

BILAG 8.2 - TILSYN OG EGENKONTROL

UDFØRT DEN [INDSÆT: DATO]

[INDSÆT: NAVN] ("Dataansvarlig") har foretaget en risikovurdering af behandlingen af personoplysninger hos Databehandleren. Risikovurderingen viser, at der er en [høj/mellem/lav] risiko ved behandlingen af personoplysningerne.

Det følgende skema er udarbejdet til brug for den Dataansvarliges tilsyn med Databehandlerens behandling af personoplysninger og tager udgangspunkt i den Dataansvarliges risikovurdering. Den Dataansvarlige gennemfører på nuværende tidspunkt tilsyn med Databehandler [halvårligt / årligt / hvert andet år].

1. DATABEHANDLER		
Databehandler	Navn: [indsæt] Adresse: [indsæt] CVR-nr.: [indsæt] Telefon: [indsæt] E-mail: [indsæt] Internt ansvarlig: [indsæt]	
2. YDELSEN/PRODUKTET SAMT LEVERINGSPERIODEN		
Ydelse/produkt	Navn: [Indsæt navnet på produktet eller ydelsen, som leveres som led i hovedaftalen fx IT-Konsulent] Beskrivelse: [Indsæt kort beskrivelse af ydelsen/produktets funktion fx IT-Support]	Leveret i perioden: [indsæt dato fra-til] ("Leveringsperioden")
3. UDFØRELSEN		
Beskrivelse	Alternativ 1: Databehandleren har gennemført en egenkontrol, som udgør et tilsyn, og bekræfter, at de kontrolmål, der knytter sig til den gennemførte kontrol er hensigtsmæssige udformede og har fungeret effektivt i hele Leveringsperioden. eller Alternativ 2: Den Dataansvarlige har udført et skriftligt/fysisk tilsyn, ved at gennemgå og få redegjort for overholdelsen af gældende regler ved hjælp af nedenstående tilsynsspørgsmål. Databehandleren oplyser, at der i Leveringsperioden har været etableret og opretholdt passende tekniske og organisatoriske foranstaltninger med henblik på at opfylde aftalen med den Dataansvarlige samt at Databehandleren har overholdt god databehandlerskik og gældende persondataregler.	

4. SYSTEMBESKRIVELSE			
4.1	Navn:	Underafsnit:	Bemærkninger:
	[Navnet på systemet/ydelsen fx IT-konsulent]	[Beskriv det overordnede kontrolmiljø]	[Eventuelle bemærkninger]
		[Beskriv risikovurdering – høj/medium/lav]	[Eventuelle bemærkninger]
		[Beskriv kontrolaktiviteter]	[Eventuelle bemærkninger]

5. TILSYN

5.1 GRUNDLÆGGENDE PRINCIPPER				
Målsætning (Forordningens artikel 5) Der er implementeret procedurer og kontroller, der sikrer, at indsamling, behandling og opbevaring af personoplysninger sker i overensstemmelse med principperne for behandling af personoplysninger.				
	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er skriftlige og praktiske procedurer, der sikrer de grundlæggende principper for behandling: - Lovlighed, rimelighed og gennemsigtighed af behandlingen - Formålsbegrænsning - Dataminimering - Personoplysningernes rigtighed - Opbevaringsbegrænsning - Integritet og fortrolighed			
B	Der er en løbende kontrol af, at principperne for behandling af personoplysninger overholdes.			
C	Procedurerne opdateres løbende og efter behov.			

5.2 HJEMMELSLISTER

Målsætning (Forordningens artikel 6)

Det retlige grundlag for behandlingen af personoplysninger er dokumenteret, fx i form af hjemmelslister, og opdateres løbende.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er hjemmelslister, hvor de enkelte data-behandlinger og deres retlige grundlag fremgår.			
B	Hjemmelslisterne opdateres løbende og i det omfang, der indføres nye behandlingssystemer eller lignende.			
C	Der sker ikke behandling af persondata uden et retligt grundlag.			
D	Det kontrolleres løbende, om der sker behandling uden retligt grundlag.			

5.3 PERSONFØLSOMME OPLYSNINGER

Målsætning (Forordningens artikel 9 og 10)

Personfølsomme oplysninger behandles kun efter klar instruks og med de fornødne garantier for behandlingens sikkerhed.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er en skriftlig politik, der fastslår, at behandling af personfølsomme oplysninger kun må ske efter klar instruks fra den Data-ansvarlige.			
B	Der sker ikke behandling af personfølsomme oplysninger uden en klar instruks herom.			
C	Der foretages løbende kontrol af, om der er sket behandling af personfølsomme oplysninger uden forudgående instruks.			

5.4 OPLYSNINGSPLIGT

Målsætning (Forordningens artikel 13 og 14)

Det er ved skriftlige procedurer sikret, at den registrerede modtager tilstrækkelig information om indsamlingen af personoplysninger, den registreredes rettigheder, klagemuligheder mv.

(Kun relevant, hvis Databehandler er pålagt at give oplysninger på vegne af Dataansvarlig eller blive selvstændig dataansvarlig)

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er en skriftlig politik, der sikrer, at den registrerede modtager oplysning om: - Kontaktoplysninger på den dataansvarlige og en eventuel DPO - Formålet med og hjemmelsgrundlaget for behandlingen - Eventuelle modtagere eller kategorier af modtagere - Eventuel overførsel til tredjelande eller internationale organisationer.			
B	Der er udarbejdet og implementeret en politik, der sikrer, at den registrerede modtager yderligere oplysninger om: - Perioden hvori personoplysningerne opbevares - Retten til indsigt, berigtigelse, sletning og begrænsning i behandlingen - Tilbagekaldelse af eventuelt samtykke - Klagemuligheder - Eventuel profilering			
C	Hvis oplysningerne ikke er indhentet hos den registrerede selv, er der endvidere en politik om at give den registrerede oplysninger om: - Kategorien af personoplysninger, der behandles - Hvorfra oplysningerne er indhentet			
D	Der er en politik for at give oplysningerne til de registrerede indenfor en rimelig frist.			
E	Politikkerne efterleves og opdateres løbende efter behov.			
F	Der foretages løbende kontrol af, at de registrerede har modtaget de oplysninger, som de har krav på, herunder oplysning om deres rettigheder.			

5.5 INDSIGTSANMODNINGER

Målsætning (Forordningens artikel 12 og 15)

Det er muligt at udlevere oplysninger om behandlingen af den registreredes personoplysninger i skriftligt format på en gennemsigtig og letforståelig måde. Der er en skriftlig politik, der sikrer, at en anmodning fra den registrerede besvares både fyldestgørende og rettidigt, og at eventuelle afslag begrundes enten direkte til den registrerede eller til den Dataansvarlige.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der kan på anmodning gives indsigt i: - Formålet med behandlingen - Kategorien af personoplysninger der behandles - Eventuelle modtagere af oplysningerne, herunder tredjelande eller internationale organisationer - Opbevaringsperioden - Retten til berigtigelse, sletning eller begrænsning i behandlingen - Klagemuligheder - Hvorfra oplysningerne er indhentet - Eventuel profilering			
B	Der er en skriftlig politik for besvarelse af anmodninger.			
C	Politikken sikrer, at anmodninger besvares skriftligt, fyldestgørende og indenfor gældende frister, samt at eventuelle afslag begrundes.			
D	Databehandleren har en politik for at videregive oplysninger i en letforståelig og gennemsigtig form.			
E	Er der modtaget anmodninger siden sidste tilsyn og antal.			
F	(Kun relevant, hvis der er modtaget anmodninger siden sidste tilsyn) Anmodningerne er behandlet korrekt.			
G	Databehandleren kontrollerer løbende, at anmodninger modtaget fra de registrerede besvares korrekt og rettidigt.			

5.6 BERIGTIGELSE, SLETNING OG BEGRÆNSNING AF OPLYSNINGER

Målsætning (Forordningens artikel 16, 17, 18 og 19)

Der er nedskrevet retningslinjer for berigtigelse, sletning og begrænsning af behandlingen af personoplysninger, herunder at det sker uden unødigt ophold. Der er endvidere nedskrevet retningslinjer for at besvare og videregive anmodninger herom til eventuelle modtagere af oplysningerne.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er en skriftlig politik, der fastlægger en procedure for at berigtige ukorrekte eller ufuldstændige oplysninger uden unødigt ophold.			
B	Der er en skriftlig politik, der sikrer, at der sker sletning af personoplysninger uden unødigt ophold i tilfælde af: - Behandlingen ikke længere er nødvendig for at opfylde behandlingens formål - Tilbagekaldelse af et samtykke - En berettiget indsigelse - Der er sket ulovlig behandling - En retlig forpligtelse			
C	Der er en skriftlig politik, der sikrer, at behandlingen af personoplysninger begrænses, hvis den registrerede har en berettiget indsigelse.			
D	Der er tekniske foranstaltninger, fx i IT-systemerne, som muliggør berigtigelse, sletning og begrænsning af oplysningerne.			
E	Der er en skriftlig politik for at videregive anmodninger om berigtigelse, sletning og begrænsning af behandlingen af personoplysninger til tredjeparter, der har modtaget oplysninger om den registrerede.			
F	Alle politikker efterleves.			
G	Alle politikker holdes løbende opdateret efter behov.			
H	Det kontrolleres løbende, at berigtigelse, sletning og begrænsning sker uden unødige ophold i overensstemmelse med de gældende politikker.			

5.7 DATABESKYTTELSE

Målsætning (Forordningens artikel 24 og 25)

Der er sikret et tilstrækkeligt teknisk og organisatorisk beskyttelsesniveau såvel fysisk omkring IT som i interne systemer gennem design og default.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er skriftlige politikker, der sikrer databeskyttelse gennem design og default.			
B	Der er skriftlige politikker, der sikrer databeskyttelse i hverdagen, som omfatter alle medarbejdere, der kommer i kontakt med persondata.			
C	Der er skriftlige politikker for Databehandlernes IT-sikkerhed og IT generelt.			
D	Ved udvikling af programmer eller indførsel af nye behandlingssystemer, sikres databeskyttelse gennem designet af programmet/behandlingssystemet.			
E	Standardindstillingerne i de fysiske og elektroniske systemer er sat op på en sådan måde, at personoplysninger ikke stilles til rådighed for et ubegrænset antal personer.			
F	Der er etableret tekniske og organisatoriske sikringsforanstaltninger, som svarer til den Dataansvarliges krav til tekniske og organisatoriske sikringsforanstaltninger, som for eksempel pseudonymisering, dataminimering, sikkerhed af fysiske lokaliteter, strøm, osv.			
G	De tekniske og organisatoriske tiltag opdateres løbende i de skriftlige politikker.			
H	Det kontrolleres løbende, at politikkerne efterleves, og at standardindstillingerne er sat op som påkrævet.			

5.8 DATABEHANDLER

Målsætning (Forordningens artikel 28 og 29)

Der er indgået databehandleraftaler, der opfylder kravene i Forordningen og databeskyttelsesloven. Der er implementeret procedurer for at sikre, at aftalevilkårene overholdes, og at der udelukkende handles efter instruks.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er en gældende databehandleraftale, der som minimum regulerer: - Udpegning af roller - Lovvalg - Forpligtelser og rettigheder - Sikkerhedsforanstaltninger - Ansvarsfordeling - Underdatabehandlere - Overførsel af data til tredjelande			
B	Eventuelle senere opdateringer til databehandleraftalen er skriftligt dokumenterede.			
C	Der sker ikke behandling uden for den Dataansvarliges instruks.			
D	Alle medarbejdere er instrueret og undervist i korrekt behandling af personoplysninger.			
E	Det kontrolleres løbende, at der ikke handles uden for instruks.			

5.9 UNDERDATABEHANDLER

Målsætning:

Der er indgået underdatabehandlertalet, der opfylder kravene i Forordningen og databeskyttelsesloven. Der er implementeret procedurer for at sikre, at aftalevilkårene overholdes, og at der udelukkende handles efter instruks.

(Kun relevant, hvis der bruges underdatabehandlere)

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er skriftlige politikker, der regulerer brugen af underdatabehandlere.			
B	Der er indgået databehandlertalet med alle underdatabehandlere, som indeholder de samme instrukser og krav, som Dataansvarlig har pålagt Databehandleren.			
C	Alle underdatabehandlere er godkendt af Dataansvarlig eller generelt godkendt og oplyst om.			
D	Der er procedurer, der sikrer, at den Dataansvarlige underrettes om eventuelle udskiftninger af underdatabehandlere, således at Dataansvarlig har mulighed for at gøre indsigelse.			
E	Der er gennemført tilsyn med alle underdatabehandlere, som aftalt i respektive databehandlertalet.			
F	Tilsynene er gennemført ved [INDSÆT: Beskrivelse]			
G	Tilsynene er dokumenteret, og den Dataansvarlige er underrettet herom.			
H	Det kontrolleres og dokumenteres løbende, at alle underdatabehandlere opfylder den Dataansvarliges instrukser og krav til behandling af persondata.			

5.10 DATAOVERFØRSLER TIL TREDJELANDE OG INTERNATIONALE ORGANISATIONER

Målsætning (Forordningens artikel 44, 45, 46 og 49)

I det omfang der foretages dataoverførsler til tredjelande og internationale organisationer, som ikke er godkendte af Kommissionen, er der sikret og dokumenteret et hjemmelsgrundlag for overførslerne.

(Kun relevant, hvis Databehandleren laver dataoverførsler til tredjelande eller internationale organisationer)

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Der er skriftlige politikker, der regulerer dataoverførsler til tredjelande og internationale organisationer.			
B	Hvis et tredjeland eller en international organisation ikke er godkendt af Kommissionen, overføres der kun data, hvis tredjelandet eller organisationen har givet de fornødne garantier for databeskyttelsen, og den registrerede har adgang til at håndhæve sine rettigheder - eller hvis der er sikret og dokumenteret et andet hjemmelsgrundlag for overførslen i overensstemmelse med Forordningens krav.			
C	Alle overførsler der foretages, er beskrevet, og overførslerne er godkendt af den Dataansvarlige.			
D	Der er implementeret retningslinjer for løbende at kontrollere og dokumentere hjemmelsgrundlaget for overførslerne.			

5.11 DATABRUD

Målsætning (Forordningens artikel 33 og 34)

Databehandleren har nedskrevne retningslinjer og procedurer for at hjælpe Dataansvarlig med rettidig og fyldestgørende anmeldelse til Datatilsynet ved eventuelle brud på persondatasikkerheden, herunder underretning af de registrerede, hvis det er pålagt Databehandleren.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Databehandleren har en skriftlig politik for håndtering af brud på persondatasikkerheden, der blandt andet sikrer, at der sker registrering af alle databrud hos Databehandleren og dennes underdatabehandlere, samt at der sker underretning til den Dataansvarlige om bruddet uden unødigt ophold.			
B	Databehandleren sikrer, at dokumentation om eventuelle databrud som minimum indeholder en beskrivelse af databruddets faktiske omstændigheder, omfang og konsekvenser samt Databehandlerens afhjælpningsforanstaltninger.			
C	I det omfang, at Databehandleren er pålagt at underrette de berørte registrerede om databruddet, har Databehandleren sikret en procedure herfor samt dokumentation for underretningen.			

5.12 RISIKOVURDERING

Målsætning (Forordningens artikel 32)

Databehandleren har nedskrevet og implementeret politikker, der sikrer, at Databehandleren foretager risikovurderinger og konsekvensanalyser af sin behandling af personoplysninger, som lever op til Persondataforordningens og Databeskyttelseslovens krav.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Databehandleren har retningslinjer for, at der løbende efter behov – og minimum én gang om året – foretages selvstændige risikovurderinger af databehandlingen hos Databehandler. Det Dataansvarlige holdes orienteret om de gennemførte risikovurderinger.			
B	Databehandleren etablerer på baggrund af sine risikovurderinger passende tekniske og organisatoriske foranstaltninger, der imødekommer det højeste sikkerhedsniveau i overensstemmelse med databehandleraftalen.			
C	Databehandlerens ledelse bekræfter, at der er gennemført de påkrævede risikovurderinger samt foretaget de nødvendige tiltag for at opretholde databeskyttelsesniveauet hos Databehandler og eventuelle underdatabehandlere.			

5.13 KONSEKVENSANALYSE OG HØRING

Målsætning (Forordningens artikel 35 og 36)

Databehandleren har nedskrevet og implementeret politikker, der sikrer, at Databehandleren foretager risikovurderinger og konsekvensanalyser af sin behandling af personoplysninger, som lever op til Persondataforordningens og -lovens krav.

	Beskrivelse	Behandlingen lever op til kontrolmålene		Bemærkninger
		Ja	Nej	
A	Databehandleren har politikker og procedurer, der sikrer, at der ved indførsel af nye typer behandlinger eller systemer hos Databehandleren - som medfører en høj risiko for de registreredes rettigheder – foretages en konsekvensanalyse, og at Dataansvarlig orienteres om resultatet af analysen.			
B	I tilfælde af, at konsekvensanalysen viser en høj risiko ved behandlingen, har Databehandleren en proces, der sikrer, at der sker forudgående høring om behandlingen hos Datatilsynet.			

5.14 ØVRIGE FORHOLD

Målsætning:

Databehandleren overholder samtlige tekniske og organisatoriske sikkerhedstiltag, der er særskilt pålagt Databehandleren i henhold til databehandleraftalen.

	Beskrivelse	Behandlingen lever op til kontrolmålene [sæt kryds]		Bemærkninger
		Ja	Nej	
A	[Indsæt eventuelle særlige krav pålagt i databehandleraftalen]			[Eventuelle bemærkninger]
B	[Indsæt eventuelle særlige krav pålagt i databehandleraftalen]			[Eventuelle bemærkninger]
C	[Indsæt eventuelle særlige krav pålagt i databehandleraftalen]			[Eventuelle bemærkninger]
D	[Indsæt eventuelle særlige krav pålagt i databehandleraftalen]			[Eventuelle bemærkninger]
E	[Indsæt eventuelle særlige krav pålagt i databehandleraftalen]			[Eventuelle bemærkninger]