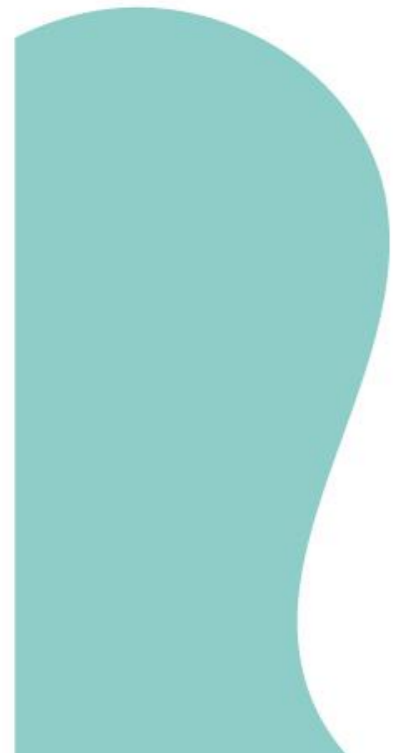




Stavanger
kommune

ROS-analyse av



Oppsummering

Det er blitt gjennomført [ROS](#)/vurdert behov for [DPIA](#) 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](#):

NAVN	STILLING / ROLLE	OPPSTART	DATO	DATO	DATO	DATO	DATO	DATO

Score Sannsynlighetsklasse – frekvens

5	Svært sannsynlig. Ofte enn én gang per uke.
4	Sannsynlig. Ofte enn én gang per måned, men sjeldnere enn én gang i uka.
3	Mindre sannsynlig – Ofte 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 Sjølvbergets 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 Sjølvbergets samlede tjenestetilbud i liten grad.	Store deler av tjenesten er utilgjengelig i opptil 4 timer eller visse tjenester utilgjengelig i 2- 24 timer. Påvirker Sjølvbergets 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 Sjølvbergets samlede tjenestetilbud i stor grad. Sjølvberget kan måtte stenge flere deler av tjenestetilbudet midlertidig.	Store og vesentlige deler av tjenesten utilgjengelig over 48 timer eller deltjenester utilgjengelig i mer enn tre dager. Påvirker Sjølvbergets samlede tjenestetilbud i svært stor grad. Sjølvberget kan måtte stenge dørene midlertidig.
Integritet	Feil i data hvor det er lave krav til kompletthet, nøyaktighet og gyldighet. F.eks. postnummer Viktig 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 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

(Ikke brukt)

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	San- synl igh et	Kon- se- kve- ns	Risi- ko- vur- deri- ng	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
<p>A!-A13 er datatilsynets råd om hva som skal undersøkes i en ROS-analyse (https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdering-av-personvernkonsekvenser/risikovurdering/)</p>											
A1	Personopplysninger behandles uten rettslig grunnlag	Det er ikke avklart hvilket behandlingsgrunnlag eller lovhjemmel som gjelder	Ulovlig bruk av personopplysninger	Lovkrav og avtaler Omdømme	1	2	3	Biblioteket gjennomfører ROS-analyse og skriver behandlingsprotokoll der behandlingsgrunnlag er art.6.1b og lovhjemmel er § 3 i Lov om folkebibliotek			3
A2	Personopplysninger behandles på en ikke rettfærdig måte	Personer opplever at behandlingen er urettferdig	Uønskede opplevelser i bibliotek.	Lovkrav og avtaler Integritet Omdømme	1	2	3	Bibliotek kortet er tilgjengelig for alle i Norge			3
A3	Det ikke er tilstrekkelig åpenhet rundt behandlingen av personopplysninger	Lånere vet ikke hva som behandles og hvorfor	Skaper unødig uro hos brukerne	Lovkrav og avtaler Omdømme	1	2	3	Personvernerklæring er tilgjengelig på bibliotek kortet.no og på Nasjonalbiblioteket	Bibliotekets egen nettside får et tillegg om bibliotek kortet som inneholder opplysninger om formål, behandlingsgrunnlag, hvilke personopplysninger som samles inn og hvordan de behandles		3
A4	Det samles inn mer personopplysninger enn det som er nødvendig for formålet	Systemet samler inn for mange og unødvendige opplysninger	Ulovlig bruk av personopplysninger	Lovkrav og avtaler Integritet Konfidensialitet Omdømme	1	2	3	Nasjonalbiblioteket har minimert innsamlingen til et absolutt minimum			3
A5	Personopplysningene som behandles ikke er korrekte	Låner eller bibliotekar på vegne av låner skriver inn feil opplysninger	Kan redusere tilgang Kan lage forsinkelser og ekstra bry for låner og bibliotekar Kan	Brukere og tilganger Menneskelige faktorer Lovkrav og avtaler Integritet	5	1	6	Låneregisteret i Bibliotek kortet rettes opp hver natt i det det kjøres oppdatering opp mot Folkeregisteret		Låner kan endre kontaktopplysninger selv og for egne barn, men ikke registrert adresse i folkeregisteret.	4
A6	Personopplysninger lagres lengre enn det som er nødvendig for formålet	Kriterier for sletting mangler. Tidsperiode for lagring er ikke fastsatt	Unødvendige data lagres	Lovkrav og avtaler Integritet Konfidensialitet Omdømme	1	2	3	Det er lagd kriterier for sletting: inaktivitet 3 år, ved dødsfall, låner ber om sletting			3
A7	Den registrerte ikke får tilstrekkelig informasjon til å gjøre et informert valg	Forstår ikke prosessen i selve registreringen eller forstår ikke konsekvensen av lagringen	Redd for å bruke tjenesten	Brukere og tilganger Tilgjengelighet Integritet Omdømme	1	2	3	Formålet å låne bøker fra alle bibliotek i Norge er et greit konsept å forstå.	Personvernerklæringen og andre informasjonstiltak om selve konseptet Bibliotek kortet vil gjøre det enklere å forstå.		3

ID	Hendelse	Årsaker	Konsekvenser	Risikokategorier	San- n- synl igh et	Kon- se- kve- ns	Risi- ko- vur- deri- ng	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
A8	Den registrerte ikke får innsyn i hvilke personopplysninger som er lagret	Låner vet ikke at det gis innsyn dersom man logger seg inn på bibliotek Kortet.no	Låner blir usikker og redd for å ta tjenesten i bruk	Brukere og tilganger Tilgjengelighet	1	2	3	Systemet tillater at låner selv logger seg inn og sjekker.	Gjøre det kjent at bruker kan sjekke og rette sine data selv		3
A9	Den registrerte ikke får korrigert eller slettet sine personopplysninger	Låner vet ikke at hen kan korrigere/slette ved å logge seg inn på bibliotek Kortet.no	Låner blir usikker og redd for å ta tjenesten i bruk	Brukere og tilganger Tilgjengelighet Integritet Konfidensialitet Omdømme	1	2	3	Systemet tillater at låner selv logger seg inn for å korrigere og slette	Låner må også orienteres om at det er folkeregisteret som skal motta endringer i navn/adresse og at det etter det blir oppdatert i Nasjonalt lånerregister.		3
A10	Det ikke er lagt til rette for dataportabilitet	Låner kan ikke overføre data fra et system til et annet	Fører til ekstra bry og tar tid	Brukere og tilganger Teknisk drift Menneskelige faktorer Lovkrav og avtaler Tilgjengelighet Integritet Konfidensialitet Omdømme	1	2	3	Systemet er rigget for dataportabilitet. Alle relevante systemer (biblioteksystemer) har integrasjon mot Nasjonalt lånerregister og opplysninger kan flyte mellom bibliotek som låner knytter seg til.			3
A11	de registrertes rettigheter ikke ivaretas ved <i>profilering</i>	Profilering kan føre til brudd på brukerrettigheter	forskjellsbehandling	Lovkrav og avtaler Integritet Omdømme	1	2	3	Ingen profilering foregår. Heller ikke lagres oversikt over aktivitet som lån, purring og annet mislighold			3
A12	Behandlingen kan resultere i diskriminering	Mennesker behandles ulikt		Integritet Omdømme	1	2	3	Ingen diskriminering			3
A13	behandlingen begrenser ytringsfrihet og religionsfrihet	Mennesker undertrykkes og forskjellsbehandles for sine meninger og tro	Undertrykkelse	Menneskelige faktorer Lovkrav og avtaler Integritet Omdømme				Ingen begrensning av ytringsfrihet og religionsfrihet			
Punktene under er mer spesifikk risiko og knyttet til systemet											
B1	Persondata kommer på avveie på grunn av svikt i/manglende rutiner.	Bibliotekansatte gir ut persondata uten at ID er forevist.	Persondata på avveie.	Menneskelige faktorer Lovkrav og avtaler Integritet Konfidensialitet Omdømme	3	2	5	Systemet har mange sikkerhetstiltak som kan forhindre dette, men menneskelig faktor kan spille inn.	Skjerpe rutiner i biblioteks publikumskontakt/skranke		3
B2	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	2	4	6	Sikkerhetsrutiner både hos databehandler og underdatabehandler sikrer mot angrep			4

ID	Hendelse	Årsaker	Konsekvenser	Risikokategorier	San- n- synl igh et	Kon- se- kve- ns	Risi- ko- vur- deri- ng	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
B3	Persondata kommer på avveie på grunn av utro tjener.	Personer med ønske om å tilegne seg personopplysninger.	Persondata på avveie. Mulighet for utpressing.	Menneskelig faktor Konfidensialitet	1	4	5	Systemet har sikkerhetstiltak. Underdatabehandler har dedikert, sikkerhetsklart personell	Biblioteket gir tilgang kun til dem som har tillatelse. Brudd på personalbestemmelsene om taushetsplikt o.l. blir eventuelt anmeldt.		3
B4	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.	Menneskelig faktor Konfidensialitet Integritet	2	2	3	I ansatt-grensesnittet er det svært få innstillinger å endre.			3
B5	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.	Konfidensialitet Integritet	2	2	3		Gode rutiner for å endre innstillinger og rydde opp i brukertilganger		4
B6	Påloggingsinformasjon til ansatte er kommet på avveie/er kompromittert.	Gjenbruk av passord/for enkle passord. Systemet utsatt for hacking.	Potensiell administratortilgang til systemet	Konfidensialitet Integritet Tilgjengelighet	3	3	6		Gode rutiner for passord og tilgang. Gode rutiner for å melde avvik		4
B7	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	3	6	Bruk av bankID og tofaktor mulig	Mulighet for å endre passord selv		4
B8	Ansatt får ikke logget inn i systemet.	Glemt passord. Innlogging er stengt ned.	Får ikke brukt tjenesten	Tilgjengelighet	3	1	4	Mulighet for gjenoppretting av passord.			3
B9	Bruker får ikke logget inn i systemet.	Glemt passord.	Får ikke brukt tjenesten	tilgjengelighet	3	1	4	Mulighet for gjenoppretting av passord.			3
B10	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.	Integritet	2	1	3	Nasjonalbiblioteket sletter etter 3 år. Det lokale biblioteket mangler opplysninger om inaktivitet for digitale tjenester og kan derfor ikke slette det lokale lånekortet.	Lokalt lånekort kan slettes etter anmodning fra låner.		3
B11	Deling	Tilknyttet bibliotek, dedikert personell hos underleverandør, Filmbib/Filmoteket	Deling mellom bibliotek skjer uten at låner vet det.	Integritet Konfidensialitet	1	2	3	Tilgang til personopplysninger er begrenset til de bibliotekene der låner er aktiv. Når låner ønsker å knytte seg til et bibliotek, og før det skjer, vil biblioteket	Filmoteket: Hjemmebibliotek sjekkes i NL		3

ID	Hendelse	Årsaker	Konsekvenser	Risikokategorier	San- n- synl igh et	Kon- se- kve- ns	Risi- ko- vur- deri- ng	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
								kun ha tilgang til et minimum av opplysninger.			
B12	Retting	Tidspunkter på dagen da det kan være feil			3	1	4	Oppdateres en gang i døgnet opp mot folkeregisteret/låner kan rette selv via biblioteksystemet eller nb			4
B13	Sletting	Bruker er redd for at personopplysninger oppbevares etter at vedk har sluttet å bruke tjenesten Ved sletting blir ikke brukeren slettet i det lokale biblioteket		Integritet Konfidensialitet	3	1	4	Kan slette selv. Inaktivitet 3 år, slettes ved Nasjonalt lånerregister Det lokale biblioteket mangler opplysninger om inaktivitet for digitale tjenester og kan derfor ikke slette det lokale lånekortet.			4
B14	Rettslig grunnlag			Lovlighet				Lov om folkebiblioteket § 3			N/A
B15	Formålsbegrensing			Lovlighet				Ingen andre formål enn det som er sagt - låne bøker og annet materiale i hele landet			N/A
B16	Dataminimering	Flere opplysninger enn nødvendig samles inn og gis tilgang til. Det kan stilles spørsmål til at adresse innsamles. Det er som oftest ingen bruk for det. Postnummer for statistikk kunne kanskje erstatte dette.		Integritet	3	1	4	Kun biblioteket der brukeren er tilknyttet, kan se alle personopplysninger. Ansatt kan ikke se hvilket bibliotek låner er tilknyttet.	(Fjerne gateadresse og beholde postnumre som brukes?) -ikke aktuelt nå		4
B17	Manglende reell innflytelse	Har ikke valg, får ikke informasjon, får ikke innsyn, o.s.v.	Låner kvier seg for å ta tjenesten i bruk	Integritet	1	1	2	God informasjon fra Nasjonalt lånerregister	God informasjon fra biblioteket		2
B18	Manglende åpenhet	Informasjonen er ikke god nok	Biblioteket har ikke sin egen personvernerklæring - detaljer om behandlinger i bibliotek er mangelfull	Omdømme	3	1	4	Nasjonalt lånerregister har egen personvernerklæring	Biblioteket utarbeider egen personvernerklæring der formål, behandlingsgrunnlag og type personopplysninger står.		2
B19	Usikkerhet om dataflyten til og fra Nasjonalt lånerregister og biblioteket				1	1	2	NBs vurdering: Se punkt B26 Et nytt bibliotek en låner vil bli låner ved får kun se basisopplysninger før sluttbruker er knyttet til det aktuelle biblioteket. Disse personopplysningene er begrenset til nødvendig informasjon slik at biblioteket kan sikre at personen som skal knyttes til biblioteket er den samme som er registrert i Nasjonalt lånerregister. Dette er fødselsdato, navn og de tre siste sifrene av	Bibliotekansatte/systemansvarlig ved biblioteket setter seg inn i dataflyten.		2

ID	Hendelse	Årsaker	Konsekvenser	Risikokategorier	San- n- synl igh et	Kon- se- kve- ns	Risi- ko- vur- deri- ng	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
								telefonnummeret. Systemleverandørene skjuler hvilke bibliotek en låner er låner ved, da heller ikke det er informasjon en ansatt har behov for. Underdatabehandlerne har forpliktet seg til tilnærmet sanntid synkronisering.			
B20	Biblioteket får ikke beskjed ved flytting/dødsfall/sletting	Usikkerhet i bibliotekene om dette: Hvordan kan bibliotekene sikre seg at sitt lokale lånerregister er oppdatert med folk som dør/flytter fra landet/trekker seg fra felles lånerregister? Kommer det til å bli sendt beskjed til hvert bibliotek låneren er tilknyttet? Eller må dette gjøres via at hvert bibliotek må ordne en integrasjon med folkeregisteret?	Vi er redde for at låner blir stående i det lokale lånerregisteret - spørre nb.no	Integritet (Riktighet)	2	1	3	NBs vurdering: Nasjonalbiblioteket bidrar ikke med oppdatering av lokalt lånerregister. må kreve av egen systemleverandør.	Bibliotekene må ta en gjennomgang om dette hos biblioteksystemet. At de oppdaterer lokale registre opp mot Nasjonalt lånerregister. Lokalt lånerregister må fortsatt røkte lokalt.		3
B21	Integrasjon med biblioteket	Biblioteket får ikke beskjed ved sletting i nasjonalt register	Låner må selv ta kontakt med de bibliotekene hen er tilknyttet		4	1	5	Når låner sletter seg selv, får hen beskjed om at slettingen ikke gjelder			5
B22	Lokale bibliotek sine lånerelement	Det lokale lånerelementet kan ikke følges dersom biblioteket har en nedre aldersgrense for å få lånekort.	Kan føre til forskjellsbehandling	Integritet Omdømme	2	1	3	Nasjonalt lånerregister har ingen nedre aldersgrense for å få lånekort	Endre det lokale lånerelementet slik at det er uten aldersgrense.		2
B23	Skoler	Skoler ønsker kanskje å bruke nasjonalt kort, men har ikke mulighet pga sikkerhetsrutiner	(VURDERES IKKE I DENNE SAMMENHENGEN – OPPVEKST/SKOLE MÅ VURDERE DETTE SELV)								
B24	Brukere registrerer andre personer enn familie eller noen i familien som de ikke er autorisert til	Vil denne brukerens ID bli loggført? Gjør NL noen oppslag mot folkeregisteret		Konfidensialitet Integritet	2	2	4	Loggføres			4

ID	Hendelse	Årsaker	Konsekvenser	Risikokategorier	San- n- synl igh et	Kon- se- kve- ns	Risi- ko- vur- deri- ng	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
		som gjelder familieforhold (Foreldreansvar?) Etter registrering: Har NL noen kobling mellom familiemedlemmer?									
B25	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.	Brukere og tilganger Teknisk drift Menneskelige faktorer Lovkrav og avtaler Tilgjengelighet Integritet Konfidensialitet Omdømme	2	2	4	Informere bruker om at rettledninger finnes på nettsida til leverandøren.	God informasjon fra biblioteket		3
Punktene B 26- B 31 gjelder uklarheter hos oss, men som er svart på av nasjonalbiblioteket. De er ikke nødvendigvis risikoer.											
B26	Uklart hvem som er behandlingsansvarlig	Det lokale biblioteket vet ikke at det er behandlingsansvarlig	Fører til manglende dokumentasjon	Menneskelige faktorer Lovkrav og avtaler Omdømme	3	1	4	NB vurderer det slik: Biblioteket man er låner ved er behandlingsansvarlig. Er man låner ved flere bibliotek er hvert av disse bibliotekene ansvarlige for opplysningene. Det er nå så få opplysninger som mulig som utveksles med et nytt bibliotek før en låner har fått varsel om at hen blir låner ved det. Det er også veldig få opplysninger en bibliotekansatt kan rette. F eks om en bibliotekansatt legger inn adressen til en låner som har hemmelig adresse, så vil den ikke dukke i nasjonalt lånerregister. Fordi registeret er koblet til Folkeregisteret vil adressefeltet til disse være sperret. Om en bibliotekansatt retter i feltene som synkroniseres mot Folkeregisteret vil også de rettes. I nasjonalt lånerregister. Og siden de ulike systemleverandørene nå oppdaterer mot registeret vil også opplysningene rettes i lokalt system. En låner kan slette seg i nasjonalt lånerregister. Da en hen fortsatt låner ved de forskjellige bibliotekene hen var låner ved. Vi kan ikke slette denne koblingen da låneren kan ha	Biblioteket erkjenner sitt behandlingsansvar og inngår databehandleravtale med Nasjonalbiblioteket.		2

ID	Hendelse	Årsaker	Konsekvenser	Risikokategorier	San- n- synl igh et	Kon- se- kve ns	Risi- ko- vur- deri ng	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
								utestående lån eller krav på seg. En låner kan be om å bli slettet ved de bibliotekene hen er låner ved. Men vil da fortsatt være i det nasjonale lånerregisteret. Også om en ikke er låner ved noe bibliotek. Og en låner kan skaffe seg Bibliotek kortet, uten å ennå å blitt låner ved noe bibliotek. Da er det Nasjonalbiblioteket som er behandlingsansvarlig.			
	Hvis en låner har meldt seg ut av nasjonalt lånerregister, er det noe som hindrer låneren fra å bli registrert inn igjen neste gang han er på et bibliotek og oppdaterer opplysningene sine?							NB's vurdering: Hvis en låner har meldt seg ut så er han ute av det nasjonale lånerregisteret. Om hen oppdaterer opplysningene sine hos sitt bibliotek blir opplysningene bare oppdatert der. Hen må bli NY nasjonal låner med nytt lånenummer. Siden registreringen er knyttet til personnummer kan en bare ha en innførsel i det nasjonale lånerregisteret.			N/A
	Hvor ofte oppdateres registrene ut til bibliotekene og til eksterne tjenester? Jeg prøvde å hjelpe en låner med Filmoteket i går og gikk inn på Bibliotek kortet.no og endret hjemmebibliotek. Men det ble ikke oppdatert da Filmoteket sjekket da hun prøvde å låne en film.							Filmoteket skal oppdatere. Det kan være de operer med en forsinkelse. Dette må Filmoteket svare på selv.	Biblioteket må undersøke med Filmoteket om hvor ofte de oppdaterer.		N/A
	Hva forskjellen på personinformasjon registrert på bibliotek kortet.no og i Biblioteksøk? Eller er det det samme?							Det er de samme			N/A

ID	Hendelse	Årsaker	Konsekvenser	Risikokategorier	San- n- synl igh et	Kon- se- kve- ns	Risi- ko- vur- dering	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
	Det står i DPIA at «Man blir også kun del av registeret hvis man aktivt selv registrerer seg på nettsidene eller i bibliotek». Man kan vel faktisk bli registrert av andre ved at de bruker BankID? Er det en sjekk på at det bare er barn av bruker som kan registreres? Blir ID for hvem som har registrert personen i nasjonalt lånekort lagret?							NB's vurdering: Det kreves ikke at noen som registrerer et barn selv har lånekort. Det skjer ved bruk av den voksnes ID og opplysningene om hvem som har logget seg inn med ID-porten for å registrere et barn, tas vare på..			N/A
	Det står i DPIAen at foresatt-tilknytning lagres. Hvordan håndteres dette? Lages det tilknytning til begge foresatte eller bare én?							NB' vurdering: Det lagres bare på den som har registrert barnet. I de lokale systemene kan flere foresatte lagres. Men utfordringen er at vi i bibliotekene ikke har en lovhjemmel som gir oss tilgang til å fastslå koblingen mellom et barn og deres foresatte. Så fort vi får på plass den lovendringen som skal til ,vil systemet rigges om. Vi ser for oss en type løsning som en bruker i helsevesenet. En foresatt logger seg inn, og får opp oversikt over sine barn, velger det barnet hen vil ha lånekort til. Registrerer det, og står som foresatt. Altså en opplysning som hentes fra Folkeregisteret. Lovhjemmelen vil sikre oss denne retten: å koble rett foresatt til rett barn. Formelt sett har ingen i bibliotekene noen mulighet til dette ennå. Våre jurister har utarbeidet et underlag, og det er oversendt Kulturdepartementet. Inntil den er på plass har vi ikke noe bedre system enn å ta vare koblingen til den som har logget seg på. Slik at vi kan identifisere vedkommende. Vi vil ha			N/A

ID	Hendelse	Årsaker	Konsekvenser	Risikokategorier	San- n- synl igh et	Kon- se- kve- ns	Risi- ko- vur- deri- ng	Nåværende tiltak	Aktuelle sannsynlighets- reducerende tiltak	Aktuelle konsekvens- reducerende tiltak	Risikovurdering etter tiltak
								på plass en lovhjemmel som sikrer alle bibliotek muligheten til å fastslå koblingen.			

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. Når behandlingen i seg selv forhindrer eller begrenser de registrertes mulighet til å utøve sine rettigheter etter loven eller avtale, eller bruke tjenester.

Vurderingsspmål

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	Vurderingsspmål	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	
11	Samles det inn og behandles opplysninger om sårbare grupper, så som f.eks. barn	x	

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

X Gjennomføres en DPIA

Ikke gjennomføres en DPIA

Begrunnelse for hvorfor det skal gjennomføres en DPIA i prosjektet

Ja på 2, 3, 10 og 11. Det bør gjennomføres DPIA, særlig med tanke på omfanget av tjenesten (lånerne i hele Norge) (10) og at det også gjelder personopplysninger om barn (11)