Overblik i forbindelse med den nye Persondataforordning

– Skema til dokumentation

DANSK UNGDOMS FÆLLESRÅD

Navn og adresse på organisationen/foreningen:		**Ansvarlig for databeskyttelse i foreningen:**	
Spørgsmål		**Eksempler**	**Risikoanalyse**
1. Hvilke persondata behandler vi?	• Typer af oplysninger - Alm. eller følsomme. • Oplysningernes ophav • Hvem deles oplysningerne med internt og eksternt (herunder hvem har adgang til de forskellige oplysninger)		Personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde der er uforenelig med disse formål Har vi aftaler med evt. eksterne?
2. På hvilket retligt grundlag behandler vi personoplysninger?	• Hvilke oplysninger behandler vi? • Hvilken retligt grundlag hviler det på?	(eks. Almindelige oplysninger: Navn, adresse, mail, telefon. Følsomme oplysninger: Børneattester Helbredsoplysninger: Allergener, psykisk sygdom Oplysninger om sociale forhold: Skilsmisseforhold, alkohol. Særlige oplysninger: CPR-numre Lovgrundlag kunne eks. Være: Persondataloven, folkeoplysningsloven, kulturministeriets og/eller kirkeministeriets bekendtgørelser, børneattestbekendtgørelsen eller kriminalregisteret.	Vi skal altid have retligt grundlag for behandling • Samtykke • Interesseafvejningsreglen • Kontrakter • Direkte lovhjemmel
3. Hvordan indhenter vi samtykke?	• Gennemgang af procedurer. Hvordan indhenter, opbevarer og dokumenterer vi samtykke.	(eks. Ved indmeldelse i foreningen modtager den registrerede vores informationsfolder, hvori vi	Samtykket skal være • Frivilligt • Specifikt • Informeret

		oplyser følgende: XXX. Herefter fremsender den registrerede selv sine oplysninger til landsorganisationen/indtaster dem via den krypterede hjemmeside og giver på denne måde sit informerede samtykke til behandlingen af oplysningerne. Ved indhentning af børneattest får den registrerede følgende information: XXX, og samtykket dokumenteres via accepten af indhentningen via NemID.	• Utvetydigt Indgives der flere samtykker samtidigt, eks. ved indmeldelse, skal de enkelte samtykker og hvad de indebærer klart kunne skelnes fra hinanden. Den registrerede skal til enhver tid kunne trække sit samtykke tilbage.
4. Behandler vi personoplysninger om børn (OBS børn under 15 år)		Eks. når en person meldes ind, beder vi om alder. Er personen under 16 år, er det forældrene der skal skrive under på/foretage indmeldelsen. Børneattester indhentes på personer fra 15 år og opefter, da det er den kriminelle lavalder i Danmark.	En vurdering af modenhed – Datatilsynets praksis peger i retning af 15 år.
5. Hvad er baggrunden for at behandle disse persondata **Hvor lang tid behandler vi personoplysningerne?**	• Hvorfor indhenter vi oplysningerne • Er de reelt nødvendige • Hvor længe gemmer vi dem		Det skal sikres, at I kun behandles personoplysninger, som er tilstrækkelige, relevante og begrænset til hvad der er nødvendigt i forhold til formålet. Det betyder også, at man skal vurdere, om man kan opnå

			formålet ved en mindre indgribende behandling.
6. Hvilken information giver vi til den registrerede?	• Gennemgang af information	(eks. Når personer melder sig ind i foreningen, får de følgende information: XXX Når vi indhenter børneattest, giver vi følgende information: XXX)	Der skal gives oplysninger om den dataansvarliges kontaktinformation, formålet med behandlingen, lovligheden af behandlingen (inkl. lagring), muligheden for at klage til datatilsynet.
7. Hvordan opfylder vi de registreredes rettigheder?	Gennemgang af procedurer, som måske skal bevirke en opdatering af information, jf. spørgsmål 3.	(Eks. vores information ved indmeldelse er lige nu)	Får den registrerede oplysninger om følgende (nye regler): • Retten til at modtage oplysning om en behandling af sine personoplysninger (oplysningspligt) • Retten til at indsigt i sine personoplysninger • Retten til at få urigtige personoplysninger berigtiget • Retten til at få sine personoplysninger slettet • Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring
8. Behandler vi persondata fysisk, hvis ja hvor?	• Hvilke oplysninger • Hvordan og hvor opbevarer vi dem		Der må ikke være adgang for uvedkommende til oplysningerne. Se på låse og andre sikkerhedsforanstaltninger. Det betyder også, at man eks. ikke må have persondata frit

			fremme såsom medlemslister eller lign.
9. I hvilke IT-systemer behandler vi persondata? **Har vi aftaler med dem?**	• Medlemssystemer • Sociale medier • Mail • Delingsværktøjer • Billedredigeringsprogrammer • Hjemmeside • Etc.?		Krav om skriftlig kontrakt om sikkerhed med databehandler (databehandleraftale) Man må ikke overføre oplysninger til tredjelande – tredjelande er lande uden for EU. Man må dermed ikke bruge programmer hvis server står uden for EU, eks. Dropbox og Google drive. Nogle programmer giver dig mulighed for at vælge en EU server mod betaling, eks. One drive. Visse sociale medier mv. laver ikke databehandleraftaler, herunder Facebook. Læg derfor ikke persondata på disse medier, medmindre I har samtykke til eks. at tage og dele billeder fra arrangementer og lign.
10. Hvilken IT-sikkerhed har vi?	• Hvordan er vores server beskyttet? • Passwords på computere, tlf., wi-fi? • Kan personer logge på systemet når de ikke er i huset? – Regler for dette? • Er printere eller lign. tilkoblet internettet?		Den dataansvarlige bør fastlægge databeskyttelsespolitikker

	• Logger vi adgange til serveren eller forsøg herpå?		
11. Hvilken IT-politik og hvilke instrukser har vi?	• Hvad må du synkronisere til privat tlf.? • Hvor ofte skal du skifte kodeord? • Må man have computere med hjem? • Hvor må medlemmerne kontakte os? • Hvad må man ligge på de sociale medier?	Eks. bliver vi lige nu kontaktet gennem Facebook af medlemmerne vedr. persondata spørgsmål?	Den dataansvarlige bør fastlægge data procedurer og kontroller Instrukser om eks. at man kun modtager medlemshenvendelser gennem e-mail.
12. Vores procedurer for datasletning og retning		Eks. medlemsoplysninger opbevares indtil personen melder sig ud. Børneattester slettes straks efter gennemlæsning. Navn og kvittering for indhentning opbevares i XX år.)	Man må kun gemme persondata så længe det er nødvendigt. Hvor ofte sletter vi? Vær særlig opmærksom på eks. børneattester, helbredsoplysninger, ansøgninger, pas numre mv. Den registrerede har ret til at hans data bliver opdateret. Vigtigt at der er en procedure for datasletning og dataretning.
13. Hvad skal vi gøre, hvis der sker et brud på persondatasikkerheden?	Hvordan opdager, rapporterer og undersøger vi brud på persondatasikkerheden? F.eks. ved hackerangreb, eller glemte dokumenter offentligt. Hvordan vurderer vi, hvor alvorligt bruddet er?	(eks. Vi dokumenterer alle brud på følgende måde: Vores dataansvarlige person logger alle uregelmæssigheder i vores medlemssystem. Medlemssystemet meddeler	Man skal udarbejde en databeredskabsplan, hvor man har en procedure for hvad der skal ske. Vær opmærksom på, hvornår Datatilsynet skal informeres.

		selv, hvis der sker brud på sikkerheden. Vi opbevarer cpr-numre og navne samt børneattester på vores foreningscomputer, som er låst inde, og som er beskyttet af password, som kun XX og XX kender til. Hvis denne bliver stjålet melder vi det til politiet og informerer bestyrelsen. Vi anmelder altid bruddet til Datatilsynet indenfor 72 timer. Hvis der er akut risiko for fysiske personer rettigheder eller frihedsrettigheder anmelder vi bruddet straks muligt til Datatilsynet. De registrerede informeres altid straks muligt.	
14. Har vi tænkt databeskyttelse ind i vores IT-systemer?	Når vi f.eks. køber et nyt IT-system eller ændrer på vores nuværende, tænker vi databeskyttelse med ind. Det gælder f.eks. følgende: At vi ikke indsamler flere oplysninger end nødvendigt. At vi ikke opbevarer oplysningerne længere end nødvendigt. At vi ikke anvender oplysningerne til andre formål, end de formål, som	Hvad kan vores IT systemer?	

	oplysningerne oprindeligt blev indsamlet til.		
15. Har vi aktiviteter i flere lande?	Hvilken EU tilsynsmyndighed tilser hvilke aktiviteter?	(eks. Behandling i Danmark af oplysninger om XX – tilses af Datatilsynet. Behandling i Tyskland af oplysninger om XX – tilses af Det tyske tilsyn.	