

# ROS-analyse av

Oppsummering

Det er blitt gjennomført [ROS](https://intranett-old.stavanger.kommune.no/Administrasjonsenheten/Okonomi-og-organisasjon/HR-stotte/HR-handboker/Handboker/Handbok-internkontroll-HMS-forside/Systematisk-HMS-arbeid/HMS-kartlegging/Risikoanalyse/)/vurdert behov for [DPIA](https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/) i **NN**, Stavanger kommune ved **NN.** Analysen har identifisert **X** mulige uønskede hendelser som kan ha konsekvenser for drift og bruk av systemet, tjenestekvalitet og personvern. Analysen har identifisert ulike tiltak for å redusere risiko.

[Her gjør vi enkelte avgrensninger. Her skriver vi risikovurderingen og konklusjon]

Ved arkivering av ROS i P360 skal den unntas offentligheten med §24 tredje led.

* Dato for oppstart av Analyse: 18.03.2024
* Analysen ble gjennomgått og oppdatert:
* Dato for [protokollført behandling:](https://stavangerkommune.sharepoint.com/sites/Personvern)

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Navn | Stilling / rolle | Oppstart  | Dato  | Dato | Dato | Dato  | Dato  | Dato  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |

|  |  |
| --- | --- |
| **Score** | **Sannsynlighetsklasse – frekvens** |
| 5 | **Svært sannsynlig**. Oftere enn én gang per uke. |
| 4 | **Sannsynlig**. Oftere enn én gang per måned, men sjeldnere enn én gang i uka. |
| 3 | **Mindre sannsynlig** – Oftere enn én gang i året, men sjeldnere enn én gang i måneden. |
| 2 | **Lite sannsynlig** – Mellom 1 og 5 år mellom hver hendelse. |
| 1 | **Ikke sannsynlig** – Sjeldnere enn hvert 5. år. |

 **Konsekvensgrad:**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Kategori** | **1: Ikke alvorlig** | **2: Mindre alvorlig** | **3: Alvorlig**  | **4: Meget alvorlig** | **5: Katastrofalt** |
| Tjenestetilbud | Visse deler av tjenesten utilgjengelig under 1 time eller deltjenester utilgjengelig i mindre enn 4 timer.Påvirker Sølvbergets samlede tjenestetilbud i ingen eller i minimal grad. | Visse deler av tjenesten utilgjengelig 1-4 timer eller deltjenester utilgjengelig i mindre enn 24 timer.Påvirker Sølvbergets samlede tjeneste-tilbud i liten grad. | Store deler av tjenesten er utilgjengelig i opptil 4 timer eller visse tjenester utilgjengelig i 2- 24 timer.Påvirker Sølvbergets samlede tjenestetilbud i moderat grad. Enkelttjeneste er ute av drift midlertidig. | Store deler av tjenesten utilgjengelig 4-48 timer eller deltjenester utilgjengelig i 24-48 timer.Påvirker Sølvbergets samlede tjenestetilbud i stor grad. Sølvberget kan måtte stenge flere deler av tjeneste-tilbudet midlertidig. | Store og vesentlige deler av tjenesten utilgjengelig over 48 timer eller deltjenester utilgjengelig i mer enn tre dager.Påvirker Sølvbergets samlede tjenestetilbud i svært stor grad. Sølvberget kan måtte stenge dørene midlertidig. |
| Integritet | Feil i data hvor det er lave krav til kompletthet, nøyaktighet og gyldighet. F.eks. postnummerViktig enkelopplysning om en enkelt bruker er endret, slettet eller feilaktig. | Feil i data hvor det er vanlige krav til kompletthet, nøyaktighet og gyldighet. F.eks. kontaktinformasjon.Personinformasjon om en enkelt bruker er endret, slettet eller feilaktig. | Feil i data hvor det er høye krav til kompletthet, nøyaktighet og gyldighet. F.eks. feil personnummer.Personinformasjon om en liten gruppe brukere er endret, slettet eller er feilaktig. | Feil i data hvor det er meget høye krav til kompletthet, nøyaktighet og gyldighet. F.eks. feil i regnskapsdata og beslutningsgrunnlag.Personinformasjon om en større gruppe bruker er endret, slettet eller er feilaktig. | Feil i data hvor det er svært høye krav til kompletthet, nøyaktighet og gyldighet. F.eks. feil i data relatert til liv og helse.Store deler av all personinformasjon registrert har blitt endret, slettet eller er feilaktig. |
| Konfidensialitet | Sensitiv informasjon på avveie internt.Beskyttelsesverdig informasjon på avveie internt eller i kontrollerbare former. | Beskyttelsesverdig informasjon på avveie eksternt.Beskyttelsesverdig informasjon på avveie eksternt. | Sensitiv informasjon på avveie eksternt.Store mengder beskyttelsesverdig informasjon på avveie eksternt. Sensitiv informasjon på avveie eksternt. | Store mengder sensitiv informasjon på avveie internt.All eller store deler av all personinformasjon i systemet er på avveie internt. | Store mengder sensitiv informasjon på avveie eksternt.All eller store deler av all personinformasjon i systemet er på avveie eksternt. |

# Behandling av personopplysninger

## Formålet med behandling av personopplysninger

## Behandlingsgrunnlag

## Persondata som blir lagret/behandlet i systemet

# Tegning av systemarkitekturen

# Hendelseskategorier

1. Personvern – generelt
2. Personvern – systemspesifikt
3. Drift og driftsstabilitet – generelt
4. Drift og driftsstabilitet – systemspesifikt

# Risikokategorier

1. Brukere og tilganger
2. Teknisk drift
3. Menneskelige faktorer
4. Lovkrav og avtaler
5. Tilgjengelighet
6. Integritet
7. Konfidensialitet
8. Omdømme

# Identifiserte uønskede hendelser og tiltak

| ID  | Hendelse | Årsaker | Konsekvenser | Risikokategorier | Sann-synlighet | Konse-kvens | Risiko-vurdering | Nåværende tiltak | Aktuelle sannsynlighets-reduserende tiltak | Aktuelle konsekvens-reduserende tiltak | Risikovurdering etter tiltak |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| A1 | Persondata kommer på avveie på grunn av svikt i/manglende rutiner. | Ved eposthenvendelser til bookbites | Persondata på avveie. | Konfidensialitet | 2 | 2 | 4 | Bibliotekarene kan ikke se personopplysninger i systemet, annet enn når de hjelper på lånerens enhet (underforstått at låner samtykker til hendelsen) | Færre feil oppstår og det blir færre grunner til å sende eposter slik at hyppigheten går ned |  | 4 |
| A2 | Persondata kommer på avveie på grunn av angrep mot systemtjener. | Dårlig sikring av systemtjener. Personer med ønske om å tilegne seg personopplysninger. | Persondata på avveie. Mulighet for utpressing. | Konfidensialitet | 1 | 3 | 4 |  |  |  | 4 |
| A3 | Persondata kommer på avveie på grunn av utro tjener. | Personer med ønske om å tilegne seg personopplysninger. | Persondata på avveie. Mulighet for utpressing. | Konfidensialitet | 2 | 3 | 5 |  |  |  | 5 |
| A4 | Ansatte beholder tilgang til systemet etter at de har sluttet i jobben. | Dårlige eller manglende rutiner om opprydding i lista over ansatte. | Uvedkommende får tilgang til systemet, kan etter tilgangsnivå endre på innstillinger og opprette nye brukere. | KonfidensialitetIntegritet | 2 | 3 | 5 | I ansatt-grensesnittet er det svært få innstillinger å endre. |  |  | 5 |
| A5 | Ansatte har flere rettigheter enn de skal ha. | Dårlig eller manglende rutiner om opprydding i lista over ansatte. Ansatte bytter jobb eller rolle som skal ha andre tilganger. | Ansatte kan gjøre ting de ikke har fått opplæring til eller har formening om hva de kan ødelegge. Kan endre på ting som de i utgangspunktet ikke skal endre på. Kan se personinformasjon som de ikke skal ha tilgang til. | KonfidensialitetIntegritet | 2 | 3 | 5 |  | Gode rutiner for å endre innstillinger og rydde opp i brukertilganger |  | 4 |
| A6 | Påloggingsinformasjon til ansatte er kommet på avveie/er kompromittert. | Gjenbruk av passord/for enkle passord. Systemet utsatt for hacking. | Potensiell administrator-tilgang til systemet  | KonfidensialitetIntegritetTilgjengelighet | 2 | 4 | 6 |  |  |  |  |
| A7 | Påloggingsinformasjon til brukere er kommet på avveie/er kompromittert. | Gjenbruk av passord/for enkle passord. Systemet utsatt for hacking. Passord lekket. Innloggingsdetaljer gitt bort. | Uvedkommende får tilgang til en annen brukers brukerkonto. Kan se hva brukeren leser og eventuelt har lest. | Konfidensialitet | 3 | 2 | 5 |  |  |  |  |
| A8 | Ansatt får ikke logget inn i systemet. | Glemt passord. Innlogging er stengt ned. | Ansatt får ikke kjøpt inn e-bøker. | Tilgjengelighet | 2 | 2 | 4 | Mulighet for gjenoppretting av passord. |  |  |  |
| A9 | Bruker får ikke logget inn i systemet. | Glemt passord. | Bruker får ikke lest e-bøker |  | 4 | 1 | 5 | Mulighet for gjenoppretting av passord. |  |  |  |
| A10 | Persondata om brukere som ikke lenger bruker bibliotekets tjenester blir lagret. | Dårlige eller manglende rutiner for sletting av inaktive brukere. | Lagrer personinformasjon som vi ikke trenger. Større konsekvenser enn nødvendig hvis informasjonen kommer ut. |  | 2 | 3 | 5 |  |  |  |  |
| B1 | Google, Facebook- og Apple-pålogging – uklart om hva personopplysningene brukes til. | Google og facebook kan selge opplysninger om din brukeradferd til andre aktører | Målrettet reklame fra kommersielle aktører – anonymisert brukeradferdsdata i kommersiell og (politisk) bruk | Integritet | 2 | 1 | 3 |  | Fraråder bruk av ekstern innlogging i personvernerklæringen? |  | 2 |
| B2 | Reklame fra Bookbites på Facebook/Instagram. | Dersom man velger facebook-pålogging, kan det føre til mer målretta reklame på facebook vedr. ebøker og elydbøker. | Irriterende, men også urovekkende fordi man ikke vet hvorfor disse reklamene kommer | Integritet | 2 | 1 | 3 |  | Gi råd om at man velger annen type pålogging ved oppstart av bookbites. |  | 2 |
| B3 | Leselogg kommer ut. | Sammenstilling av data kan avsløre mye om en person |  |  | 1 | 4 | 5 |  |  |  | 5 |
| B4 | Google Analytics – personopplysninger kommer Google i hende |  |  |  | 2 | 1 | 3 |  |  | Skrudd på anonymiseringsfunksjon i Google Analytics. | 3 |
| B5 | Bruker får ikke koblet opp lånekortet mot biblioteket | Bruker taster feil lånekortnummer eller PIN. Bruker er ikke registrert hos det aktuelle biblioteket, kun hos andre bibliotek. Låner forstår ikke feilmelding. | Bruker får ikke brukt systemet. |  | 3 | 1 | 3 | Informere bruker om at rettledninger finnes på nettsida til leverandøren.  | God informasjon fra biblioteket |  | 2 |
| B6 | Bruker er uenig i at det lagres låne- og søkehistorikk | Har samtykket i alle vilkår ved innlogging | Bruker er engstelig for at personopplysninger kommer på avveie eller blir misbrukt | IntegritetKonfidensialitet | 2 | 4 | 6 | Informere om at bruker kan slå av samtykket i appen |  |  | 4 |
| B7 | Bruker har skrudd av lånehistorikk ved en feil | Har tidligere samtykket, men har skrudd av ved en feil | Får ikke igjen historikken | IntegritetTilgjengelighet | 2 | 3 | 5 | Bruker får en advarsel når hen velger å skru av samtykket. Bruker velger derfor å avbryte handlingen |  |  | 5 |
| C1 | Bibliotekets nettverk er nede. | Vedlikehold av tjenere eller nettverks-infrastruktur i kommunen, fysisk nettverksbrudd, feilkonfigurering. | Ansatte kan ikke kjøpe inn nye bøker/lisenser uten å bytte nettverk. | Tilgjengelighet | 3 | 1 | 4 |  |  |  |  |
| C2 | Systemtjener for Bookbites er nede. | Vedlikehold av tjenere eller nettverks-infrastruktur hos Bookbites, fysisk nettverksbrudd, angrep på tjenermaskin. | Brukere kan ikke låne bøker. Bibliotek kan ikke kjøpe nye bøker/lisenser eller veilede i bruk av Bookbites |  | 1 | 4 | 5 |  |  |  |  |
| C3 | System kan ikke gjenopprettes etter nedetid/feil/kræsj. | Ondsinnet angrep, dårlige backup-rutiner | Brukere kan ikke låne bøker. Bibliotek kan ikke kjøpe nye bøker/lisenser eller veilede i bruk av Bookbites |  | 1 | 4 | 5 |  |  |  |  |
| C4 | Systemet er ikke tilgjengelig på grunn av feil ved oppgradering av system eller server | Servere blir ikke startet opp riktig. Oppgradering feiler. | Brukere kan ikke låne bøker. Biblioteket kan ikke kjøpe nye bøker/lisenser eller veilede i bruk av Bookbites |  | 1 | 4 | 5 |  |  |  |  |
| C5 | Funksjonalitet fungerer ikke etter oppdatering. | Funksjonalitet ikke testet godt nok for implementering. Forskjellig driftsmiljø og -regler hos IT-avdelingen. Dårlig informasjon fra systemleverandør. | Potensiale for at data kan gå tapt eller bli endret. Nye rutiner er ikke laget. |  | 2 | 3 | 5 |  |  |  |  |
| C6 | Varslet nedetid på systemet. | Regelmessig vedlikehold, oppgradering av system eller tjenermaskin. | Brukere og bibliotek mister midlertidig tilgang til systemet. | Tjenestekvalitet | 2 | 2 | 4 | Tid til å forberede driftsavbruddet. Oftest lagt til tidspunkt hvor vi rammes minst mulig. |  |  |  |
| C7 | System blir utsatt for ondsinnet angrep. | Persondata er interessant for uvedkommende. Ønske om å skade Sølvberget eller Allbok/Bokbasen. Forsøk på løsepengeutpressing. | Systemet kan være utilgjengelig over en lengre periode. Kan miste kontroll over persondata og beholdningsdata |  | 1 | 4 | 5 |  |  |  |  |
| C8 | Leverandør av system går konkurs eller trekker systemet fra markedet. | Dårlig lønnsomhet, for kravstore kunder, har lovet for mye, taper anbudskonkurranser. | Kan miste tilgang til system og e-medier kjøpt i systemet. Må sannsynligvis finne et nytt system for e-utlån. |  | 1 | 4 | 5 | Svært etablert leverandør. Avtale er inngått med BS E-bok (eies av Biblioteksentralen) som for tida har Bookbites som leverandør av appen.  |  |  |  |
| C9 | Kritisk feil skjer utenfor leverandørens åpningstid.  | Systemet brukes hele døgnet, men begrenset åpningstid på kundestøtte. | Brukere får ikke lånt bøker. |  | 1 | 3 | 3 |  |  |  |  |
| D |  |  |  |  |  |  |  |  |  |  |  |

# Trenger systemet en DPIA vurdering?

En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i løsningen ivaretas.

Artikkel 35 i Lov om behandling av personopplysninger (personopplysningsloven) definerer når det er påkrevd å gjøre en DPIA, hva den skal inneholde og hvem som skal gjennomføre den. Vurderingen av personvernkonsekvenser skal gjennomføres før databehandlingen starter.

Artiklene som det er referert til i denne malen henviser til denne loven. Du finner loven i sin helhet her. Se også personvernforordningen (GDPR). Datatilsynet har skrevet en veileder som går igjennom regelverket. Den finner du her.

## Når må en DPIA gjennomføres?

«Dersom det er sannsynlig at en type behandling, særlig ved bruk av ny teknologi og idet det tas hensyn til behandlingens art, omfang, formål og sammenhengen den utføres i, vil medføre en høy risiko for fysiske personers rettigheter og friheter, skal den behandlingsansvarlige før behandlingen foreta en vurdering av hvilke konsekvenser den planlagte behandlingen vil ha for vernet av personopplysninger.» (GDPR art.35.1)

Kriterier når DPIA kan bli et krav når to eller flere av følgende kriterier er oppfylt:

1. Evaluering eller scoring, spesielt knyttet til arbeidsresultater, økonomisk situasjon, helse, personlige preferanser eller interesser, oppførsel og adferd, lokasjon og bevegelser osv.
2. Automatiserte beslutninger med juridisk eller tilsvarende betydning.
3. Systematisk overvåking av registrerte.
4. Særlige kategorier personopplysninger eller andre sensitive personopplysninger av høy personlig karakter (sistnevnte spesielt knyttet de enkeltes «friheter», men kan også omfatte f.eks. økonomiske og finansielle opplysninger).
5. Databehandling i stort omfang, som at det er et stort antall registrerte involvert, store mengder data, mange ulike typer data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv.
6. Kombinering eller sammenstilling av datasett.
7. Personopplysninger vedrørende spesielt sårbare registrerte (som barn, ansatte, psykisk syke, asylsøkere, eldre, pasienter mv.).
8. Innovativ eller nyskapende bruk av personopplysninger, som f.eks. bruk av biometriske data for tilgangskontroll, Internet of Things-løsninger, velferdsteknologi osv.
9. 9. Når behandlingen i seg selv forhindrer eller begrenser de registrertes mulighet til å utøve sine rettigheter etter loven eller avtale, eller bruke tjenester.

Vurderingsspørsmål

Dersom svaret er "ja" på ett eller flere av spørsmålene nedenfor, kan det bety at det er behov for en DPIA.
Dersom det besluttes at det ikke er behov for å gjennomføre en DPIA, skal det begrunnes hvorfor.

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr** | **Vurderingsspørsmål** | **Ja**  | **Nei** |
| 1. | Er dette et nytt prosjekt eller prosess? |  x |   |
| 2. | Vil prosjektet innebære innsamling av ny informasjon om enkeltpersoner? |   |  x |
| 3. | Vil prosjektet be enkeltpersoner om å gi informasjon om seg selv? |  x |   |
| 4. | Vil informasjon om enkeltpersoner bli delt med organisasjoner eller personer som ikke tidligere har hatt rutinemessig tilgang til informasjonen? |  x |   |
| 5. | Skal du bruke informasjon om enkeltpersoner som er innsamlet for et formål, men der opplysningene for tiden ikke er eller ikke lenger er i bruk (ikke behandles utover lagring)? |   |  x |
| 6. | Innebærer prosjektet at du bruker ny teknologi som kan oppfattes som inngripende for personvernet? For eksempel, bruk av biometri eller ansiktsgjenkjenning? |   | x |
| 7. | Vil prosjektet resultere i at du tar beslutninger eller gjennomfører tiltak mot enkeltpersoner på måter som kan ha en betydelig innvirkning på dem? |   |  x |
| 8. | Basert på typen informasjon om enkeltpersoner, er det spesielt sannsynlig at bekymringen for eller forventninger til personvernet vil øke? |   |  x |
| 9. | Vil prosjektet kreve at du kontakter personer på måter som de kan finne inngripende? |   |  x |
| 10 | Vil prosjektet innebære databehandling i stort omfang, som at det er et stort antall registrerte involvert, store mengder data, mange ulike typer data, lang varighet av behandlingen, stor geografisk utbredelse av behandlingen osv? |   | x  |

For denne løsningen/prosjektet er det besluttet at det skal:

☐ Gjennomføres en DPIA

x Ikke gjennomføres en DPIA

|  |
| --- |
| **Begrunnelse for hvorfor det skal/ikke skal gjennomføres en DPIA i prosjektet** |
| **Det samles ikke inn særlige kategorier personopplysninger. Selv om det samles inn personopplysninger om barn er det ingen andre alvorlige risiki ved behandlingen av personopplysningene. Personopplysninger som er et resultat av sammenstilling av personopplysninger, som f.eks. ved innhenting av brukeradferdsdata, gis kun i psevdonymisert form.**  |