Personvernkonsekvensvurdering
(DPIA - Data Protection Impact Assessment)

Kort beskrivelse av gjennomføring av DPIA ved bruk av dette verktøyet:		
Benyttede arkfaner:		
"Initialvurdering"	Innledende grunnleggende informasjon, deltakere, initielle spørsmål som avdekker om behov for full DPIA eller ikke.	
Dersom konklusjon av initialvurdering er full DPIA:		
"Systematisk beskrivelse"	Grundig gjennomgang av behandlingen og dennes omfang.	
"Nødvendighet og proporsjonalitet"	Påvise at forordningen etterleves og at rettigheter og friheter ivaretas.	
"Risikovurdering"	Vurdere uønskede hendelser og risikoen og årsak for disse, og deretter foreslå/anbefale tiltak for å mitigere risikoen.	
"Rapport"	Rapport "genereres" fra de tidligere fanene. Må fylles ut videre fra "(6) Vurdering og synspunkter til behandlingen og dens risikoer (restrisiko):", deltakernes vurdering og felles konklusjon. Til sist skal behandlingsansvarlig validere, konkludere og til slutt signere.	Datatilsynet - DPIA
"Skisse"	Lag en skisse over løsningen og dataflyten slik at man enklere får en god forståelse av hvordan personopplysningene flyter gjennom hele behandlingen.	
"Risikotabell"	Basert på Bærum kommunes forankrede risikoappetitt, kan benyttes som hjelp til utfylling av sannsynlighet og konsekvens (som gir risikoverdien).	
"Endringslogg"	Før opp endringer utført i dokumentet, møter, møtedeltakere. Oppføringer av vedlegg og aktuelle lenker kan også legges inn her som ytterligere dokumentasjon.	
"Skjules"	Data/input til nedtrekksmenyer etc ligger her (noe ustrukturert og kan hende må tilpasses noe). Denne fanen bør skjules når verktøy tas i bruk.	

Datatilsynet:
"Vurdering av personvernkonsekvenser (DPIA)
En vurdering av personvernkonsekvenser (Data Protection Impact Assessment - DPIA) skal sikre at personvernet til de som er registrert i løsningen ivaretas. Dette er en plikt etter det nye personvernregelverket. Artikkel 35 definerer når det er påkrevd å gjøre en DPIA, hva den skal inneholde og hvem som skal gjennomføre den."

Personopplysningsloven Artikkel 35

Hvordan gjennomføre en DPIA?

Det finnes ulike metoder for å gjennomføre en vurdering av personvernkonsekvenser (DPIA), men de har noen felles kriterier.
I forordningen fastsettes noen minimumskriterier for hva en vurdering av personvernkonsekvenser skal inneholde (artikkel 35 nr. 7):

a) En systematisk beskrivelse av de planlagte behandlingsaktivitetene og formålene med behandlingen.

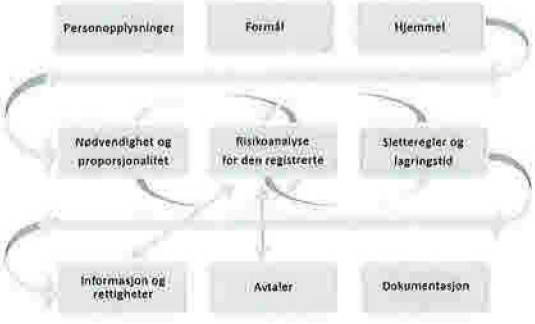
b) En vurdering av om behandlingsaktivitetene er nødvendige og står i et rimelig forhold til formålene.

c) En vurdering av risikoene for de registrertes rettigheter og friheter

d) De planlagte tiltakene for å håndtere risikoene og for å påvise at forordningen overholdes.
I tillegg er ansvarlighet et viktig personvernprinsipp, så til slutt må man bedømme og evaluere, og eventuelt godkjenne. I denne fasen har ledelsen eller styret den viktigste rollen. Arbeidet skal sammenstilles og funn presenteres for ledelsen.

Arbeidsgruppen 29 (WP29) - Veileder

Figur 1 (under) oppsummerer og illustrerer den alminnelige, gjentakende prosessen ved gjennomføring av en vurdering av personvernkonsekvenser:



Figur 2 - Oversikt over stejvis prosess for personvernskonsekvensvurderingen

Personvernkonsekvensvurdering
(DPIA - Data Protection Impact Assessment)

Hensikt med DPIA	Det er obligatorisk å utføre en personvernkonsekvensvurdering (DPIA) dersom det er sannsynlig at en type behandling av personopplysninger kan medføre en høy risiko for fysiske personers personvern, deres rettigheter og friheter (personvernforordningen, artikkel 35). Personvernkonsekvensvurderingen skal utføres *før* behandlingen starter og skal alltid være vurdert av personvernombudet.

(1) Innledende informasjon

Organisasjonsenhet/ sektor:	- Velg -
Kommunalsjef/ behandlingsansvarlig:	
Navn på behandling som vurderes: *(Tjeneste, system, anskaffelse, prosess etc)*	KS Fiks MinSide
Type behandling/ behandlingsaktiviteter: (Overordnet beskrivelse og omfang av behandling av personopplysninger)	MinSide er eit samlingsplass for innbyggjar for å kunne finne lenker til alle offentlege tenester, samt utsend post kjem fram her. Eigedom og informasjon frå kartverket er også knytt inn på MinSide.
Formål (Mål, hensikt, gevinst ved behandlingen (Art. 5b))	Samle alle lenker på ein oversiktleg plass til offentlege tenester som inneber personinformasjon. Formålet med Minside er å gje innbyggjar enkel og effektiv moglegheit for innsyn i brev og fakturaer vedkomande har mottatt frå kommuner ein har et forhold til.
Rettslig grunnlag/ behandlingsgrunnlag (Det må finnes et lovlig grunnlag (Art. 5a, 6.1) (*Ved flere rettslige grunnlag, benytt også kommentarfelt*))	Utøve offentlig myndighet (lov) (art. 6.1 e)
Hjemmel (Ved lovpålagt tjeneste, allmenn interesse, offentlig myndighet (Art. 6.3))	Offentleglova Forvaltningsloven (§ 18) Personopplysningsloven (personvernforordningens art. 5, 1. pkt.)
Kommentarer til innledende informasjon:	KS Fiks MinSide kan brukast av innbyggjar med dei må ikkje. Frivillighetsbasert.

Deltakere - Viktig at alle interessenter er representert ved full DPIA	
Behandlingsansvarlig eller delegert ansvarleg/representant:	
Personvernombud:	Bård Harry Bolstad Eikefet
Representant(er) for den/de registrerte: Begrunn dersom det ikke er relevant å innhente deres synspunkter (Art. 35.9)	Her er ikkje den registerte naudsynt å ta med, grunna det er i hovudsak ikkje nye opplysinger som oppstår her, men lenker vidare til andre system. Ein kan også la ver å nytte systemet.

Andre: (Eks. prosjektleder, jurist, IT-sikkerhet, IT-drift, databehandler)	KS (enkel informasjon frå deira mal), Geir André Bakke
Kommentarer til deltakere:	

(2) Systematisk beskrivelse av behandlingen

2.1 Formål

Behandlingens formål (preutfylles fra fanen Initialvurdering)

Samle alle lenker på ein oversiktleg plass til offentlege tenester som inneber personinformasjon. Formålet med Minside er å gje innbyggjar enkel og effektiv moglegheit for innsyn i brev og fakturaer vedkomande har mottatt frå kommuner ein har et forhold til.

Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte?	Nei
Innebærer behandlingen prediksjon av atferd, profilering av, rangering av, evaluering eller poengsetting av individer? (preutfylles fra fanen Initialvurdering)	***Nei***
Brukes personopplysningene for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte? Gjelder også sammenstilling av opplysninger og bruk til andre formål enn oppgitt/infomert (preutfylles fra fanen Initialvurdering)	***Nei***
Brukes personopplysningene for å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte gjennom matching/sammenstilling, og videre benytte dette til hensikter som det var vanskelig for den registrerte å forestille seg?	Nei
Vil personopplysningene viderebehandles til nye eller andre formål?	Nei

Dette er eit innsynsverktøy, difor blir det nei på desse felta.

Vurdering av om formålet er godt nok beskrevet:

Vurdering av om behandlingens formål er godt nok beskrevet:	Ok

2.2 Behandlingsgrunnlag

Behandlingsgrunnlag (preutfylles fra fanen Initialvurdering)

Utøve offentlig myndighet (lov) (art. 6.1 e)

Beskriv/begrunn behandlingsgrunnlaget

Kommunen har ein plikt til å vise informasjon den behandlar om innbyggjarar, og gjere informasjon forståeleg. Dette systemet skal bidra til at relevant informasjon er lett tilgjengeleg for innbyggjarane som ynskjer innsyn.

Hjemmel (ved lovpålagt tjeneste) (preutfylles fra fanen Initialvurdering)

Offentleglova
Forvaltningsloven (§ 18)
Personopplysningsloven (personvernforordningens art. 5, 1. pkt.)

Evt. kommentar til 2.2 Behandlingsgrunnlag:

Vurdering av om behandlingsgrunnlaget er godt nok beskrevet:

Vurdering av om behandlingsgrunnlaget er godt nok beskrevet:	Ok

2.3 Behandlingens art

Hvem samles det inn personopplysninger om (kategorier registrerte, eksempelvis ansatte, elever, barn, innbyggere, pasienter, kryss av for aktuelle)?

Kategorier av registrerte	Innhentet (Velg "X")	Kommentar
Innbyggere	X	
Ansatte		
Barn/ungdom		
Foreldre/foresatte		
Elever		
Eldre		
Pasienter		
Asylsøkere		

Politikere		
Beredskapshjem/fosterforeldre		
Slektninger/nettverk/venner		
Institusjoner/myndighetspersoner		
(Legg til flere ved behov)		

Hvordan samles personopplysningene inn (samles opplysningene inn fra den registrerte selv og/eller andre kilder)?
Samlast inn frå andre relevante system, for å gjere informasjonen tilgjengeleg for innbyggjar.
Hvor behandles og lagres/oppbevares personopplysningene (eks.: lokalt, i sky)?
I sky. KS.
Hvordan lagres personopplysningene (format, eks. database, tekstdokument, regneark, papir)?
Database.
Geografisk omfang av behandling (lokalt i kommunen, eksternt hos leverandør, i Norge, EU/EØS, 3. land)?
I Noreg.
Hvem har tilgang til personopplysningene (eks. saksbehandler, IT-operatør, leverandør etc)?
Innbyggjar. Leverandør. Kommunen har tilgang til informasjonen i dei enkelte systema, men ikkje via KS systemet.

Brukes det ny teknologi eller eksisterende teknologi hvor personvernkonsekvenser ikke har blitt vurdert? (preutfylles fra fanen Initialvurdering)	*Nei*
Evt. kommentar til 2.3 Behandlingens art:	
Vurdering av om behandlingens art er godt nok beskrevet:	
Vurdering av om behandlingens art er godt nok beskrevet:	Ok

2.4 Behandlingens omfang

Hvilke typer av alminnelige personopplysninger behandles (kryss av for aktuelle)?

Type personopplysning	**Innhentet** (Velg "X")	**Årsak innhenting** (Benyttes ved behov)	**Hentet fra** (Benyttes ved behov)
Fornavn	X	*Verifisering og identifisering.*	*Altinn*
Etternavn	X	*Verifisering og identifisering.*	*Altinn*
Adresse	X	*Verifisering og identifisering.*	*Altinn*
Telefonnummer	X	*Verifisering og identifisering.*	*Altinn*
Epostadresse	X	*Verifisering og identifisering.*	*Altinn*
Personnummer	X	*Verifisering og identifisering.*	*Altinn*
Fødselsnummer	X	*Verifisering og identifisering.*	*Altinn*
(Legg til alle innhentede personoppl.)			

Omfatter behandlingen særlige kategorier av personopplysninger, eller personopplysninger av svært personlig karakter? Rase, eller etnisk opphav, politiske meninger, religiøs eller filosofisk oppfatning, fagforeningsmedlemskap, genetiske data, biometriske data som kan identifisere en enkeltperson, helsedata, beskrivelse av kjønnsliv, eller seksuell orientering (preutfylles fra fanen Initialvurdering)	*Ja*

Hvilke særlige kategorier av personopplysninger behandles (kryss av for aktuelle)?

Type personopplysning	Innhentet (Velg "X")	Årsak innhenting (Benyttes ved behov)	Hentet fra (Benyttes ved behov)
Rasemessig eller etnisk opprinnelse			
Politisk oppfatning			
Religion			
Filosofisk overbevisning			
Fagforeningsmedlemskap			
Genetiske opplysninger			
Biometriske opplysninger			
Helseopplysninger			
Seksuelle forhold			
Seksuell legning			
Straffedommer			
Lovovertredelser			
Fritekstfelt hvor det er risiko for at kan inneholde særlige kategorier av personopplysninger (ustrukturert)			

Antall registrerte involvert?

Kommune spesifikt (cirka antall)

Antall typer/volum av personopplysninger, detaljeringsgrad?

sjå punkt 2.4.

Frekvensen av behandlingen/systematisk behandling (innhentes en gang, flere ganger, kontinuerlig)?

Kontinuerlig.

Lagringstiden for personopplysningene (tidsavgrenset, til evig tid, lovpålagt, formål oppnådd)?

Så lenge informasjon eksisterer i dei andre systema.

Gjennomføres det behandling i stor skala? Høyt antall registrerte eller høy prosentdel av innbyggere, stor mengde data, mange ulike typer data, dekker stort geografisk område, eller foregår over lengre tid, herunder permanent (preutfylles fra fanen Initialvurdering)	*Ja*
Er skisse som viser flyten av personopplysninger gjennom behandlingens alle faser opprettet? Lagre flytskjemaet som: "ÅÅÅÅ-MM-DD DPIA for behandlingsnavn - Vedlegg A" eller kopier skissen til arkfanen "Skisse" i dette dokumentet.	Ja

Flytskjema er laga av KS og lagt til under fana "skisse"

Evt. kommentar til 2.4 Behandlingens omfang:

Vurdering av om behandlingens omfang er godt nok beskrevet:

Mangler "antall registrerte", då kommunen må legge dette inn sjølv.	Mangler

2.5 Konteksten behandlingen utføres i

Kan den registrerte oppfatte behandlingen som uforutsigbar? (Viktig at den registrerte vurderer!) **Beskriv hvordan behandlingen vil oppfattes fra den registrertes synsvinkel.**	Nei
Beskriv:	
Vil den registrerte ha en *særskilt* forventning om at personopplysningene er nødvendige og korrekte? (Viktig at den registrerte vurderer!)	Ja
Beskriv:	
Omfatter behandlingen personopplysninger om sårbare registrerte? **Sårbare individer er i en svak maktposisjon i forhold til den som behandler data, og har derfor begrenset evne til å motsette seg. Eksempler kan være; barn, psykisk syke, pasienter, rusavhengige, asylsøkere, eldre og arbeidstakere** (preutfylles fra fanen Initialvurdering)	***Ja***
Evt. kommentarer:	
Omfatter behandlingen innovativ bruk av teknologi eller organisatoriske verktøy, hvor tilknyttet risiko enda ikke er kjent? **Eksempelvis nye app'er, velferdsteknologi eller kunstig intelligens (AI)** (preutfylles fra fanen Initialvurdering)	***Nei***
Evt. kommentarer:	
Matches eller sammenstilles flere datasett? **Datasett som tidligere ble behandlet av to eller flere aktører, eller med to eller flere hensikter, slås sammen og kan nyttes til hensikter som det var vanskelig for den registrerte å forestille seg når samtykke ble innhentet** (preutfylles fra fanen Initialvurdering)	***Nei***
Evt. kommentarer:	
Evt. kommentar til 2.5 Behandlingens kontekst:	
Vurdering av om behandlingens kontekst er godt nok beskrevet:	
Vurdering av om behandlingens kontekst er godt nok beskrevet:	Ok

2.6 Innebygd personvern	
Er innebygd personvern hensyntatt ved utviklingen av løsningen? (tilgangsstyring, dataminimering, sletting ivaretatt, nedtrekksmenyer heller enn fritekstfelter, "Privacy by design", art. 25)	Ja
Er personverninnstillinger som standard på? (Ikke flere felter for personopplysninger enn nødvendig samles inn eller vises, opplysninger slettes når formål oppnådd, det finnes et lovlig formål for innsamling, muligheter for innsyn i egne opplysninger, "Privacy by default", art. 25)	Ja
Er behandlingen av personopplysninger tilstrekkelig godt informert? (F.eks. gjennom en personvernerklæring)	Ja
Personvererklæring på innloggingssida. Informasjon til innbyggjarane om systemet på kommunen sine kanalar.	
Hvordan ivaretar informasjonssystemet/løsningen som benyttes til behandlingen kravet til innebygd personvern og personvern som standardinnstilling? (Se link i fanen Endringslogg)	
Systemet er laga for at ein skal få innsyn i eigne opplysinger. Kommunen har ikkje tilgang til det som ligg på minside, og fagsystema bak er tilgangsstyrt. Innbyggjaren får kun opp informasjon som er relevant for seg, og ikkje andre innbyggjarar sine opplysingar.	
Vurdering av om innebygd personvern for behandlingen er godt nok beskrevet:	
Vurdering av om innebygd personvern for behandlingen er godt nok beskrevet:	Ok

2.7 Bruk av databehandler	
Benyttes databehandler i forbindelse med behandlingen?	Ja
Er databehandleravtale etablert?	Ja

Hvilke garantier gir databehandleren for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen vil gjennomføres?	
Beskriv kort:	
Evt. kommentar til 2.7 Bruk av databehandler:	
Vurdering av om bruk av databehandler er godt nok beskrevet:	
	Ok

2.8 Tekniske og organisatoriske sikkerhetstiltak	
Er risiko- og sårbarhetsanalyse (RoS) gjennomført?	Ja
Evt. kommentarer:	
Hvilke tekniske og organisatoriske sikkerhetstiltak er implementert for å ivareta personopplysningssikkerheten?	
Henviser til RoS	
Hvordan blir informasjonssikkerheten ivaretatt i informasjonssystemet/løsningen?	
Henviser til RoS	
Hvordan blir informasjonssikkerheten av personopplysninger ivaretatt utenfor selve informasjonssystemet/løsningen (tilgang for personell ved driftsrelaterte oppgaver, tilgang på databaser, tilgang på backup etc)?	
Avtaleruglert med leverandør. Tilsette i kommunen har kun tilgang til data i fagsystema dei oppstår. Rutine.	
Er det utarbeidet rutiner for tilgangskontroll, rollebasert tilgangsstyring, autorisering (bruker/IT-personell/leverandør)?	
Avtaleregulert med leverandør.	
Evt. kommentar til 2.8 Tekniske og organisatoriske sikkerhetstiltak:	
Vurdering av om tekniske og organisatoriske sikkerhetstiltak er godt nok beskrevet:	
Gjennomføre ROS, og komme tilbake til dette punktet.	Ok

(3) Nødvendighet og proporsjonalitet

3.1 Vurdering av personvernprinsippene	
Personvernprinsippene	
Baseres behandlingen på et tydelig rettslig grunnlag?	Ja
Er det rettslige grunnlaget gyldig og rimelig?	Ja
Hvordan vil åpenhet bli ivaretatt i behandlingen?	
Her får innbyggjarar tilgang til sine opplysinger som blir nytta i kommunen, eventuelt lenker til andre system med meir informasjon (eksempelvis Helsenorge.no).	
Formålsbegrensning	
Er formålet klart definert? (Viktig at den registrerte vurderer!)	Ja
Samsvarer formålet forventningene til den registrerte? (Viktig at den registrerte vurderer!)	Ja
Kan formålet oppnås med anonyme eller pseudonyme alternativer?	Nei
Evt. kommentarer:	
Dataminimering	
Er alle personopplysningene som samles inn nødvendige for å oppnå formålet?	Ja
Er det mulig å begrense innsamlingen av personopplysninger?	Nei
Er det mulig å redusere detaljgraden av personopplysninger?	Nei
For ein sikker pålogging så må ein ha opplysningane. For at innbyggjarane skal kunne få innsyn, så må også informasjonen kome fram i dette systemet. Formålet med systemet dett vekk om ein begrenser eller redusere innsamling og detaljgrad.	
Riktighet	
Hvordan holdes personopplysningene korrekte og oppdaterte?	
Med integrasjon med andre system som "eig" informasjonen.	
Ut fra den registrertes rettigheter, er det behov for kontradiksjon (det vil si den registrertes anledning til å imøtegå det som den behandlingsansvarlige har registrert)?	Ja
Ikkje nytte systemet. Kan innhente informasjon om seg via andre kanalar (eksempelvis via innsynsbegjæring). Om ein finn informasjon om seg som er feil, så vil ein kunne henvende seg til kommunen for retting.	
Lagringsbegrensning	
Blir personopplysningene slettet når formålet er oppnådd, i så fall hvordan?	Ja
Det som er på KS vil bli sletta.	
Integritet og fortrolighet	
Er det det gjennomført ROS-analyse av informasjonssystemet? (preutfylles fra 2.8)	***Ja***
Brukes databehandler? (preutfylles fra 2.7)	***Ja***
Er det opprettet databehandleravtale? (preutfylles fra 2.7)	***Ja***
Er personopplysningssikkerheten tilstrekkelig ivaretatt?	Ja
Henviser til RoS	
Evt. kommentar til 3.1 Vurdering av personvernprinsippene:	
Vurdering av om personvernprinsippene er godt nok beskrevet:	
	Ok

3.2 Den registrertes rettigheter og friheter	
Den registrertes rettigheter	
Hvordan gis informasjon om behandlingen til den registrerte?	
Personvererklæring på innloggingssida. Informasjon til innbyggjarane om systemet på kommunen sine kanalar.	
Innsyn i egne personopplysninger	
Hvordan kan den registrerte utøve retten til innsyn i egne personopplysninger?	
Med å logge seg inn i systemet. Opplysinger som er på ID-porten må dei henvende seg til Difi.	
Korrigering av egne personopplysninger	
Skal det være mulig for den registrerte å korrigere sine egne personopplysninger (jf formål og behandlingsgrunnlag)?	Nei
Hvordan kan i så fall den registrerte utøve denne rettigheten?	

Dei kan henvende seg å få korrigert opplysinger som er i systemet, menst personopplysingane vil kome frå Folkeregisteret.
Sletting av egne personopplysninger
Skal det være mulig for den registrerte å slette sine egne personopplysninger (jf formål og behandlingsgrunnlag)? — Nei
Hvordan kan i så fall den registrerte utøve denne rettigheten?
Dei kan henvende seg å få korrigert opplysinger som er i systemet, menst personopplysingane vil kome frå Folkeregisteret.
Begrensning av behandling av personopplysninger
Hvordan kan den registrerte utøve retten til å begrense behandlingen av egne personopplysninger?
Ved å kontakte kommunen.
Dataportabilitet
Hvordan kan den registrerte utøve retten til dataportabilitet?
Ikkje relevant. Opplysinger i KS ligg i andre system som er meir relevant for dette punktet.
Innsigelse mot behandlinger
Hvordan kan den registrerte utøve retten til innsigelse mot behandlingen?
Ved å ikkje nytte system.
Automatiserte avgjørelser og profilering
Vil behandlingen av personopplysninger ha som mål å ta beslutninger som får betydning for den registrerte? (preutfylles fra fanen Initialvurdering) — *Nei*
Hvis behandlingen innebærer automatiserte avgjørelser og profilering, hvordan kan den registrerte reservere seg mot slik behandling?
Beskriv:
Evt. kommentar til 3.2 Den registrertes rettigheter og friheter:
Vurdering av om den registrertes rettigheter er godt nok beskrevet:
Vurdering av om den registrertes rettigheter er godt nok beskrevet: — Ok

3.3 Den registrertes friheter
Vurderinger rundt den registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK).
Hvordan tar behandlingen hensyn til retten til privatliv og kommunikasjonsvern? (Viktig at den registrerte vurderer!)
Opplysinger er kun tilgjengeleg ved personleg pålogging. Kommunen har ikkje tilgang til logg for innlogging.
Hvordan tar behandlingen hensyn til retten til ikke å bli diskriminert? (Viktig at den registrerte vurderer!)
Ikkje relevant.
Hvordan tar behandlingen hensyn til retten til tanke-, tros- og religionsfrihet? (Viktig at den registrerte vurderer!)
Ikkje relevant.
Hvordan tar behandlingen hensyn til retten til ytrings- og informasjonsfrihet? (Viktig at den registrerte vurderer!)
Ikkje relevant.
Evt. kommentar til 3.3 Den registrertes friheter:
Vurdering av om den registrertes friheter er godt nok beskrevet:
Vurdering av om den registrertes friheter er godt nok beskrevet: — Ok

(4) Risiko for uønskede hendelser og (5) tiltak for å redusere disse for den registrertes rettigheter og friheter

Risikoer knyttet til personopplysningsvernet og anbefalte tiltak												
	Hvordan ivaretar behandlingen konfidensialiteten/fortroligheten til informasjonen om den registrerte, og hva kan det i verste fall føre til hvis informasjonen kommer uvedkommende i hende?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak			Dette feltet kan benyttes om det skulle være merknader/kommentarer som kan være nyttig å ha med.
	Risikomomenter	Konsekvens	Eksisterende tiltak	S	K	R	Anbefalte tiltak	S	K	R	Merknad
Konfidensialitet	Uvedkommande får tak i innlogginga til Innbyggjaren.	Uvedkommende får tilgang til opplysninger gjennom MinSide.	Ingen eksisterande tiltak.	2	3	6	- Legge ved i informasjonsskriv til innbyggjarar om at BankID-en er høgt personleg og ikkje skal delast. - Informasjon at innbyggjar bør logge ut av systemet når dei er ferdig. - Legge ved i skriv at ein kan potensielt kome inn på andre system når ein er innlogga på MinSide.	1	3	3	
						0				0	
						0				0	
						0				0	
						0				0	
						0				0	
						0				0	
						0				0	
						0				0	
						0				0	

	Hvordan ivaretar behandlingen integriteten/riktigheten til informasjonen om den registrerte, og hva kan det i verste fall føre til hvis informasjonen er uriktig?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak			Dette feltet kan benyttes om det skulle være merknader/kommentarer som kan være nyttig å ha med.
	Risikomomenter	Konsekvens	Eksisterende tiltak	S	K	R	Anbefalte tiltak	S	K	R	Merknad
Integritet	Ingen informasjon blir oppretta her. Den henter ut informasjon frå andre system, så her vil DPIA og rutiner for desse inntreffe.					0				0	
						0				0	
						0				0	
						0				0	
						0				0	

	Hvordan ivaretar behandlingen tilgjengeligheten til informasjonen om den registrerte, og hva kan det i verste fall føre til hvis informasjonen ikke er tilgjengelig?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak			Dette feltet kan benyttes om det skulle være merknader/kommentarer som kan være nyttig å ha med.
	Risikomomenter	Konsekvens	Eksisterende tiltak	S	K	R	Anbefalte tiltak	S	K	R	Merknad
Tilgjengelighet	System er ute av drift. Nedetid eksempelvis på grunn av oppdatering på server, nettverk ute etc.	Innbyggar får liten eller ingen tilgang til relevant informasjon fra kommunen.	Kommunen får beskjed om nedetid og legg ut informasjon på relevante kommunikasjonskanalar, jamføre rutine.	2	2	4	Vidareføring av ekisterande tiltak.	2	2	4	
						0				0	
						0				0	
						0				0	
						0				0	

	Hvordan ivaretar behandlingen åpenheten rundt informasjonen om den registrerte, og hvilke konsekvenser kan det få for den registrertes personvern om tilstrekkelig informasjon ikke er gitt?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak			Dette feltet kan benyttes om det skulle være merknader/kommentarer som kan være nyttig å ha med.
	Risikomomenter	Konsekvens	Eksisterende tiltak	S	K	R	Anbefalte tiltak	S	K	R	Merknad
Åpenhet	Innbyggar får manglande/mangelfull informasjon om behandlinga av informasjon i MinSide.	Vil ikkje ta i bruk systemet.	Påbegynt arbeid med å laga informasjon.	2	1	2	Ferdigstilling og utsending av informasjonsskriv på relevante kanalar. Samt informasjon på Min side.	1	1	1	

						0				0			
						0				0			
						0				0			
						0				0			

	I hvilken grad er kompleksiteten/uforutsigbarheten i behandlingen høy og tilsvarende vanskelig for den registrerte å forstå, og hvilke konsekvenser kan det få for den registrertes personvern om kompleksiteten av behandlingen ikke er gitt eller forstått?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak			Dette feltet kan benyttes om det skulle være merknader/kommentarer som kan være nyttig å ha med.
Forutsigbarhet	Risikomomenter	Konsekvens	Eksisterende tiltak	S	K	R	Anbefalte tiltak	S	K	R	Merknad
	Forstår ikkje informasjonsskriv.	Brukar ikkje systemet. Logger seg ikkje ut.	Påbegynt arbeid med å laga informasjon.	2	3	6	Ferdigstilling og utsending av informasjonsskriv på relevante kanalar. Samt informasjon på Min side. Få brukarperspektiv på informasjonsskriv før utsending.	1	3	3	
						0				0	
						0				0	
						0				0	
						0				0	

	Hvordan ivaretar behandlingen den registrertes muligheter for medbestemmelse/påvirkining, og hvilke konsekvenser kan det få for den registrertes personvern om den ikke har dette?			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak			Dette feltet kan benyttes om det skulle være merknader/kommentarer som kan være nyttig å ha med.
Medbestemmelse	Risikomomenter	Konsekvens	Eksisterende tiltak	S	K	R	Anbefalte tiltak	S	K	R	Merknad
	Informasjon her blir gjort tilgjengeleg for den enkelte personen. Dette systemet er for at kommunen skal kunne utføre sin plikt om openheit for innbyggar. Innbyggar blir oppretta via Folkeregisteret og vil ikkje kunne motsette seg dette. Men den vil kunne motsette seg å benytte systemet.					0				0	
						0				0	
						0				0	
						0				0	
						0				0	

	Vurder hvordan de registrertes friheter i forhold til Den europeiske menneskerettskonvensjonen (EMK) er tatt hensyn til. Retten til privatliv og kommunikasjonsvern, retten til ikke å bli diskriminert, tanke-, tros- og religionsfrihet, ytrings- og informasjonsfrihet			Risiko			Foreslåtte tekniske eller organisatoriske tiltak som vil kunne redusere risikoen for uønskede hendelser	Risiko etter tiltak			Dette feltet kan benyttes om det skulle være merknader/kommentarer som kan være nyttig å ha med.
Friheter	Risikomomenter	Konsekvens	Eksisterende tiltak	S	K	R	Anbefalte tiltak	S	K	R	Merknad
	Ikkje relevant					0				0	
						0				0	
						0				0	
						0				0	
						0				0	

Behandlingen - Etter gjennoførte tiltak	
Ny beskrivelse av behandlingen	Dersom tiltak bestemmes iverksatt og behandlingen endres, tegn evt. nytt flytskjema og legg inn i samme fil som det opprinnelige flytskjemaet. Lagre flytskjemaet eks. som: "ÅÅÅÅ-MM-DD DPIA for behandlingsnavn - Vedlegg A" eller kopiér skissen til arkfanen "Skisse" i dette dokumentet.

Rapport - Data Protection Impact Assessment

(Skal, med få unntak, være offentlig tilgjengelig)

(1) Innledende informasjon

(Innhentet fra tidligere arkfaner)

Navn på tjeneste	KS Fiks MinSide
Behandling	MinSide er eit samlingsplass for innbyggjar for å kunne finne lenker til alle offentlege tenester, samt utsend post kjem fram her. Eigedom og informasjon frå
Formål	Samle alle lenker på ein oversiktleg plass til offentlege tenester som inneber personinformasjon. Formålet med Minside er å gje innbyggjar enkel og effektiv
Behandlingsgrunnlag	Utøve offentlig myndighet (lov) (art. 6.1 e)
Hjemmel	Offentleglova Forvaltningsloven (§ 18)
Kommentarer	KS Fiks MinSide kan brukast av innbyggjar med dei må ikkje. Frivillighetsbasert.

Konklusjon initiell vurdering:	Full DPIA
Det er to "Ja" eller flere, det vurderes derfor at det er sannsynlig at behandlingen vil innbære en høy risiko for fysiske personers personvern, deres rettigheter og friheter - full DPIA skal gjennomføres	

(2) Vurdering av Systematisk beskrivelse

(Innhentet fra tidligere arkfaner)

Behandlingens formål	Vurdering av om behandlingens formål er godt nok beskrevet:	
Behandlingens grunnlag	Vurdering av om behandlingsgrunnlaget er godt nok beskrevet:	
Behandlingens art	Vurdering av om behandlingens art er godt nok beskrevet:	
Behandlingens omfang	Mangler "antall registrerte", då kommunen må legge dette inn sjølv.	
Konteksten behandlingen utføres i	Vurdering av om behandlingens kontekst er godt nok beskrevet:	
Innebygd personvern	Vurdering av om innebygd personvern for behandlingen er godt nok beskrevet:	
Bruk av databehandler	0	
Tekniske og organisatoriske sikkerhetstiltak	Gjennomføre ROS, og komme tilbake til dette punktet.	

(3) Vurdering av Nødvendighet og proporsjonalitet

(Innhentet fra tidligere arkfaner)

Personvernprinsippene	0	
Den registrertes rettigheter	Vurdering av om den registrertes rettigheter er godt nok beskrevet:	
Den registrertes friheter	Vurdering av om den registrertes friheter er godt nok beskrevet:	

(4) Risikoer og (5) tiltak som må/bør vurderes

(Innhentet fra tidligere arkfaner)

Område	Risikomomenter	Risiko S	Risiko K	Risiko R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko etter S	Risiko etter K	Risiko etter R
Konfidensialitet	Uvedkommande får tak i innlogginga til innbyggjaren.	2	3	6	- Legge ved i informasjonsskriv til innbyggjarar om at BankID-en er høgt personleg og ikkje skal delast. - Informasjon at innbyggjar bør logge ut av systemet når dei er ferdig. - Legge ved i skriv at ein kan potensielt kome inn på andre system når ein er innlogga på MinSide.			1	3	3
Konfidensialitet	0	0	0	0	0			0	0	0
Konfidensialitet	0	0	0	0	0			0	0	0
Konfidensialitet	0	0	0	0	0			0	0	0
Konfidensialitet	0	0	0	0	0			0	0	0
Konfidensialitet	0	0	0	0	0			0	0	0
Konfidensialitet	0	0	0	0	0			0	0	0
Konfidensialitet	0	0	0	0	0			0	0	0
Konfidensialitet	0	0	0	0	0			0	0	0
Konfidensialitet	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	Risiko K	Risiko R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko etter S	Risiko etter K	Risiko etter R
Integritet	Ingen informasjon blir oppretta her. Den henter ut informasjon frå andre system, så her vil DPIA og rutiner for desse inntreffe.	0	0	0	0			0	0	0
Integritet	0	0	0	0	0			0	0	0
Integritet	0	0	0	0	0			0	0	0
Integritet	0	0	0	0	0			0	0	0
Integritet	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	Risiko K	Risiko R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko etter S	Risiko etter K	Risiko etter R
Tilgjengelighet	System er ute av drift. Nedetid eksempelvis på grunn av oppdatering på server, nettverk ute etc.	2	2	4	Vidareføring av eksisterande tiltak.			2	2	4
Tilgjengelighet	0	0	0	0	0			0	0	0
Tilgjengelighet	0	0	0	0	0			0	0	0
Tilgjengelighet	0	0	0	0	0			0	0	0
Tilgjengelighet	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	Risiko K	Risiko R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko etter S	Risiko etter K	Risiko etter R
Åpenhet	Innbyggar får manglande/mangelfull informasjon om behandlinga av informasjon i MinSide.	2	1	2	Ferdigstilling og utsending av informasjonsskriv på relevante kanalar. Samt informasjon på Min side.			1	1	1
Åpenhet	0	0	0	0	0			0	0	0
Åpenhet	0	0	0	0	0			0	0	0
Åpenhet	0	0	0	0	0			0	0	0
Åpenhet	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	Risiko K	Risiko R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko etter S	Risiko etter K	Risiko etter R
Forutsigbarhet	Forstår ikkje informasjonsskriv.	2	3	6	Ferdigstilling og utsending av informasjonsskriv på relevante kanalar. Samt informasjon på Min side. Få brukarperspektiv på informasjonsskriv før utsending.			1	3	3
Forutsigbarhet	0	0	0	0	0			0	0	0
Forutsigbarhet	0	0	0	0	0			0	0	0
Forutsigbarhet	0	0	0	0	0			0	0	0
Forutsigbarhet	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	Risiko K	Risiko R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko etter S	Risiko etter K	Risiko etter R
Medbestemmelse	Informasjon her blir gjort tilgjengeleg for den enkelte personen. Dette systemet er for at kommunen skal kunne utføre sin plikt om openheit for innbyggar. Innbyggar blir oppretta via Folkeregisteret og vil ikkje kunne motsette seg dette. Men den vil kunne motsette seg å benytte systemet.	0	0	0	0			0	0	0
Medbestemmelse	0	0	0	0	0			0	0	0
Medbestemmelse	0	0	0	0	0			0	0	0
Medbestemmelse	0	0	0	0	0			0	0	0
Medbestemmelse	0	0	0	0	0			0	0	0

Område	Risikomomenter	Risiko S	Risiko K	Risiko R	Anbefalte tiltak	Ansvarlig for oppfølgning	Frist	Risiko etter S	Risiko etter K	Risiko etter R
Friheter	Ikkje relevant	0	0	0	0			0	0	0
Friheter	0	0	0	0	0			0	0	0
Friheter	0	0	0	0	0			0	0	0
Friheter	0	0	0	0	0			0	0	0
Friheter	0	0	0	0	0			0	0	0

Bærum kommune - risikotabell

		Ubetydelig konsekvens 1	Liten konsekvens 2	Moderat konsekvens 3	Alvorlig konsekvens 4	Katastrofal konsekvens 5
Svært høy sannsynlighet	5	Moderat (5)	Moderat (10)	[illegible]	[illegible]	[illegible]
Høy sannsynlighet	4	Lav (4)	Moderat (8)	[illegible]	[illegible]	[illegible]
Moderat sannsynlighet	3	Lav (3)	Moderat (6)	Moderat (9)	[illegible]	[illegible]
Liten sannsynlighet	2	Lav (2)	Lav (4)	Moderat (6)	Moderat (8)	Moderat (10)
Svært liten sannsynlighet	1	Lav (1)	Lav (2)	Lav (3)	Lav (4)	Moderat (5)

Mørk rødt:
Strakstiltak. (Meget kritisk = fare for liv og helse)
Rødt:
Tiltak må iverksettes – utarbeid tiltaksplan
Gult:
Det må vurderes om tiltak skal iverksettes
Grønt:
Ikke nødvendig å iverksette tiltak

(6) Vurdering og synspunkter til behandlingen og dens risikoer (restrisiko):	
Behandlingsansvarliges vurdering:	
Den registrertes vurdering:	
Personvernombudets vurdering:	Har vert mangen gode diskusjoner og drøftinger rundt innhald i DPIAen. Ser at systemet kan bli eit godt hjelpe middel for kommune til å vere meir gjennomsiktig, mot den enkelte innbyggjar.
Andre representanters vurdering:	

Konklusjon fra deltakere (velg fra nedtrekkslisten):	*Ja/Nei*
- Velg -	

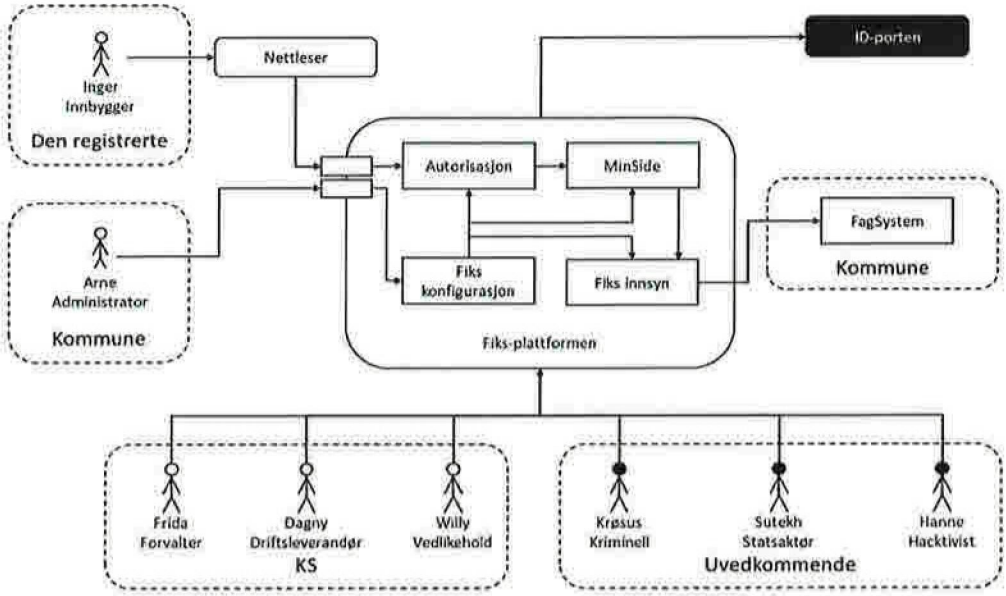
(7) Ledelsens validering av DPIA
Ledelsens vurdering av risikobildet
Ledelsen vurderer anbefalte tiltak, restrisiko og beslutter handlingsplan

Konklusjon fra ledelsen	
Ledelsen beslutter og begrunner om DPIA er (velg fra nedtrekkslisten) :	*Ja/Nei*
- Velg -	

Behandlingsansvarliges signatur/dato (benyttes ved full DPIA):
Signatur/dato: 5/9-22

- HUSK Å LEGGE BEHANDLINGSAKTIVITETEN INN I KOMMUNENS BEHANDLINGSOVERSIKT -

2.4 Behandlingens omfang - Skisse med dataflyt



Aktør/interessent	Rolle	Ansvar for sikring
Inger Innbygger	Representerer innbygger som logger seg inn på MinSide via ID-porten for å få tilgang til egne fakturaer eller post fra de kommunene/fylkeskommunene Inger har et forhold til, og som har delt informasjon på MinSide.	Har selv ansvar for å håndtere egen PC og egne påloggingsopplysninger på en forsvarlig måte.
Arne Administrator	Kommunens administrator på Fiks-plattformen	Ansvar for å konfigurere opp løsningen på vegne av kommunen. Dvs. delegere ansvar for/gi tilgang til aktuelle brukere/bydelsansvarlige osv.
Frida Forvalter	KS' ansvarlige for å følge opp kommunene og deres behov for å bistand med tjenesten.	Ansvar for å ha løpende dialog og kommunikasjon med kommunene.
Dagny Driftsleverandør	KS' tekniske driftspersonell. En tjeneste levert av ekstern profesjonell driftsaktør.	Ansvar for å ivareta den driftstekniske sikringen av tjenesten, som nettverk, serverplattform, systemer og applikasjoner.
Willy Vedlikehold	Programvareutvikler	Utrede og utbedre feil og problemer som måtte oppstå i tjenesten.
Krøsus Kriminell	Representerer kriminelle som for egen eller andres vinning er ute etter å stjele, manipulere eller sabotere informasjon.	Ikke noe ansvar!
Sutekh Statsaktør	Representerer fremmede statsmakter som er ute etter å kompromittere miljøet og stjele, manipulere eller sabotere.	Ikke noe ansvar!
Hanne Hacktivist	Representerer aktivister som for «saken» stjeler, manipulerer eller saboterer.	Ikke noe ansvar!

Risikotabell - må være forankret i ledelsen

Bærum kommune - risikotabell

		Ubetydelig konsekvens 1	Liten konsekvens 2	Moderat konsekvens 3	Alvorlig konsekvens 4	Katastrofal konsekvens 5
Svært høy sannsynlighet	5	Moderat (5)	Moderat (10)	Høy (15)	Katastrofal (20)	Katastrofal (25)
Høy sannsynlighet	4	Lav (4)	Moderat (8)	Høy (12)	Høy (16)	Katastrofal (20)
Moderat sannsynlighet	3	Lav (3)	Moderat (6)	Moderat (9)	Høy (12)	Høy (15)
Liten sannsynlighet	2	Lav (2)	Lav (4)	Moderat (6)	Moderat (8)	Moderat (10)
Svært liten sannsynlighet	1	Lav (1)	Lav (2)	Lav (3)	Lav (4)	Moderat (5)

Sannsynlighet

Nivå	Beskrivelse	Veiledning
1	Det er svært lite sannsynlig at hendelsen vil inntreffe.	Inntreffer sjeldnere enn årlig og/eller ingen kjente sårbarheter/trusler.
2	Det er lite sannsynlig at hendelsen vil inntreffe.	Inntreffer årlig høyst årlig og/eller få eller ingen kjente sårbarheter/trusler.
3	Det er moderat sannsynlig at hendelsen vil inntreffe.	Inntreffer høyst månedlig og/eller kjente mindre alvorlige sårbarheter/trusler.
4	Det er høy sannsynlig at hendelsen vil inntreffe.	Inntreffer ukentlig og/eller kjente alvorlige sårbarheter/trusler.
5	Det er høy sannsynlighet for at hendelsen vil inntreffe.	Inntreffer daglig og/eller svært alvorlige kjente sårbarheter/trusler.

Konsekvens

Nivå	Beskrivelse	Veiledning
1	Den aktuelle konsekvensen for den registrertes personvern, anseelse og/eller personlig integritet vurderes som ubetydelig.	- Hendelsen kan føre til forbigående, mindre økonomisk tap for den registrerte. - Hendelsen kan føre til midlertidig og begrenset tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern ikke er tilstrekkelig ivaretatt i en svært kort periode og uten å involvere særlige kategorier/sårbare grupper.
2	Den aktuelle konsekvensen for den registrertes personvern, anseelse eller personlig integritet er lav, kan vurderes som noe krenkende og/eller påvirker helse i noen grad.	- Hendelsen kan føre til midlertidige eller mindre alvorlige helsemessige konsekvenser for den registrerte. - Hendelsen kan føre til forbigående økonomisk tap for den registrerte. - Hendelsen kan føre til midlertidig eller begrenset tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern ikke er tilstrekkelig ivaretatt i en svært kort periode eller uten å involvere særlige kategorier/sårbare grupper. - Den registrertes tillit til kommunen utfordres midlertidig.
3	Den aktuelle konsekvensen for den registrertes personvern, anseelse eller personlig integritet er moderat, kan oppfattes som krenkende og/eller påvirker helse.	- Hendelsen kan føre til midlertidige eller noe mer alvorlige helsemessige konsekvenser for den registrerte. - Hendelsen kan føre til økonomisk tap av noe varighet for den registrerte. Hendelsen kan føre til midlertidige eller noe mer alvorlige tap av den regis- trertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern krenkes noe mer alvorlig. - Den registrertes tillit til kommunen utfordres.
4	Den aktuelle konsekvensen for den registrertes personvern, anseelse eller personlig integritet er alvorlig, kan oppfattes som svært krenkende og/eller kan medføre tap av liv.	- Hendelsen kan føre til varige eller alvorlige helsemessige konsekvenser for den registrerte. - Hendelsen kan føre til økonomisk tap av betydelig varighet for den registrerte. - Hendelsen kan føre til varig eller alvorlig tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern krenkes alvorlig. - Den registrertes tillit til kommunen utfordres.
5	Den aktuelle konsekvensen for den registrertes personvern, anseelse eller personlig integritet er svært alvorlig, kan oppfattes som svært krenkende og/eller kan medføre tap av liv.	- Hendelsen kan føre til tap av liv (for den registrerte). - Hendelsen kan føre til varige og alvorlige helsemessige konsekvenser for den registrerte. - Hendelsen kan føre til varig og betydelig økonomisk tap for den registrerte. - Hendelsen kan føre til varig og alvorlig tap av den registrertes omdømme. - Hendelsen kan føre til at den registrertes rett til personvern krenkes på en svært alvorlig måte. - Den registrerte og samfunnet taper tillit til kommunen.

DPIA - Møte/endringslogg				
Versjon	Dato	Endringsbeskrivelse	Endret av	Deltakere

Lenker til omtalte referanser	
Personopplysningsloven	https://lovdata.no/dokument/NL/lov/2018-06-15-38
Datatilsynets MÅ -liste	https://www.datatilsynet.no/regelverk-og-verktoy/veiledere/vurdering-av-personvernkonsekvenser/nar-ma-man-gjennomfore-en-vurdering-av-personvernkonsekvenser/
Personopplysningsloven, artikkel 35	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_35#gdpr/ARTIKKEL_35
Personopplysningsloven, artikkel 5	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_5#gdpr/ARTIKKEL_5
Personopplysningsloven, artikkel 9	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_9#gdpr/ARTIKKEL_9
Personopplysningsloven, artikkel 10	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_10#gdpr/ARTIKKEL_10
Personopplysningsloven, artikkel 6	https://lovdata.no/dokument/NL/lov/2018-06-15-38/gdpr/ARTIKKEL_6#gdpr/ARTIKKEL_6
Innebygd personvern	https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/innebygd-personvern/programvareutvikling-
Den europeiske menneskerettighetskonvensjon (EMK)	https://www.regjeringen.no/no/tema/utenrikssaker/menneskerettigheter/id1160/

Vedlegg til DPIA				

Signert for