Databeskyttelseslovgivningen

Præsentation til lokalforeninger/klubber

HJERTE FORENINGEN

Formål med præsentationen

Som opfølgning på præsentationen, der blev afholdt forud for Repræsentantskabsmødet d. 26. maj 2018, er følgende præsentation blevet tilpasset.

Formålet er:

- at sikre en ensartet viden om databeskyttelseslovgivningen og håndtering af persondata på tværs af lokalforeninger/klubber.
- at sikre der foreligger en ensartet præsentation, der kan bruges til at klæde resten af bestyrelsesmedlemmerne på, både de eksisterende og når nye kommer til.

Præsentationen sendes til alle formænd, og det anbefales, den bliver gennemgået med resten af bestyrelsesmedlemmerne.

HJERTE FORENINGEN

Indhold i præsentationen

- Formål med præsentationen
- Baggrunden for den nye persondatalovgivning
- Basisprincipper for behandling af personoplysninger
- Rettighederne vi alle har og får
- Hvad er en personoplysning, og hvornår er den følsom?
- Hvad betyder det for jer i lokalforeninger/klubber?
- Krav om tilstrækkelig sikkerhed, men hvad betyder det?
- Hvornår er lokalforeninger/klubber dataansvarlige, og hvad betyder det set fra medlemmet?
- Eksempler på spørgsmål/svar fra hverdagen

HJERTE FORENINGEN

Hvorfor kommer der en ny persondatalov (persondatalovgivningen)?

- Den gamle persondatalov var baseret på et EU direktiv, som hvert medlemsland selv skulle tilpasse og implementere nationalt. Dette resulterede i forskellige fortolkninger, som EU nu ønsker skal strømlines, så der er færre forskelle på tværs af landegrænserne.
- Den gamle persondatalov er blevet erstattet af en ny databeskyttelsesforordning, der trådte direkte ind som en lov i alle medlemslande fra den 25. maj 2018.
- Ny teknologi har også udfordret den gamle persondatalov, og det er tydeligt, der har været behov for en stramning af reglerne overfor ”smarte” virksomheder, der overvåger vores adfærd – ofte uden vores vidende.
- …og dette er kun begyndelsen. EU har flere forordninger på vej med yderligere stramninger for behandlingen af personoplysninger.

HJERTE FORENINGEN

Hvornår gælder forordningen?

Forordningen siger:

- ”Denne forordning finder anvendelse på **behandling af personoplysninger**, der helt eller delvist foretages ved hjælp af **automatisk databehandling**, og på anden ikke-automatisk behandling af personoplysninger, **der er eller vil blive indeholdt i et register.”**

Med andre ord:

- Forordningen gælder for IT-behandling af personoplysninger **samt** manuel behandling af personoplysninger, **hvis** disse efterfølgende arkiveres i et register (IT-system eller papirarkiv).

Såfremt der findes en mere specifik lov, f.eks. bogføringsloven eller markedsføringsloven, er det denne, der skal følges.

HJERTE FORENINGEN

Hvornår gælder forordningen?

I er fx omfattet af reglerne, når:

- I downloader medlemslisten fra HF's medlemssystem.
- I bruger kontaktoplysningerne i medlemslisten til at sende e-mails til medlemmerne eller andre frivillige.
- I modtager e-mails fra medlemmerne eller andre frivillige.

MEN…

Det er også manuel behandling af personoplysninger, som er omfattet, hvis oplysningerne er eller vil blive indeholdt i et register. Det er nemlig, når personoplysninger bruges på en måde, som gør det let og hurtigt at søge i dem, at behovet for at beskytte dem bliver aktuelt.

- Det betyder, at når I bruger medlemslisten i en papirudgave, så er behandlingen også omfattet af reglerne, fordi der er tale om en manuel behandling af oplysningerne.

HJERTE FORENINGEN

Hvilke rettigheder får vi alle?

- **Oplysningspligt** (”hvad gør I med mine data og hvorfor?”)
- **Ret til indsigt** (”jeg ønsker en kopi af de personoplysninger, I har registreret om mig!”)
- **Ret til berigtigelse** (”I har forkerte oplysninger om mig, de skal rettes!”)
- **Ret til sletning** (”slet mig fra jeres systemer!”)
- **Ret til begrænsning af behandling** (”stop jeres behandling af mine oplysninger, men I må ikke slette dem!”)
- **Ret til indsigelse** enten pga. særlige personlige årsager eller mod direkte markedsføring.
- **Ret til dataportabilitet** (”jeg flytter, hjælp mig!”)
- **Ret til menneskelig behandling** (”systemet må have regnet forkert, jeg vil have en af jeres medarbejdere til at kigge på det en ekstra gang”)

Særlige forhold kan gøre, at man ikke kan udøve en eller flere af sine rettigheder, fx er det ikke i samfundets interesse, at vi kan blive slettet hos SKAT.

HJERTE FORENINGEN

Hvad er en personoplysning?

Hvad siger forordningen:

- »personoplysninger«: **enhver form for information om** en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås **en fysisk person**, **der direkte eller indirekte kan identificeres**, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

Med andre ord:

- En personoplysning er enhver form for oplysning om en fysisk person, som direkte eller indirekte kan bruges til at identificere personen.
- En personoplysning kan være en oplysning som **direkte** kan identificere en person f.eks. navn og cpr.nr, men det kan også være alle tænkelige former for oplysninger, som **mere indirekte** kan være med til at identificere en person, f.eks. adresse, e-mailadresse, telefonnummer, medlemsnummer, fotos.

HJERTE FORENINGEN

Almindelige personoplysninger

Langt de fleste personoplysninger, som vi behandler i Hjerteforeningen er **almindelige personoplysninger**, fx navn og kontaktoplysninger (adresse, telefonnummer, e-mail) på medlemmer, dine frivilligkolleger og andre, du hjælper som frivillig.

Eksempel:
Medlemslisterne over medlemmerne i jeres lokalområde indeholder kun almindelige personoplysninger, og de oplysninger kan I uden videre bruge, når I kommunikerer med medlemmerne om jeres aktiviteter i lokalforeningen.

HJERTE FORENINGEN

Hvornår er en personoplysning følsom?

- Race eller etnisk oprindelse.
- Politisk, religiøs eller filosofisk overbevisning.
- Fagforeningsmæssigt tilhørsforhold.
- Genetiske eller biometriske data med det formål entydigt at identificere en fysisk person.
- Helbredsoplysninger
- Seksuelle forhold eller seksuelle orientering.
- Særregler for CPR nummer (almindelig personoplysning, men beskyttes på samme niveau som følsomme og må kun benyttes når det er nødvendigt, eksempelvis ved indberetning til det offentlige)
- Samt straffedomme og lovovertrædelser, der kun må behandles under kontrol af en offentlig myndighed/hjemlet ved lov.

I Hjerteforeningen kommer vi typisk i kontakt med følsomme oplysninger som helbredsoplysninger og cpr-numre (markeret med gul).

HJERTE FORENINGEN

Behandling af følsomme personoplysninger

Der er sjældent behov for at behandle følsomme oplysninger, men hvad gør man, hvis det er nødvendigt?

- I skal være særligt opmærksomme, når I behandler følsomme oplysninger
- En behandling af følsomme personoplysninger kan som regel **kun** ske med et samtykke fra de personer, som de følsomme oplysninger handler om, eller hvis loven decideret foreskriver, at vi skal behandle dem.
- Hvis I uopfordret modtager følsomme oplysninger – f.eks. hvis et medlem i en mail fortæller om sit helbred, så husk at slette mailen efterfølgende.
- Når I indberetter honorar til en foredragsholder eller instruktør til administrationen, må I gerne modtage foredragsholderens CPR-nummer og sende det til administrationen, da det følger af skattelovgivningen. Vær opmærksom på at slette mailen bagefter.

Hvis det er nødvendigt for jer at behandle følsomme oplysninger, må I meget gerne tage kontakt til vores databeskyttelsesrådgiver Tor Valstøm, der kan hjælpe med at undersøge, om I må behandle oplysningerne, og om I har behov for et samtykke.

HJERTE FORENINGEN

Hvad betyder dette for jer?

EU kommissionen har i slutningen af april udgivet en kort guide for organisationer, der behandler personoplysninger som biaktivitet. Eksempelvis kartoteker med almindelige kontaktoplysninger på medlemmer og frivillige, for at kunne planlægge og afholde arrangementer.

Seks af punkterne er relevante for jer:

1. Lav intern dokumentation af de personoplysninger, der behandles.
2. Informer om formålet med behandlingen af personoplysninger.
3. Slet unødvendige oplysninger.
4. Sørg for fornuftig sikkerhed både menneskeligt og i IT.
5. Indgå databehandleraftaler i nødvendigt omfang.
6. Vær forberedt på eventuelle brud på persondatasikkerheden.

HJERTE FORENINGEN

Hvad betyder dette for jer?

1. Lav intern dokumentation af de personoplysninger I har - og hvilke formål de behandles til

- Som dataansvarlig har man pligt til at have en skriftlig, elektronisk beskrivelse af, hvilke personoplysninger man behandler og til hvilke formål.
- Hjerteforeningen har udarbejdet et udkast til en skabelon (udvidet fortegnelse), I kan bruge.

Eksempel på aktivitet, der skal fremgå af beskrivelsen:

- Formål: Afholde hjertecafé.
- Personoplysninger: Navne og kontaktoplysninger på deltagere.

Brug skabelonen "Udvidet fortegnelse"

HJERTE FORENINGEN

Hvad betyder dette for jer?

2. Giv kortfattet, ærlig og letforståelig oplysning om formål, når I indsamler personoplysninger

Ofte vil formålet være selvforklarende, men hvis det ikke er, skal man skrive en kortfattet supplerende information.

Tænk over om det er åbenlyst, hvad oplysningerne skal benyttes til – hvis det ikke er, så tilføj en uddybende forklaring.

Særligt i forhold til billeder:

Datatilsynet anbefaler samtykke ved portrætfotos – hvorimod der ikke behøves samtykke ved situationsbilleder, eksempelvis fra arrangementer.

☛ *Brug skabelonen "samtykkeerklæring" for en god ordens skyld, hvis der er tale om et portrætfoto, eller hvis du skriver navnene på dem der er afbildet. (Hjerteforeningen har udarbejdet et udkast til en samtykkeerklæring)*

HJERTE FORENINGEN

Hvad betyder dette for jer?

3. Slet unødvendige oplysninger

Oplysninger der er irrelevante, enten pga. alder eller formål, skal slettes.

Eksempel:
Slet/makulér oplysninger, der ikke længere er relevante. Hvis du f.eks. udskriver en midlertidig liste med deltagere, så sørg for at den bliver destrueret, når du er færdig med den – med mindre den skal genbruges i anden sammenhæng.

Eksempel:
Slet/makulér oplysninger på en frivillig, der ikke længere ønsker at hjælpe, pga. personlige årsager.

HJERTE FORENINGEN

Hvad betyder dette for jer?

4. Sørg for fornuftig sikkerhed både menneskeligt og i IT-systemerne

Del kun personoplysninger i nødvendigt omfang, hold IT-systemer opdateret og pas på personoplysningerne, så I også har folks tillid i fremtiden.

(Uddybes på de to slides "Hvornår har man opnået fornuftig sikkerhed")

HJERTE FORENINGEN

Hvad betyder dette for jer?

5. Indgå databehandleraftaler i nødvendigt omfang

Mange, f.eks. Microsoft Office 365, Google Gmail, laver automatisk en databehandleraftale, når I opretter en konto, men I kan have andre samarbejdspartnere, hvor der er behov for at indgå en skriftlig aftale.

- Databehandlere er oftest IT-systemer, der er hostet eksternt.

Der er ikke behov for databehandleraftaler med samarbejdspartnere, blot fordi der udveksles personoplysninger. Det er fx ikke et krav ifm. service af en kopimaskine, der benyttes til udskrift af følsomme personoplysninger. Her anbefaler Datatilsynet, at der indgås en fortrolighedsaftale.

Hvis I har behov for at videregive personoplysninger til andre, så tag endelig fat i Hjerteforeningens Databeskyttelsesrådgiver Tor Valstrøm, der kan hjælpe med den rette aftale.

HJERTE FORENINGEN

Hvad betyder dette for jer?

6. Ved eventuelle brud på persondatasikkerheden

Når det sker, skal man indenfor 72 timer fra fejlen opdages, indberette til Datatilsynet via www.datatilsynet.dk

Hjerteforeningen bistår gerne med hjælp, hvis uheldet sker en dag.

☛ *Brug skabelonen "databrudslog" til at notere sikkerhedsbrister i. Her kan I også se, hvilke typer oplysninger, Datatilsynet forventer at modtage fra jer.*

HJERTE FORENINGEN

Hvornår har man opnået fornuftig sikkerhed?

- Husk at der i hver lokalforening/klub bør være én persondataansvarlig, og at det ofte vil være formanden, der er eller udpeger denne. Vedkommende skal sørge for at fortælle alle, at de skal informere den persondataansvarlige, hvis noget går galt.
- Sørg for at hele bestyrelsen er informeret om, at sikring af personoplysninger er et ansvar vi løfter i fællesskab.
- Del kun personoplysninger når det er nødvendigt, fx kun deltagerlister med dem, der står for afvikling af arrangementet.
- Husk adgang også er fysisk - sørg for at låse personoplysninger inde/lægge dem væk, hvis de er på papir og uden opsyn.
- Hold styr på hvor jeres personoplysninger er - uanset om de er elektroniske eller på papir.

HJERTE FORENINGEN

Hvornår har man opnået fornuftig sikkerhed?

Når I arbejder digitalt:

- Hold IT-systemer og software opdateret - Windows 10 er væsentligt mere sikker end tidligere versioner.
- Hvis der et muligt, benyt gerne kryptering.
- Når du sender personoplysninger via e-mail, så check modtageradressen en ekstra gang - inden du trykker på send.
- Husk sikkerhedskopi.
- Slå kodeord/pinkode til på jeres IT-udstyr.
- Husk kodeord er som undertøj – skift dem ofte og lad være med at dele dem med andre.

HJERTE FORENINGEN

Hvem er dataansvarlig for dagligdagens aktiviteter?

Hjerteforeningen

- Dataansvarlig for ”konceptet” (hovedvedtægterne)
- Dataansvarlig for stamdatasættet (”telefonbogen”)

Lokalforeningen/klubben

- Vælger selv **formålet** personoplysninger behandles til – *så længe det ligger inden for rammerne af vedtægterne.*
- Vælger selv **hvilke** personoplysninger, der behandles.
- Vælger selv **hvem** der behandles personoplysninger om (eksv. nye potentielle medlemmer.)
- Vælger selv **hvordan** personoplysningerne behandles.
- Vælger selv **hvornår** personoplysninger bør slettes (f.eks.en liste fra et tidligere lokalarrangement.)

HJERTE FORENINGEN

Hvad betyder det at være dataansvarlig?

- Er en person utilfreds med jeres behandling af personoplysninger, skal personen kunne rette henvendelse direkte til jer og bede om ændret adfærd.
  Hvis en person ikke ønsker invitationer fremover, skal I respektere dette.
- Er personens oplysninger behandlet usikkert af jer, har I selv ansvaret for handlingen.
  Hvis der sker en fejl med personoplysninger, skal I indberette det til datatilsynet.
- Ønsker personen en kopi af de personoplysninger, I har om dem, kan kun I udlevere det.
- Ønsker personen viden om, hvem I har delt deres oplysninger med, vil kun I kunne svare.

HJERTE FORENINGEN

Eksempler fra hverdagen

Spørgsmål:

Skal vi så slette alle vores gamle mails?

Svar:

Nej, naturligvis ikke. Men det er vanskeligt at adskille irrelevante mails fra vigtige mails.

- Overvej om der hos jer kan være en nem aldersgrænse for, hvornår en mail er irrelevant, eksempelvis efter 6 år, og slet så alle der er ældre end dette.
- Gør det til en vane i hverdagen at rydde op hurtigt i alle mails med følsomme personoplysninger – lad være med at lade følsomme mails hobe sig op.
- Gør det til en vane i hverdagen at gemme vigtige mails, der ikke må slettes, eksempelvis i et særligt arkiv til lang tids opbevaring.

HJERTE FORENINGEN

Eksempler fra hverdagen

Spørgsmål:

Skal vi alle have en makulator?

Svar:

Nej, naturligvis ikke med mindre, I har en i forvejen.

- Sørg dog for at rive papirer med helbredsoplysninger i små nok stykker til, at man ikke længere kan læse indholdet.

HJERTE FORENINGEN

Eksempler fra hverdagen

Spørgsmål:

Må vi ikke længere sende almindelige e-mails? (skal vi skifte til Sikker Mail?)

Svar:

I må gerne bruge almindelige e-mails.

- Udfordringen med almindelige e-mails er, at man ikke kan være sikker på, om indholdet overføres krypteret via internettet, og af samme årsag har nogle enkelte organisationer valgt at droppe almindelige e-mails helt og tvinge alle de korresponderer med til at benytte enten e-Boks eller en Sikker Mail løsning.
- Har I noget meget følsomt, I gerne vil sende på en e-mail, kan I evt. sætte en kode på Word-dokumentet (i menuen Filer) og sende koden til modtageren via SMS. Så er indholdet krypteret, og I har beskyttet jer mod, at indholdet kan læses af andre end den person, der har koden.

HJERTE FORENINGEN

Kontakt os gerne for spørgsmål

Kontakt Hjerteforeningens Databeskyttelsesrådgiver
Tor Valstrøm på: dpo@hjerteforeningen.dk