Nye persondataregler

V. Henriette Tarris-Tramm & Mikkel Wrang

DANSK UNGDOMS FÆLLESRÅD

Program

- Velkomst og præsentation
- Oplæg
- Hvad gør vi her fra?
- Opsamling og afsluttende spørgsmål

Der bliver afholdt en pause undervejs med sandwich.

Velkomst og præsentation

Kort om reglerne

- *EU vedtog i 2016 nye regler for behandling af personoplysninger, General Data Protection Regulation (GDPR) – eller Persondataforordningen. Forordningen træder i kraft d. 25. maj 2018.*

- *Som supplement til Persondataforordningen, er der ved at blive gennemført en ny dansk persondatalov. Loven forventes tidligst færdig slut februar i år.*

- *Det grundlæggende nye i reglerne, som er relevant for jer som foreninger er fortegnelsespligten og kravet om fysiske og gennemarbejdede politikker og processer vedr. behandling af persondata.*

RO PÅ!!!

De nye regler giver god mening – det handler grundlæggende om at;

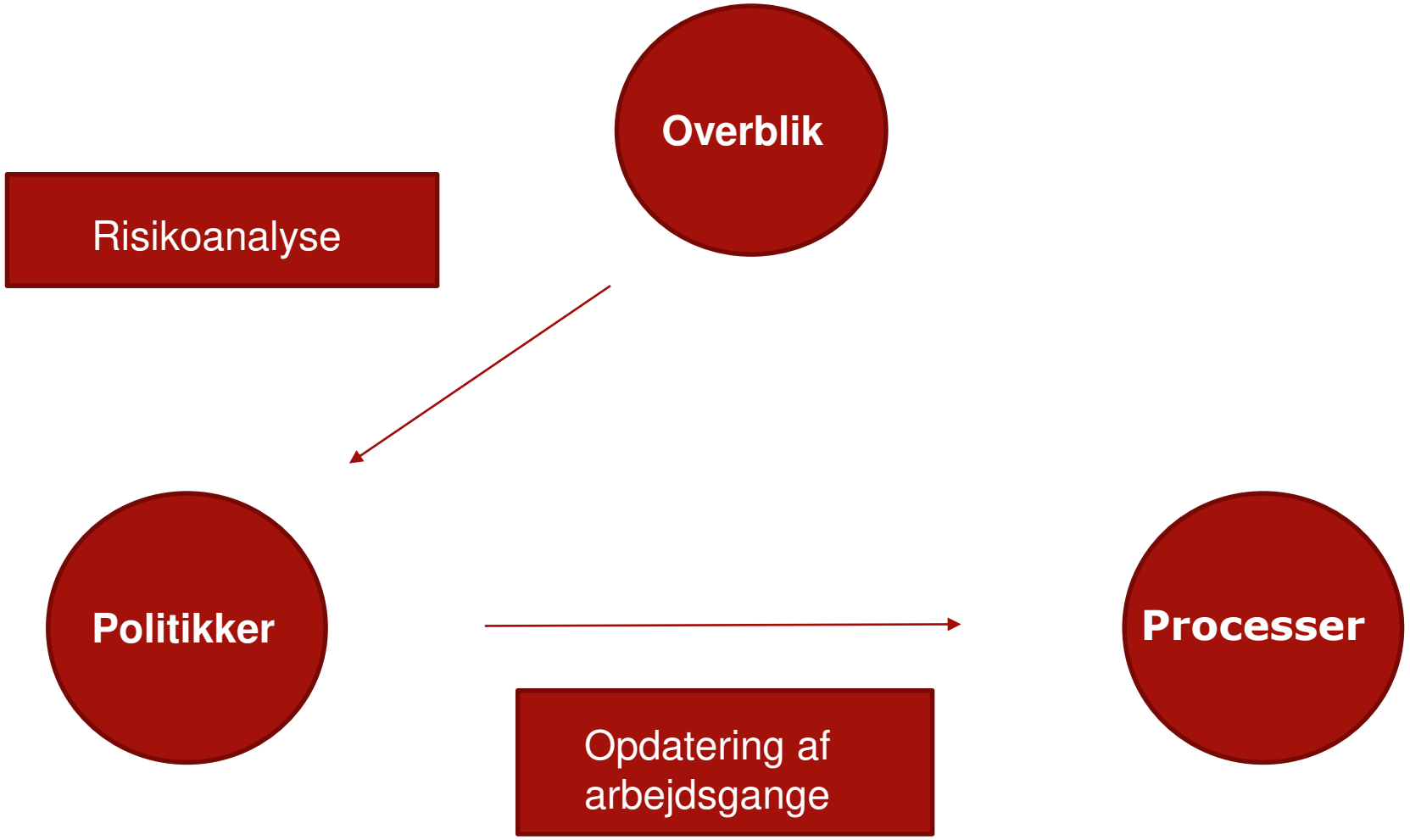
1) Skabe overblik over hvilke persondata I har, og hvordan behandler I dem

2) Hvordan passer overblikket med forordningens regler? Hvad skal I ændre for at leve op til forordningens regler?

3) Lave politikker for hvordan I og jeres lokalafdelinger behandler persondata

4) Opdatere jeres arbejdsgange og skrive dem ned

5) Udarbejde processer der sikrer i opretholder compliance


Overblik
Risikoanalyse
Politikker
Processer
Opdatering af arbejdsgange

Persondata

- **Hvad er persondata?**

Ved persondata forstås enhver form for information om en identificeret eller identificerbar fysisk person (den registrerede). Eks. fulde navn, adresse, CPR-nummer, tlf. nummer, helbredsforhold, politisk og religiøs overbevisning, etnisk oprindelse, seksuel orientering, billeder, fingeraftryk etc…

- **Kategorier af personoplysninger**

Skelner mellem to former for persondata – almindelige og følsomme persondata.

Alm. = Eks. Navn, mail, adresse, tlf-nummer, civil status, brugernavn, medlemsnummer, stilling, bankkonto, foto…

Følsomme = Eks. helbredsoplysninger, allergier, politisk/religiøs overbevisning, fagforenings-forhold, statsborgerskab, børneattester, CPR-nummer

Generelle principper

Reglerne er lavet med borgeren/registrerede i centrum, og principperne skal også forstås ud fra denne tankegang.

- **Rimelighed:** Behandlinger af persondata skal være rimelige.
- **Gennemsigtighed:** Det skal være muligt for registrerede at gennemskue hvad der registreres og behandles om vedkommende.
- **Saglighed:** Indsamling af personoplysninger skal ske i overensstemmelse med det udtrykkeligt fastslåede og legitime/saglige formål.
- **Formålsbestemthed:** Indsamlede oplysninger må ikke på et senere tidspunkt anvendes i uforenelighed med indsamlingsformålet.

Principperne skal gennemsyre hele arbejdet med persondata

Generelle principper (2)

- **Proportionalitet:** Grundlæggende skal der arbejdes ud fra et princip om dataminimering.
- **Datakvalitet:** De indsamlede data skal holdes opdateret og være korrekte.
- **Tidsbegrænsning:** Oplysningerne må kun opbevares så længe det er nødvendigt for at opfylde formålet. Ønsker man at bevare oplysningerne længere må de anonymiseres.
- **Sikkerhed:** De betroede data skal beskyttes med tekniske og organisatoriske foranstaltninger der medfører tilstrækkelig sikkerhed.

Principperne skal gennemsyre hele arbejdet med persondata

Persondata

- **Dataansvarlig**

  En forening der afgør til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger. Eks. er landsorganisationen og en lokalafdeling.

  1) Den dataansvarlige har ansvaret for at efterleve og dokumentere overholdelsen af persondataloven.

  2) Den dataansvarlige har pligt til anmelde til Datatilsynet hvis der har været eks. et hackerangreb på deres personoplysningerne

- **Databehandler**

  Et selskab som behandler personoplysninger på vegne af den dataansvarlige. Eks. leverandører af IT-systemer, et firma der sender medlemsblade ud.

Der skal laves en databehandleraftale mellem den dataansvarlige og databehandleren

Persondata
Eksempel dataansvarlige/behandlere

Medlemmet indsender oplysninger til KU.
KU = dataansvarlige.

Leverandør af medlemssystem/hjemmeside = Databehandler → Databehandleraftale

Firma der udsender medlemsblad = Databehandler → Databehandleraftale

Banken/mobilepay der modtager medlemmernes indbetaling af kontingent = Databehandler → Databehandleraftale

Behandling af Persondata

- Hvad er en behandling?

  Indsamling, registrering, systematisering, opbevaring, tilpasning/ændring, søgning, brug, videregivelse, sammenstilling/sammenkørsel, sletning.

Kort sagt alt man gør med persondata!

Sarah melder sig ind i Adventistspejderne via hjemmesiden. Sarahs persondata bliver indsamlet, registreret i medlemssystemet og opbevaret på en fysisk medlemsliste i den lokale trup.

Sarah bliver mor til tvillinger og har ikke længere tid til at være spejder. Hun melder sig derfor ud – Hun bliver slettet i medlemssystemet.

Adventistspejdernes nyhedsblad sendes fysisk ud til alle medlemmer – dette får de trykkeren til. Sarahs adresse videregives til trykkeriet.

Sarah flytter – hendes nye adresse bliver tilpasset i medlemssystemet

Retligt grundlag for behandling

- Samtykke
- Interesseafvejningsreglen
- Kontrakter
- Direkte hjemmel fra lovgivningen

Samtykke

- *Frivilligt, specifikt, informeret og utvetydig viljestilkendegivelse der bekræfter, at personoplysninger må behandles.*

- **Frivilligt:** Registrerede skal have et reelt og frit valg.
- **Specifikt:** Præcis angivelse af formål og konkret. Dette sikres ved at opdele samtykket. Samtykket skal klart skældes fra indmeldelsesformular og skal være letforståeligt og i lettilgængelig form og et sprog der matcher målgruppen.
- **Informeret:** Registrerede skal være klar over, hvad der gives samtykke til. Ingen formkrav. Registrerede skal oplysning om, at samtykket til enhver tid kan trækkes tilbage.
- **Utvetydig viljestilkendegivelse:** Det kan enten være i form af en underskrift eller en anden aktiv handling i form af et kryds i et felt.
- Alder – vurdering af modenheden (formentligt 15 år jf. Datatilsynets praksis)

Eksempler på indhold for samtykker

- Deling af billeder
- Videregivelse – intern el. ekstern
- Markedsføring
- Analyser
- Helbredsoplysning (allergier, handicap), såvel til registrering som opbevaring, men husk, at det skal være proportionalt
- Andre temaer (?)

Eksempel på samtykke i forbindelse med medlemskab

I forbindelse med mit medlemskab af Europæisk Ungdom giver jeg her med samtykke til følgende:

- □ At billeder af mig taget i forbindelse med aktiviteter i foreningen må offentliggøres på sociale medier o.lign.

- □ At helbredsoplysninger må registreres om mig i situationer hvor det er relevant, f.eks. Madallergier i forbindelse med arrangementer hvor der er bespisning, eller arrangementer med overnatning hvor det i øvrigt kan være relevant at kende til skavanker o. lign. Oplysninger slettes straks efter, de ikke er relevante længere.

OBS!

Husk på, at det er vigtigt at overveje og støtte sig til det rette grundlag – man må ikke bare ”opkræve” samtykker for alt.

Interesseafvejningsreglen

- Interesseafvejningsreglen kan anvendes som retligt grundlag for behandling af personoplysninger, så længe man kun behandler almindelige persondata, altså INGEN følsomme oplysninger

- Kort fortalt: Ud fra idéen om at der er forskel på kommerciel behandling af persondata og almennyttig (herunder foreningsmæssig) behandling af persondata, går man ud fra, at medlemmets (/den registreredes) interesser er i overensstemmelse med foreningens (/datansvarliges) interesser.

Kontrakter

- Det vil ikke så ofte være relevant for foreninger udover ved ansættelser eller honorarudbetaling, kørselsrefusioner osv.

- Dog er samtykke fortsat nødvendigt hvis man vil mere end at udbetale løn, registrere stamdata. Det kan f.eks. være brug af billede på hjemmeside, oprettelse af pårørendekontaktlister.

Direkte hjemmel fra lovgivningen

- Ved indberetning af medlemsliste til kommunen i forbindelse med folkeoplysningstilskud vil folkeoplysningsloven fungere som retligt grundlag for at lokalforeningen må udlevere sin medlemsliste til kommunen i forbindelse med udbetaling af folkeoplysningsstøtte.

Behandling af alm vs. følsomme personoplysninger

- Følsomme personoplysninger må som udgangspunkt ikke registreres og behandles. Der skal derfor foreligge et retligt grundlag for behandlingen og behandlingen skal i øvrigt være i overensstemmelse med de generelle principper.

- 'Jo mere' følsom en personoplysninger er, jo stærkere grundlaget være for behandlingen. Ligesom man også skal passe endnu mere på oplysningerne jo mere følsomme de er.

Oplysningspligt

- **Oplysningspligt (persondatameddelelse)**

Som dataansvarlige har I pligt til at give medlemmet (den registrerede) information om, at I indsamler persondata om vedkommende i en computer eller et register (husk også fysisk i mapper).

- **Indhold**

Den registrerede skal bl.a. have information om

- Den dataansvarliges navn, adresse og kontaktoplysninger.
- Formålet med registreringen
- Hvem der regelmæssigt sker videregivelse til
- Retten til at bede om indsigt
- Hvor længe oplysningerne gemmes

- **Tidsfrist**

Oplysningspligten skal opfyldes snarest muligt og i almindelighed inden for 10 dage.

- **Eksempel – Hvornår er der oplysningspligt**

Indmeldelse

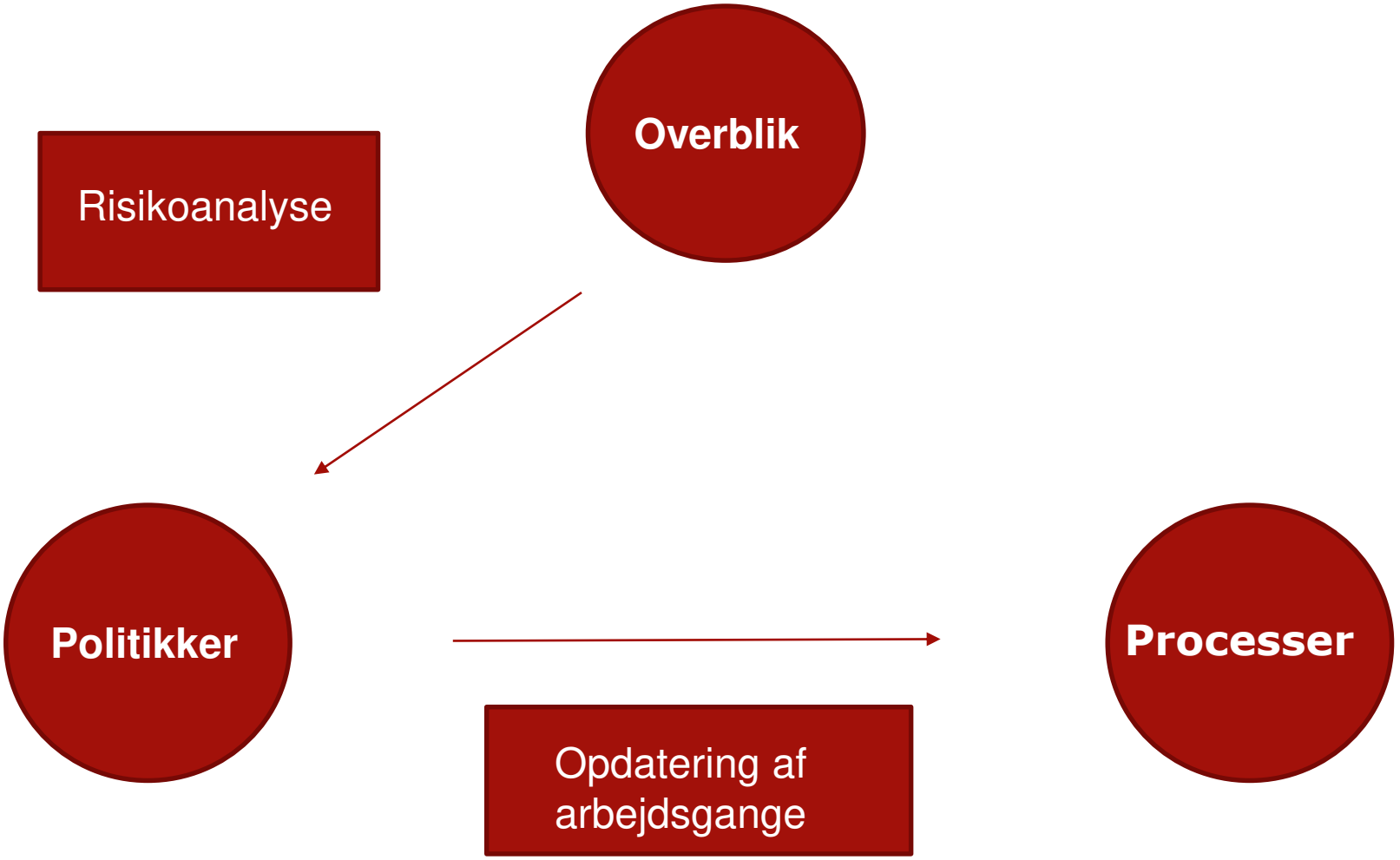
Indsendelse af jobansøgning

Udmeldelse / sletning

- Det klare udgangspunkt: Udmeldelse -> sletning
- Evt. grundlag for alligevel at beholde medlemsoplysninger i en periode, fx regler om at gemme regnskabsmateriale mv. i bogføringsloven.
- Begrunder man opbevaringen af et udmeldt medlems oplysninger med f.eks. medlemsrevision, så må man kun gemme de nødvendige oplysninger, såsom stamoplysninger og oplysninger om kontingentbetalinger, men f.eks. Ikke historik over hvilke arrangementer medlemmet har deltaget i eller lignende.
- Det vil også være muligt at beholde medlemsoplysningerne med henblik på fastholdelse i en begrænset periode. Dog aldrig mere end 12 mdr.

Husk altid princip om dataminimering.

Hvad nu herfra?


Risikoanalyse
Overblik
Politikker
Processer
Opdatering af arbejdsgange

Step 1) Overblik

- Skabe et her og nu billede af hvilke persondata I har, hvor de ligger i jeres system(er) og hvordan I behandler dem

- DUF har udarbejdet et skema, som kan være til hjælp. Se på de tre første kolonner.

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	Samtykket skal være • Frivilligt • Specifikt

Step 2) Risikoanalyse

- Når I har dannet jer et overblik over informationer – skal I i gang med en risikoanalyse.

- I risikoanalysen ser I på, om de oplysninger I har fundet frem til i step 1, lever op til reglerne i forordningen. DUF har i fjerde kolonne i skemaet, skrevet de ting I skal være opmærksomme på.

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	Samtykket skal være • Frivilligt • Specifikt

Step 2) Risikoanalyse

Et eksempel på hvordan I anvender risikoanalysen;

- I har i step 1 fundet frem til, at I ikke i dag indhenter samtykke til at dele billeder af medlemmerne fra arrangementer. I opdager nu, at det kræver et retligt grundlag at behandle persondata, herunder at dele billeder på de sociale medier (jf. spørgsmål 5 og 6 i skemaet). I må derfor vurdere hvordan I kan indhente samtykke fra medlemmerne fremadrettet, og hvad samtykket skal indeholde for at leve op til forordningen.

- I har i step 1 fundet frem til, at I anvender Dropbox til at dele eks. medlemslister mv. I opdager nu, at man ikke må ”give oplysninger videre” til et tredjeland, altså lande uden for EU (jf. spørgsmål 9 i skemaet). Har man en almindelig konto på Dropbox, opbevarer den ikke jeres data på servere indenfor EU. Hvis I skal leve op til forordningen, bliver I derfor nødt til at finde et andet program at dele filer i – og lave en politik om, at der ikke deles persondata i Dropbox (HUSK på hvor mange oplysninger der defineres som persondata!)

Step 3) Politikker og instrukser

- På baggrund af jeres overblik og risikoanalyse i step 1 og 2, skal I nu udarbejde de politikker og instrukser der skal til, for at I fremadrettet kan overholde forordningen.

Disse politikker kunne eks. omhandle:

- IT-sikkerhedspolitik
- Den frivillige lederes rolle og ansvar i forhold til persondata
- Børneattester
- Jobansøgninger
- Ansættelseskonktrakter
- Hvilke programmer må vi anvende til at dele filer i
- Hvor og hvordan gemmer vi vores persondata
- Hvornår sletter vi persondata
- Hvordan indhenter vi persondata

Frivillig lederrolle i persondata

- Udfordringen med at få de frivillige ledere til forstå, at de har et stort ansvar i forhold til at overholde persondatareglerne.
- Medlemslister kan ikke hænge i spejderhytten
- Medlemslisterne kan heller ikke sendes til hotmail-adresse, skal man måske have en e-mailadresse fra foreningen?
- Gå forrest i forhold til de unge medlemmer for, at få det indarbejdet i kulturen.

Step 4) Opdatering af arbejdsgange

- I de tidligere step har I fundet frem til hvor der skal foretages ændringer i jeres nuværende arbejdsgange, systemer mv. og hvilke ændringer I skal foretage.

- Step 4 er der hvor I sørger for at ændringerne bliver foretaget. Eks. opdaterer/ændrer samtykker, vælger nye delingsprogrammer, smider gamle oplysninger ud I ikke længere har behov for/må gemme…

Step 5) Processer

- I step 5 skal I udarbejde nogle processer, der sikrer at I overholder jeres nye politikker og arbejdsgange.

- I skal finde en der er ansvarlig for at der eks. bliver slettet mails så ofte som I har besluttet, eller at der ikke ligger personoplysninger og flyder på kontoret? Hvad gør I hvis processerne ikke bliver fulgt?

- For at gøre det nemmest for jer selv, opret et skema med de forskellige processer. Sæt et felt ind til at skrive dato og oplysninger ind. Eks.

Proces	Hvor ofte	Dato	I orden	Ansvarlig
Tjek at arkivskabe er låst	1 x mdr.	18/2	+	HTA
Tømmer medarbejderne papirkurven i Outlook løbende	1 x ½ år	18/2	+	HTA
Har vi persondata liggende fremme	1x mdr	18/2	+	MW

Hvad gør man ved sikkerhedsbrud?

- Få et overblik over situationen!

- Identificer og overvej bruddet herunder risikoen, datamængden og subjektet.

- Det skal vurderes om den registrerede skal informeres om sikkerhedsbruddet, der er altid tale om en konkret afvejning.
- Hvis det er slemt, skal bruddet anmeldes til Datatilsynet indenfor 72 timer.
  - Beskrive karakteren af bruddet
  - Antallet og kategorierne af berørte datasubjekter og registreringer
  - Angive kontaktoplysninger på den dataansvarlige
  - Anbefalinger og/eller beskrivelse af de foranstaltninger den dataansvarlige har iværksat/vil iværksætte for at afhjælpe bruddet

- Vurderer I det ikke er et slemt brud, er pligten at I skal føre en log og skrive ned, at I har lavet ovenstående vurdering.

I tvivl? Kontakt Datatilsynet!

Vejledninger og lovgivning fremadrettet

- Den nye persondatalov forventes at blive vedtaget 20. februar 2018
- Der mangler stadig centrale vejledninger fra Datatilsynet:

Emne	Offentliggørelse
Generel informationspjece om forordningen	√
Databeskyttelsesrådgiver	√
Overførsler af personoplysninger til tredjelande	√
Samtykke	√
Dataansvarlige og databehandlere	√
Adfærdskodekser og certificeringsordninger	√
Fortegnelse	√
Databeskyttelse gennem design og standardinstillinger	feb-18
Konsekvensanalyse	feb-18
Håndtering af brud på persondatasikkerheden	feb-18
Behandlingssikkerhed	feb-18
Registreredes rettigheder	feb-18
Databeskyttelse på det ansættelsesretlige område	feb-18

Spørgsmål

Tak for i dag!

Vi afholder persondataworkshop d. 28. februar kl. 11-17 på DUF

Spørgsmål kan rettes til
Juridisk konsulent Mikkel Wrang på mw@duf.dk tlf. 60 20 14 45