Internkontrollskjema for behandling av personopplysninger

Systemnavn/Behandlingsaktivitet:	
Systemnummer:	
Saksnummer i arkivsystemet:	
Behandlingsansvarlig:	
Databehandler:	
Dato (når ble skjemaet opprettet og ev. revidert):	
Internkontrollskjemaet er fylt ut av:	

1. Behandling av personopplysninger

1.1. Beskrivelse av systemet og formålet

Hva er formålet/formålene med systemet og hvorfor opprettes det? Det skal foreligge et behov for behandlingen og det skal ikke behandles flere personopplysninger enn det som er nødvendig.

Beskriv her:

Hvem er behandlingsansvarlig og databehandler, og hvorfor er rollefordelingen slik?

Beskriv her:

***Dersom du (virksomheten din) er databehandler**: hvem er du databehandler for, og oppgi saksnummer i arkivsystemet hvor databehandleravtalen er lagret.*

Hvem er vår virksomhet databehandler for:	
Saksnummer i arkivsystemet for hvor databehandleravtalen er lagret:	

1.2. Har du vurdert om behandlingen krever en personvernkonsekvensvurdering (DPIA), jf. artikkel 35?

En vurdering av personvernkonsekvenser (DPIA) er en prosess som skal beskrive behandlingen av personopplysningene og vurdere om behandlingen er nødvendig og proporsjonal. Den skal også bidra til å håndtere de risikoene behandlingene medfører for enkeltpersoners rettigheter og friheter ved å vurdere dem og fastsette risikoreduserende tiltak.

Det kreves ikke at det skal gjennomføres en DPIA for alle behandlinger av personopplysninger som vi gjennomfører. For en rekke av våre behandlinger vil det være tilstrekkelig å fylle ut dette internkontrollskjemaet (med tilhørende risikovurdering).

Du kan lese mer om DPIA på Datatilsynets nettside her:
https://www.datatilsynet.no/rettigheter-og-plikter/virksomhetenes-plikter/vurdere-personvernkonsekvenser/vurdering-av-personvernkonsekvenser/

Du skal alltid gjennomføre en DPIA ved:

- *En systematisk og omfattende vurdering av personlige aspekter ved fysiske personer som er basert på automatisert behandling, herunder profilering, og som danner grunnlag for avgjørelser som har rettsvirkning for den fysiske personen eller på liknende måte i betydelig grad påvirker den fysiske personen.*
- *Behandling av særlig kategori av personopplysninger i stor skala.*
  (Særlig kategori av personopplysninger er personopplysninger om rasemessig eller etnisk opprinnelse, politisk oppfatning, religion, filosofisk overbevisning eller fagforeningsmedlemskap, samt behandling av genetiske opplysninger og biometriske opplysninger med det formål å entydig identifisere (og ikke bare autentisere) en fysisk person, helseopplysninger eller opplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering).

Du skal også gjennomføre en DPIA, dersom du svarer «ja» på to eller flere av spørsmålene nedenfor:

Spørsmål:	Svar: Ja eller nei? (ved behov, utfyll svaret ditt)
Innebærer behandlingen en evaluering eller poengvurdering av de registrerte eller av karakteristikker/evner til de registrerte?	
Omfatter behandlingen avgjørelser som treffes automatisk uten menneskelig påvirkning?	
Hvis det treffes en automatisert avgjørelse som nevnt over, har den betydelige konsekvenser for de registrerte? F.eks. de registrerte blir nektet å søke på en stilling, de mottar ikke bistand, det innkalles andre myndigheter som kan påvirke de registrertes liv betydelig – eks. Barnevernet	
Innebærer behandlingen systematisk overvåkning, for eksempel ved bruk av Internett (online atferdssporing)?	

Involverer den behandling av særlige kategorier av personopplysninger?	
Dreier det seg om en behandling av personopplysninger i stor skala? F.eks. enten fordi den omfatter et stort omfang registrerte, en stor mengde data, gir dybdeinnsikt i de registrertes liv/vaner/preferanser osv.	
Vil to eller flere datasett sammenstilles? F.eks. at personopplysninger fra ulike systemer sammenstilles.	
Omfatter behandlingen av personopplysninger registrerte med et særlig beskyttelsesbehov? F.eks. barn, eller personer med særbehov/funksjonshemning osv.	
Tar behandlingen i bruk ny teknologi som kan anses som inngripende eller brukes eksisterende/ny teknologi i nye sammenhenger? F.eks. IoT-relatert teknologi, bruk av biometrisk data for identifisering, teknologi som tradisjonelt ikke brukes til undervisning, app'er, ML eller AI-støttet psykometri i profilering/undersøkelser osv.	
Vil konteksten for behandlingen begrense mulighetene de registrerte har til å utøve sine rettigheter? F.eks. fordi de ikke får mulighet til å påvirke/unngå behandlingen, har begrenset informasjon eller innsyn, får ikke slette opplysninger, får ikke stoppe at de deles, osv.	

Dersom behandlingen av personopplysninger krever at det gjennomføres en DPIA, trenger du ikke fylle ut mer i internkontrollskjemaet. ***Du må i stedet gjennomføre en DPIA.***

NB! DPIA erstatter ikke risikovurderingen din. Du må altså fortsatt gjennomføre en risikovurdering. *Grunnen til dette er at risikovurderingen har som formål å fastsette hva som er tilfredsstillende nivå på organisatoriske og tekniske sikkerhetstiltak for en behandling av personopplysninger, mens ved risikovurderingen i en DPIA skal vi vurdere om behandlingen av personopplysninger kan gjennomføres, og vurderingen skal gjøres ut fra den registrertes perspektiv.*

Alternativt*: Beskriv i korte trekk hvorfor du mener at behandlingen ikke krever at det gjennomføres en DPIA.*

Beskriv her:

1.3. Oversikt over personopplysninger som behandles og hva brukes personopplysningene til

Angi kategorier av registrerte (eks. ansatte, fagforeningsmedlemmer, elever, studenter, barnehagebarn, foreldre osv.):

I tabellen nedenfor skal du angi hvilke personopplysninger som behandles og hvilke som ev. er særlige kategorier av personopplysninger, og beskrive din (ev. din databehandlers) behandling av personopplysningene. Behandling av personopplysninger kan f.eks. være innsamling, registrering, sammenstilling, lagring og utlevering av personopplysninger eller en kombinasjon av slike bruksmåter. NB: du skal ikke beskrive formålet (hvorfor) med hver enkelt behandling her, det skal du gjøre i punkt 1.4. ***Det du skal beskrive her, er hvordan du bruker personopplysningene.***

Personopplysninger som behandles	***Alminnelig eller særlig kategori av personopplysninger (se definisjon i punkt 1.4)***	***Hvordan bruker du personopplysningene (hvilke behandlinger, se hjelpetekst over)?*** **Det du fyller inn her må du også fylle inn i tabellen i punkt 1.4*	***Omfang (volum av personopplysninger i tall eller prosent)***
[Eks. navn]	[Alminnelige]	[registrering av bruker, innlogging i systemet, lagring, kommunikasjon med den registrerte, forskning]	[Brukere i systemet er 5000]
[Eks. helseopplysning]	[Særlig kategori]	[tilrettelegging av eksamen.]	[antall brukere i systemet: XX]

1.4. Det rettslige grunnlaget for behandlingen

Behandlingen må ha et rettslig grunnlag. Uten det har vi ikke lov til å utføre behandlingen. Omfatter behandlingen flere formål, må hvert formål ha et eget behandlingsgrunnlag.

Du skal angi hvilket rettslig grunnlag som foreligger for behandlingen av alminnelige personopplysninger (som er regulert i artikkel 6). Dersom behandlingen innebærer at du også behandler særlige kategorier av personopplysninger (som er regulert i artikkel 9), skal du angi det rettslige grunnlaget i artikkel 9 ***i tillegg****.*

De mest aktuelle rettslige grunnlagene i ***artikkel 6 nr. 1*** *(alminnelige personopplysninger) er:*

- *Bokstav a) samtykke fra den registrerte; for at samtykket skal være gyldig som rettslig grunnlag, må samtykket være frivillig, spesifikt, informert og en utvetydig viljesytring fra den registrerte, se artikkel 7. Samtykket må kunne dokumenteres. Hvis disse vilkårene ikke er oppfylt, kan samtykke som rettslig grunnlag ikke brukes. Du bør konferere med personvernombudet før samtykke benyttes. Husk å beskrive om vilkårene for samtykke er oppfylt i tabellen under, under «kommentar».*
- *Bokstav b) behandlingen er nødvendig for å oppfylle en avtale den registrerte er part i, eller for å gjennomføre tiltak på den registrertes anmodning før en avtaleinngåelse*
- *Bokstav c) behandlingen er nødvendig for å oppfylle en rettslig forpliktelse som påhviler den behandlingsansvarlige*
- *Bokstav e) behandlingen er nødvendig for å utføre en oppgave i allmennhetens interesse eller utøve offentlig myndighet som den behandlingsansvarlige er pålagt*
- *Bokstav f) behandlingen er nødvendig for formål knyttet til de berettigede interessene som forfølges av den behandlingsansvarlige eller en tredjepart, med mindre den registrertes interesser eller grunnleggende rettigheter og friheter går foran og krever vern av personopplysninger, særlig dersom den registrerte er et barn. Alle behandlinger som begrunnes i bokstav f) krever at vi gjennomfører en vurdering av våre interesser mot de registrertes egne interesser, for å avgjøre om våre interesser forsvarlig kan gå foran de registrertes interesser.*
  NB: bokstav f kan ikke brukes av offentlige myndigheter som ledd i utførelsen av deres oppgaver. Et eksempel der offentlige myndigheter kan bruke bokstav f er når det behandles personopplysninger ifm. innlogging i et system. Den berettigede interessen er å ha sikkerhet i løsningen, og det er ikke noe den offentlige myndigheten gjør som ledd i utførelsen av sine offentlige oppgaver.

Både bokstav c og bokstav e i artikkel 6 krever et nasjonalt rettsgrunnlag i tillegg (i hovedsak lov- eller forskriftsbestemmelse, men unntaksvis kan også vedtak og oppdragsbrev være supplerende nasjonalt rettsgrunnlag). ***Husk å angi det nasjonale rettsgrunnlaget for behandlingen din i tabellen nedenfor.***

*De (mest) aktuelle rettslige grunnlagene for behandling av særlige kategorier av personopplysninger i **artikkel 9 nr. 2** er:*

- *Bokstav a) samtykke fra den registrerte*
  Se kommentar til artikkel 6 nr.1 bokstav a)

- *Bokstav b) Behandlingen er nødvendig for at den behandlingsansvarlige eller den registrerte skal kunne oppfylle sine forpliktelser og utøve sine særlige rettigheter på områdene arbeidsrett, trygderett og sosialrett.*

- *Bokstav g) behandlingen er nødvendig av hensyn til viktige allmenne interesser*

- *Bokstav j) Behandlingen er nødvendig for arkivformål i allmennhetens interesse, for formål knyttet til vitenskapelig eller historisk forskning eller for statistiske formål.*

*Bokstav b), g) og j) i artikkel 9 krever supplerende nasjonalt rettsgrunnlag i tillegg. **Husk å angi hva som er det nasjonale rettsgrunnlaget for behandlingen i beskrivelsen nedenfor.***

Fyll ut:

Behandling *Her setter du inn behandlingene du har listet opp under «Hvordan bruker du personopplysningene» i punkt 1.3.	***Formål***	***Rettslig grunnlag (se aktuelle rettslige grunnlag i teksten over), og ev. supplerende nasjonalt rettsgrunnlag***	***Kommentar***
[Tilrettelegging av eksamen]	[Å gi elever som har krav på det, en tilrettelegging av eksamen]	[artikkel 6 nr. 1 bokstav c og e, artikkel 9 nr. 2 bokstav g, med forskrift til opplæringsloven § 3-29 som supplerende rettsgrunnlag]	

1.5. Innhenting av personopplysninger

Her skal du angi hvor personopplysningene innhentes fra. Hentes personopplysningene fra den registrerte selv, fra andre etater, andre behandlingsansvarlige (eks. Skoler, statsforvalteren), fra andre systemer, eller produseres personopplysningene i din virksomhet, ev. innhentes opplysningene fra andre?

Beskriv her:

1.6. Ekstern utlevering av personopplysninger

Utleverer vi personopplysningene til noen (som ikke er vår databehandler)? Angi hjemmel for utlevering av personopplysningene (forutsatt at dette er forskjellig fra det rettslige grunnlaget angitt i punkt 1.4). Angi videre hvem personopplysningene skal og kan utleveres til. Utleveres personopplysningene til den registrerte, til andre etater eller andre eksterne systemer?

Beskriv her:

1.7. Intern deling av personopplysninger

Her skal du angi hvilke andre systemer i virksomheten din personopplysningene deles med.

Beskriv her:

1.8. Informasjon til den registrerte

Her skal du oppgi hvordan den registrerte informeres om behandlingen av personopplysningene, jf. Art. 13 og/eller 14. Du skal beskrive hvilken informasjon som er gitt til den registrerte og hvordan informasjonen blir gitt. Angi også om den registrerte kan få fjerntilgang til egen informasjon, eks. ved å logge seg inn og se egen profil.

Beskriv her:

1.9. Hvordan kan den registrerte ivareta sine rettigheter?

Beskriv hvordan vi tilrettelegger for at den registrerte kan utøve sine rettigheter i systemet og/eller hvordan den registrerte kan be om innsyn, retting, supplering, sletting eller portabilitet av sine personopplysninger, trekke tilbake et samtykke, motsette seg en behandling eller be om begrensning av en behandling. Hvis vi anser at noen av disse rettighetene ikke gjelder her, redegjør for det og beskriv hvorfor.

Beskriv her:

1.10. Kvalitetskontroll av personopplysningene

Her skal du angi hvordan vi kontrollerer at personopplysningene er korrekte og oppdaterte, jf. Art. 5 nr. 1 d. Hvordan slettes eller rettes uriktige eller ufullstendige personopplysninger?

Beskriv her:

1.11. Personvern som standardinnstilling og innebygd personvern

Her skal du angi hvilke egnede tekniske og organisatoriske tiltak som er gjort for å sikre at det som standard kun blir behandlet personopplysninger som er nødvendige for hvert spesifikke formål, jf. Art. 25 (f.eks. pseudonymisering og dataminimering). Hvis behandlingen utføres av en databehandler på vegne av virksomheten din, angi om vi har stilt krav til innebygd personvern til systemet i databehandleravtalen eller andre avtaler.

Beskriv her:

1.12. Bevarings- og sletterutiner

Hensynet med dette punktet er å sikre at systemer som inneholder personopplysninger som er bevaringsverdig (dvs. informasjon av stor kulturell eller forskningsmessig verdi, eller som inneholder rettslig eller annen viktig dokumentasjon) blir bevart. Arkivet skal involveres i denne vurderingen på forhånd.

Videre skal det angis hvor lenge personopplysninger behandles/lagres og hvilke sletterutiner (dato, tidsrom, hendelse, automatisert/manuell sletting) som er etablert jf. Art. 5 nr. 1 e.

Dato for kontakt med arkivet, og konklusjon av om opplysningene er arkivpliktig eller ikke.	
Angi hvor lenge det er nødvendig å bevare opplysningene, og forklar bakgrunnen for oppbevaringsperioden.	
Foretas det automatisk eller manuell sletting?	
Hvor ofte (frekvens) slettes opplysningene?	
Hvordan kontrolleres det at sletting er korrekt utført?	

Dato for sendt kassasjonssøknad	

2. Informasjonssikkerhet

2.1. Sikkerhetstiltak og risikovurderinger

Dato for (ev. siste) risiko- og sårbarhetsvurdering (ROS-vurdering)	
Beskriv hvordan opplysningene er tilstrekkelig sikret (nevn de viktigste tiltakene) mot uautorisert eller ulovlig behandling, utilsiktet tap, ødeleggelse eller skade jf. art. 32. Oppdater beskrivelsen av tiltakene ved nye ROS-vurderinger eller gjennomførte tiltak.	
Angi det vi anser å være de høyeste risikoene for de registrerte, inkludert om vi mener den registrerte kan bli overrasket over behandlingen, deler av behandlingen eller resultat av behandlingen. Angi om det ble søkt veiledning fra personvernombudet og om det er planlagt ytterligere tiltak for å minimere risiko.	
Er systemet virksomhetskritisk? Dvs. et system som er kritisk/essensielt for at virksomheten din får utført sine oppgaver/leveranser.	

3.Databehandler for virksomheten

Her skal du opplyse om eventuelle andre enn virksomheten din som skal behandle personopplysningene. Du skal oppgi (per databehandler):

- *navnet på databehandleren,*
- *saksnummer for databehandleravtalen i arkivsystemet,*
- *hva databehandleren har ansvar for,*
- *hvor alle behandlingene fysisk skal gjennomføres,*
- *om det skjer behandlinger (f.eks. kundestøtte, utvikling eller lagring) i tredjeland (land utenfor EU/EØS) – enten av databehandler selv eller underdatabehandlere,*
- *hvilket land og hvilket overføringsgrunnlag som foreligger dersom det skjer behandling i tredjeland. Overføringsgrunnlag kan f.eks. være EU-standardbestemmelser/SCC, Bindende Virksomhetsregler (BCC), EU-kommisjons vedtak om tilstrekkelig beskyttelsesnivået, eller godkjent sertifiseringsmekanisme*
- *om det ble gjennomført en risiko- eller personvernkonsekvensvurdering før inngåelse av databehandleravtalen, dersom det skjer behandling i tredjeland.*

Fyll inn: