonen er *lov om behandling av personopplysninger* 14. april 2000 nr. 31 (personopplysningsloven). Lovens formål er å beskytte den enkelte mot at personvernet blir krenket gjennom behandling av personopplysninger, og å bidra til at personopplysninger blir behandlet i samsvar med grunnleggende personvernhensyn, inkludert behovet for personlig integritet, privatlivets fred og tilstrekkelig kvalitet på personopplysninger.[11] Krenkelse av personvernet kan forstås som situasjoner og forhold der den enkeltes personopplysninger blir brukt på måter som går på tvers av innarbeidede oppfatninger av personvern, og som kan medføre en belastning for den enkelte. Dette kan for eksempel dreie seg om at informasjon tilflyter personer som ikke har tjenstlig behov for å se den, formidling og salg av opplysninger eller generelt at personopplysninger kommer «på avveie».

Loven definerer *personopplysninger* som opplysninger og vurderinger som kan knyttes til en enkeltperson, og *behandling av personopplysninger* som enhver bruk av personopplysninger, som for eksempel innsamling, registrering, sammenstilling, lagring og utlevering. Loven gjelder for all behandling av personopplysninger som skjer helt eller delvis med elektroniske hjelpemidler.[12] DFØ behandler og lagrer personlig informasjon fra statlige lønnsmottakere i sitt lønns- og personalsystem, og må derfor følge retningslinjene og kravene som følger av personopplysningsloven.

Behandling av personopplysninger skjer i dag hovedsakelig i elektroniske systemer, og dette medfører at informasjonssikkerhet spiller en avgjørende rolle i å sikre opplysningene. For å oppnå beskyttelse av den enkeltes personopplysninger stiller loven krav til at systemer som inneholder slike opplysninger, skal ha god sikkerhet. Personopplysningsloven krever i § 13 at den behandlingsansvarlige og databehandleren gjennom planlagte og systematiske tiltak skal sørge for tilfredsstillende informasjonssikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet ved behandling av personopplysninger.

«Kravet til konfidensialitet skal sikre at informasjon ikke blir gjort tilgjengelig for uvedkommende. Det betyr at personopplysninger skal være beskyttet mot uautorisert innsyn under behandlingen, f. eks ved bruk, transport og lagring.»

«I integritetskravet ligger at informasjon ikke skal kunne endres utilsiktet eller av uvedkommende. Kravet til integritet må ikke forveksles med krav til kvalitet som er knyttet til riktigheten av personopplysningene.»

«Kravet til tilgjengelighet skal sikre at personopplysningene er tilgjengelig for rettmessige brukere når de har behov for det for å kunne utføre sine oppgaver.»

Ot.prp. nr. 92 (1998–99), kapittel 16, Kommentarer til enkeltparagrafer, § 13.

Loven definerer den behandlingsansvarlige som den som bestemmer formålet med behandlingen av personopplysninger og hvilke hjelpemidler som kan brukes, og databehandleren som den som behandler personopplysninger på vegne av den behandlingsansvarlige.[13] Sagt med andre ord er den behandlingsansvarlige den som har bestemmelsesrett over personopplysningene og den elektroniske behandlingen av opplysningene, mens databehandleren er den som utfører arbeid for den behandlingsansvarlige.[14] Dette kan for eksempel skje gjennom utsetting av tjenester til en ekstern virksomhet.

DFØ innehar begge rollene da de er behandlingsansvarlig for personopplysningene til sine egne ansatte og databehandler for personopplysningene de behandler for kundene sine.[15]

[11] Personopplysningsloven § 1.
[12] Personopplysningsloven §§ 2 og 3.
[13] Personopplysningsloven § 2, 4) og 5).
[14] Michal Wiik Johansen mfl. (2001) *Personopplysningsloven, kommentarutgave*. Oslo: Universitetsforlaget, s. 71–72.
[15] Dette bekreftes i avtalen mellom DFØ og kundene: DFØs standardavtale del 1, punkt 8.1.2.

Databehandleren har etter loven et selvstendig ansvar for å ha tilfredsstillende informasjonssikkerhet og for å verne personopplysningene som behandles på vegne av de behandlingsansvarlige.

Av lovforarbeidene går det fram at tilfredsstillende informasjonssikkerhet forutsetter etablering av både organisatoriske og tekniske sikkerhetstiltak. En vurdering av hvilke tiltak som må til for å oppnå lovens krav om tilfredsstillende informasjonssikkerhet, skal skje på bakgrunn av risikoanalyse, og sikringen av konkrete personopplysninger avhenger av hvilke trusler opplysningene er utsatt for.[16]

Nærmere regler om organisatoriske og tekniske sikkerhetstiltak går fram av *forskrift om behandling av personopplysninger* (personopplysningsforskriften), kapittel 2.[17]

Tekniske standarder og veiledere
Personopplysningsforskriften gir ikke detaljerte, konkrete krav til hvordan tekniske sikkerhetstiltak bør innrettes. Anerkjente tekniske standarder på informasjonssikkerhetsområdet må dermed også legges til grunn i revisjonen.

Direktoratet for forvaltning og IKT (Difi) anbefaler norske virksomheter å basere seg på NS-ISO/IEC 27001 ved etablering av internkontroll på informasjonssikkerhetsområdet og søke støtte i NS-ISO/IEC 27002 ved valg og implementering av risikoreduserende tiltak.[18] Datatilsynet uttaler at for å oppfylle de kravene personopplysningsloven stiller når det gjelder informasjonssikkerhet, må virksomheter som et minimum følge alle obligatoriske krav i NS-ISO/IEC 27001.[19]

Det vil også være behov for å se benytte bransjestandarder og leverandøranbefalinger for å identifisere sikringstiltak som er relevante for ulike tekniske løsninger.[20] Videre utgjør Datatilsynets veiledere en relevant kilde for tolkning av kravene i lov og forskrift, og for hvordan virksomheter bør legge opp arbeidet sitt med personopplysninger og informasjonssikkerhet.[21]

5.2. Kriterier, problemstilling 1 – grunnlag for å planlegge sikkerhetstiltak

For å besvare problemstillingen om hvorvidt DFØ har etablert de grunnleggende organisatoriske eller forberedende tiltakene som bør være på plass for å oppnå tilfredsstillende informasjonssikkerhet, er følgende kriterier lagt til grunn:

Sikkerhetsmål og -strategi
I personopplysningsforskriften § 2-3 er det spesifisert at formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi skal beskrives i sikkerhetsmål. Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi. Datatilsynet anbefaler at virksomhetens ledelse årlig går gjennom sikkerhetsmål og sikkerhetsstrategi.[22]

Risikovurdering
Personopplysningsforskriften § 2-4 krever at det skal føres oversikt over hva slags personopplysninger som behandles. Virksomheten skal selv fastlegge kriterier for hva som er akseptabel risiko forbundet med behandlingen av personopplysninger. Videre forutsettes det at den behandlingsansvarlige skal gjennomføre risikovurdering for å klarlegge sannsynligheten for og konsekvenser av sikkerhetsbrudd. Ny risikovurdering skal gjennomføres ved endringer som har betydning for informasjonssikkerheten. Resultatet av risikovurderingen skal sammenlignes med de fastlagte kriteriene for akseptabel risiko, og risikovurderingen skal dokumenteres.

Avtale mellom databehandler og behandlingsansvarlig

---

[16] Ot.prp. nr. 92 (1998–99) *Om lov om behandling av personopplysninger (personopplysningsloven)*. Kapittel 16: Merknader til de enkelte paragrafene.
[17] Personopplysningsloven § 13 fjerde ledd sier at Kongen kan gi forskrift om informasjonssikkerhet ved behandling av personopplysninger, herunder nærmere regler om organisatoriske og tekniske sikkerhetstiltak. Personopplysningsforskriften er fastsatt ved kgl.res. 15. desember 2000 med hjemmel i lov av 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).
[18] Difi 30.10.2015: «*Internkontroll/styringssystem / ledelsessystem for informasjonssikkerhet*». <https://www.difi.no/fagomrader-og-tjenester/digitalisering-og-samordning/standarder/referansekatalogen/internkontroll-styringssystem-ledelsessystem-informasjonssikkerhet>
[19] Datatilsynet (07.03.2017) *Skjema for internkontroll*. <https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/etablering-internkontroll/internkontroll-skjema-egenkontroll/>
[20] Som for eksempel NSM (2017) *Grunnprisipper for ikt-sikkerhet*, The Center for Internet Security (CIS): *Critical Security Controls (CSC) for effective cyber defense*, og SAP Security Baseline Template.
[21] Blant annet Datatilsynet (2000) *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer* og Datatilsynet (2009): *Databehandleravtaler etter personopplysningsloven og helseregisterloven - Veileder*.
[22] Jf. «Virksomhetens ledelse skal jevnlig, eksempelvis årlig, gjennomgå sikkerhetsmål og strategi» (Datatilsynet [2000] *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer*, s.7).

Ifølge personopplysningsloven § 15 kan en databehandler ikke behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. I avtalen med den behandlingsansvarlige skal det også gå fram at databehandleren plikter å gjennomføre slike sikringstiltak som følger av lovens § 13.

En slik avtale kalles en databehandleravtale, og formålet med denne avtalen er blant annet at den behandlingsansvarlige skal kunne forsikre seg om at databehandleren har et tilstrekkelig sikkerhetsnivå.[23]

Datatilsynet har utarbeidet en veileder til databehandleravtaler[24] som setter opp en del minimumskrav til hva som bør være med i en slik avtale. Blant annet omtales følgende momenter:

- Det skal gå klart fram av avtalen hva som er formålet med behandlingen av personopplysningene.
- Det skal gå tydelig fram av avtalen hva databehandleren skal gjøre med personopplysningene.
- Hvis databehandleren skal utlevere personopplysninger til andre eksterne parter, må dette gå klart fram av avtalen.
- Hvis databehandleren gjør bruk av underleverandører av tjenester, skal dette gå klart fram av avtalen.
- Avtalen må klargjøre hva databehandleren skal ha på plass av sikringstiltak for å ivareta konfidensialitet, integritet og tilgjengelighet for behandling av personopplysninger, jf. personopplysningsforskriftens kapittel 2.

I DFØs avtaler med kundene om levering av lønns- og regnskapstjenester står det at avtalen er å anse som en databehandleravtale.[25]

DFØ har satt ut driften av lønns- og personalsystemet SAP til firmaet Evry. Vilkårene og kravene som er knyttet til disse driftsoppgavene, kommer fram i en egen driftsavtale mellom DFØ og Evry, som også omfatter en separat databehandleravtale. Revisjonen vil vurdere disse databehandleravtalenes innhold opp mot lovens krav og Datatilsynets minimumskrav.

Ansvars- og myndighetsforhold
Personopplysningsforskriften stiller i § 2-7 første og andre ledd krav om at det skal etableres og dokumenteres klare ansvars- og myndighetsforhold for bruk av informasjonssystemer. Datatilsynet påpeker at det er viktig at ansvar og myndighet relatert til drift av informasjonssystemet (driftsledelse) og for oppfølging av sikkerhetsarbeid (sikkerhetsledelse) er klarlagt. Videre må ansvarsforholdene være besluttet av virksomhetens ledelse, dokumenteres og gjøres kjent for virksomhetens medarbeidere.[26]

Enkelte av kriteriene som er beskrevet i avsnittene ovenfor, er konkretisert gjennom NS-ISO/ IEC 27001:2017 og NS-ISO/IEC 27002:2017 samt veiledninger fra Datatilsynet. Dette er nærmere utdypet under beskrivelsen av funn i kapittel 6.1.

5.3. Kriterier, problemstilling 2 – systematiske tiltak for informasjonssikkerhet

Personopplysningsforskriftens kapittel 2 operasjonaliserer lovens generelle krav om sikkerhetstiltak og består av en rekke krav om tiltak. For å besvare problemstillingen om DFØs etablering av systematiske/tekniske tiltak for å sikre tilfredsstillende informasjonssikkerhet for personopplysningene tar vi utgangspunkt i følgende krav fra forskriften:

Konfigurasjon av systemet
Ifølge personopplysningsforskriften § 2-7 tredje og fjerde ledd skal informasjonssystemet konfigureres slik at tilfredsstillende informasjonssikkerhet oppnås. Konfigurasjonen av systemet skal dokumenteres og ikke endres uten autorisasjon.

Autorisert personell
§ 2-8 første ledd i personopplysningsforskriften krever at medarbeidere hos den behandlingsansvarlige bare skal bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk. Tredje ledd krever at autorisert bruk av informasjonssystemet registreres.

---

[23] Datatilsynet (13.06.2017) *Hva er en databehandleravtale?* <https://www.datatilsynet.no/regelverk-og-skjema/veiledere/databehandleravtale/?id=7361>
[24] Datatilsynet (2009) *Databehandleravtaler etter personopplysningsloven og helseregisterloven - Veileder.*
[25] DFØs standardavtale del 1, punkt 8.1.2.
[26] Datatilsynet (2000) *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer.* Kommentarer til § 2-7, s. 9.

Sikring av konfidensialitet og integritet
Personopplysningsforskriften §§ 2-11 første og andre ledd og 2-13 første og andre ledd slår fast at det skal treffes tiltak mot uautorisert innsyn og endring, der konfidensialitet og integritet er nødvendig. Sikkerhetstiltakene skal også hindre uautorisert innsyn og endring i annen informasjon med betydning for informasjonssikkerheten. § 2-13 tredje ledd setter krav til at det skal treffes tiltak mot ødeleggende programvare.

Kryptering
§ 2-11 tredje ledd krever at personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, skal krypteres eller sikres på annen måte når konfidensialitet er nødvendig. I Datatilsynets veiledning til bestemmelsen er det presisert at reglene for kryptering også gjelder for overføring via private datalinjer, som er utenfor det området virksomheten har sikret mot uautorisert adgang.

Uautorisert bruk
Personopplysningsforskriften § 2-14 første ledd stiller krav om at sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Tredje ledd utdyper at sikkerhetstiltak skal omfatte tiltak som ikke kan påvirkes eller omgås av medarnbeiderne.

Kriteriene som beskrives ovenfor, er konkretisert gjennom NS-ISO/IEC 27002:2017, leverandøranbefalinger fra SAP og Microsoft samt uttalelser og anbefalinger fra Datatilsynet, NSM og Center for Internet Security. Dette er nærmere utdypet under beskrivelse av funn, jf. kapittel 6.2.

5.4. Kriterier, problemstilling 3 – oppfølging av sikkerhetstiltak og leverandør

Problemstillingen skal svare på hvordan DFØ følger opp sikkerhetsstrategi og implementerte sikkerhetstiltak internt, for å forsikre seg om at strategi og tiltak fungerer som forutsatt. Videre ser vi på hvordan DFØ følger opp og har kontroll med driftsleverandøren Evrys sikring av personopplysningene i SAP-systemet.

Sikkerhetsrevisjoner
Personopplysningsforskriften § 2-5 krever at sikkerhetsrevisjoner av bruk av informasjonssystemer skal gjennomføres jevnlig. Revisjonen skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Resultatet fra sikkerhetsrevisjonen skal dokumenteres. Datatilsynet utdyper at dette dreier seg om å etterprøve sikkerhetsarbeidet for å verifisere at de sikkerhetstiltakene som er besluttet etablert, faktisk er satt i verk og fungerer som forutsatt. Tilsynet anbefaler sikkerhetsrevisjoner på årlig basis.[27] Forskriftens § 2-3 fjerde ledd stiller krav om at informasjonssystemet jevnlig skal gjennomgås for å klarlegge om det er hensiktsmessig i forhold til virksomhetens behov, og om sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat.

Oppfølging av leverandør
Personopplysningslovens § 13 tredje ledd sier at en behandlingsansvarlig som lar andre få tilgang til personopplysninger, skal påse at disse oppfyller kravene til sikkerhetstiltak. Vi forutsetter at det samme «påse»-kravet også må gjelde for en databehandler som lar andre få tilgang til et system som inneholder personopplysninger. Det følger av personopplysningsforskriftens § 2-15 tredje ledd at leverandører skal tilfredsstille kravene til sikkerhetstiltak i forskriftens kapittel 2. Videre går det fram av femte ledd at den behandlingsansvarlige skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet.

Det er av vesentlig betydning, både for DFØ og for DFØs kunder, at DFØ kan forsikre seg om at Evry har gode systemer og rutiner for å sikre personopplysningene i SAP-systemet. For å oppnå dette må det forventes at DFØ har en jevnlig oppfølging og kontroll av Evry, for å sikre at de etterlever driftsavtalen og lovens krav til sikring av personopplysningene. Datatilsynet har i sin veiledning angitt at dette kan oppnås ved at den behandlingsansvarlige meddeles resultater fra ledelsesgjennomganger, sikkerhetsrevisjoner og avviksbehandling som er relevant for forholdet til leverandøren.[28]

Kriteriene som går fram ovenfor, er konkretisert gjennom NS-ISO/ IEC 27001:2017 og NS-ISO/IEC 27002:2017 og en veileder fra Datatilsynet. Dette er nærmere utdypet under beskrivelse av funn, jf. kapittel 6.3.

---

[27] Datatilsynet (2000) *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer.* Kommentarer til § 2-5, s.8.
[28] Datatilsynet (2000) *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer.* Kommentarer til § 2-15.

6 Funn

6.1. Problemstilling 1: Har DFØ etablert et grunnlag for å planlegge sikkerhetstiltak som sørger for tilfredsstillende informasjonssikkerhet for personopplysninger i SAP?

6.1.1. Sikkerhetsmål og sikkerhetsstrategi

I personopplysningsforskriften § 2-3 er det spesifisert at formålet med behandling av personopplysninger og overordnede føringer for bruk av informasjonsteknologi, skal beskrives i sikkerhetsmål. Valg og prioriteringer i sikkerhetsarbeidet skal beskrives i en sikkerhetsstrategi.

Datatilsynet uttaler at sikkerhetsmål vil omfatte beslutninger om til hva og hvordan informasjonsteknologi skal benyttes i virksomheten. Eksempler på slike beslutninger kan være valg av hvilken behandling av personopplysninger som skal skje med elektroniske hjelpemidler, hvordan virksomheten forholder seg til opplysninger som må sikres både med hensyn til konfidensialitet og tilgjengelighet, og føringer for medarbeideres eventuelle private bruk av informasjonssystemet. Videre påpeker Datatilsynet at sikkerhetsstrategien vil omfatte grunnleggende beslutninger om organisering og gjennomføring av sikkerhetsarbeidet. Eksempler på slike beslutninger kan være fordeling av arbeidsoppgaver for drift og informasjonssikkerhet mellom ledelse, drifts- og sikkerhetspersonell og den enkelte bruker, eventuelt krav til at konfidensielle personopplysninger behandles i informasjonssystem uten tilkobling til eksterne datanett, og bruk av leverandører for å få utført sikkerhetsoppgaver. Datatilsynet anbefaler at virksomhetens ledelse gjennomgår sikkerhetsmål og sikkerhetsstrategi årlig.[29]

Revisjonen har gått gjennom DFØs styringsdokumenter på informasjonssikkerhetsområdet:

- ***Styringssystem for informasjonssikkerhet*** har som formål å tydeliggjøre hvordan DFØ følger opp og ivaretar informasjonssikkerhet. Det presiseres at informasjonssikkerhet er en integrert del av virksomhetens helhetlige styring og kontroll, og at den må sees i sammenheng med DFØs øvrige dokumentasjon relatert til virksomhetens styring og kontroll, herunder rolle- og prosessbeskrivelser. DFØs styringssystem skal sikre at skjermingsverdig informasjon, både DFØs egen og kundenes, skal behandles på en sikker måte. Det går fram at dette også gjelder informasjon som har krav om beskyttelse gjennom personopplysningsloven. Det skal gjøres en systematisk vurdering av om ulike sikkerhetstiltak etterleves og fungerer som forutsatt. Prosedyrer for avvikshåndtering og sikkerhetshendelser er omtalt, og det går fram at ledelsen i DFØ skal gjennomgå sikkerhets- og beredskapssituasjonen i virksomheten minimum tre ganger per år. Dokumentet ble oppdatert i mai 2014.

- ***Sikkerhetspolicy*** beskriver generelle sikkerhetsmål. Av 17 sikkerhetsmål er det to som berører personopplysninger. Mål 4 omtaler at den fysiske sikkerheten i DFØ skal hindre uautorisert adgang til lokaler der skjermingsverdig informasjon, inkludert personopplysninger, lagres og behandles. Mål 11 sier at alle som ber om det, skal få generell informasjon om DFØs behandling av personopplysninger. Dokumentet ble oppdatert i februar 2015.

- ***Organisering av sikkerhet- og beredskapsarbeidet – roller og ansvar*** beskriver detaljert hvordan DFØs sikkerhetsorganisasjon er, med vekt på hvilket ansvar og hvilken rolle direktør, avdelingsdirektører, sikkerhetsleder, sikkerhetskoordinator, linjeleder og ansatte har. Ledelsen er tydeliggjort med navn, avdeling/rolle og mobilnummer. De ulike rollenes oppgaver er konkretisert i dokumentet. Dokumentet ble oppdatert i mai 2017.

- ***Sikkerhetsstandard*** tar for seg de sikkerhetstiltakene DFØ må sette i verk og vedlikeholde for å ivareta nødvendig konfidensialitet, integritet og tilgjengelighet i sine tjenester. Organisering av sikkerhet, administrasjon av aktiva, fysisk og miljømessig sikkerhet, tilgangskontroll og utvikling og vedlikehold av informasjonssystemer er noen av temaene.

[29] Datatilsynet (2000) *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer*. Kommentarer til § 2-3.

Det opplyses at DFØ har fire typer informasjonsaktiva: sikkerhetsgradert informasjon, beskyttelsesgradert informasjon, personopplysninger og unntak fra innsynsretten. Det går ikke fram hvilke personopplysninger det er snakk om, eller i hvilke ikt-systemer slike opplysninger er aktuelle å behandle.

Dokumentets siste kapittel tematiserer overensstemmelse med juridiske krav, hvor sikring av data og beskyttelse av personopplysninger er viet et eget punkt. Her er formålet med personopplysningsloven gjengitt, og det presiseres at loven omfatter all behandling av denne typen opplysninger, manuelt så vel som elektronisk. Det går fram at dersom brudd på informasjonssikkerhet har ledet til uautorisert utlevering av personopplysninger, skal sikkerhetssjefen varsles. Det blir ikke sagt hvordan DFØ konkret skal gå fram for å etterleve regelverket knyttet til personvern, men innledningsvis i kapitlet slås det fast at «målet er å unngå brudd på [...] statlig regelverk [...] og ethvert krav til sikkerhet». Dokumentet ble oppdatert i desember 2013.

DFØ uttaler at det er tungvint og tidkrevende å oppdatere dagens dokumenter. Oppdateringene skjer etter behov, og det er ikke en fast oppdateringsfrekvens på dem. Det hender det er nødvendig med endringer, for eksempel etter hendelser eller øvelser. Hvis én ting endres i dokumentene, er det mye annet som også må endres.

DFØ opplyser at strategidokumentene ligger lett tilgjengelig for alle ansatte på intranettet. Alle dokumentene er godkjent av ledelsen. Godkjenning gjennomføres som beslutninger i ledergruppen.

Vurdering
DFØ har flere separate styringsdokumenter som alle beskriver ulike sider ved informasjonssikkerheten i virksomheten. Det er naturlig å se dokumentene i sammenheng, og til sammen utgjør de en helhetlig sikkerhetsstrategi. Strategien fanger opp sentrale elementer beskrevet av Datatilsynet – for eksempel fordeling av arbeidsoppgaver mellom ledelse og driftspersonell, redegjørelse for organisatoriske valg og krav til informasjonssikkerhetsarbeidet. Dokumentene er godkjent av ledelsen, og de er tilgjengelige for de ansatte på DFØs intranett. Videre har DFØ utarbeidet en rekke sikkerhetsmål. Sikkerhetsmålene er generelle og beskriver hvordan DFØs ulike aktiviteter skal beskyttes mot interne og eksterne trusler. To av sikkerhetsmålene berører personopplysninger.

Sikkerhetsmål og -strategi er på plass slik personopplysningsforskriftens § 2-3 andre og tredje ledd krever, og inneholder elementer som er i tråd med Datatilsynets anbefalinger. Gjennomgangen av dokumentene viser imidlertid at det er lite eksplisitt omtale av personopplysninger i DFØs styringsdokumentasjon om informasjonssikkerhet. Det er ingen formuleringer som viser hva som er formålet med at DFØ behandler slike opplysninger, noe som er et krav i personopplysningsforskriften. Omtale og vurderinger av personopplysninger er først og fremst knyttet til hva som må til for å ha en generelt god informasjonssikkerhet i virksomheten.

Med unntak av dokumentet «Organisering av sikkerhet- og beredskapsarbeidet», som sist ble endret våren 2017, blir styringsdokumentene som utgjør DFØs sikkerhetsstrategi, sjelden oppdatert eller revidert. Dette viser at DFØ ikke dokumenterer at de følger opp Datatilsynets anbefaling om årlig å gjennomgå sikkerhetsmål og -strategi.

6.1.2. Klassifisering av og oversikt over personopplysninger som behandles i DFØs systemer

Personopplysningsforskriften § 2-4 første ledd krever at det skal føres oversikt over hva slags personopplysninger som behandles, og at det skal fastlegges kriterier for akseptabel risiko forbundet med behandlingen av personopplysninger. NS-ISO/IEC 27002 anbefaler at aktiva tilknyttet informasjon eller behandling av informasjon identifiseres og registreres, og at det utpekes en eier som har ansvar for de enkelte aktiva. Videre anbefales det at informasjon klassifiseres i henhold til juridiske krav, verdi, kritikalitet og sensitivitet. Dette for å sikre at informasjonen har et tilstrekkelig beskyttelsesnivå.[30]

DFØs *Sikkerhetsstandard* omtaler at alle aktiva som som krever beskyttelse av informasjon, programvare og fysiske aktiva, skal eies av en person (rolle) eller linjeleder. Det kommer videre fram at gradering eller klassifisering av aktiva skal sikre at DFØs aktiva eller aktiva de behandler på andres vegne, får nødvendig

[30] NS-ISO/IEC 27002:2017, kap. 8.1. og 8.2.

beskyttelse gjennom sikringstiltak. Tjenesteeier har ansvaret for å vurdere risiko og anbefale sikkerhetsnivå. Dokumentet har en tabell som viser at DFØ med utgangspunkt i personopplysningsloven klassifiserer personopplysninger i to typer, sensitive personopplysninger og personopplysninger.[31]

DFØ har et dokument kalt *Informasjonsaktiva*, som blant annet inneholder en oversikt over de ulike typene personopplysninger DFØ behandler, og i hvilke IT-systemer disse opplysningene ligger. Sensitive personopplysninger er skilt ut i egne linjer. Det går fram at informasjon om medlemskap i fagforening er den eneste sensitive personopplysningen som håndteres i SAP.[32]

Dokumentet beskriver ikke eksplisitt hvilke beskyttelsesnivå som kreves for de ulike personopplysningene. For SAP er det satt opp enkelte stikkordsmessige beskyttelsestiltak, men det kommer ikke fram om det er strengere sikringskrav for sensitive personopplysninger enn for vanlige personopplysninger. Dokumentet inneholder et eget avsnitt kalt «Akseptabel risiko», men dette ser ikke ut til å være utfylt, og det går ikke fram hvilke risikonivåer som anses som akseptable for behandlingene av opplysningene. Lønnsavdelingen blir beskrevet som tjenesteeier for SAP.

DFØ opplyser i intervju at *Informasjonsaktiva*-dokumentet ble utarbeidet og benyttet i forbindelse med en særskilt risikovurdering av personopplysninger som ble gjennomført i 2013, og at det er aktuelt å bruke dette som input i nye risikovurderinger på området.[33]

Vurdering
Revisjonen viser at DFØ etterlever personopplysningsforskriftens krav til identifisering av hvilke personopplysninger virksomheten behandler, og ISO-anbefalinger om klassifisering av informasjonsaktiva.

Dokumentet *Informasjonsaktiva* angir enkelte generelle beskyttelsestiltak for SAP, men ønsket beskyttelsesnivå for opplysningene eller hva som er akseptabel risiko for behandlingene av opplysningene, kommer i liten grad fram.

6.1.3. Risikovurderinger

Personopplysningsforskriften § 2-4 andre ledd krever at det gjennomføres risikovurderinger for å klarlegge sannsynlighet for og konsekvenser av sikkerhetsbrudd. Vurdering av risiko er sentralt i alt sikkerhetsarbeid. Tradisjonelt består en risikovurdering av tre hovedaktiviteter: å identifisere uønskede hendelser (risikoelementer), å vurdere risikoens sannsynlighet og konsekvens og å evaluere og håndtere risikoen. Håndtering kan gjøres ved for eksempel å innføre beskyttelses- eller kontrolltiltak som begrenser risikoen.[34]

Risikovurderinger og personopplysninger
Risikovurderinger utarbeides på flere nivåer i DFØ. Avdelingene gjennomfører risikovurderinger om høsten i forbindelse med arbeidet med egen virksomhetsplan.[35] DFØs overordnede risikovurdering, som baseres på de avdelingsvise, er en del av den årlige halvårsrapporten til Finansdepartementet. DFØ opplyser i intervju at risikoene i den overordnede vurderingen bør kunne finnes igjen i risikovurderinger på lavere nivå.[36]

Overordnet risikovurdering
Gjennomgang av den overordnede risikovurderingen for 2017 viser at DFØ identifiserer to risikomomenter som kan relateres til arbeidet med behandling av personopplysninger: *skjermingsverdige data på avveie* og *angrep fra ondsinnet programvare*.[37] Førstnevnte er vurdert som en moderat risiko, sistnevnte som kritisk. De oppførte tiltakene knyttet til disse risikomomentene framstår som lite konkrete. Det er for eksempel ikke satt opp aktuelle sikkerhetstiltak, verken for SAP eller for de andre systemene som inneholder skjermingsverdige data og/eller personopplysninger. Det kan imidlertid argumenteres for at dette er naturlig i en risikovurdering på overordnet

---

[31] DFØ (2013) *Sikkerhetsstandard*, kap. 4, s. 8–9.
[32] Opplysninger om helseforhold regnes som sensitive personopplysninger, men slik informasjon om lønnstakerne ligger i andre systemer enn SAP.
[33] Verifisert referat fra intervju med DFØ 1. november 2017.
[34] ISO/IEC 27001:2017 kap. 6.1.2.
[35] DFØ (2017) *Halvårsrapport 2017*, kap. 3.1, s. 16.
[36] Verifisert referat fra intervju med DFØ 1. november 2017.
[37] DFØ (2017) *Halvårsrapport 2017*, kap. 3.2, s. 19–33. Disse risikofaktorene ble også omtalt i den overordnede risikovurderingen i 2016.

nivå. Innholdet i risikovurderingene på nivåene under bør imidlertid kunne forventes å være mer spesifikke og konkrete.[38]

Avdelingsvise risikovurderinger
Lønnsavdelingen utarbeider årlig en egen risikovurdering, som er en del av avdelingens virksomhetsplan for budsjettåret. Dokumentgjennomgang viser at lønnsavdelingens risikovurdering for 2017 består av 12 risikomomenter. Ingen av momentene er relatert til IKT-sikkerhet eller sikring av personopplysninger. Verken risiko for skjermingsverdig informasjon på avveie eller risiko for ondsinnede angrep blir omtalt i lønnsavdelingens risikovurdering. Det er dermed vanskelig å se en klar sammenheng eller rød tråd mellom risikovurderingene på overordnet nivå og risikovurderingene på avdelingsnivå.

Andre risikovurderinger
DFØ uttaler i intervju at risikovurderinger av personopplysninger og ikt-systemene i hovedsak skjer i form av risiko- og sårbarhetsanalyser (ROS).[39] Revisjonen har ikke mottatt dokumentasjon på at det er gjennomført ROS-analyser eller andre typer vurderinger av sikkerheten i ikt-systemene. DFØ opplyser videre at en ROS-analyse for IT-seksjonen er under utarbeidelse, men at denne ikke er ferdig på revisjonstidspunktet.

I 2013 engasjerte DFØ Devoteam AS til å gjennomføre en vurdering av risiko forbundet med behandling av personopplysninger i DFØ. Devoteam konkluderte blant annet med at DFØ burde utarbeide rutiner for regelmessige risikovurderinger knyttet til personopplysninger og kriterier for å vurdere personvernkonsekvenser.[40]

Risikovurderinger ved endringer
Personopplysningsforskriftens § 2-4 andre ledd krever at det skal gjennomføres nye risikovurderinger dersom det skjer endringer som har betydning for informasjonssikkerheten. Videre har DFØ satt som krav til seg selv at «Ved utsetting av tjenester (outsourcing) til ekstern virksomhet, skal det før kontrakt signeres foreligge en risikovurdering med hensyn til leverandørens evne til å ivareta krav til sikkerhet med hensyn til konfidensialitet, integritet og tilgjengelighet».[41] I intervju opplyser DFØ at det skal utarbeides risikovurderinger i forbindelse med prosjekter som medfører endringer med betydning for informasjonssikkerhet og personopplysninger, for eksempel ved større endringer i systemer, rutiner, lovkrav eller eksterne trusselbilder. Revisjonen har sett nærmere på tre konkrete endringer/prosjekter knyttet til lønnssystemet SAP.

- DFØ inngikk ny avtale med Evry om levering av driftstjenester for SAP i juni 2016. DFØ uttaler i intervju at det ikke ble utført noen risikovurdering i forkant av kontraktsinngåelsen med Evry. Hovedårsaken til dette opplyses å være at kontrakten med Evry ikke innebar noen endringer i sourcingstrategien til DFØ. Teknisk drift av SAP var allerede outsourcet.[42]

- I februar 2017 ble IBM Evrys underleverandør av driftstjenester for SAP. Evry opplyser i intervju at dette blant annet innebærer at driftsenheten for SAP nå ligger hos IBM, og at de har ansvaret for serverpark, nettverk og drift av systemene. Evry har fortsatt ansvaret for oppfølging av kunden DFØ.[43] Revisjonen har ikke mottatt dokumentasjon på at DFØ har gjennomført vurderinger av informasjonssikkerheten ved denne endringen.

- Evry gikk høsten 2017 over fra å benytte Oracle til SAP HANA som database for SAP. Dette var et stort prosjekt som ble utført i perioden april til desember 2017.[44] DFØ opplyser i intervju at det ikke ble gjennomført en egen vurdering i DFØ av mulige sikkerhetskonsekvenser forut for denne endringen. DFØ bygget utelukkende på Evrys risikovurderinger.

Oppfølging av risiko gjennom aktivitets- og tiltakslister

---

[38] I DFØs veileder til internkontroll kommer det fram at «Det vil være naturlig at ledelsen ved risikovurderinger på virksomhetsnivå tar i betraktning vurderinger som er gjennomført på lavere nivåer. På denne måten vil risikoer som er synliggjort i risikovurderingen på lavere nivåer, gi relevant informasjon til risikovurderingen på virksomhetsnivå.» DFØ (2013) Veileder i internkontroll. Kap. 4.2.2.
[39] Verifisert referat fra intervju med DFØ 1. november 2017. (Revisjonen har forstått det slik at ROS-analyser i DFØ er en separat type vurdering, som skiller seg noe fra risikovurderinger).
[40] Devoteam (2013) *Vurdering av risiko forbundet med behandling av personopplysninger i DFØ.*
[41] DFØ (2014) Styringssystem for informasjonssikkerhet. Kap. 7.2.
[42] Verifisert referat fra intervju med DFØ 1. november 2017.
[43] Verifisert referat fra intervju med DFØ og Evry/IBM 1. desember 2017.
[44] DFØ: Migreringsplan for HANA-prosjektet. Mottatt 15. februar 2018.

DFØ informerer i intervju om at lønnsavdelingens seksjoner har aktivitets- og tiltakslister, som brukes for å følge opp vedtatte tiltak som seksjonene skal jobbe med, og er en del av DFØs rapporteringssystem. Listene kan ifølge DFØ inneholde aktiviteter som gjelder gjennomføring av tiltak som følger av risikovurderinger.[45]

Gjennomgang av listene for seksjon for applikasjonsforvaltning (LA App) og stabsseksjon (LA Stab) viser at de blant annet inneholder tiltak og aktiviteter for å følge opp lønnsavdelingens risikovurdering for 2017.[46] Denne risikovurderingen inneholder ingen spesifikke risikomomenter knyttet til informasjonssikkerhet og/eller sikring av personopplysninger, og aktivitetslistene inneholder heller ingen tiltak som eksplisitt blir beskrevet å skulle følge opp disse områdene. Enkelte av oppfølgingstiltakene kan sies å være aktiviteter som bidrar til bedre sikkerhet generelt, for eksempel oppfølging av autorisasjonsskjemaer, kontroll av roller i SAP (LA Stab) og supportpakker og implementering av ulike endringer og oppdateringer i systemene (LA App). DFØs overordnede risikovurdering for 2017 viser til risikomomentene *skjermingsverdige data på avveie* og *angrep fra ondsinnet programvare*. Det blir ikke referert til disse risikoene i aktivitetslistene og det framkommer ingen tiltak som er ment å følge dem opp.

Vurdering
DFØ vurderes å ikke etterleve personopplysningsforskriftens krav om å gjennomføre risikovurderinger for å klarlegge sannsynlighet for og konsekvenser av sikkerhetsbrudd, samt nye risikovurderinger ved endringer som har betydning for informasjonssikkerheten.

Revisjonen viser at DFØ har vurdert enkelte risikomomenter når det gjelder informasjonssikkerhet og sikring av personopplysninger på overordnet nivå, men at det er få og uklare beskrivelser av tiltak. Revisjonen viser videre at risikovurderinger fra lønnsavdelingen ikke inneholder vurderinger av risiko av informasjonssikkerhet eller behandlingen av personopplysninger. Det er heller ikke dokumentert at dette gjennomføres i andre typer vurderinger eller evalueringer. Relevante risikomomenter fra overordnedet risikovurdering, hvorav én er i kritisk kategori, kan ikke gjenfinnes i risikovurderinger til lønnsavdelingen. Avdelingen er systemansvarlig for SAP, og ut fra dette ville vi forventet at risiko knyttet til informasjonssikkerhet og personopplysninger var en del av avdelingens risikovurderinger. Det er også vanskelig å se noen rød tråd fra virksomhetsnivå til avdelings- og seksjonsnivå når det gjelder tiltak for å møte identifisert risiko på informasjonssikkerhetområdet. Revisjonen har identifisert tre endringer eller prosjekter hvor DFØ ikke har vurdert risiko og konsekvenser for informasjonssikkerheten, inkludert personopplysninger.

Manglende regelmessige risikovurderinger knyttet til personopplysninger var også en av merknadene i Devoteams gjennomgang av DFØs behandling av personopplysninger fra 2013. Revisjonen viser at disse anbefalingene ikke har blitt fulgt opp av DFØ i ettertid.

6.1.4. Databehandleravtale mellom DFØ og Evry

Personopplysningsloven § 15 første ledd sier at en databehandler ikke kan behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Andre ledd omtaler at det i avtalen med den behandlingsansvarlige også skal gå fram at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13. Datatilsynet har utarbeidet en veileder som beskriver hva en slik databehandleravtale bør inneholde for å være i tråd med regelverket.

DFØ har en avtale med Evry om drift av lønns- og personalsystemet SAP[47]. Avtalen ble inngått 18. juni 2016, med virkning fra 1. april 2017, og den løper i fire år. Evry var også DFØs leverandør av SAP-tjenester i perioden 2012–2016. Avtalen består av hovedavtalen og ti bilag, herunder databehandleravtale.

I revisjonen er følgende deler av avtalen gjennomgått:

[45] Verfisert referat fra intervju med DFØ 1. november 2017
[46] Revisjonen har mottatt aktivitetslister for LA Stab og LA App, begge sist endret 30. november 2017. Aktivitetslistene til seksjonene LA App og LA Stab anses mest relevante for revisjonen, siden disse har ansvar for henholdsvis forvaltning og utvikling av SAP, og kundekoordinering, prosjektstyring og porteføljeforvaltning, i tillegg til et delt ansvar for oppfølging av leverandøren Evry.
[47] Avtale mellom DFØ og Evry om kjøp av driftstjenester knyttet til maskinvare, infrastruktur og programvare. Signert 18.06.2016.

Oversikt over viktige deler av avtalen mellom DFØ og Evry

Dokumentnavn	Innhold
Hovedavtalen	Overordnede bestemmelser knyttet til leveringen av tjenestene
Kundens kravspesifikasjon (bilag 1)	DFØs kravspesifikasjoner og spesifiseringer av det som skal leveres
Leverandørens løsningsspesifikasjon (bilag 2)	Evrys beskrivelser av løsningen, basert på kravspesifikasjonen fra DFØ
Administrative bestemmelser (bilag 6)	Partenes representanter, leverandørens nøkkelpersonell, godkjente underleverandører og møteoversikt for regelmessige møter mellom DFØ og Evry
Databehandleravtale (bilag 10)	Bestemmelser som skal gjelde mellom behandlingsansvarlig (DFØ) og databehandler (Evry) vedrørende behandlingen av personopplysninger

DFØs databehandleravtale med Evry er i revisjonen vurdert mot Datatilsynets veileder til databehandleravtaler. I tillegg er omtale av og krav til sikring av personopplysninger i avtalens øvrige bilag vurdert.

Formålet med behandlingen av personopplysninger
Datatilsynets anbefaling er at det skal gå klart fram av avtalen hva som er formålet med behandlingen av personopplysningene.

Databehandleravtalen har et avsnitt kalt «Avtalens formål» (pkt. 1). Avsnittet beskriver ikke direkte hva som er formålet med Evrys behandling av personopplysninger. Det henvises generelt til at databehandleren ikke har anledning til å behandle data på andre måter enn det som er nødvendig for utførelsen av tjenestene som nevnt i SSA-D, bilag 1–9 (det vil si hele den øvrige avtalen). Formålet med behandlingen av personopplysningene kommer heller ikke fram i noen av de øvrige avsnittene i avtalen. DFØ opplyser i intervju at det skulle vært henvist klarere til formålet med Evrys behandling av personopplysningene i databehandleravtalen.[48]

Beskrivelse av hvordan personopplysningene skal behandles
Datatilsynets anbefaling er at det tydelig skal gå fram av avtalen hva databehandler skal gjøre med personopplysningene. For eksempel bør det opplyses om det skal foretas innsamling av opplysninger, om de skal bearbeides på noen måte, om de skal oppbevares eller lagres, eller om det skal skje en kobling mot andre registre og opplysninger.

Analyse av databehandleravtalen viser at den ikke inneholder tydelige beskrivelser av hva Evry skal, eller kan, gjøre med personopplysningene. Avtalen omtaler generelt at «Databehandler skal følge de rutiner og instrukser for behandlingen som behandlingsansvarlig til enhver tid har bestemt skal gjelde».[49] Det blir ikke henvist til hvilke rutiner og instrukser dette er, eller hva som er innholdet i dem.

Bruk av underleverandører og eventuell overføring til utlandet
Hvis databehandleren gjør bruk av underleverandører for levering av tjenester, skal dette ifølge Datatilsynet gå klart fram av databehandleravtalen. Dersom det er aktuelt at personopplysninger skal overføres til utlandet, må også dette reguleres i avtalen.

Databehandleravtalen mellom DFØ og Evry omtaler bruk av underleverandører og krever at hvis databehandleren skal benytte underleverandør, så skal dette avtales skriftlig med behandlingsansvarlig før behandlingen av personopplysninger starter. Avtalen regulerer også overføringer til utlandet og slår fast at databehandleren ikke har rett til å overføre personopplysninger til utlandet, verken internt i virksomheten eller til andre, uten forutgående samtykke fra den behandlingsansvarlige.[50]

[48] Verifisert referat fra intervju med DFØ 1. november 2017.
[49] Databehandleravtale mellom DFØ og Evry, pkt. 2.
[50] Databehandleravtale mellom DFØ og Evry, pkt. 3 og 4.

Databehandleravtalen inneholder ikke krav om at personopplysninger kun skal lagres i Norge, men det beskrives i DFØs kravspesifikasjon at data, inkludert sikkerhetskopier, under hele avtaleperioden skal lagres i Norge. Det kreves også at leverandøren ikke skal gi ansatte eller underleverandører lokalisert utenfor Norge tilgang til DFØs data uten forutgående samtykke.[51] Se også omtale av behandling av opplysninger i utlandet i kapittel 6.3.3 nedenfor.

Beskrivelse av informasjonssikkerhetstiltak
Datatilsynet anbefaler at avtalen må klargjøre hva databehandleren skal ha på plass av sikringstiltak for å ivareta konfidensialitet, integritet og tilgjengelighet for behandling av personopplysninger, jf. personopplysningsforskriftens kapittel 2.

Databehandleravtalen omtaler generelt at databehandlere skal oppfylle de kravene som lov og forskrift stiller, og at rutiner og tiltak for å oppfylle disse skal dokumenteres av databehandleren og være tilgjengelig på de behandlingsansvarliges forespørsel.[52] Databehandleravtalen inneholder reguleringer av sikringstiltak på en del av de områdene som Datatilsynet anbefaler, herunder avvikshåndtering, taushetsplikt, sikkerhetsrevisjoner, dokumentasjon av rutiner og hva som skal skje med opplysningene etter at avtalen er opphørt. Gjennomgangen viser også noen svakheter ved beskrivelser av sikringstiltak i databehandleravtalen.

Det er ikke beskrevet krav eller tiltak for tilgangskontroll og tilstrekkelige kontrollmekanismer, som for eksempel loggføring. Dette er beskrevet i DFØs kravspesifikasjon,[53] men databehandleravtalen henviser ikke til dette.

Datatilsynet anbefaler også at avtalen bør inneholde bestemmelser om hvilken type personell som skal ha tilgang til personopplysningene. Databehandleravtalen inneholder ingen regulering av dette eller hvilket omfang slike tilganger bør ha. DFØs kravspesifikasjon inneholder heller ikke spesifikke krav til hvilke grupper ansatte som skal ha tilgang til personopplysninger eller omfanget av slike tilganger. Det er imidlertid et krav at Evry skal beskrive metoder for å hindre uautorisert tilgang til DFØs systemer eller data. I Evrys løsningsspesifikasjon blir det under dette kravet beskrevet at det er driftskonsulenter som skal ha tilgang, og at disse bare skal ha tilgang til det som er nødvendig for å utføre de respektive oppgavene.[54]

Omtale og krav til sikring av personopplysninger i avtalens øvrige bilag
Databehandleravtalen er en særskilt avtale for å regulere krav om og tiltak for beskyttelse av personopplysninger. Driftsavtalen inneholder i tillegg andre dokumenter hvor DFØ kan stille krav til Evry som har relevans for sikring av personopplysningene. Hele avtalekomplekset er derfor gjennomgått for å undersøke om og hvordan DFØ har omtalt krav til sikring av personopplysninger.

Krav til informasjonssikkerhet
Tiltak for informasjonssikkerhet henger tett sammen med tiltak for å sikre personopplysninger, og det er i mange tilfeller flytende overganger mellom hva som kategoriseres som det ene eller det andre. DFØ stiller i hovedavtalen et generelt krav til at Evry skal dokumentere at de følger gjeldende regelverk og anerkjente standarder for informasjonssikkerhet, og henviser til at særskilte krav for informasjonssikkerhet skal framgå av kravspesifikasjonen (bilag 1).[55]

Kravspesifikasjonen fra DFØ, som spesifiserer driftstjenestene som skal leveres etter avtalen, og som Evry har svart på i sin løsningsspesifikasjon, inneholder et eget kapittel med krav til informasjonssikkerhet. Dette består blant annet av krav om:

- lagring av data i Norge
- tilgang til data utenfor Norge
- følge beste praksis for håndtering av informasjonssikkerhet (hva som er beste praksis, blir ikke omtalt)
- oversikt over tilganger til systemene og gjennomføring av logging
- månedlig rapportering av brukernes aksessering av systemer

[51] Avtale mellom DFØ og Evry, bilag 1, pkt. 1.11.2.1 og 1.11.2.2 i kravspesifikasjon.
[52] Databehandleravtale mellom DFØ og Evry, pkt. 5.
[53] Bilag 1, DFØs kravspesifikasjon. Pkt. 1.11.2.4: Krav om at Evry til enhver tid skal ha oversikt over ansatte med tilgang til DFØs systemer, og loggføre ansattes pålogging til systemene. Pkt. 1.11.2.8: Krav om rutine for logging og identifikasjon av upersonlige brukere. Pkt. 1.11.2.9: Krav om at Evry skal beskrive metode og/eller rutiner for å hindre uautorisert tilgang til DFØs systemer eller data.
[54] Bilag 1, DFØs kravspesifikasjon. Pkt. 1.11.2.9. Samme pkt. i bilag 2, Evrys løsningsspesifikasjon.
[55] Hovedavtalen pkt. 9.4 Informasjonssikkerhet.

- beskrivelse av metode for å hindre uautorisert tilgang til DFØs systemer eller data

Krav til sikring av personopplysninger spesielt
Hovedavtalen omtaler at hvis det er relevant for avtalen, skal partene i bilag 1 (kravspesifikasjon) og 2 (løsningsspesifikasjon) gjøre det klart hvordan personopplysninger skal behandles, og om og i tilfelle hvordan de kan overlates til andre for lagring og bearbeiding. Videre står det at bilagene skal inkludere regulering av relevante tiltak som følger av personopplysningsloven med forskrift, herunder oppfyllelse av kravene om sikkerhetsmål, sikkerhetsstrategi, risikovurdering og forholdsmessig sikring av opplysningene.[56]

DFØs kravspesifikasjon er gjennomgått, og den inneholder ingen eksplisitt omtale av hvordan Evry skal behandle personopplysningene. Det er heller ikke satt konkrete krav til Evry om å utarbeide sikkerhetsmål og -strategi og risikovurderinger vedrørende personopplysninger. Når det gjelder krav til sikring av opplysningene, er det satt generelle krav til informasjonssikkerhet uten at disse er koblet til personopplysninger. Det DFØ *har* stilt krav til, er at Evry skal sørge for at tilbudt løsning og tjenester til enhver tid er i samsvar med lovbestemte sikkerhetskrav, for eksempel personopplysningsloven med tilhørende forskrifter.[57]

Vurdering
Databehandleravtalen mellom DFØ og Evry inneholder beskrivelser av mange av de sentrale elementene Datatilsynet anbefaler at en slik avtale skal inneholde. Det er likevel enkelte mangler og svakheter opp mot anbefalingene som gjør det uklart hva som er rammene for Evrys behandling av personopplysninger, og hvilke krav DFØ stiller til Evrys sikkerhetstiltak for å sikre personopplysninger.

Det kommer ikke klart fram i databehandleravtalen hva som er formålet med Evrys behandling av personopplysninger, eller hvordan og på hvilken måte opplysningene skal behandles og håndteres. Databehandleravtalen inneholder enkelte krav til tiltak for å sikre personopplysningene, men revisjonen savner en mer konkret omtale av tiltak for tilgangskontroll og kontrollmekanismer for å følge opp tilganger. Bildet nyanseres av at DFØ stiller krav til informasjonssikkerhetstiltak i kravspesifikasjonen, men det er ikke koblet eller henvist til disse kravene i databehandleravtalen.

Revisjonen viser at DFØ overfor Evry har stilt krav til informasjonssikkerhet generelt, men i mindre grad regulert eller satt krav til relevante tiltak for å følge opp personopplysningsloven og -forskriften.

Revisjonen vurderer på bakgrunn av dette at DFØ delvis etterlever personopplysningslovens krav til at det skal gå fram av avtale at databehandleren plikter å gjennomgå slike sikringstiltak som følger av § 13.

Finansdepartementet opplyser i tilbakemelding på utkast til rapport at DFØ skal signere en ny databehandleravtale med Evry i mai 2018, og at bestemmelser for Evrys behandling av personopplysninger vil bli ytterligere klargjort i avtalen.

6.1.5. Databehandleravtale mellom DFØ og kundene

Personopplysningsloven § 15 første ledd sier at en databehandler ikke kan behandle personopplysninger på annen måte enn det som er skriftlig avtalt med den behandlingsansvarlige. Andre ledd omtaler at det i avtalen med den behandlingsansvarlige også skal gå fram at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13. Datatilsynet har utarbeidet en veileder som beskriver hva en slik databehandleravtale bør inneholde for å være i tråd med regelverket.

Avtalen mellom DFØ og kundene om leveranse av lønns- og regnskapstjenester består av en hoveddel kalt standardavtalen eller hovedavtalen. Denne er lik for alle kunder.[58] I tillegg består avtalen av fire vedlegg. Standardavtalen inneholder ikke en separat databehandleravtale som vedlegg, men avtalens punkt 8.1.2 fastslår at standardavtalen i seg selv anses å være en databehandleravtale. DFØ arbeider med å fornye tjenesteavtalene

[56] Hovedavtalen pkt. 9.2 Personopplysninger.
[57] Bilag 1, DFØs kravspesifikasjon, pkt. 1.11.3.1.
[58] Staten er ett rettssubjekt. En avtale mellom to statlige virksomheter har derfor ikke de samme kontraktsrettslige virkningene som en avtale mellom to selvstendige rettssubjekter. Partene kan for eksempel ikke reise søksmål knyttet til avtalen. Det framgår av avtalens punkt 10.2.4 at DFØ ikke er erstatningsansvarlig utover eventuell erstatning eller annen kompensasjon fra underleverandør som blir utbetalt til DFØ.

med kundene, inkludert en databehandleravtale.[59] DFØ opplyser i intervju at ny databehandleravtale skal tas i bruk sammen med nye kundeavtaler i løpet av 2018.[60] Revisjonen har tatt utgangspunkt i standardavtalen som var gyldig for de fleste kundene i 2017.

Revisjonen har vurdert standardavtalen mot anbefalinger i Datatilsynets veileder for databehandleravtaler.

Formålet med behandlingen av personopplysninger
Datatilsynets anbefaler at det skal gå klart fram av avtalen hva som er formålet med behandlingen av personopplysninger.

I avtalen står det at «Leverandøren har plikt og rett til å behandle personopplysninger i samsvar med Avtalen, herunder den avtalte arbeidsdelingen, og personopplysningsloven med forskrifter».[61] Dette kan forstås som at formålet for behandlingen vil kunne leses ut av arbeidsdelingen mellom partene. Arbeidsdelingen kommer fram i et eget vedlegg til avtalen.[62] Den viser arbeidsdelingen mellom DFØ og den enkelte kunde for ulike aktiviteter og arbeidsoppgaver i lønnsprosessen. Det går ikke ekplisitt fram hvilke aktiviteter som innebærer behandling av personopplysninger. Enkelte elementer, for eksempel «Vedlikehold av start, slutt og endringer av faste data for ansatte» og «Registrering av variable data for ansatte», kan indikere en behandling av personopplysninger. Ut fra den øvrige avtaleteksten kan man forstå at DFØs behandling av personopplysninger vil ha med beregning og utbetaling av lønn å gjøre.

DFØ bekrefter i intervju at formålet med behandling av personopplysninger ikke er definert klart og tydelig, og at avtalen på dette punktet er noe utdatert.[63]

Bekrivelse av hvordan personopplysningene skal behandles
Datatilsynets anbefaler at det skal gå tydelig fram av avtalen hva databehandleren skal gjøre med personopplysningene. For eksempel bør det opplyses om det skal samles inn opplysninger, om de skal bearbeides på noen måte, om de skal oppbevares eller lagres, eller om det skal skje en kobling mot andre registre og opplysninger.

Revisjonen viser at standardavtalen ikke inneholder noen tydelig beskrivelse av hva DFØ skal gjøre med personopplysningene. Det kommer heller ikke fram noen konkret beskrivelse av dette i avtalens vedlegg. Arbeidsdelingsskjemaet inneholder informasjon om at DFØ skal vedlikeholde og registrere faste og variable data for ansatte, uten at det er forklart hva som ligger i dette.

Punkt 8.1.2 i avtalen viser til at leverandøren ikke kan behandle personopplysningene på annen måte enn det som er avtalt, og heller ikke overføre, overlate eller på annen måte gi tredjepart tilgang til personopplysningene. Avtaleteksten beskriver ikke nærmere hva slags type behandling som er avtalt for personopplysninger, herunder om det foreligger begrensninger i hva databehandleren kan gjøre med personopplysningene.

DFØ bekrefter i intervju at det i dagens avtale ikke blir særskilt omtalt *hvordan* DFØ skal behandle personopplysninger. De påpeker at dagens løsning ikke er tilfredsstillende, og at det kommer fram lite informasjon i avtalen om hva DFØ bruker personopplysningene til. DFØ uttaler at innsamlede opplysninger benyttes for å støtte opp under lønnsprosessen, og at det bare blir spurt etter personopplysninger for å kunne behandle sakene i henhold til de enkelte lønnsprosessene.

Bruk av underleverandører og eventuell overføring til utlandet
Hvis databehandleren gjør bruk av underleverandører for å levere tjenester, skal dette ifølge Datatilsynet gå klart fram av avtalen. Dersom det er aktuelt at personopplysninger skal overføres til utlandet, må også dette reguleres i avtalen.

Under punkt 2 i avtalen omtales det at leverandøren kan benytte eksterne underleverandører ved oppfyllelsen av avtalen. Eventuell overføring av personopplysninger til utlandet er imidlertid ikke nevnt i avtaleteksten.

---

[59] DFØ orienterte om dette i kartleggingsmøte med Riksrevisjonen 15. juni 2017.
[60] Verifisert referat fra intervju med DFØ 1. november 2017.
[61] Standardavtalens pkt. 8.1.2.
[62] Vedlegg 3-1 til standardavtalen.
[63] Verifisert referat fra intervju med DFØ 1. november 2017. DFØ opplyser i interrvjuet at de har utarbeidet utkast til en separat databehandleravtale, som vil bli en del av det nye avtaleverket med kundene, som tas i bruk i løpet av 2018.

Beskrivelse av informasjonssikkerhetstiltak
Datatilsynet anbefaler at avtalen klargjør hva databehandleren skal ha på plass av sikringstiltak for å ivareta konfidensialitet, integritet og tilgjengelighet for behandling av personopplysninger, jf. personopplysningsforskriftens kapittel 2. Veilederen har flere eksempler på hvilke tiltak avtalen bør ha bestemmelser om.

Avtalens punkt 8.2 angir at leverandøren skal ha etablert tilfredsstillende system for informasjonssikkerhet for personopplysningene gjennom planlagte og systematiske tiltak. Videre gis det generelle bestemmelser for informasjonssikkerheten, som også berører personopplysningene.

Sammenholdt med Datatilsynets anbefaling om beskrivelse av relevante sikringstiltak mangler DFØs avtale med kundene:

- konkrete beskrivelser av tiltak for tilgangskontroll og loggføring
- klargjøring av hvem som har ansvar for å melde avvik til Datatilsynet
- beskrivelse av hvilke fysiske sikringstiltak som skal være på plass
- beskrivelse av hva slags type personell/ansatte som skal ha tilgang til personopplysningene
- regulering av gjennomføring av sikkerhetsrevisjoner

DFØ opplyser i intervju at de ikke har utarbeidet noe dokument eller oversikt til bruk for kundene, som viser hvilke konkrete sikkerhetstiltak DFØ skal ha på plass for å sikre personopplysningene i henhold til personopplysningsloven og -forskriften.[64]

DFØ opplyser videre at dokumentet *Sikkerhetsstandard* omtaler sikkerhetstiltak, men at dette er unntatt offentlighet fordi det kan medføre risiko dersom all informasjon blir offentlig kjent, og at det derfor ikke deles med kundene. DFØ opplyser at det generelt er lite henvendelser fra kunder om behandlingen av personopplysninger.

Sletting av opplysninger
Datatilsynets veiledning anbefaler at det klargjøres hva som skal skje med lagrede personopplysninger etter at avtalen eventuelt opphører, for eksempel om opplysningene og lagrede sikkerhetskopier skal tilbakeføres eller slettes. Avtalen inneholder ikke bestemmelser om dette.

Vurdering
Revisjonen viser at avtalen som majoriteten av kundene har med DFØ på revisjonstidspunktet, ikke følger opp sentrale anbefalinger fra Datatilsynet om hva en databehandleravtale bør inneholde. Blant annet blir ikke formålet med behandlingen angitt, hvordan DFØ skal behandle opplysningene kommer ikke tydelig fram, det er manglende omtale av konkrete sikringstiltak, og avtalen regulerer ikke eventuelle overføringer av data til utlandet og hva som skal skje med kundenes personopplysninger når avtalen opphører.

Revisjonen vurderer ut fra dette at DFØ ikke fullt ut etterlever personopplysningslovens krav i § 15 til at det i avtale skal gå fram at databehandleren plikter å gjennomføre slike sikringstiltak som følger av § 13.

Det er risiko for at kundene ikke har tilfredsstillende informasjon om hva DFØ gjør for å beskytte personopplysningene til deres ansatte, og om DFØ sikrer opplysningene på en måte som er i tråd med regelverket. Dette gjør det vanskelig for kundene å vurdere om sikringen er god nok i forhold til deres ønskede nivå for sikkerheten.

6.1.6. Ansvars- og myndighetsforhold for lønnssystemet SAP

Personopplysningsforskriften stiller i § 2-7 første og andre ledd krav om at det skal etableres og dokumenteres klare ansvars- og myndighetsforhold for bruk av informasjonssystemer. Med dette forstår vi at virksomheten må ha etablert et system der det går klart fram hvem eller hvilke roller som er ansvarlig for ulike sider ved et system. Datatilsynet påpeker at det er viktig at ansvar og myndighet relatert til drift av informasjonssystemet (driftsledelse)

[64] Verifisert referat fra intervju med DFØ 1. november 2017.

og for oppfølging av sikkerhetsarbeid (sikkerhetsledelse), er klarlagt. Videre må ansvarsforholdene være besluttet av virksomhetens ledelse, dokumenteres og gjøres kjent for virksomhetens medarbeidere.[65]

Ansvarsforholdene for sikkerhetsarbeidet i DFØ blir beskrevet i flere policydokumenter.[66] Det beskrives at DFØs direktør har det overordnede ansvaret for sikkerheten i DFØ. Avdelingsledere er ansvarlige for sikkerheten i sin avdeling, og ansvaret omfatter alle aktiva (informasjon, personell, lokaler, systemteknisk) som avdelingen forvalter. Ansvaret dekker gjennomføring av sikkerhetstiltak og kontroll av at sikkerheten er ivaretatt i avdelingen.

I tillegg beskrives en egen rolle som sikkerhetsleder, som har et overordnet koordinerings- og kontrollansvar for etterlevelse av sikkerhetspolicy og sikkerhetsbestemmelser i organisasjonen. DFØ opplyser i intervju at strategidokumentene ligger lett tilgjengelig for alle ansatte på intranettet. Alle dokumentene er godkjent av ledelsen.[67]

I DFØs sikkerhetsstandard presenteres begrepet *systemeier*. Systemeier beskrives å ha «det funksjonelle ansvaret for systemet (tjenesten med underliggende applikasjoner og infrastruktur) som f.eks. å avklare oppgraderinger, brukeropplæring, utvikling av rutiner for bruk av systemet, sikre at utnyttelsen er best mulig, sikre at løsningen er fornuftig i forhold til kost/nytte, følge opp drift og videre utvikling mot ev.leverandør».[68] I et annet avsnitt i standarden står det imidlertid at: «Når det gjelder rollen som systemeier er denne uavklart pr. d.d.».

I notat om fordeling av systemroller, er innholdet i rollen systemeier beskrevet annerledes. Systemeierrollen beskrives her som en mer strategisk rolle. Systemeieren skal blant annet ha ansvar for at systemet støtter opp under prosesser og tjenester, og at systemet videreutvikles i tråd med overordnede strategier. Notatet presenterer også to andre systemroller: *systemansvarlig* og *systemforvalter*. Systemansvarlig er ansvarlig for at systemet leverer avtalt funksjonalitet og kvalitet mens systemforvalteren har det operative ansvaret for å holde systemet oppdatert og for å ivareta systemteknisk drift, utvikling og vedlikehold.[69] De tre rollene blir presentert som hierarkiske med systemeieren på topp.

KPMG gjennomførte i 2017 en kartlegging av IT-styringen i DFØ. [70] Kartleggingen omtaler uklarheter rundt eierskap til informasjonssikkerhet og at ansatte synes det er komplisert å forholde seg til begreper som tjenesteeier, systemeier, prosesseier, systemansvarlig og systemforvalter. Det uttales i rapporten at det er sannsynlig at det i flere sammenhenger snakkes forbi hverandre i mangel på en felles begrepsforståelse.

Den mottatte listen over systemroller for de ulike systemene viser at det er avdelingsdirektør for lønnsavdelingen som er systemeier for SAP, og som må forstås å ha det øverste ansvaret for systemet. Rollene systemansvarlig og systemforvalter for SAP er tillagt ansatte i seksjon for applikasjonsforvaltning (LA App).[71] Seksjonen har ansvar for å forvalte og utvikle SAP.[72]

Vurdering

Revisjonen viser at DFØ formelt har avklart ansvarsforholdene for sikkerhetsarbeidet. Ansvars- og myndighetsforhold for lønnssystemet SAP er avklart i den forstand at systemrollene er fordelt til navngitte personer. Revisjonen viser imidlertid at innholdet og ansvarsfeltet for rollen som systemeier er uklart, da rollen blir ulikt presentert i forskjellige styringsdokumenter. KPMGs undersøkelse bekrefter at en slik uklarhet er reell. Uklare ansvarslinjer kan blant annet medføre risiko for at feil ikke blir rettet, at feil ikke blir oppdaget, eller at systemet ikke blir holdt oppdatert eller vedlikeholdt.

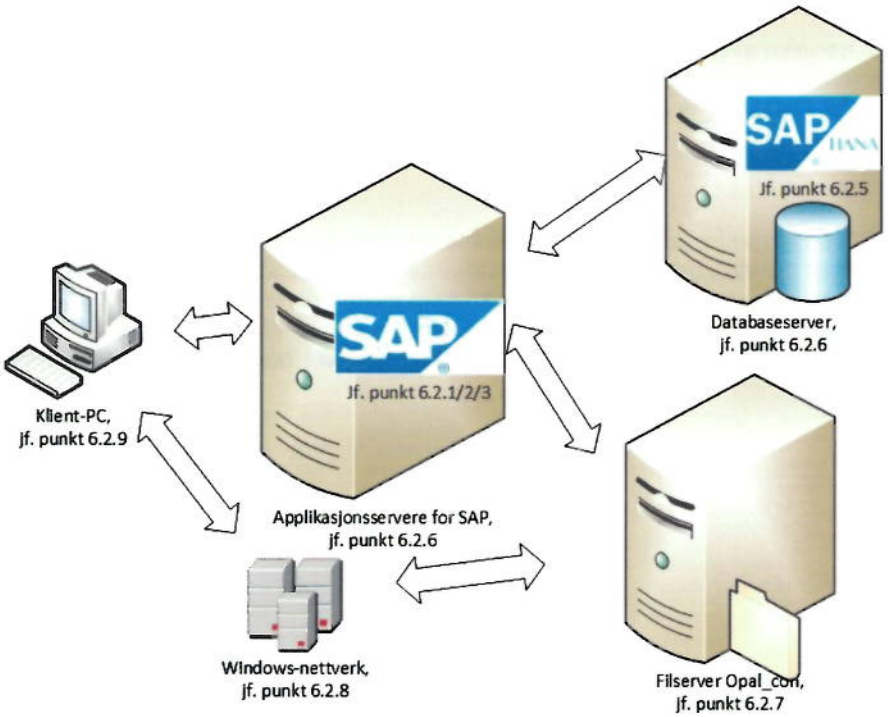
---

[65] Datatilsynet (2000) *Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer.* Kommentarer til § 2-7, s. 9.
[66] DFØ (2015) *Sikkerhetspolicy*. DFØ (2017) *Organisering av sikkerhets- og beredskapsarbeidet – Roller og ansvar.*
[67] Verifisert referat fra intervju med DFØ 1. november 2017.
[68] DFØ (2013) *Sikkerhetsstandard.* Kap. 2, s. 5.
[69] DFØ: Notat av 07.05.2017 – Beslutningssak – fordeling av systemroller.
[70] IT-styring. Evaluering av KPMG datert 7. juli 2017.
[71] DFØ: Oversikt systemer og systemroller. Sist oppdatert 24. november 2017.
[72] DFØ: Virksomhetsplan for lønnsavdelingen 2017, kap. 2.2, s. 7.

6.2. Problemstilling 2: Har DFØ sikret at det gjennomføres systematiske tiltak som sørger for tilfredsstillende informasjonssikkerhet for personopplysninger i SAP?

Under denne problemstillingen gjennomgås gjennomføring av tiltak for å sikre personopplysninger som behandles i DFØs oppsett av SAP. Et systemmiljø for SAP er komplisert. Figuren nedenfor gir et svært forenklet bilde som et grunnlag for å illustrere hva som er kontrollert i denne revisjonen:

- Behandling av lønns- og personaldata skjer i SAP, jf. punkt 6.2.1, 6.2.2 og 6.2.3.
- Alle servere som ligger til grunn for SAP, driftes av Evry/IBM. Omtale av driftsleverandørens tilgangsrettigheter er omtalt i punkt 6.2.4.
- Programvaren som ligger til grunn for SAP, ligger på applikasjonsservere, jf. punkt 6.2.6.
- Lønns- og personaldataene lagres i en database (SAP Hana), jf. punkt 6.2.5.
- Databasen ligger på en databaseserver, jf. punkt 6.2.6.
- Rapporter fra SAP for kundevirksomheter, samt data som skal lastes inn i SAP, lagres på filserveren Opal_con, jf. punkt 6.2.7.
- Det benyttes et Windows-basert nett med katalogtjenesten Active Directory for å autentisere brukere og administrere tilgangsrettigheter, jf. punkt 6.2.8. Revisjonen er begrenset til DFØs ansatte.
- En bruker kobler seg til SAP via programvare på sin PC. Sikring av brukeres PC-er er omtalt i punkt 6.2.9. Revisjonen er begrenset til DFØs ansatte.
- Kryptering av kommunikasjon mellom de ulike servere mv. er omtalt i punkt 6.2.10.



Illustrasjon: Riksrevisjonen

Det er utarbeidet et vedlegg hvor detaljert informasjon om DFØs tekniske sikkerhetstiltak er omtalt. Vedlegget er unntatt offentlighet[73].

6.2.1. Sikker konfigurasjon av SAP

Ifølge personopplysningsforskriften § 2-7 tredje ledd skal informasjonssystemer konfigureres slik at man oppnår tilfredsstillende informasjonssikkerhet. Med «konfigurasjon» menes informasjonssystemets utforming, det vil si utstyr og program samt sammenkoblinger mellom disse.[74] Konfigurasjonen skal dokumenteres og ikke endres uten autorisasjon fra den behandlingsansvarliges daglige leder.

Nasjonal sikkerhetsmyndighet anbefaler at det etableres en sikker konfigurasjon av maskin- og programvare som et grunnlag for virksomhetens sikkerhet, og at det systematisk verifiseres at denne konfigurasjonen etterleves.[75] Leverandøren SAP legger til grunn en tilsvarende metode ved å etablere en standard for sikker konfigurasjon av SAP («SAP Security Baseline Template») og ved å tilgjengeliggjøre verktøy som kan verifisere etterlevelse av denne standarden. [76] Leverandøren beskriver standarden som minimums sikkerhetskrav og generelt en beste praksis som vil gjelde for alle SAP-systemer uavhengig av risikovurdering.

Krav til konfigurasjon
I avtalen med Evry om drift av lønnssystemet har DFØ stilt krav om at leverandøren til enhver tid skal følge beste praksis for håndtering av informasjonssikkerhet i forbindelse med tjenesten og systemer.[77] Leverandøren har akseptert dette punktet i avtalen uten at det er spesifisert nærmere.[78] Leverandørens løsningsspesifikasjon gir beskrivelser av systemmiljøet og omtaler blant annet løsninger for tilgangskontroll.[79] Løsningen er basert på leverandørens standardplattformer og standardtjenester.

Det er i avtaledokumenter fra DFØ ikke vist til noe dokumentasjon fra leverandører eller andre som grunnlag for å vurdere begrepet «beste praksis». DFØ bekrefter i intervju at det ikke er definert hva som ligger i begrepet beste praksis for SAP eller for databasen som benyttes for systemet.[80] Selv om det i avtalen legges til grunn at beste praksis skal anvendes, uttaler DFØ at det vil ta tid å nå opp til beste praksis etter overgangen til ny database i 2017.[81]

Verktøy for å sikre etterlevelse av en sikker konfigurasjon
DFØ anvender flere rapporter som kan gi grunnlag for å verifisere om en standard for sikker konfigurasjon av SAP etterleves:[82]

- *Earlywatch Alert (EWA).* Denne kjøres ukentlig. Denne er driftsrelatert, men inneholder et kapittel om sikkerhet som dekker enkelte kritiske momenter i SAPs standard for sikker konfigurasjon.
- *SAP OS/DB Migration Check.* Denne benyttes ifølge DFØ ved større endringer. Formålet med rapporten er å gi støtte ved skifte av operativsystem eller database. Den omfatter enkelte sikkerhetsrelaterte aspekter.
- *SAP Security Optimization Service* (SOS). Dette er en mer omfattende verifisering mot standard konfigurasjon. Rapporten kjøres ifølge DFØ sjelden. Den ble kjørt etter forespørsel fra Riksrevisjonen i forbindelse med denne revisjonen. DFØ opplyser at rapporten forrige gang ble kjørt i 2016.

Analyse av en rapport fra SAP Security Optimization Service (SOS-rapporten) som ble kjørt i forbindelse med denne revisjonen, viser svakheter i DFØs oppsett av SAP, spesielt når det gjelder tilgangsrettigheter og arbeidsdeling, jf. punkt 6.2.2. DFØ opplyser at det er mye i rapporten direktoratet vurderer å følge opp.[83] Det var på møtetidspunktet ikke laget noen prioriteringsliste, men DFØ vil prioritere punktene med høy prioritet fra SAP. En del av avvikene kan ifølge DFØ forklares ut fra kundespesifikke forhold.

---

[73] Jf. offentlighetsloven § 13, jf. riksrevisjonsloven § 15.
[74] Datatilsynet: Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer, omtale av forskriftens § 2-7.
[75] Nasjonal sikkerhetsmyndighet (2017) *NSMs grunnprinsipper for ikt-sikkerhet – versjon 1.0.*
[76] SAP Knowledge Base Article 2253549. The SAP Security Baseline Template.
[77] Avtale mellom DFØ og Evry, bilag 1 – kundens kravspesifikasjon, punkt 1.1.2.1 og 1.11.2.3.
[78] Avtale mellom DFØ og Evry, bilag 2 – vedlegg 1 – utfylt kravspesifikasjon, punkt 1.11.2.3.
[79] Avtale mellom DFØ og Evry, bilag 2 – Leverandørens løsningsspesifikasjon.
[80] Verifisert referat fra intervju med DFØ 1. desember 2017.
[81] Verifisert referat fra intervju med DFØ 14. desember 2017.
[82] Verifisert referat fra intervju med DFØ 1. desember 2017 og 14. desember 2017.
[83] Verifisert referat fra intervju med DFØ 14. desember 2017.

DFØ mener SOS-rapporten tar lang tid å kjøre, og at EWA-rapportene fanger opp de forholdene som er av betydning.[84] EWA-rapporten legger vekt på drift, men enkelte sentrale sikkerhetsavvik tas opp, for eksempel manglende logging og bruk av standardkonto på databasenivå, samt at det er mange brukere som har kritiske autorisasjoner i SAP, jf. punktene 6.2.2 og 6.2.5.[85] Selv om rapporten kjøres ukentlig, er ikke disse sikkerhetsmessige svakhetene fulgt opp av DFØ på revisjonstidspunktet i begynnelsen av desember 2017.

DFØ opplyser i intervju at ved behov for endringer som følge av rapportene diskuterer DFØ og IBM anbefalingene fra rapportene.[86] IBM utarbeider en endringsanmodning som godkjennes av DFØ. DFØs gjennomgang av rapportene for øvrig, inkludert punkter der DFØ velger å akseptere risiko, kan ikke dokumenteres.

Vurdering
Revisjonen viser at DFØ ikke etterlever kravet om å dokumentere hvordan SAP skal konfigureres for å sikre tilfredsstillende informasjonssikkerhet. Det foreligger bare generelle krav som ikke er konkretisert, ikke en definert sikker konfigurasjon, slik NSM anbefaler. DFØ har dermed heller ikke rutiner for systematisk å måle om en sikker konfigurasjon etterleves, selv om det tas ut rapporter som kan brukes til dette. Manglende kontroll med konfigurasjon gir risiko for at systemet settes opp på måter som kan eksponere sensitiv informasjon for uvedkommende.

6.2.2. Sikring av SAP

Ifølge personopplysningsforskriften § 2-8 første ledd skal medarbeidere hos den behandlingsansvarlige bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk. Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystemet, jf. § 2-14 første ledd. Personopplysninger hvor konfidensialitet er nødvendig, skal beskyttes mot uautorisert innsyn, jf. § 2-11 første ledd.

Roller og rettigheter
Standarden NS-ISO/IEC 27002:2017 anbefaler at det legges til grunn et prinsipp om at tilgang til systemer og informasjon bør begrenses til det som er nødvendig for å utføre pålagte arbeidsoppgaver for den enkelte.[87]

I rapporten fra SAP Security Optimization Service (SOS-rapporten) tas det opp en rekke punkter som gjelder tilganger til ulike funksjoner. Analyse av rapporten viser at det er faste grupper av ansatte som går igjen på de fleste punktene. Dette er som oftest

- ansatt i Lønnsavdelingen i DFØ (i underkant av 200 brukere)
- ansatt i seksjon for applikasjonsforvaltning i DFØ (ca. 40 brukere)

Analysen viser at alle ansatte innen hver av disse gruppene har de samme rettighetene i SAP. DFØ uttaler i intervju at det ikke er lagt til grunn en mer finmasket fastsettelse av rettigheter i SAP ut fra den enkeltes arbeidsoppgaver innenfor disse gruppene ansatte.[88]

Analyse av rapporten viser at alle ansatte i lønnsavdelingen har tilgang til blant annet å resette passord, låse opp brukerkontoer, kjøre jobber under en annen brukerkonto og endre alle tabeller med persondata. Når det gjelder autorisasjon til funksjoner mener DFØ det er vanskelig å skille mellom behov de ulike ansatte i lønnsavdelingen har.[89] DFØ har dermed valgt å tildele rettigheter til større grupper (for eksempel hele lønnsavdelingen) heller enn å avgrense rettighetene til hver enkelt bruker til de konkrete arbeidsoppgavene vedkommende har. Lite differensierte tilganger til SAP i DFØs lønnsavdeling ble tatt opp av Riksrevisjonen allerede ved revisjonen av regnskapet for 2011.[90]

Som en del av revisjonen er det forespurt om mer detaljerte uttrekk som viser hvilke brukere som har de ulike rettighetene som er nevnt ovenfor. Dette er ikke mottatt.

---

[84] Verifisert referat fra intervju med DFØ 1. desember 2017.
[85] SAP Service Report – EarlyWatch Alert for perioden 27. november 2017–3. desember 2017.
[86] Verifisert referat fra intervju med DFØ 1. desember 2017.
[87] NS-ISO/IEC 27002:2017 punkt 9.1.1.
[88] Verifisert referat fra intervju med DFØ 1. desember 2017.
[89] Verifisert referat fra intervju med DFØ 14. desember 2017.
[90] Brev fra Riksrevisjonen til DFØ 8. mars 2012.

Finansdepartementet opplyser i tilbakemelding på utkast til rapport at tilgangene må ses i sammenheng med DFØs omorganisering av økonomitjenesteområdet i perioden 2013-2016. En effektiv prosessorganisering forutsetter ifølge departementet at alle ansatte som arbeider med lønn i DFØ har tilgang til alle kundedata på alle klienter i SAP. DFØs valg skal reflektere en balanse mellom hensynet til effektivitet, brukervennlighet, fleksibilitet og risiko.

Superbrukere
I NS-ISO/IEC 27002:2017 legges det til grunn at tildeling og bruk av privilegerte tilgangsrettigheter bør begrenses og kontrolleres, og at de bør tildeles ut fra tjenstlig behov og fra hendelse til hendelse.[91] Leverandøren SAP legger til grunn at profil som superbruker ikke bør tildeles noen brukere med mulig unntak av nødbrukerkontoer dersom bruk av disse er tilstrekkelig kontrollert og overvåket.[92]

SOS-rapporten viser at om lag 17 brukerkontoer[93] har rettighet som superbruker i SAP.[94] DFØ opplyser i intervju at dette er tekniske brukerkontoer og driftsleverandøren Evry/IBMs superbrukere.[95] DFØ har ikke gjort noen vurderinger av hvor store tilganger Evry/IBM trenger. Det er ifølge DFØ ikke mulig for virksomheten å forutse hva driftsleverandør trenger av tilganger, og de opplever det som lite hensiktsmessig å begrense tilganger. DFØ bemerker at driftsleverandøren uansett har tilganger til SAPs database.

Krav til passord i SAP
NS-ISO/IEC 27002:2017 punkt 9.4.3 anbefaler at virksomheten har et styringssystem som kvalitetssikrer passord. Det anbefales blant annet videre at styringssystemet tvinger fram valg av kvalitetspassord og bytte av passord med jevne mellomrom. Leverandøren SAPs minimumsstandard har i tillegg anbefalinger til andre parametere om passord.[96]

Analyse av uttrekk viser at det er satt krav til minimumslengde, kompleksitet mv. for passord, men at disse ikke etterlever anbefalinger fullt ut på flere punkter. Sikkerhetskrav for SAP må ses i sammenheng med at systemet inneholder data om mange personer, inkludert personer med beskyttelsesbehov, og noe informasjon som er definert som sensitiv. Spesielt DFØs egne ansatte har tilgang til mye informasjon.

DFØ uttaler at størstedelen av brukerne autentiseres via DFØ-ID og ikke passord i SAP. Passordkravene for DFØ-ID er noe strengere enn DFØs policy for passord og kravene i SAP.[97]

Standard brukerkontoer
Ved installasjon av SAP blir det opprettet en del brukerkontoer med standard navn og passord, som til dels har store rettigheter i systemet. Brukerkontoene og passordene er offentlig kjent og brukes ved dataangrep. Leverandøren SAP anbefaler derfor at standardpassord for disse kjente brukerkontoene endres, og i tillegg enkelte andre sikkerhetstiltak. [98]

Analyse av rapporter og uttrekk viser at passord er endret slik som anbefalt, men at ikke alle andre sikkerhetstiltak for å beskytte standard brukerkontoer er gjennomført som anbefalt.

Vurdering
Revisjonen viser at DFØ ikke etterlever krav i personopplysningsforskriften om at brukere bare skal være autorisert for å utføre pålagte oppgaver, ved ikke å tilpasse tilgangsrettigheter for ansatte til oppgavene deres. DFØ etterlever heller ikke kravene i personopplysningsforskriften om å beskytte personopplysninger mot uautorisert innsyn og sette i verk sikkerhetstiltak som skal hindre uautorisert bruk av informasjonssystemet. Tildeling av rettigheter til driftsleverandør er videre ikke begrenset til tjenstlig behov i samsvar med anbefalinger i ISO-standard og leverandøren SAP. Tilganger utover tjenstlig behov øker risiko for uautorisert tilgang til personopplysninger. Svake krav til autentisering øker videre risiko for at uvedkommende kan få tilgang til personopplysninger.

6.2.3. Utviklingsmiljøer for SAP

---

[91] NS-ISO/IEC 27002:2017 punkt 9.2.3.
[92] SAP Security Baseline Template v. 1.9, punkt 2.4.
[93] DFØ har fordelt kundevirksomhetene på ulike klienter. Det varierer noe mellom klienter hvor mange som har denne profilen.
[94] SAP Security Optimization Service Report, punkt 3.2.
[95] Verifisert referat fra intervju med DFØ 14. desember 2017.
[96] SAP Security Baseline Template v. 1.9, punkt 2.3.
[97] Brev fra DFØ til Finansdepartementet av 24.04.2018. Kommentarer til Riksrevisjonens utkast til rapport for 2017 om sikring av personopplysninger.
[98] SAP Security Baseline Template v. 1.9, punkt 2.4 og 4.4.

Det skal treffes tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig, jf. personopplysningsforskriften § 2-11 første ledd. Personopplysningsforskriften stiller i § 2-7 første ledd krav om at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemer.

Reelle data i testmiljø

NS-ISO/IEC 27002:2017 anbefaler at bruk av driftsdata som inneholder personlige identifiserbar informasjon eller annen konfidensiell informasjon bør unngås for testformål.[99] Hvis slike data allikevel brukes for testformål, anbefaler standarden at alle sensitive data beskyttes gjennom fjerning eller modifisering. Samme prosedyre for tilgangskontroll bør videre benyttes i utviklingssystem som i produksjonssystemet – det bør kreves egen autorisasjon hver gang driftsdata kopieres til et testmiljø, og driftsdata bør slettes fra testmiljøet straks testingen er fullført.

DFØ opplyser i intervju at det finnes reelle persondata i test-, utvikling- og sandkassemiljøene for SAP.[100] Tilganger og rettigheter til dataene styres ifølge DFØ på samme måte uavhengig av hvilket miljø en bruker skal ha tilgang til.

Finansdepartementet uttaler i tilbakemelding på utkast til rapport at reelle persondata i test- og utviklingsmiljø er et bevisst valg for å sikre best mulig kvalitet i test og reduksjon av kostnadene. Det opplyses imidlertid at DFØ vurderer denne praksis opp mot nye og strengere krav på dette området i EUs personvernforordning.

Produksjons- og utviklingsansvar

NS-ISO/IEC 27002:2017 anbefaler at miljøer for test, utvikling og drift bør være separert for å redusere risiko for uautorisert tilgang eller endringer i driftsmiljøet. Hvis utviklings- eller testpersonell har tilgang til driftsmiljø, pekes det i standarden på at de har mulighet til å introdusere uautorisert og utestet kode eller endre driftsdata.[101] For SAP spesielt anbefaler den tyske brukerforeningen for systemet at ingen tilpasninger eller utvikling bør skje i produksjonssystemer, og at utviklere bør ha begrensede eller ingen rettigheter i produksjonssystemer.[102]

Ut fra de foreliggende rollebeskrivelsene synes både drifts- og utvikleransvaret for SAP å være tillagt rollen systemforvalter. Både drifts- og utviklermiljøet til SAP ligger i seksjon for applikasjonsforvaltning i DFØ (LA App).

DFØ opplyser i intervju at de ikke driver så mye med utvikling i tradisjonell betydning, det er mer spisset utvikling i forbindelse med tilpasninger av funksjonalitet.[103] DFØ uttaler i intervju at «Noen ansatte i LA app er utviklere i betydning av at man kan endre program eller tabell. Rettighetene for dette ligger i autorisasjonsrollene. I tillegg må man ha en utviklernøkkel utstedt av SAP for å få endre i programmet. Også konsulenter som skal jobbe med endringer må ha dette. Konsulenter får tilgang til produksjonssystemet hvis de skal gjøre noe der, ellers kun test og utvikling. Konsulenter kan se alle data. Det opereres med samme type tilgang i både test, utvikling og produksjon».

Analyse av uttrekk av liste over brukere med utviklernøkler viser at følgende har tilgang til utviklernøkler:

- 11 ansatte i seksjon for applikasjonsforvaltning
- ansatte hos driftsleverandør som drifter systemet
- 16 eksterne konsulenter
- enkelte andre ansatte i blant annet IT-seksjonen i DFØ

Ved siden av utviklerrettigheter har alle ansatte i LA App vide rettigheter i produksjonssystemet for SAP.[104] Ansatte i IBM som drifter SAP for DFØ, er superbrukere i produksjonssystemet, jf. foregående punkt.

Rapport om IT-styring i DFØ fra KPMG omtaler intervjuer med ansatte hvor det går fram at mange i organisasjonen savner klare ansvarsforhold mellom drift og utvikling. Det beskrives at én av konsekvensene av å blande utvikling og drift er at prosjekter ofte ikke avsluttes som planlagt, at de bare ebber ut eller gjenoppstår med nytt navn. [105]

Vurdering

---

[99] NS-ISO/IEC 27002:2017 punkt 14.3.1.
[100] Verifisert referat fra intervju med DFØ 1. desember 2017.
[101] ISO 27002: 2017 pkt. 12.1.4.
[102] Deutschsprachige SAP®-Anwendergruppe e.V.(DSAG): Best Practice Guidelines for Development Practical tips on the ABAP Development, punkt 8.1.4.
[103] Verifisert referat fra intervju med DFØ 14. desember 2017
[104] Verifisert referat fra møter mellom DFØ og Riksrevisjonen 1. og 14. desember 2017.
[105] IT-styring. Evaluering av KPMG datert 7. juli 2017.

Revisjonen viser at DFØ ikke fullt ut etterlever krav om tiltak mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. DFØ etterlever ikke anbefalingen i ISO-standarden om at driftsdata ikke bør benyttes for testformål, men tilgangskontroller er satt i verk som et kompenserende tiltak. Driftsdata i test- og utviklingsmiljøer øker risikoen for uautorisert tilgang til persondata fordi det øker angrepsflaten.

Revisjonen viser videre at DFØ ikke etterlever krav i personopplysningsforskriften om at det skal etableres klare ansvars- og myndighetsforhold for bruk av informasjonssystemer. Drifts-, test- og utviklingsmiljøer er ikke separert, og mange utviklere har vide tilganger i produksjonssystem for SAP, som ikke er i samsvar med anbefalinger i ISO-standarden og bransjestandarder. Dette bruddet på arbeidsdeling gir risiko for at utviklere kan introdusere feil i programkode eller manipulere data direkte i produksjonssystemet.

6.2.4. Tilgang til DFØs IT-infrastruktur for ansatte i Evry og IBM Services

Ifølge personopplysningsforskriften § 2-8 første ledd skal medarbeidere hos den behandlingsansvarlige bare bruke informasjonssystemet for å utføre pålagte oppgaver og selv være autorisert for slik bruk. NS-ISO/IEC 27002:2017 anbefaler at det etableres en formell prosess for forvaltning av brukertilgang.[106] Prosessen anbefales å omfatte endring av tilgangsrettigheter ved nye jobber eller roller, umiddelbar fjerning av rettigheter til personer som har forlatt organisasjonen, og periodisk gjennomgang av tilgangsrettigheter. Privilegerte tilgangsrettigheter bør ifølge standarden begrenses og kontrolleres.

Revisjonen har mottatt uttrekk av brukere i Evry og IBM Services som viser hvem som tilgangsrettigheter per 1. september og 17. november 2017. Analyse av uttrekket viser at det er vesentlige forskjeller i tilgangene på de to tidspunktene. Per 1. september er det totalt 272 ansatte i Evry og IBM Services som har tilgang til DFØs IT-miljø. Dette er redusert til 128 brukere per 17. november. Analyse viser for øvrig følgende:

- 177 brukere har mistet tilgangsrettighetene sine i denne perioden.
- Det har kommet til 33 nye brukere.
- Per 1. september hadde 119 brukere tilgang på operativsystemnivå i DFØs IT-miljø. Per 17. november er dette redusert til 26.
- Per 1. september hadde 39 av Evrys brukere tilgang på operativsystemnivå i DFØs IT-miljø. Per 17. november er det ingen som har denne tilgangen.

Listene viser at det er mange brukere som er blitt deaktivert i denne perioden. DFØ mener at noen av de store endringene i brukerrettigheter kan skyldes overgang til ny database i 2017.[107]

Ved revisjon av DFØs regnskap for 2011 tok Riksrevisjonen opp at DFØ ikke hadde kjennskap til hvor mange personer hos leverandøren som hadde tilgang til SAPs database.[108] I sitt svar opplyser DFØ at de hadde mottatt en oversikt fra Evry som viste at 27 personer fordelt på tre områder hadde tilgang til DFØs systemer på dette tidspunktet.[109] Det konstateres at det var vesentlige færre personer hos leverandøren som hadde tilgang til DFØs systemer på dette tidspunktet.

Revisjonen viser at tilgangsrettigheter for ansatte i Evry og IBM Services ble vesentlig redusert i løpet av høsten 2017. Den store endringen indikerer at rutiner for å holde tilgangsrettigheter oppdatert ved endringer ikke har etterlevd anbefalinger i ISO-standarden og dermed krav i personopplysningsforskriften om bare å ha autorisasjoner for å utføre pålagte oppgaver. Større tilgangsrettigheter enn nødvendig øker risikoen for at personopplysninger kan komme på avveie.

6.2.5. Sikring av SAPs database

Ifølge personopplysningsforskriften § 2-14 første ledd skal sikkerhetstiltak hindre uautorisert bruk av informasjonssystemet og gjøre det mulig å oppdage forsøk på slik bruk. Videre setter personopplysningsforskriften § 2-11 første og andre ledd krav om beskyttelse mot uautorisert innsyn i

---

[106] NS-ISO/IEC 27002:3013 punkt 9.2.1 og 9.2.3.
[107] Verifisert referat fra møte mellom DFØ og Riksrevisjonen 14. desember 2017.
[108] Brev fra Riksrevisjonen til DFØ 8. mars 2012.
[109] Brev fra DFØ til Riksrevisjonen 30. mars 2012.

personopplysninger hvor konfidensialitet er nødvendig og annen informasjon med betydning for informasjonssikkerheten. Ifølge personopplysningsforskriften § 2-8 tredje ledd skal autorisert bruk av informasjonssystemet registreres. Datatilsynet har avklart at dette gjelder nødvendig logging for gjennomføring av avviksbehandling, inkludert oppklaring av sikkerhetsbrudd, og for drift av informasjonssystemet.

Tilgangskontroller
NS-ISO/IEC 27002:2017 anbefaler at brukere av informasjonssystemene tildeles brukerkontoer med unike navn, slik at den enkelte kan knyttes til og holdes ansvarlig for sine handlinger.[110] Privilegerte rettigheter bør ifølge standarden tildeles på bakgrunn av tjenstlig behov og fra hendelse til hendelse. Krav til utløp av privilegerte rettigheter bør være definert. For upersonlige brukerkontoer bør konfidensialiteten til hemmelig autentiseringsinformasjon ivaretas når den deles, for eksempel ved å bytte passord hyppig.

[redacted]

Analyse av uttrekk fra databasen viser at det ikke benyttes personlige brukerkontoer for å administrere databasen. Det er bare tre aktive brukerkontoer med passord i databasen. [redacted]

Analyse av uttrekk viser at krav til passord i passordpolicy definert i databasen ikke etterlever anbefalinger på flere punkter[112] – blant annet viser uttrekket at databasen er konfigurert slik at passord ikke har utløpsdato.

DFØ opplyser i intervju at for å kunne benytte en brukerkonto mot databasen må man ha rettigheter som gir tilgang til driftleverandørens nettverk og til DFØs servere, samt tilgang til passorddatabasen for å kunne hente ut passordet.[113] Det går fram av avtalen mellom DFØ og Evry at det benyttes tofaktorautentisering for administratorers tilgang til administrasjonsnettverket fra ikke forhåndsgodkjente nettverk.[114]

Logging
NS-ISO/IEC 27002:2017 anbefaler at hendelseslogger som registrerer brukeraktiviteter, avvik, feil og informasjonssikkerhetshendelser, produseres, oppbevares og gjennomgås regelmessig.[115]

Analyse av uttrekk fra databasen viser at logging med hensyn til sikkerhet ikke er aktivert i databasen, og det er dermed heller ikke lagt inn noen policy for hva som skal logges. Det innebærer at handlinger foretatt av administratorer ikke er sporbare, hverken med hensyn til hvem som har utført aktiviteter, eller hva som er gjort. Svakheten går fram av de ukentlige Earlywatch Alert (EWA)-rapportene som DFØ mottar, jf. punkt 6.2.1.

DFØ opplyser at rapporten OS/DB Migration Report ble lagt til grunn ved innføring av SAP Hana.[116] Ved gjennomgang av rapporten oppdaget DFØ at systemet var satt opp slik at ingen logging blir utført. Det er opprettet endringssak for å endre dette. På revisjonstidspunktet i desember 2017 var imidlertid ikke endringen gjennomført. DFØ opplyser at sikkerhetslogging nå er iverksatt.[117]

Vurdering
Revisjonen viser at DFØ ikke etterlever kravene i personopplysningsforskriften om at sikkerhetstiltak skal hindre uautorisert bruk av eller innsyn i informasjon i SAPs database. Autorisert bruk av databasen registreres ikke. Det var på revisjonstidspunktet heller ikke etablert logger som kan gjøre det mulig å oppdage forsøk på uautorisert bruk. Begge deler er krav i medhold av personopplysningsforskriften. [redacted]
Manglende logging innebærer at handlinger foretatt av administratorer eller andre direkte i databasen ikke er sporbare. Eventuelle dataangrep eller uønskede hendelser vil vanskelig kunne oppdages eller analyseres. Manglende bruk av personlige brukerkontoer svekker videre mulighet til å identifisere hvem som har gjort ulike endringer i databasen.

---

[110] NS-ISO/IEC 27002:3013 punkt 9.2.1 og 9.2.3.
[111] SAP HANA Security Guide punkt 6.4.
[112] SAP HANA Security Guide, punkt 7.3.
[113] Referat fra møte mellom Riksrevisjonen og DFØ 14. desember 2017.
[114] Avtale mellom DFØ og Evry, bilag 2: Leverandørens løsningsspesifikasjon, side 36.
[115] NS-ISO/IEC 27002:3013 punkt 12.4.1
[116] Referat fra møte mellom Riksrevisjonen og DFØ 1. desember 2017.
[117] Brev fra DFØ til Finansdepartementet av 24.04.2018. Kommentarer til Riksrevisjonens utkast til rapport for 2017 om sikring av personopplysninger.

6.2.6. Sikring av database- og applikasjonsservere for SAP

Sikkerhetstiltak skal hindre uautorisert bruk av informasjonssystem med personopplysninger og gi beskyttelse mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig, og annen informasjon med betydning for informasjonssikkerheten, jf. personopplysningsforskriften §§ 2-11 første og andre ledd og 2-14 første ledd. Videre skal skal autorisert bruk av informasjonssystemet registreres, ifølge personopplysningsforskriften § 2-8 tredje ledd.

Tilgangskontroller i databaseserver for SAP
NS-ISO/IEC 27002:2017 anbefaler at brukere av informasjonssystemene tildeles brukerkontoer med unike navn, slik at den enkelte kan knyttes til og holdes ansvarlig for handlingene sine.[118] Privilegerte rettigheter bør ifølge standarden tildeles på bakgrunn av tjenstlig behov og fra hendelse til hendelse. Krav til utløp av privilegerte rettigheter bør være definert. For generiske brukerkontoer bør konfidensialiteten til hemmelig autentiseringsinformasjon ivaretas når den deles, for eksempel ved å bytte passord hyppig. Både Nasjonal sikkerhetsmyndighet[119] og Center for Internet Security[120] anbefaler at autentisering basert på flere faktorer[121] legges til grunn ved pålogging som systemadministrator. Dersom dette ikke er mulig, anbefaler Center for Internet Security passord lenger enn 14 tegn.

Analyse av uttrekk av data viser at det bare er fire generiske aktive brukerkontoer på operativsystemnivå på databaseserveren. Personlige brukerkontoer brukes ikke på serveren.

Det går fram av avtale mellom DFØ og Evry at det benyttes to-faktorautentisering for administratorers tilgang til administrasjonsnettverket fra ikke forhåndsgodkjente nettverk.[122] Administratorer hos driftsleverandøren vil via administrasjonsnettverket få tilgang til databaseserveren via en egen server som benyttes som en inngangsport til DFØs systemer. Analyse av uttrekk viser at det er 22 personer fra driftsleverandøren som har tilgang til databaseserveren via denne inngangsporten, hvorav ni systemadministratorer har permanent superbrukertilgang.[123] I tillegg er det opplyst at de andre administratorene kan søke om superbrukertilgang i begrensede perioder. Uttrekk mottatt fra DFØ viser at det ble søkt og innvilget midlertidig tilgang som superbruker på databaseservere totalt 73 ganger i 2017. Analyse av uttrekk av logg fra serveren viser at det er superbrukeren som benyttes til pålogging mot serveren i de fleste tilfeller.

Analyse av uttrekk fra systemet viser at det er krav til passord, men at disse ikke fullt ut etterlever anbefalinger. DFØ opplyser i intervju at rutiner skal sikre at passord til brukere på serveren endres hver 90. dag.[124] Analyse av uttrekk fra serveren viser at det er noe lenger siden passord ble endret, og at systemet er satt opp slik at passordene aldri utløper.

Logging på database- og applikasjonsservere for SAP
NS-ISO/IEC 27002:2017 anbefaler at hendelseslogger som registrerer brukeraktiviteter, avvik, feil og informasjonssikkerhetshendelser, produseres, oppbevares og gjennomgås regelmessig.[125] Leverandøren Microsoft har utarbeidet sikkerhetsbaseliner[126] for ulike Windows-produkter. Disse beskriver leverandørens anbefalinger til oppsett av systemet og viser blant annet hva leverandøren mener bør logges.[127] Nasjonal sikkerhetsmyndighet har utgitt tilsvarende sikkerhetsbaseliner med angivelse av hva som bør logges, som en veiledning for personell som administrerer og utvikler ugraderte systemer i offentlig forvaltning, primært departementer og store sentrale etater.[128]

---

[118] NS-ISO/IEC 27002:3013 punkt 9.2.1 og 9.2.3.
[119] Nasjonal sikkerhetsmyndighet (2017) *NSMs grunnprinsipper for ikt-sikkerhet – versjon 1.0.* Punkt 2.3
[120] The Center for Internet Security (CIS): Critical Security Controls (CSC) for effective cyber defense, punkt 5 og 16
[121] Multifaktorautentisering er en metode for tilgangskontroll hvor en bruker bare får adgang etter å ha presentert flere separate bevis for sin identitet til en autentiseringsmekanisme – vanligvis minst to av følgende kategorier: kunnskap (noe man vet, for eksempel passord), besittelse (noe man har) og inherence (noe man er).
[122] Avtale mellom DFØ og Evry, bilag 2: Leverandørens løsningsspesifikasjon, side 36.
[123] Uttrekk SD3732671, mottatt 21. februar 2018.
[124] Referat fra møte mellom Riksrevisjonen og DFØ 14. desember 2017.
[125] NS-ISO/IEC 27002:3013 punkt 12.4.1
[126] Sikkerhetsbaseline refererer til en samling sikkerhetsinnstillinger og deres anbefalte verdier, jf. publikasjon U-08 Windows, Sikkerhetsbaseliner fra Nasjonal sikkerhetsmyndighet.
[127] Microsoft (31.10.2017) *Windows security baselines*. <https://docs.microsoft.com/en-us/windows/device-security/windows-security-baselines>.
[128] Nasjonal sikkerhetsmyndighet (09.01.2018) *Veiledning for systemteknisk sikkerhet*. <https://www.nsm.stat.no/publikasjoner/regelverk/veiledninger/veiledning-for-systemteknisk-sikkerhet/>. U-10 Grunnsikring av Windows Server 2012 R2

Analyse av uttrekk fra databaseserveren viser at logging med hensyn til sikkerhet ikke er i samsvar med anbefalinger. I intervju opplyser DFØ at server som fungerer som inngangsportal, logger hvem som aksesserer databaseserveren, og at denne loggen skannes for avvik.

Applikasjonsservere kjører SAPs programvare. Analyse av hva som logges på operativsystemnivå på disse serverne, viser at DFØ bare følger anbefalinger fra Microsoft om logging på 10 av 19 innstillinger. For de øvrige logger DFØ mindre, slik at blant annet endringer som mislykkes, ofte ikke logges. Nasjonal sikkerhetsmyndighet har mer omfattende anbefalinger om logging, hvor DFØs oppsett bare samsvarer med anbefalingene på 4 av 54 innstillinger.

Vurdering
Revisjonen viser at DFØ ikke fullt ut etterlever krav i personopplysningsforskriften om sikkerhetstiltak som skal hindre uautorisert bruk av databaseserver og beskytte mot uautorisert innsyn. I tillegg etterleves ikke krav i forskriften om at autorisert bruk av informasjonssystemet skal registreres fullt ut, fordi det logges mindre enn anbefalt på database- og applikasjonsservere, jf. anbefalinger i ISO-standard og fra leverandør. Svake krav til autentisering øker risiko for uautorisert tilgang, og når man ikke benytter personlige brukerkontoer, er det vanskelig å spore aktiviteter tilbake til en person. Handlinger foretatt av administratorer på servene er ikke sporbare. Dette gir risiko for at hendelser som dataangrep ikke oppdages, eller at det ikke foreligger grunnlag for analyse når sikkerhetshendelser oppdages.

6.2.7. Sikring av filserver Opal_con

Opal_con er en filserver som benyttes for utveksling av filer mellom DFØ og kundene både på lønns- og regnskapsområdet. Eksempler på rapporter som ligger på serveren: [129]

- Rapport TN1 (trekk i lønn for medlemskap i fagforening)
- Rapport K27 (oppgjørsrapport fra NAV for refusjon av sykepenger, adopsjons- eller fødselspenger)
- Rapporter fra tidsregistreringssystemer og turnussystemer som kunder laster opp
- Rapporter om masterdata i SAP

DFØ har gjennomført en utredning om å erstatte systemet. Det er imidlertid ikke foreløpig satt ned et prosjekt som skal gjennomføre dette.

Ifølge personopplysningsforskriften § 2-14 første ledd skal sikkerhetstiltak hindre uautorisert bruk av informasjonssystem med personopplysninger. Videre setter personopplysningsforskriften § 2-11 første ledd krav om beskyttelse mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig. Medarbeidere hos den behandlingsansvarlige skal bare bruke informasjonssystemet for å utføre pålagte oppgaver, og selv være autorisert for slik bruk, jf. personopplysningsforskriften § 2-8 første ledd. Ifølge personopplysningsforskriften § 2-13 tredje ledd skal det settes i verk tiltak mot ødeleggende programvare.

Tilgangskontroll i Opal_con
Standarden NS-ISO/IEC 27002:2017 anbefaler at eiere av aktiva fastsetter hensiktsmessige regler for tilgangskontroll og begrensninger i tilgang for bestemte brukerroller.[130] Det legges til grunn et prinsipp om at tilgang til systemer og informasjon bør begrenses til det som er nødvendig for å utføre pålagte arbeidsoppgaver for den enkelte. Standarden anbefaler videre at tilgangsrettigheter til brukere som har fått nye roller i organisasjonen eller sluttet i organisasjonen, bør endres eller slettes umiddelbart.[131]

Det er ulike måter å logge seg på Opal_con for ulike grupper av brukere:[132]

- Web-brukere: fagbrukere hos kundevirksomheter som kun skal motta informasjon fra DFØ bruker i et web-grensesnitt.
- SSH: fagbrukere hos kundevirksomheter som også skal kunne laste opp informasjon til DFØ må benytte et eget program for sikker overføring.

---

[129] Referat fra møte mellom DFØ og Riksrevisjonen 1. desember 2017.
[130] NS-ISO/IEC 27002:2017 punkt 9.1.1.
[131] NS-ISO/IEC 27002:2017 punkt 9.2.2.
[132] Referat fra møte mellom DFØ og Riksrevisjonen 14. desember 2017.

- Active Directory: DFØs egne ansatte kan se filer i Windows Filutforsker som styres ved hjelp av integrasjon med Active Directory.

Analyse av uttrekk viser:

- Mange web-brukere har ikke vært logget inn på lang tid. Av totalt 1 417 brukere i virksomhetene viser analysen at 608 (43 prosent) ikke har vært logget inn siste halvår og 322 brukere (23 prosent) ikke siden 2015 eller tidligere.
- SSH-brukere er upersonlige, og det er ikke aktivert logging som viser når brukerne logger seg på Opal_con.
- 274 interne brukere i DFØ har tilgang til Opal_con. De fleste er knyttet til en og samme gruppe. Dette indikerer at det ikke er noen finmasket differensiering av tilgangsrettigheter til Opal_con basert på tjenstlig behov.

Driftsleverandørs administrasjon av filserveren Opal_con
NS-ISO/IEC 27002:2017 anbefaler at privilegerte brukerrettigheter tildeles på bakgrunn av tjenstlig behov.[133]

Som en del av revisjonen har DFØ oversendt regneark som dokumenterer driftsleverandørs administratortilganger til Opal_con.[134] I tillegg til tilgangsrett til serveren må en bruker ha tilgang til å hente ut passord fra et digitalt passordhvelv. Analyse viser at 47 personer har tilgang til server og passordhvelv, men loggen viser at bare 19 personer har hentet ut passord for tilgang til serveren i perioden fra 1. januar 2017 til 20. februar 2018. Enkelte av disse har aksessert passordhvelvet ofte, andre bare én eller noen få ganger.

Administrasjon av database for brukere av Opal_con
NS-ISO/IEC 27002:2017 anbefaler at brukere av informasjonssystemene tildeles brukerkontoer med unike navn, slik at den enkelte kan knyttes til og holdes ansvarlig for handlingene sine.[135]

Tilgangsrettigheter for web-brukere av Opal_con administreres i en database. Analyse av uttrekk fra databasen viser at det ikke er personlige brukerkontoer i databasen. Det benyttes kun generiske brukerkontoer. Dette inkluderer også standard brukerkonto fra installasjon av databasen.

Systemoppdatering av database
NS-ISO/IEC 27002:2017 anbefaler at informasjon om tekniske sårbarheter i systemer hentes inn jevnlig. [136] Når en potensiell teknisk sårbarhet er identifisert, bør organisasjonen ifølge standarden identifisere de tilknyttede risikoene og tiltakene som skal settes i verk. NSM anbefaler at sikkerhetsoppdateringer installeres så fort som mulig.[137] NSM framhever dette tiltaket som et av de fire viktigste tiltakene mot dataangrep.[138]

DFØ opplyser i intervju at databasen som inneholder brukerinformasjon for web-brukere, benytter en eldre versjon av en database som ikke har vært oppdatert på flere år.[139] Brukerstøtte for versjonen har sluttet, slik at leverandøren ikke utsteder sikkerhetsoppdateringer lenger. Alle utgitte sikkerhetsoppdateringer er heller ikke installert.

Passordkrav for Opal_con
NS-ISO/IEC 27002:2017 punkt 9.4.3 anbefaler at virksomheten har et styringssystem som kvalitetssikrer passord. Det anbefales blant annet videre at styringssystemet tvinger fram valg av kvalitetspassord. Ifølge Datatilsynet er krav til beskyttelse ved behandling av sensitive personopplysninger høye, og bruk av sterk autentisering skal derfor vurderes som et av sikkerhetstiltakene.[140] Sterk autentisering er som hovedregel en form for autentisering med flere faktorer.

Krav til passord i Opal_con for web- og SSH-brukere er opplyst av DFØ:[141] Det er satt minimumskrav til kvalitet for passord som vil gi en viss sikkerhet for at den som logger seg på er den vedkommende utgir seg for.

---

[133] NS-ISO/IEC 27002:3013 punkt 9.2.1 og 9.2.3.
[134] Regneark mottatt fra DFØ 21. februar 2018.
[135] NS-ISO/IEC 27002:3017 punkt 9.2.1 og 9.2.3.
[136] NS-ISO/IEC 27002:2017 punkt 12.6.1.
[137] Nasjonal sikkerhetsmyndighet (2017) *NSMs grunnprinsipper for ikt-sikkerhet – versjon 1.0*. Punkt 3.2
[138] Nasjonal sikkerhetsmyndighet (2016) *Fire effektive tiltak mot dataangrep (sjekkliste nr. 1)*. <https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf>.
[139] Referat fra møte mellom DFØ og Riksrevisjonen 14. desember 2017.
[140] Datatilsynet (2017) *Bruk av sterk autentisering*. <https://www.datatilsynet.no/regelverk-og-skjema/behandle-personopplysninger/sterk-autentisering/>.
[141] Svar fra DFØ ved oversendelse til Riksrevisjonen mottatt 30. januar 2018. Svaret er ikke underbygget med et uttrekk eller skjembilde fra systemet.

Passordkrav for DFØs egne ansatte ved tilgang til Opal_con vil følge av passordkrav i Group policy i Windows-baserte nettverk, se punkt 6.2.8.

Vurdering
Revisjonen viser at filserveren Opal_con, som inneholder sensitive personopplysninger, ikke er tilstrekkelig sikret mot uautorisert innsyn og bruk, jf. personopplysningsforskriften §§ 2-11 og 2-14. Revisjonen viser at tilgangen til Opal_con ikke er begrenset til tjenstlig behov hverken for sluttbrukere eller administratorer – det er bare stilt minimumskrav til passord, det forekommer upersonlige brukerkontoer, og pålogging logges ikke for alle. Videre gjør manglende oppdateringer av databasen for brukere systemet sårbart for ødeleggende programvare, jf. personopplysningsforskriften § 2-13 tredje ledd. Totalt gir dette risiko for at uvedkommende kan få tilgang til personopplysninger. Det er videre mangler som gjør det vanskelig å spore brukeres aktiviteter og risiko for at uautorisert tilgang ikke blir oppdaget.

6.2.8. Sikring av Windows-nettverk i DFØ

DFØ benytter et Windows-basert nettverk internt i virksomheten. I dette er Active Directory en katalogtjeneste som benyttes til å administrere nettverket, inkludert administrasjon, autentisering og autorisering av brukere. DFØ benytter også tjenesten til å administrere tilganger til Opal_con for interne brukere.

Ifølge personopplysningsforskriften §2-14 første ledd skal sikkerhetstiltak hindre uautorisert bruk av informasjonssystem med personopplysninger. Videre setter personopplysningsforskriften § 2-11 første og andre ledd krav om beskyttelse mot uautorisert innsyn i personopplysninger hvor konfidensialitet er nødvendig, og annen informasjon av betydning for informasjonssikkerheten.

Administratorroller
Administratorroller gir blant annet tilgang til all informasjon på maskiner i nettverket og muligheter til å etablere og endre brukerkontoer og tilganger. Anerkjente standarder anbefaler at man begrenser og kontrollerer tildeling av slike privilegerte tilgangsrettigheter.[142] De bør tildeles brukere på grunnlag av tjenstlig behov. Leverandøren Microsoft anbefaler at ingen brukere er medlem av grupper med store rettigheter som domeneadministratorer i den daglige driften, men at disse gruppene bare tildeles medlemmer ved installasjon og krisehåndtering. [143] Microsoft anbefaler at alle administratorgrupper ses i sammenheng selv om de gir ulike rettigheter, fordi et medlem av en av disse gruppene kan skaffe seg tilgang til de andre. Microsoft understreker at systembrukere, kontoer som programmer bruker til å logge seg på, bare må få tildelt nødvendig privilegier for at programmene kan kjøre som normalt.

Analyse av uttrekk av data viser at mange brukerkontoer har ulike roller som administratorer i DFØs Windows-baserte nettverk. Dette inkluderer både personlige brukerkontoer og systembrukere. Enkelte av brukerkontoene har ikke blitt benyttet på lengre tid. Passord for systembrukere utløper ikke, og det forekommer at de ikke har blitt endret på flere år.

Passord
NS-ISO/IEC 27002:2017 punkt 9.4.3 anbefaler at virksomheten har et styringssystem som kvalitetssikrer passord. Det anbefales blant annet videre at styringssystemet tvinger fram valg av kvalitetspassord og bytte av passord med jevne mellomrom. Leverandøren Microsoft anbefaler at det settes strenge krav til autentisering ved bruk av kontoer med privilegerte rettigheter, i utgangspunktet autentisering basert på flere faktorer (noen man vet, noe man har, eller noe man er).[144] Bransjeanbefalinger for kvalitet på passord for alle brukere viser blant annet anbefalinger om minimum passordlengde på 14 tegn, historikk som husker 24 passord og at det brukes en funksjon for passordkompleksitet.[145]

---

[142] NS-ISO/IEC 27002:2017 punkt 9.2.3, jf. 9.2.5
[143] Microsoft (31.05.2017) *Best Practices for Securing Active Directory*. <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>.
[144] Microsoft (31.05.2017) *Best Practices for Securing Active Directory*. <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/best-practices-for-securing-active-directory>.
[145] Microsoft Security Baselline for Windows 10 og Nasjonal sikkerhetsmyndighets sikkerhetsbaseline for Windows server 2012 R2 (U-10).

Analyse av uttrekk av data viser at DFØ har lavere krav til passordlengde og passordhistorikk for egne ansattes ved pålogging på nettverk. Noen kontoer for personlige brukere er satt opp slik at det ikke er krav om å skifte passord, inkludert enkelte administratorer.

Vurdering
Revisjonen viser at DFØ ikke etterlever faglige anbefalinger i ISO-standarden og fra leverandøren Microsoft for sikring av Windows-baserte nettverk. Dermed har ikke DFØ satt i verk tilstrekkelige tiltak for å hindre uautorisert innsyn og bruk av systemer i samsvar med personopplysningsforskriften. Det er flere brukerkontoer som har privilegerte tilgangsrettigheter enn det som anbefales, og kravene til passord er lavere enn anbefalt. Utvidede rettigheter er et mål ved de fleste dataangrep. Mange brukerkontoer med høye rettigheter øker risiko for at en angriper lykkes å få tak i slike rettigheter. Svake krav til autentisering øker risikoen for at en angriper kan skaffe seg tilgang til DFØs systemer ved å knekke passord.

6.2.9. Sikring av klient-PC-er i DFØ

Ifølge personopplysningsforskriften §2-14 første ledd skal sikkerhetstiltak hindre uautorisert bruk av informasjonssystem med personopplysninger. Dette skal ifølge tredje ledd omfatte tiltak som ikke kan påvirkes eller omgås av medarbeiderne. Videre skal det ifølge forskriften § 2-13 tredje ledd treffes tiltak mot ødeleggende programvare.

[redacted]

Programvare på klienter
I NS-ISO/IEC 27002:2017 punkt 12.6.2 anbefales at det etableres og tas i bruk regler for installering av programvare brukere kan installere. Standarden anbefaler at en streng policy defineres og håndheves. Organisasjonen bør identifisere hvilke typer programvareinstallering som er tillatt, og hva som er forbudt. NSM legger til grunn at bare autorisert programvare bør kjøre på virksomhetens enheter, og at det bare installeres programvare med nødvendig funksjonalitet for å støtte virksomhetens forretningsprosesser.[148]

[redacted]

Analyse av uttrekk av programvare på et utvalg klienter viser at det på enkelte finnes programvare som verktøylinjer, som tidligere har blitt benyttet til å spre skadevare.[150] Det forekommer også tilfeller av installerte spill / spillplattformer.

---

[146] Nasjonal sikkerhetsmyndighet (2016) *Fire effektive tiltak mot dataangrep (sjekkliste nr. 1)*. <https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf>.
[147] Verifisert referat fra møte mellom DFØ og Riksrevisjonen 29. november 2017.
[148] Nasjonal sikkerhetsmyndighet (2017) NSMs grunnprinsipper for ikt-sikkerhet – versjon 1.0. Punkt 2.3.
[149] Referat fra møte mellom DFØ og Riksrevisjonen 29. november 2017.
[150] NetworkWorld (17.03.2017) *Ask.com serves as a conduit for malware – again.* <https://www.networkworld.com/article/3181902/security/ask-com-serves-as-a-conduit-for-malware-again.html>.

Sikkerhetsoppdatering
NS-ISO/IEC 27002:2017 anbefaler at informasjon om tekniske sårbarheter i systemer hentes inn jevnlig. [151] Når en potensiell teknisk sårbarhet er identifisert, bør organisasjonen ifølge standarden identifisere de tilknyttede risikoene og tiltakene som skal settes i verk. NSM anbefaler at sikkerhetsoppdateringer installeres så fort som mulig.[152] NSM framhever dette tiltaket som et av de fire viktigste tiltakene mot dataangrep.[153]

DFØ opplyser i intervju at det ikke foreligger noen policy eller retningslinje for oppdatering av programvare på klienter.[154] Operativsystem og Office-pakken på klienter blir automatisk oppdatert ved at Windows Update skal være påslått, men det er mulig for brukeren å utsette oppdateringer eller slå av automatiske oppdateringer. Det er ifølge DFØ en risiko i forbindelse med oppdateringer at enkelte har en bærbar DFØ-PC hjemme som de sjelden bruker, og der det er lett å utsette oppdateringer.

DFØ opplyser at det ikke finnes faste rutiner for oppdatering av tredjepartsprogramvare. Analyse av uttrekk av programvare på klienter viser at enkelte klienter ikke har oppdatert Microsoft Windows, og at enkelte klienter har utdatert tredjepartsprogramvare. Det er kjente svakheter knyttet til de eldre versjonene av programvare som ble funnet.

Scanning og overvåkning av klientene
I NS-ISO/IEC 27002:2017 punkt 13.1.1 legges det til grunn at for å beskytte nettverk mot uautorisert adgang bør systemer i nettverk autentiseres og systemtilkobling til nettverket begrenses. NSM anbefaler at virksomheter aktivt sporer og kartlegger alle maskinvareenheter, programvare og tjenester i nettverket.[155]

DFØ opplyser at antivirusprogram på virksomhetens stasjonære klienter overvåkes via et sentralt managementsystem.[156] Dette brukes ikke for bærbare PCer, hvor man ikke har et eget managementsystem. [redacted] DFØ uttrykker at et managementsystem for bærbare PCer er ønskelig på sikt.

[redacted]

Vurdering
Revisjonen viser at for sikring av klienter etterlever DFØ ikke krav i personopplysningsforskriften om sikkerhetstiltak for å hindre uautorisert bruk av informasjonssystem og tiltak mot ødeleggende programvare. [redacted]

Svakheter med sikringen av klienter øker risiko for infeksjon med skadevare og kan gi en angriper muligheter til å skaffe seg et fotfeste i DFØs nettverk og derigjennom få tilgang til personopplysninger. Dette kan ses i sammenheng med at angrep fra ondsinnet programvare er vurdert som kritisk i DFØs overordnede risikovurdering for 2017, jf. punkt 6.1.3.[157]

6.2.10. Kryptering av kommunikasjon

Ifølge personopplysningsforskriften § 2-11 tredje ledd skal personopplysninger som overføres elektronisk ved hjelp av overføringsmedium utenfor den behandlingsansvarliges fysiske kontroll, krypteres eller sikres på annen måte når konfidensialitet er nødvendig. Datatilsynet har i kommentar til bestemmelsen klarlagt at reglene for kryptering også gjelder for overføring via private datalinjer som er utenfor det området virksomheten har sikret mot uautorisert adgang.[158]

---

[151] NS-ISO/IEC 27002:2017 punkt 12.6.1.
[152] Nasjonal sikkerhetsmyndighet (2017) NSMs grunnprinsipper for ikt-sikkerhet – versjon 1.0. Punkt 3.2.
[153] Nasjonal sikkerhetsmyndighet (2016) *Fire effektive tiltak mot dataangrep (sjekkliste nr. 1)*. <https://www.nsm.stat.no/globalassets/dokumenter/veiledninger/systemteknisk-sikkerhet/s-01-fire-effektive-tiltak-mot-dataangrep.pdf>.
[154] Referat fra møte mellom DFØ og Riksrevisjonen 29. november 2017.
[155] Nasjonal sikkerhetsmyndighet (2017) NSMs grunnprinsipper for ikt-sikkerhet – versjon 1.0. Punkt 1.2.
[156] Referat fra møte mellom DFØ og Riksrevisjonen 29. november 2017.
[157] DFØ (2017) *Halvårsrapport 2017*. Kap. 3.2, s. 19–33. Disse risikofaktorene ble også omtalt i den overordnede risikovurderingen i 2016.
[158] Datatilsynet (2000) Sikkerhetsbestemmelsene i personopplysningsforskriften med kommentarer.

DFØ har i kravspesifikasjon for drift av SAP satt krav om at datatrafikk over hovedlinjen skal være kryptert.[159] Leverandøren har opplyst i sin løsningsspesifikasjon at hovedsambandet er kryptert, men at backupsambandet ikke er kryptert.[160]

For lønnssystemet SAP opplyser DFØ i intervju at kommunikasjon mellom klientene og serveren skal være kryptert.[161] Det er videre opplyst at kommunikasjonen mellom modulene i SAP er kryptert. [redacted]

Vurdering
Revisjonen viser at krav i personopplysningsforskriften om kryptering av kommunikasjon av personopplysninger utenfor DFØs eget nett etterleves for flere grensesnitt, men at det er enkelte grensesnitt der kommunikasjon ikke er tilstrekkelig beskyttet i henhold til forskriftens krav. [redacted]

6.3. Problemstilling 3: Følger DFØ opp at sikkerhetsstrategi og iverksatte tiltak for informasjonssikkerhet i egen virksomhet og hos leverandøren Evry fungerer som forutsatt?

6.3.1. Sikkerhetsrevisjoner

Personopplysningsforskriften § 2-5 krever at sikkerhetsrevisjoner av bruk av informasjonssystemer skal gjennomføres jevnlig. Revisjonen skal omfatte vurdering av organisering, sikkerhetstiltak og bruk av kommunikasjonspartner og leverandører. Resultatet fra sikkerhetsrevisjonen skal dokumenteres. Datatilsynet utdyper at dette handler om å etterprøve sikkerhetsarbeidet for å verifisere at de sikkerhetstiltakene som er besluttet etablert, faktisk er satt i verk og fungerer som forutsatt. Tilsynet anbefaler sikkerhetsrevisjoner på årlig basis. ISO-standarden anbefaler at virksomheters styring og implementering av informasjonssikkerhet blir uavhengig revidert ved planlagte intervaller.

Revisjonen har bedt DFØ om å få oversendt dokumentasjon på alle internt eller eksternt gjennomførte sikkerhetsrevisjoner fra de siste tre årene. Ingen dokumentasjon på dette er mottatt. DFØ bekrefter at det ikke er gjennomført noen interne sikkerhetsrevisjoner i DFØ de siste årene.[164]

DFØ startet en sikkerhetsrevisjon av Evry høsten 2017, men denne er på revisjonstidspunktet ikke ferdigstilt. DFØs forrige revisjon av Evry var i 2012. DFØ opplyser i intervju at hovedårsaken for å sette i gang revisjonen i 2017 er den nye avtalen mellom Evry og DFØ, samt Evrys ferske partnerskap med IBM. DFØ opplyser videre at det ikke er fastsatt noen bestemt syklus for når eller hvor ofte store sikkerhetsrevisjoner skal gjennomføres.[165] DFØ har i dokumentet *Styringssystem for informasjonssikkerhet* selv lagt til grunn at det minimum hvert andre år skal gjennomføres en vurdering av etterlevelsen av egen sikkerhetsstandard.[166]

---

[159] Bilag 1 Kravspesifikasjon til avtale mellom DFØ og Evry, punkt 1.7.3.
[160] Bilag 2 Leverandørens løsningsspesifikasjon til avtale mellom DFØ og Evry, punkt 1.7.7.
[161] Verifisert referat fra intervju med DFØ 1. desember 2017 og 14. desember 2017.
[162] Verifisert referat fra intervju med DFØ 14. desember 2017.
[163] DFØ (2018) *Riksrevisjonens utkast til revisjonsrapport for 2017 om sikring av personopplysninger.* Brev fra DFØ til Finansdepartementet av 24.04.2018
[164] Skriftlig tilbakemelding fra DFØ på oppfølgingsspørsmål i revisjonen, mottatt av Riksrevisjonen 30.01.2018.
[165] Verfisert referat fra intervju med DFØ 1. november 2017.
[166] DFØ (2014) *Styringssystem for informasjonssikkerhet.* Kap. 11.2.

Revisjonen viser at DFØ ikke etterlever kravet i personopplysningsforskriften om å gjennomføre sikkerhetsrevisjoner av informasjonssystemer på jevnlig basis. Dette innebærer at DFØ har et svakt grunnlag for å vite om sikkerhetstiltak etterleves og har ønsket virkning både internt hos DFØ og i forhold til DFØs underleverandører.

6.3.2. Oppfølging av informasjonssikkerhet

Ifølge personopplysningsforskriften § 2-3 fjerde ledd skal bruk av informasjonssystemet jevnlig gjennomgås for blant annet å sikre at sikkerhetsstrategien gir tilfredsstillende informasjonssikkerhet som resultat. Resultatet fra gjennomgangen skal ifølge bestemmelsens femte ledd dokumenteres og benyttes som grunnlag for eventuell endring av sikkerhetsmål og strategi.

Oppfølging av sikkerhetstiltak gjennom måling av og rapportering fra system
I NS-ISO/IEC 27001:2017 anbefales at en organisasjon evaluerer informasjonssikkerhetsprestasjoner og virkningen av styringssystemet for informasjonssikkerhet. Det anbefales at organisasjonen bestemmer hva som skal overvåkes og måles, metodene for dette, når det skal gjøres, når resultatene skal evalueres, og hvem som har ansvar for de ulike trinnene. I bransjeanbefalinger blir fastsettelse av måleparametere og kontinuerlig måling mot disse ansett som avgjørende faktorer for en virksomhets sikkerhet.[167]

Revisjonen har ikke fått dokumentert at DFØ har etablert noen måleparametere for informasjonssikkerheten utover systemers oppetid. DFØ uttaler i intervju at ikke alle sikkerhetstiltak som er satt i verk, er like lette å måle at fungerer. Enkelte tiltak kan måles ut fra antall hendelser. Som eksempel nevner DFØ tiltak for å redusere antall angrep utenfra. Her kan man se ut fra statistikk om de iverksatte tiltakene virker eller ikke.[168]

Leverandøren SAP har etablert en standard for sikker konfigurasjon og oppsett av SAP-systemet, som kan bidra til å måle oppnåelse av tilfredsstillende informasjonssikkerhet.[169] SAP har tilgjengeliggjort verktøy/rapporter som på ulike måter kontrollerer systemets oppsett opp mot standarden. Som vist i kapittel 6.2.1 tar DFØ ut flere slike rapporter, som kan gi grunnlag for å verifisere at standarden etterleves. Gjennomgang av DFØs bruk av rapportene viser at DFØ ikke har satt krav til akseptable resultater ut fra rapportene, og at DFØ ikke følger opp sikkerhetsmessige svakheter som blir identifisert gjennom rapportene på en systematisk måte.

Ledelsesgjennomganger
NS-ISO/IEC 27001:2017 anbefaler at organisasjonens øverste ledelse gjennomgår ledelsessystemet for informasjonssikkerhet med planlagte mellomrom for å sikre at det er velegnet, tilstrekkelig og virkningsfullt. Dette skal inkludere status for tiltak, endringer i interne og eksterne forhold, informasjon om informasjonssikkerhetsprestasjon, tilbakemeldinger og resultater fra risikovurderinger. Resultatet skal dokumenteres og inkludere muligheter for kontinuerlig forbedring og endringer i ledelsessystemet.

DFØ har i dokumentet *Styringssystem for informasjonssikkerhet* satt et internt krav til at ledelsen i DFØ tre ganger årlig skal ha en gjennomgang av DFØs sikkerhets- og beredskapssituasjon. Sikkerhetssjef er ansvarlig for å utarbeide rapport og foreta gjennomgang.[170] Revisjonen har ikke mottatt dokumentasjon på resultater fra ledelsesgjennomganger i DFØ eller annen dokumentasjon på oppfølging av etterlevelse av sikkerhetspolicy og sikkerhetsbestemmelser.

Vurdering
Revisjonen viser at det ikke er etablert et helhetlig system for å måle eller evaluere om sikkerhetstiltak fungerer som forutsatt, som anbefalt i ISO-standarden. Dette innebærer at DFØ ikke har grunnlag for å vite om sikkerhetstilstanden er tilfredsstillende og gir risiko for at svak sikkerhet på områder ikke blir oppdaget. DFØ etterlever dermed ikke kravet i personopplysningsforskriften om å jevnlig gjennomgå informasjonssystemet for å oppnå tilfredsstillende informasjonssikkerhet.

6.3.3. Oppfølging av leverandøren Evry

---

[167] The Center for Internet Security (CIS): Critical Security Controls (CSC) for effective cyber defense.
[168] Verifisert referat fra intervju med DFØ 1. november 2017.
[169] SAP Knowledge Base Article 2253549 – The SAP Security Baseline Template.
[170] DFØ (2017) *Styringssystem for informasjonssikkerhet*. Kapittel 10.

Personopplysningsloven § 13 tredje ledd sier at en behandlingsansvarlig som lar andre få tilgang til personopplysninger, for eksempel en databehandler, skal påse at disse oppfyller kravene til sikkerhetstiltak. Revisjonen legger til grunn at det samme «påse»-kravet også gjelder for en databehandler som lar andre få tilgang til et system som inneholder personopplysninger. Det følger av personopplysningsforskriftens § 2-15 tredje ledd at leverandører skal tilfredsstille kravene til sikkerhetstiltak i forskriftens kapittel 2. Videre går det fram av femte ledd at behandlingsansvarlig skal ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende informasjonssikkerhet. Datatilsynet angir at den behandlingsansvarlige som et ledd i oppfølgingen for eksempel kan meddeles resultater fra ledelsesgjennomganger, sikkerhetsrevisjoner og avviksbehandling som er relevant for forholdet til leverandøren.

NS-ISO/IEC 27002:2017 anbefaler at virksomheten regelmessig bør overvåke og gjennomgå leverandørers tjenesteleveranser.

Risikovurderinger, sikkerhetsmål og strategi
Leverandørens risikovurderinger, ledelsesgjennomganger, sikkerhetsmål eller strategi er vurderinger og beslutninger som kunne bidratt til at DFØ fikk informasjon om hvordan nivået på sikkerheten er i Evry, inkludert hvordan Evry sikrer personopplysningene som behandles og lagres i systemene. Som omtalt i 6.1.4 inneholder avtalen med Evry ingen konkrete krav til at leverandøren skal utarbeide og oversende slik dokumentasjon. Det er heller ikke opplyst at den blir hentet inn fra Evry rutinemessig.

Riksrevisjonen påpekte også i 2012 at DFØ ikke hadde hentet inn risikovurderinger eller rapporter som dokumenterte hvordan leverandøren av driftstjenester for SAP sikret data og informasjon.[171]

Rapportering fra Evry
Ifølge avtalen skal Evry månedlig, og eventuelt etter forespørsel fra DFØ, sende en rapport over hvilke ansatte som har aksessert DFØs systemer, inkludert bruk av fellesbrukere / upersonlige brukere.

DFØ opplyser i intervju at det månedlig mottar rapport om upersonlige brukerkontoer fra Evry, som kontrolleres i DFØ. Evry rapporterer ikke om bruk av personlige brukerkontoer som har aksessert DFØs systemer. De personlige brukerkontoene som Evrys ansatte har i SAP, har alle sterke privilegier (jf. punkt 6.2.2). DFØ opplyser at man ikke har noen oppfølging av bruk av disse brukerkontoene.[172] Gjennomgang av rapportene viser at det heller ikke foretas rapportering av tilgang til underliggende infrastruktur, for eksempel database og databaseserver.

DFØ mottar også månedlige SLA-rapporter fra Evry. Disse viser resultater av målinger opp mot avtalt tjenestenivå for et sett parametere, inkludert nedetid/oppetid for systemene, tap av data / data på avveie og responstid. Ingen av de mottatte SLA-rapportene viser avvik for data på avveie. Det er ikke satt måleparametere for sikker konfigurasjon av systemene eller sikkerhetsovervåkning.

Møtepunkter mellom Evry og DFØ
Avtalen mellom DFØ og Evry slår fast at det skal gjennomføres regelmessige møter mellom partene. Det skal avholdes et årlig møte på strategisk nivå, kvartalsvise møter på taktisk nivå og driftsmøter hver 14. dag. DFØ informerer i intervju om at driftsmøtene er av operativ karakter, og at kvartalsmøtene avholdes på ledernivå. De årlige strategiske møtene tar for seg framtidsbilder og overordnede saker.

Revisjonen har mottatt kopier av møtereferater som viser at driftsmøter og kvartalsmøter avholdes i tråd med bestemmelsene i avtalen. Gjennomgang av et utvalg møter viser at driftsmøtene tar opp operative og sikkerhetsmessige saker som gjelder driften av SAP, for eksempel oppdateringer og vedlikehold. Kvartalsmøtene omhandler blant annet drift i forrige periode, endringer i avtalen og gjensidig orientering om nyheter og pågående/planlagte prosjekter. Personopplysninger har ikke vært et tema i dialogen mellom DFØ og Evry slik den framstår i referat fra driftsmøtene. I referat fra de kvartalsvise møtene er personopplysninger brakt på bane som følge av en konkret hendelse.

Vurdering
Revisjonen viser at DFØ ikke etterlever krav om å ha kunnskap om sikkerhetsstrategien hos kommunikasjonspartnere og leverandører, og jevnlig forsikre seg om at strategien gir tilfredsstillende

[171] Brev fra Riksrevisjonen til DFØ av 8. mars 2012.
[172] Verifisert referat fra intervju med DFØ og Evry 14. desember 2017.

informasjonssikkerhet. DFØ mottar rapporter fra Evry om enkelte sider ved leverandørens sikkerhetstiltak, men det er ikke etablert en formalisert og systematisk rapportering om viktige elementer i den tekniske informasjonssikkerheten. Svakheter ved rapporteringen gjør det vanskelig for DFØ å vurdere om leverandørens sikkerhetsarbeid er tilfredsstillende. Det er derfor risiko for at informasjon ikke er beskyttet slik DFØ forutsetter.

6.3.4. Tilgang til data utenfor Norge

I DFØs avtale med Evry slås det fast at Evry ikke kan gi ansatte eller underleverandører utenfor Norge tilgang til DFØs data uten samtykke fra DFØ.[173] DFØ har bekreftet overfor Riksrevisjonen at så lenge DFØ har mottatt driftsleveranser fra Evry på lønnsområdet, har partene vært enige om at all databehandling skal skje i Norge, og at ingen utenfor landets grenser skal ha tilgang til personopplysninger i DFØs systemer.[174] Videre har Evry erklært at de ikke under noen omstendigheter har behandlet eller lagret DFØs data i utlandet, eller latt utenlandsk arbeidskraft behandle DFØs data gjennom fjerntilgang.[175] Finansdepartementet har uttalt at departementet i styringsdialogen med DFØ har vært særlig opptatt av adgangen til å behandle personopplysninger i utlandet, og at departementet har vært nøye med å sette tydelige krav til direktoratet.[176]

Revisjonens gjennomgang av referater fra kvartalsmøter mellom DFØ og Evry viser imidlertid at data har blitt overført til utlandet. I mars/april 2017 ble det oppdaget at konsulenter tilhørende Evrys avdeling i Riga hadde hatt tilgang til og behandlet saker fra DFØ i Evrys interne saksbehandlingssystem. Tilgangene ble da sperret, men allikevel oppsto det et nytt avvik i mai. Tre saker var blitt behandlet fra Riga, og DFØ ba Evry om å undersøke om sakene inneholdt personopplysninger, og om noen derfra kunne se DFØs saker eller ha tilgang til dem.[177]

I kvartalsmøtet høsten 2017 ble det bekreftet fra Evry at personopplysninger ikke var involvert i de tre sakene, samtidig som det ble klart at ytterligere 164 saker hadde blitt behandlet av Evrys ansatte i Riga. DFØ ba på nytt Evry om å undersøke forholdet og gi tilbakemelding på om noen i Riga har hatt tilgang til eller mulighet til innsyn i DFØs saker.[178]

I årets siste kvartalsmøte mellom DFØ og Evry er det ingen omtale av hva som er status for de resterende 164 sakene som DFØ ble gjort oppmerksom på i det forrige møte mellom partene.

Dokumentgjennomgang viser at referatene fra den formelle styringsdialogen mellom Finansdepartementet og DFØ ikke inneholder direkte omtale av eller henvisninger til hverken Riga-saken eller Evry.[179]

DFØ opplyser i en tilbakemelding til Riksrevisjonen at de i mars 2017 ble underrettet om at Evry skulle flytte en servicedesk til Riga, og at de da sørget for en presisering i avtalen med Evry. Her ble det understreket at alle data fortsatt skulle være lagret på Evrys datasentre i Norge, og at alle operasjoner knyttet til tjenestene ville skje fra steder innenfor Norge. I månedsskiftet mars/april ble så DFØ orientert om at noen tekniske saker var blitt distribuert gjennom Evrys kontor i Riga til Evrys datasenter i Norge. Evry informerte da DFØ om hvilke tiltak som var satt i verk for å hindre gjentakelse av dette.[180]

DFØ påpeker at de omtalte sakene ikke ble *behandlet* i Riga, men at de ble *distribuert* derfra til behandling i Norge. Sakene var av teknisk karakter og involverte verken kundesaker eller personsensitive data, men DFØ uttaler at de til tross for dette tok forholdet på alvor, siden avtalen om lagring/behandling av data i Norge er uomtvistelig. På tross av tett oppfølging gjentok imidlertid hendelsen seg, men det ble konkludert med at også disse sakene var tekniske og ikke innheholdt personsensitive opplysninger. På bakgrunn av leverandørens redegjørelse og beskrivelse av tiltak ble avviket ansett som lukket og håndtert.

DFØ opplyser at man vurderte å varsle departementet da avvikene oppsto. Etter å ha kartlagt omfanget og fått klarhet i at det bare dreide seg om tekniske saker, og ingen personsensitive opplysninger, ble det imidlertid avgjort at dette kunne håndteres internt. DFØ opplyser at avvikene har medført at det er satt i verk tiltak som skal sikre at ingen brukere utenfor Norge får tilgang til DFØs saker.[181]

---

[173] DFØs kravspesifikasjon punkt 1.11.2.2.
[174] E-post fra DFØ via Finansdepartementet av 4. mai 2017.
[175] Erklæring fra Evry til DFØ av 3 mai 2017.
[176] E-post fra Finansdepartementet til Riksrevisjonen 4. mai 2017.
[177] Referat fra 2. kvartalsmøte mellom DFØ og Evry 27. juni 2017.
[178] Referat fra 3. kvartalsmøte mellom DFØ og Evry 6. september 2017.
[179] Referat fra etatsstyringsmøter 6. april og 28. september 2017.
[180] E-post fra DFØ til Riksrevisjonen av 12. mars 2018.
[181] Ibid.

I en ny tilbakemelding til Riksrevisjonen informerer DFØ om at enkelte av sakene har hatt vedlegg, med personopplysninger begrenset til navn og e-postadresser.[182]

Revisjonen viser at Evry i strid med avtalen med DFØ har distribuert saker til utlandet. DFØ har opplyst at sakene ikke inneholdt sensitive personopplysninger, men personopplysninger som navn og e-postadresser. DFØ har fulgt opp leverandøren etter at forholdet ble kjent, men har ikke informert Finansdepartementet om forholdet til tross for at departementet i styringsdialogen med DFØ har vært særskilt opptatt av adgangen til å behandle personopplysninger i utlandet. DFØ uttaler at hendelsen var et avvik fra avtalen de har med leverandøren, men at de ikke opplevde det som et så vesentlig avvik at det var grunn til å varsle Finansdepartementet.[183]

7 Konklusjoner

En av DFØs hovedoppgaver er å håndtere lønnsutbetalinger for 79 000 ansatte i 171 statlige virksomheter. I dette arbeidet benyttes datasystemet SAP, som driftes av underleverandøren Evry.

For å levere lønnstjenestene må DFØ behandle store mengder personopplysninger om arbeidstakere i lønnssystemet. Det er viktig, både for enkeltmenneskene og for virksomhetene, at personopplysninger som blir samlet inn og behandlet i et system, blir sikret på best mulig måte. Dersom personopplysninger kommer på avveie eller blir misbrukt, kan det få store konsekvenser for den det gjelder, for eksempel i form av identitetstyveri eller innsyn i personlige forhold som kan oppleves som belastende. Personopplysningsloven med forskrift har som formål å bidra til at slike opplysninger beskyttes, slik at borgernes grunnleggende behov for personvern ivaretas.

Målet med revisjonen har vært å kontrollere om DFØ sørger for tilfredsstillende informasjonssikkerhet ved behandling av personopplysninger i lønns- og personalsystemet SAP, i henhold til krav i personopplysningsloven med forskrift og anbefalinger i anerkjente standarder. Tre problemstillinger belyser ulike sider ved DFØs arbeid med sikring av personopplysninger.

Informasjonssikkerhet og sikring av personopplysninger handler om å sette mål for og krav til sikkerheten og sikkerhetsarbeidet, identifisere risiko som kan true informasjonssikkerheten, sette i verk hensiktsmessige tiltak for å sikre informasjonen og følge opp at de iverksatte tiltakene virker. Revisjonen viser svakheter ved flere sider av DFØs arbeid med å sikre personopplysningene:

- DFØs grunnlag for å planlegge sikkerhetstiltak er svakt på grunn av mangelfulle risikovurderinger og databehandleravtaler
- DFØs iverksatte sikkerhetstiltak for å sikre informasjonen i SAP og underliggende infrastruktur har vesentlige svakheter.
- DFØs oppfølging av om iverksatte tiltak fungerer som forutsatt, og oppfølgingen av leverandøren Evry er mangelfull.

Funnene fra revisjonen gjør at DFØ på flere områder vurderes å ikke etterleve relevante krav i personopplysningsloven og forskriften når det gjelder sikring av personopplysningene i SAP. Dette øker risikoen for at personopplysninger kan komme på avveie eller misbrukes.

Problemstilling 1: ***Har DFØ etablert et grunnlag for å planlegge sikkerhetstiltak som sørger for tilfredsstillende informasjonssikkerhet for personopplysninger i SAP?***

DFØ har etablert et grunnlag for å planlegge sikkerhetstiltak i form av skriftlige sikkerhetsmål og sikkerhetsstrategi, rutiner for risikovurderinger og avtaler med kunder og leverandør. Revisjonen viser likevel at det er vesentlige svakheter ved flere av disse elementene. Dette kan blant annet gjøre det vanskelig å få på plass gode sikringstiltak for å beskytte personopplysningene som behandles. Revisjonen viser manglende etterlevelse av personopplysningsloven og forskriften basert på følgende funn:

[182] E-post fra DFØ til Riksrevisjonen av 22. mars 2018.
[183] DFØ (2018) *Riksrevisjonens utkast til revisjonsrapport for 2017 om sikring av personopplysninger.* Brev fra DFØ til Finansdepartementet av 24.04.2018

- DFØ har etablert sikkerhetsmål og -strategi, men formålet med behandling av personopplysninger er ikke klargjort.
- Dokumentene som utgjør sikkerhetsstrategien, blir ikke jevnlig oppdatert.
- DFØ har identifisert hvilke personopplysninger virksomheten behandler, men ønsket beskyttelsesnivå og akseptabel risiko kommer i liten grad fram.
- DFØ har vurdert risikomomenter vedrørende informasjonssikkerhet på et overordnet nivå, men risikovurderinger for behandling av personopplysninger foreligger ikke.
- Det er få og uklare beskrivelser av forbedrings- og sikringstiltak som følge av identifiserte risikoer.
- Standardavtalen mellom DFØ og kundene og databehandleravtalen mellom DFØ og Evry har mangler og svakheter sett opp mot Datatilsynets veileder om hva slike avtaler bør inneholde.
    - Databehandleravtale med Evry har svakheter ved beskrivelse av krav til sikkerhetstiltak og formål med behandlingen av personopplysninger.
    - Avtalen med kundene angir ikke formål med behandlingen av personopplysninger, hvilke måter DFØ skal behandle opplysningene på, og har mangelfull omtale av konkrete sikringstiltak.
- Ansvars- og myndighetsforhold for sikkerhetsarbeidet samlet sett er formelt avklart, mens det for lønnssystemet SAP er uklart hvilket ansvar som er tillagt rollen som systemeier.

Manglende bruk av risikovurderinger som et verktøy til å få fram uønskede hendelser som kan true sikkerheten til personopplysningene, reduserer muligheten til å utarbeide gode forbedrings- og sikringstiltak. Dette innebærer risiko for at nødvendige sikkerhetstiltak ikke blir satt i verk, eller at feil eller lite effektive tiltak blir brukt. Mangel på regelmessige risikovurderinger for personopplysninger var også en av merknadene i et konsulentfirmas gjennomgang av DFØs behandling av personopplysninger i 2013. Situasjonen synes uendret.

Svakhetene i avtalen mellom DFØ og kundene gjør det vanskelig for kundene å vurdere om DFØ sikrer opplysningene på en måte som er i tråd med regelverket, og om sikringen er god nok i forhold til ønsket nivå for sikkerheten. DFØ opplyser at den gjeldende standardavtalen mellom dem og kundene skal fases ut, og at en ny driftsavtale med en ny, separat databehandleravtale skal rulles ut til kunder i løpet av 2018. En del kunder har allerede gått over til den nye avtalen.[184] Det er positivt at DFØ har satt i verk forbedringstiltak og tilbyr en avtale med en separat databehandleravtale. Dette kan bidra til at det blir klarere for kundene hvilket formål DFØ har med behandlingen av personopplysninger, og hvordan opplysningene behandles og sikres. Finansdepartementet opplyser i tilbakemelding på utkast til rapport at DFØ skal signere en ny databehandleravtale med Evry i mai 2018, og at bestemmelser for Evrys behandling av personopplysninger vil bli ytterligere klargjort i avtalen.

Problemstilling 2: *Har DFØ sikret at det gjennomføres systematiske tiltak som sørger for tilfredsstillende informasjonssikkerhet for personopplysninger i SAP?*

DFØ har gjennomført tiltak for å sørge for tilfredsstillende sikkerhet for personopplysninger i SAP, men det er vesentlige mangler ved flere av tiltakene. Dette gir risiko for at personopplysninger kan komme på avveie både ut fra bevisste og ubevisste handlinger fra DFØs egne ansatte, eller ved at eksterne utnytter svakheter for å få tak i informasjon fra virksomheten.

Revisjonen viser manglende etterlevelse av personopplysningsloven og forskriften basert på følgende funn:

- Det er bare satt krav om at konfigurasjon av SAP skal følge «beste praksis» uten å beskrive hva det betyr, og det er ikke etablert et system for å følge opp at konfigurasjon etterleves.
- Tilganger i SAP er ikke begrenset til tjenstlig behov for DFØs ansatte. Tilgangsrettigheter er bare basert på en grov inndeling av ansatte i grupper.
- Driftsleverandørens ansatte har ubegrenset tilgang i SAP uten at dette er vurdert eller følges opp av DFØ.
- Skillet mellom driftsmiljøet og test- og utviklingsmiljøene i SAP er ikke tilstrekkelig. Det brukes reelle data i test- og utviklingsmiljøene, og utviklere har rettigheter i driftsmiljøet.

[184] Per 30.01.2018 har 13 kunder signert den nye avtalen, jf. epost fra DFØ av 30.01.2017.

[redacted]

- Krav til autentisering ved passord mv. ligger på et minimumsnivå i SAP og på infrastruktur som denne bygger på.

[redacted]

- Det er flere administratorer enn anbefalt for DFØs Windows-baserte nettverk.
- Klient-PC-er er ikke sikret i samsvar med anbefalinger.

Svak informasjonssikkerhet i DFØs leveranser av lønnstjenester ble tatt opp av Riksrevisjonen allerede i 2012. Vide tilgangsrettigheter og mangelfull oppfølging av leverandør var svakheter som ble tatt opp, og disse svakhetene er også påvist i årets revisjon. Revisjonen viser at det er gjennomgående svakheter i sikkerhetstiltak i DFØ, og at det ikke er satt krav som kan gi et tilfredsstillende sikkerhetsnivå hos underleverandører. DFØs arbeid med informasjonssikkerhet synes ikke å sikre at minimumstiltakene for tilfredsstillende sikkerhet blir gjennomført.

Revisjonen viser også manglende sammenheng mellom DFØs risikovurderinger og sikkerhetstiltak. For eksempel klassifiserer DFØ i den overordnede risikovurderingen angrep fra ondsinnet programvare som kritisk. Dataangrep starter oftest mot PC-er som benyttes av brukere. Til tross for risikovurderingen framstår sluttbrukeres PC-er som svakt sikret.

Problemstilling 3: *Følger DFØ opp at sikkerhetsstrategi og iverksatte tiltak for informasjonssikkerhet i egen virksomhet og hos leverandøren Evry fungerer som forutsatt?*

DFØ har mangelfull oppfølging av at sikkerhetsstrategi og iverksatte tiltak for informasjonssikkerhet fungerer som forutsatt. Virksomheten har dermed ikke et godt grunnlag for kontinuerlig forbedring av sikkerhetsstrategi og tiltak. Dette gir risiko for at det finnes svakheter som gjør at personopplysninger eksponeres for uvedkommende uten at DFØ har kjennskap til dette.

Revisjonen viser manglende etterlevelse av personopplysningsloven og forskriften basert på følgende funn:

- DFØ har ikke gjennomført sikkerhetsrevisjoner av leverandør mellom 2012 og 2018.
- DFØ har ikke gjennomført interne sikkerhetsrevisjoner de siste årene.
- DFØ har ingen dokumenterte gjennomganger eller evalueringer av sikkerhetsstrategi eller sikkerhetstilstanden.
- DFØ har ingen måleparametere for sikkerhet som gjelder konfidensialitet eller integritet, og dermed heller ikke rapportering på disse områdene.
- Det er ikke etablert en formalisert og systematisk rapportering fra Evry om oppfølging av den tekniske informasjonssikkerheten.

DFØ har ansvar for at også leverandører etterlever sikkerhetskravene i personopplysningsloven. Revisjonen viser imidlertid at DFØ overlater sikkerhet med hensyn til konfidensialitet til leverandøren Evry. DFØ krever at drift av systemet skal følge «beste praksis», men definerer ikke hva dette betyr.

Allerede i 2012 påpekte Riksrevisjonen at DFØ hadde svak oppfølging av leverandøren med hensyn til sikkerheten i SAP. At de samme svakhetene fortsatt ikke er rettet opp, indikerer at DFØs prosesser for forbedring av sikkerhetsstrategi og tiltak ikke fungerer.

Den omtalte saken der DFØ oppdaget at Evry, i strid med avtalen, behandlet saker i utlandet, illustrerer risikoen ved å outsource sentrale tjenester. Etter undersøkelser ble det i dette tilfellet avklart at enkelte saker inneholdt personopplysninger, men at disse ikke var sensitive. Revisjonen konstaterer at Finansdepartement ikke ble orientert om forholdet, selv om avtalebruddet potensielt kunne fått konsekvenser for registrerte personopplysninger.

DFØ er en viktig tjenesteleverandør i norsk forvaltning og er ekspertorgan for økonomi- og virksomhetsstyring i staten. Det er av vesentlig betydning at DFØ, som leverandør av lønnstjenester til et stort antall statlige virksomheter, har innrettet arbeidet med informasjonssikkerhet på en slik måte at krav i personopplysningsregelverket etterleves. Revisjonen viser at DFØ har et forbedringspotensial på en rekke områder. Kontroll- og konstitusjonskomiteen har uttalt at mangelfull styring og oppfølging av informasjonssikkerhet i statlige virksomheter er svært alvorlig.[185]

De identifiserte svakhetene blir mer relevante ved innføringen av det nye personvernregelverket (GDPR), noe som aktualiserer større interesse for og vektlegging av å sikre personopplysninger, både blant folk flest og blant DFØs kunder. For DFØs kunder er det av avgjørende betydning at de kan føle seg trygge på at DFØ behandler og lagrer personopplysningene til deres ansatte på en sikker måte, og at behandlingen er i tråd med eksisterende og framtidig regelverk.

[185] Innst.115 S (2017–2018) *Innstilling til Riksrevisjonens rapport om den årlige revisjon og kontroll for budsjettåret 2016.*