Vurdering av personvernkonsekvenser (DPIA) for behandling av personopplysninger i <Systemnavn>

Systemnavn	<Systemnavn>
Systemnummer	
Saksnummer i arkivsystemet. Husk også saksnr. der databehandleravtalen er lagret.	
Hvem er behandlingsansvarlig (virksomheten din eller tredjepart)?	
Hvem er databehandler (virksomheten din eller tredjepart)?	
Dato for når personvernombudet er involvert	
Er de registrerte eller deres representant blitt kontaktet? Hvis ja, hvilken dato?	
Hvem har utarbeidet DPIA?	
Dato for utført DPIA	

Dette skjemaet er basert på Datatilsynets maler og er ment å dekke det minimum en vurdering av personvernkonsekvenser (Data Protection Impact Assessment) må inneholde.

Skjemaets kap.1 inneholder en systematisk beskrivelse av formål og den behandlingen av personopplysninger du ønsker å gjennomføre. I kap. 2 skal du vurdere om den behandlingen du ønsker (ref. kap. 1) er nødvendig og rimelig i forhold til formålet. I skjemaets kap. 3 skal risikoen for de registrertes rettigheter og friheter vurderes. Det fjerde og siste kap. tar for seg planlagte tiltak for å håndtere risiko, garantier og sikkerhetstiltak for å sikre vern av personopplysninger. I tillegg sammenstilles arbeidet og presenteres for ledelsen.

Det du skal beskrive eller vurdere er satt i normal skrift. Tekst i *kursiv* nedenfor, er ment som veiledning.

1. Beskrivelse av behandlingen av personopplysninger

Formålet med å fylle ut dette punktet er å gi en fullstendig oversikt over behandlingen av personopplysninger som gjøres med dette systemet. Du skal beskrive hva som er behandlingens art, omfang og formål. Det må gå klart frem her hva personopplysningene er planlagt å brukes til.

1.1 Beskrivelse av prosjektet (løsning, tjeneste og system) og behov for DPIA.

Presenter prosjektet/systemet ved å gi det en overordnet beskrivelse:
Beskriv hvorfor det er nødvendig med en DPIA. F.eks. at behandlingen er i stor skala eller medfører en systematisk overvåkning:

1.2 Behandlingens formål

Her skal du beskrive formålet med behandlingen av personopplysninger. Pass på at du får med alle formålene, også eventuelle formål ved viderebehandling (eks. statistikk eller forskning). Husk på at det skal foreligge et faktisk behov for behandlingen, og det skal ikke behandles flere personopplysninger enn det som er nødvendig for å oppnå formålet/formålene med behandlingen.

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Hovedformålet med løsningen/systemet.	
Formålet med behandlingen av personopplysninger, også eventuell sekundærbruk.	
Er formålet å treffe avgjørelser om enkeltpersoner basert på systematisk og omfattende analyse av personlige aspekter?	
Vil behandlingen ha som mål å ta beslutninger som får betydning for den registrerte?	
Skal personopplysningene brukes til å profilere den registrerte?	
Vil personopplysningene brukes til å avdekke ukjente sider eller for å gjenkjenne mønstre ved den registrerte?	
Andre tilleggsformål?	

1.3 Behandlingens omfang

Her må du få med en beskrivelse av alle personopplysninger som behandles.
I denne beskrivelsen må du minimum ha med følgende:

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Hvilke personopplysninger samles inn?	
Hvilke kategorier og typer av personopplysninger er det snakk om (alminnelig eller særlig kategori)?	
Hvilke kategorier av registrerte er det snakk om (barn, elever, voksne, ansatte)?	
Antall registrerte	
Datavolumet. Det vil typisk si antall variabler eller detaljeringsgrad.	
Frekvensen av de ulike behandlingene som gjennomføres. Det kan være en gang, flere ganger, regelmessig, kontinuerlig el.	

Lagringstiden på personopplysningene. Det kan være tidsavgrenset periode, permanent el.	
Det geografiske området for behandlingene. Det kan være lokalt, regionalt, nasjonalt, internasjonalt el.	
Er det annet du ønsker å opplyse om her?	

1.4 Behandlingens art/behandlingsaktiviteter

Her skal du beskrive det du planlegger å gjøre med personopplysningene f.eks. innsamle, registrere, sammenstille, analysere, lagre og utlevere. Alle handlingene du planlegger å gjøre med opplysningene, må beskrives. Det er vist til noen eksempler, men dette er ikke en uttømmende liste.

1.4.1 Innsamling av personopplysninger

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Hvordan får vi/henter vi inn opplysningene?	
Samles opplysningene inn fra de registrerte selv eller fra andre?	
Samles det inn data fra ulike steder?	
Er måten dataene hentes inn på særlig inngripende overfor den registrerte? (F.eks. sporing, overvåking, fingeravtrykk osv.).	
Samles det inn flere opplysninger enn det som er nødvendig?	
Hvilken informasjon gis til den registrerte (jf. art. 13 og 14)?	
Er det noe annet du ønsker å opplyse om her?	

1.4.2 Hva skal personopplysningene brukes til?

Beskriv her

1.4.3 Lagring og sletting

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Hvordan lagrer vi personopplysningene?	
Hvor lagres personopplysningene og for hvor lenge?	
Hvilke kriterier har vi satt for å fastsette lagringstiden?	
Når skal personopplysningene slettes? Hvor lenge lagrer vi personopplysningene etter at formålet med behandlingen er over?	

Har vi utarbeidet rutiner for sletting? Herunder kontroll på at databehandler sletter dersom det er databehandler som skal gjennomføre dette?	
Får den registrerte informasjon om - muligheten for sletting av opplysninger -hvordan dette i så fall vil skje, og kan den registrerte selv slette egne opplysninger?	
Fremgår det av lov eller forskrift at vi kan nekte sletting? Hvis ja, oppgi hvor det fremgår. *Arkiv skal involveres i denne vurderingen.* *Arkiv skal også kontaktes og involveres før personopplysninger faktisk slettes.* *Du skal sette inn dato for kontakt med arkiv, og resultatet av kontakten.* *Dersom kassasjonssøknad sendes, setter du inn dato for når søknaden ble sendt.*	
Er det noe annet du ønsker å opplyse om her?	

1.4.4 Tilgang til/interne mottakere av personopplysninger

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Beskriv alle som har tilgang til eller mottar personopplysningene	
Hva har vi av tilgangskontroll og hvilke rutiner har vi for dette?	
Hvordan deles opplysningene mellom avdelinger internt i virksomheten?	
Hvilke opplysninger deles med hvilke avdelinger og hva er formålet med delingen til de ulike avdelingene?	
Er det noe annet du ønsker å opplyse om her?	

1.4.5 Deling/utlevering/overføring

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Hvilke eksterne virksomheter deler vi personopplysningene med, og hva mottar de ulike virksomhetene av personopplysninger?	

Hva er formålet med delingen, og hva er det rettslige grunnlaget for delingen?	
Overfører vi opplysningene til land innenfor EU/EØS?	
Overfører vi personopplysninger til tredjeland eller internasjonale virksomheter/organisasjoner? Hvis ja, hva er det rettslige grunnlaget for overføringen? Her må vi forklare hvordan vi sikrer etterlevelse av forordningen ved overføring til utlandet, og hvilket regelverk/atferdsnormer/bransjenormer/ retningslinjer som gjelder ved overføringen og hvordan vi sikrer at dette etterleves.	
Hvordan overføres og/eller tilgjengeliggjøres personopplysningene?	
Hvilke forholdsregler tas for å beskytte personopplysninger? Krever vi taushetserklæringer? Signeres databehandleravtaler?	
Hvilke sikkerhetstiltak har vi for deling/utlevering/overføring av personopplysninger?	
Har vi identifisert alle (under)databehandlere?	
Gir databehandleren tilstrekkelige garantier for at egnede tekniske og organisatoriske tiltak som sikrer at behandlingen er i samsvar med forordningen vil gjennomføres? List opp ev. garantier.	
Er det noe annet du ønsker å opplyse om her?	

1.4.6 Retting

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Kan vi rette feil i den registrertes opplysninger? I så fall hvordan, og hvilke rutiner har vi?	
Kan den registrerte selv rette feil i egne personopplysninger?	

Gis det informasjon til den registrerte om muligheten til å rette opplysninger og om hvordan retting kan gjøres?	
Er det noe annet du ønsker å opplyse om her?	

1.5 Vurdering av sammenhengen behandlingen utføres i (kontekst)

Her skal behandlingen vurderes i et større bilde. Alle interne og eksterne faktorer som kan påvirke forventninger eller konsekvenser vurderes her.

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Behandler vi personopplysninger fra ulike datasett, som er innsamlet for ulike formål og fra ulike behandlingsansvarlige?	
Fra hvilke kilder får vi/innhenter vi dataene?	
Er det kobling mellom systemer eller registre der dataene behandles opp mot andre informasjonssystemer? (F.eks. for å få ny informasjon om den registrerte)	
Er det gjort erfaringer tidligere med tilsvarende type behandling?	
Er det noen nåværende allmenn bekymring for den beskrevne måten å behandle personopplysninger på?	
Hvilken relasjon har den behandlingsansvarlige med de registrerte? Beskriv maktforholdet.	
I hvilken grad har den registrerte kontroll over sine personopplysninger?	
Vil den registrerte ha en særlig forventning om at personopplysningene er nødvendige og korrekte, at de behandles med konfidensialitet, og om retten til privatliv?	
Vil det behandles personopplysninger om barn eller andre som må anses som særlig sårbare?	
Beskriv hvordan behandlingen vil oppfattes fra de registrertes synsvinkel – kan de registrerte f.eks. oppfatte behandlingen som uforutsigbar?	
Er det noe annet du ønsker å opplyse om her?	

1.6 Informasjonssikkerhet og ansvarsforhold

Her må du beskrive informasjonssikkerheten og ansvarsforholdene i systemet. For å besvare en del av disse spørsmålene må vi ha hjelp av vår databehandler/systemleverandør.

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Er systemet bygget fra bunnen av hos oss, eller er det «hyllevare» vi har fått installert?	
Er programvaren (enten hos oss eller hos leverandøren) bygget med innebygget personvern som standardinnstilling? Beskriv de organisatoriske og tekniske tiltakene som er gjort for å sikre dette.	
Tas ny teknologi i bruk eller brukes eksisterende teknologi på en ny måte? Er det eventuelle relevante fremskritt innen teknologi eller sikkerhet?	
Beskriv hvordan informasjonssystemet, infrastrukturen, tjenestene, driftsmiljø, ytre grenser, informasjonssystemets tilstøtende grensesnitt med andre systemer det er koblet mot fungerer, og hvordan personopplysningene overføres mellom systemene.	
Er det - eksterne eller interne krav til løsningen? - retningslinjer eller tiltak som må etterleves? - sikkerhetsstandard som må overholdes? Er alle planlagte og iverksatte tekniske og organisatoriske tiltak egnet til å sikre personopplysningenes konfidensialitet, integritet og tilgjengelighet?	
Er det noe annet du ønsker å opplyse om her?	

2. Behandlingen(e)s nødvendighet og proporsjonalitet

Her skal du kvalitetssikre at de valgene du har beskrevet under punkt 1 oppfyller personvernprinsippene. Dette betyr at de er legitimert og nødvendige, og at valgene du har gjort står i et rimelig forhold til formålene som skal oppnås.

Dersom vurderingene i punktene nedenfor viser at det er nødvendig å forbedre eller endre noe i dagens praksis, skal dette gjennomgås. Du skal da foreslå tiltak for å bedre personvernet for den registrerte.

2.1 Rettslig grunnlag

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Hva er det rettslige grunnlaget for alle behandlingsaktivitetene? *Vi skal vise til personvernforordningen, lov eller forskrift for alle behandlingsaktiviteter, også ved utlevering til forskning.*	
Kommer det tydelig frem for de registrerte hvilken artikkel, lov eller forskrift vi har som grunnlag for å behandle personopplysningene?	
Vurder hvordan åpenhet overfor den registrerte ivaretas i behandlingen	

2.2 Formålsbegrensning

Formålene for behandling av personopplysninger skal være spesifikt og uttrykkelig angitt, og det skal være et berettiget formål.

	Forklar og beskriv.
Hva er formålet/formålene med behandlingen av personopplysningene?	
Vurder om formålene er klart definert.	
Vurder om formålene er definert slik at det samsvarer med forventningene til den registrerte	
Vurder og begrunn hvorfor formålet ikke kan oppnås med en mindre inngripende behandling.	
Vurder og begrunn om formålet kan oppnås med anonyme eller pseudonyme alternativer. Kan vi det, skal vi også velge den løsningen.	
Er det noe annet du ønsker å opplyse om her?	

2.3 Dataminimering

Personopplysningene vi behandler skal være adekvate, relevante og begrenset til det som er nødvendig for å oppnå formålene.

	Forklar og beskriv.
Vurder om formålet med behandlingen av personopplysninger kan oppnås ved å hente inn færre data, f.eks. mindre detaljerte opplysninger eller mindre sensitive opplysninger. Kan vi det, må vi også velge den løsningen.	
Begrunn nødvendigheten og relevansen for den enkelte variabel av personopplysning sett opp mot formålet som skal oppnås.	

Er det noe annet du ønsker å opplyse om her?	

2.4 Riktighet

Personopplysningene skal være korrekte og oppdaterte.

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Beskriv hvordan vi sikrer at vi holder personopplysningene oppdaterte og korrekte, både med og uten den registrertes involvering.	
Har vi nødvendige funksjoner for å rette og slette uriktige opplysninger? *Beskriv funksjonene, ev. hvorfor vi ikke*	
Ut fra den registrertes perspektiv; er det behov for kontradiksjon rundt personopplysningene?	
Er det noe annet du ønsker å opplyse om her?	

2.5 Lagringsbegrensning

Personopplysningene skal slettes eller anonymiseres når formålet med behandlingen er nådd.

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Lagres personopplysningene etter at formålet er nådd? *Her må du vurdere hver enkelt personopplysning eller kategori av personopplysning,* *opp mot når sletting inntreffer eller når vi anonymiserer / pseudonymiserer personopplysningene.*	
Hvilke garantier må være på plass dersom personopplysningene skal lagres lenger/etter at formålet er nådd? Personopplysningene kan lagres lenger på grunn av: • arkivformål i allmennhetens interesse, • formål knyttet til vitenskapelig eller historisk forskning • for statistiske formål.	
Er det noe annet du ønsker å opplyse om her?	

2.6 Ivaretakelse av de registrertes rettigheter

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.
Hvordan gis informasjonen til den registrerte? *Er det f.eks. gjennomsiktig og rettferdig behandling? Se (art. 12-14).*	
Dersom behandlingen er basert på samtykke fra personene det gjelder: • Hvordan er samtykket innhentet (art. 7 og 8)? • Er samtykket frivillig, uttrykkelig og spesifikt? • Kan vi dokumentere det? • Kan samtykket trekkes tilbake like enkelt som det gis? *Merk at samtykket ikke må forveksles med kontrakt eller personvernerklæring.*	
Hvordan ivaretas den registrertes rett til innsyn? *Se art. 15*	
Hvordan ivaretas den registrertes rett til retting og sletting? *Se art. 16 og 17.*	
Hvordan ivaretas den registrertes rett til innsigelser og begrensning av behandling? *Se art. 18, 19 og 21.*	
Hvordan ivaretas den registrertes rett til dataportabilitet? *Se art. 20.* *Merk at dette sjelden er aktuelt for våre behandlinger.*	
Hvordan håndheves forbudet mot automatiserte individuelle avgjørelser, herunder profilering? *Se art. 22.*	
Er det noe annet du ønsker å opplyse om her?	

2.7 Ivaretakelse av de registrertes friheter

	Forklar og beskriv.
Hvordan ivaretas de registrertes friheter gitt i Den europeiske menneskerettskonvensjonen når det gjelder: - retten til privatliv og kommunikasjonsvern - retten til ikke å bli diskriminert, tanke-, tros-, og religionsfrihet - ytrings- og informasjonsfrihet?	
Er det noe annet du ønsker å opplyse om her?	

3. Risikoen for de registrertes rettigheter og friheter, og de planlagte tiltakene virksomheten har for å håndtere risikoene

3.1. Sikkerhetstiltak og risikovurderinger

Bruk excel-skjema til å gjennomfør en egen risikovurdering med utregning av poeng. Regnearket skal følge som vedlegg til denne DPIA'en.

3.2. Samlet vurdering av risikobildet

Her skal du gi din skriftlige oppsummering av risikobildet som regnearket viser. Du skal spesifikt angi hvilke nye tiltak som eventuelt må iverksettes for at risikoen skal være akseptabel.

Gi din oppsummering her:

3.3 Personvernombudets råd

Personvernombudet skal involveres <u>før</u> det igangsettes behandling av personopplysninger. Se art. 35 nr. 2 og art. 39 nr. 1 bokstav c.

Oppgi her om personvernombudet har vært involvert og hvilke råd ombudet har gitt. Utdyp om ombudets råd er tatt til etterretning eller ikke. Følger dere ikke personvernombudets råd, utdyp hvorfor og hvordan.

Redegjør her:

3.4 De registrertes synspunkter

De registrerte skal så langt det er mulig høres. Beskriv når og hvordan de registrertes synspunkt er innhentet. Forklar nærmere dersom de registrertes synspunkter ikke etterfølges.

Mener du det ikke er mulig å innhente de registrertes, eller deres representants, synspunkt, må du begrunne det.

Redegjør her:

4. Ledelsens gjennomgang og vurdering av den gjennomførte DPIA

Ledelsen er ansvarlig dersom virksomheten bryter regelverket for personvern. De skal derfor involveres i arbeidet med denne DPIA. Beskriv hva du har gjennomført av følgende:

	Forklar og beskriv. Svarer du ja eller nei, må du begrunne svaret.

Ledelsen er gjort oppmerksom på at; - vi behandler personopplysninger - det medfører høy risiko for den registrertes rettigheter og friheter.	
Ledelsen er gjort kjent med: - den gjennomførte DPIA - identifisert risiko - foreslåtte tiltak og risikovurderingen som er gjennomført	
Ledelsen er gjort oppmerksom på at det å ikke gjennomføre en DPIA eller å utføre dette feil, kan medføre betydelige administrative bøter.	
Ledelsen er gjort kjent med avdelingens tiltak for å overholde av personvernforordningen.	
Ledelsen er gjort kjent med tiltakene som er iverksatt for å gi tilstrekkelig informasjonssikkerhet.	
Ledelsen er gjort kjent med de kartlagte risikoene ved behandlingen av personopplysninger. De er også gjort kjent med eventuell handlingsplan for tilleggstiltak basert på risiko, med estimert tids- og kostnadsramme.	
Ledelsen er gjort kjent med personvernombudets råd og anbefalinger om behandlingen av personopplysninger i systemet.	
Ledelsen er gjort kjent med de registrertes eller deres representanters synspunkter.	

Ledelsen skal deretter:	*Vurder og beskriv*
- avgjøre om de iverksatte tiltakene er tilstrekkelige og akseptable, sett opp mot restrisikoen - avgjøre om handlingsplanen for tilleggstiltak er akseptabel. *Merk at vurderingen må inkludere personvernombudets råd og anbefalinger, og synspunkter fra de registrerte eller deres representant.*	
- beslutte om behandlingen kan starte opp - beslutte om det er behov for ytterligere undersøkelser, tiltak osv. *Hvis de beslutter det, skal revidert DPIA legges frem for ledelsen på nytt* - beslutte om behandlingen skal avvises *En avvisning vil si at det er for stor risiko til at vi kan behandle disse personopplysningene på denne måte i dette tilfellet*.	