# Persondata i spejderarbejde

## EN VEJLEDNING I EU'S PERSONDATAFORORDNING OG HVORDAN VI PASSER GODT PÅ HINANDENS PERSONOPLYSNINGER

Spejdernes Administrationsfællesskab | Juli 2020

# Indhold

## Hvad er persondataforordningen, og hvorfor er den vigtig?

Det bliver mere og mere vigtigt, at vi passer godt på hinandens persondata. Som spejdergruppe ligger I inde med et væld af personoplysninger på medlemmer, forældre og andre tilknyttede til gruppen.

Den 25. maj 2018 trådte en ny forordning i kraft, som betyder, at alle EU-lande er forpligtet til at efterleve de samme regler med kun få undtagelser.

Forordningen handler ikke om os som organisation og forening, men om vores medlemmer og andre, hvis persondata vi opbevarer. Det vigtigste at huske på er, at *det er data, som vi låner i en begrænset periode, og i den periode har vi ansvaret for, at det behandles sikkert og korrekt*.

Denne vejledning kommer med et bud på, hvad I skal være opmærksomme på, samt hvordan I kommer godt i gang og i mål med at implementere reglerne og opbygge en god dataskik. Korpset leverer forskellige skabeloner, som I kan finde på dds.dk/persondata, efterhånden som de bliver klar.

Skulle I miste fokus undervejs så husk, at det vigtigste i hele processen er, at vi gør os umage med at passe godt på folks oplysninger og at vi med lidt sund fornuft kommer rigtig langt.

**OBS:**

Denne vejledning opdateres løbende, som der kommer nye fortolkninger af reglerne til.

Det er vigtigt at notere sig, at **denne vejledning ikke er udtømmende i forhold til forordningens regler**. Vi har forsøgt at beskrive de vigtigste ændringer i forhold til den nuværende praksis, og hvad vi tænker er mest relevant for jer ude i grupperne og enhederne.

## Hvad er persondata?

Persondata er enhver form for information om en fysisk person, som kan bruges til at identificere den pågældende. Dette kan være de åbenlyse, så som navn, medlemsnummer, adresse, telefonnummer og billeder, men også IP-adresser og pseudonymiseret data er personoplysninger, da de kan føres tilbage til en fysisk person.

Der skelnes mellem følsomme og almindelige personoplysninger. De ovenfor nævnte eksempler er alle af almindelig karakter, hvorimod følsomme personoplysninger er oplysninger om bl.a. race eller etnisk oprindelse, politisk, religiøs og filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af helbredsoplysninger.

De fleste af de oplysninger, vi behandler om medlemmer og frivillige (fx navn, alder, e-mail, medlemsnummer og kontooplysninger) er altså almindelige personoplysninger. Vi skal dog stadig gøre rede for, hvordan og hvorfor vi behandler dem. Helbredsoplysninger er følsomme, og dem skal I derfor være særligt forsigtige med. Det gælder fx, når I spørger til allergier eller fysiske skavanker på tilmelding til ture og arrangementer.

Cpr.-numre og børneattester er ikke omfattet af forordningen og falder derfor ikke ind under de to kategorier. Som hidtil og efter dansk lovgivning skal de behandles fortroligt.

Du kan med fordel læse mere om de forskellige typer af oplysninger på Datatilsynets hjemmeside (https://www.datatilsynet.dk/generelt-om-databeskyttelse/hvad-er-personoplysninger).

## Hvordan behandler vi persondata?

I skal i grupperne og enhederne forsøge at sikre, at de personer, der har adgang til og håndterer persondata, kender de grundlæggende principper for god databehandling.

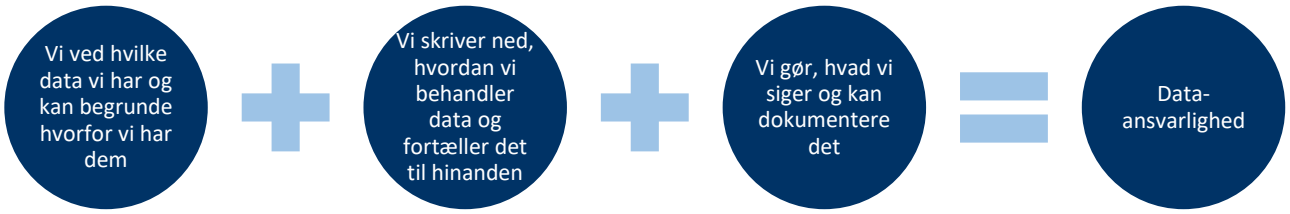
**Kogt helt ned til et par linjer er grundprincipperne, at vi indsamler så få data som muligt og beholder dem så kort tid som muligt – så snart formålet med indsamlingen af data er opnået, skal vi i princippet skille os af med det igen.**

I de tilfælde hvor vi ikke arbejder efter grundprincipperne (se eksempler herunder) og kan dokumentere det, skal vi have optimeret vores databehandling.

Når vi behandler personoplysninger skal vi bl.a. sørge for, at:

- vi har ret til at behandle den data vi indsamler
- dem vi indsamler data om ved det og ved, hvad vi bruger den til
- vi kun bruger data til det formål, vi har indsamlet det til
- vi kun indsamler need-to-know data
- vi sletter data, vi ikke har brug for længere
- vi opdaterer forkerte oplysninger
- vi beskytter data og nøje overvejer, hvem i gruppen eller enheden, der har adgang til data
- vi behandler persondata ansvarligt - her kommer man rigtig langt ved hjælp af sin sunde fornuft.

Som dataansvarlig har I ansvaret for og skal kunne dokumentere, at I overholder grundprincipperne for databehandling. Dataansvarlighed kan forklares gennem følgende model:




## Hvornår er databehandling lovlig?

Når du skal sikre dig, at din behandling af persondata er lovlig, skal du skele til følgende gode grunde (hjemler). I skal foretage jer et bevidst valg om, på hvilket grundlag I behandler personoplysninger. Er der ikke noget lovligt grundlag, er I nødt til at stoppe behandlingen.

**I vil typisk bruge følgende som grundlag for jeres behandling af medlemmernes personoplysninger:**

1. **Samtykke**
   Medlemmet har givet udtrykkeligt samtykke og dermed selv indvilget i at vedkommendes data behandles, ex helbredsoplysninger, allergier, skader, brug af portrætbilleder[1] og videregivelse af oplysninger.

2. **Opfyldelse af en kontrakt/aftale**
   Behandlingen er nødvendig for at opfylde en kontrakt/aftale som medlemmet er en del af, ex de oplysninger I skal bruge for at kunne opkræve kontingent, for at medlemmet kan betale for en tur eller når medlemmet køber merchandise.

3. **Retlig forpligtelse**
   Behandlingen er nødvendig for jeres overholdelse af en retlig forpligtelse, ex de oplysninger I skal bruge til at søge tilskud fra kommunen, eller når I gemmer regnskabsoplysninger på baggrund af bogføringsloven.

4. **Interesseafvejningsreglen**
   Behandlingen er nødvendig for at I som dataansvarlige kan forfølge en legitim (berettiget) interesse, så længe den ikke overstiger medlemmets interesse. Et eksempel herpå kan være, når vi beder om pårørendes kontaktoplysninger, når vi tager på tur for at kunne kontakte dem i tilfælde af uheld.

[1] Datatilsynet ændrede i september 2019 praksis i forhold til offentliggørelse af billeder på nettet. Hvor offentliggørelse af portrætbilleder tidligere har krævet et udtrykkeligt samtykke lægges der nu op til, at en offentliggørelse af portrætbilleder uden samtykke fra den berørte person beror på en helhedsvurdering af billedet og formålet med offentliggørelsen. Man satte i sin tid Medlemsservice op til at kunne håndtere samtykke til portrætbilleder og det står uændret efter Datatilsynets nye vurdering af den grund, at det for mange af jer, er rart med et overblik over de spejdere, der ikke ønsker deres billeder offentliggjort, hvilket de naturligvis stadig har ret til at frabede sig.

## Den registreredes rettigheder

En af de større grundsten i forordningen er den registreredes rettigheder. En registreret er den person, hvis personoplysninger bliver behandlet af en dataansvarlig (jer). I har oplysningspligt. Det betyder, at I skal oplyse registrerede om bl.a. hvilke data I indsamler, formålet med behandlingen, hvem I deler oplysningerne med og hvor lang tid, I beholder dem.

**Herudover har den registrerede bl.a. ret til:**

- løbende at få indsigt i, hvordan hans eller hendes oplysninger behandles og at få udleveret en kopi af de personoplysninger der behandles (gælder også billeder)
- at få rettet/opdateret forkert data (gælder også videregivet data)
- at blive glemt (herunder at få slettet data)
- at tilbagekalde samtykke

Vi er derfor nødt til at opsætte nogle procedurer for, hvordan vi håndterer en henvendelse fra en registreret, som ønsker at gøre brug af én af sine rettigheder, inden for en rimelige tidsperiode. Det er derfor også vigtigt, at vi til enhver tid sørger for, at de oplysninger vi gemmer er opdaterede og rigtige. Får vi ex en henvendelse fra et medlem, der ønsker at melde sig ud eller ønsker hjælp til at ændre oplysninger på sit stamblad, skal vi have reageret på henvendelsen inden der er gået fire uger fra de henvender sig første gang.

## Dataansvarlige og databehandlere

### Rollen som dataansvarlig

Den dataansvarlige er den der bestemmer, hvilke personoplysninger der skal behandles, hvorfor de behandles og ikke mindst hvordan. Den dataansvarlige (= jer) har ansvaret for at behandle folks oplysninger efter reglerne og at I kan dokumentere, at I overholder de nye regler. I vælger selv, hvem i gruppen og enheden, der er ansvarlig for at implementere de nye regler, men det er gruppen som helhed, der bærer ansvaret, ikke blot den person, der sidder med opgaven til daglig.

### Start med det enkle der ligger lige for

Når I tager fat på arbejdet med de nye regler, fokuser da i første omgang på det, der ligger lige foran jer. Det er ofte det der er billigst og har størst effekt:

- ✓ I har styr på jeres IT-sikkerhed og sikrer jer bl.a., at ikke alle har adgang til al data.

- ✓ I deler kun oplysninger med relevante personer i gruppen og enheden, og de personer er sat ind i de nye regler. Graden af information kan med fordel tilpasses de forskellige funktioner i gruppen og enheden. En generel info-aften om det nye fokus på privatlivsbeskyttelse ville derfor også være en rigtig god idé.

- ✓ I tager stilling til, hvad I gør, hvis nogle som ikke skulle have haft adgang til data har fået det alligevel (= brud på datasikkerheden).

- ✓ I har gyldige databehandleraftaler på jeres 'leverandører'/samarbejdspartnere (ex. Medlemsservice (indgår i dataaftalen med korpset), Dropbox, Google osv.). Korpsets advokater har udarbejdet et udkast til en standard databehandleraftale, der lever op til forordningens krav, som I kan finde på dds.dk/persondata.

- ✓ I har en fortegnelse over jeres behandling af persondata og retningslinjer for, hvornår I sletter data, som I ikke længere har brug for. Opsætning og overholdelse af egne sletteregler og kontroller er vigtigt at få på plads for at kunne dokumentere dataansvarlighed.

### Databehandlerens forpligtelser

Med den nye forordning får også databehandlere (fx Medlemsservice, Dropbox, Google etc.) flere krav at leve op til og har bl.a. ansvaret for, at:

- man ikke behandler data på andre måder end aftalt med den dataansvarlige
- udarbejde rapporter over behandlingsaktiviteter
- implementere passende tekniske og organisatoriske sikkerhedsforanstaltninger
- informere den dataansvarlige ved sikkerhedsbrud
- man ikke overgiver opgaven til andre databehandlere uden skriftlig tilladelse fra den dataansvarlige.

## Hvordan dokumenterer vi vores behandling af persondata?

Vi skal kunne dokumentere, at vi overholder forordningens krav og skal kunne forklare, hvad der sker med data fra de indsamles, til de slettes. Vi skal bl.a. beskrive:

- Hvilke typer data der behandles
- Formålet med behandlingerne
- Kategorier af registrerede personer (fx spejdere, forældre, frivillige) og modtagere af oplysninger (fx Medlemsservice, Google)
- Angivelse af tidsfrister for sletning af oplysninger

Beskriv hvilke data I har, og hvordan I behandler dem. Brug med fordel korpsets skabelon, som I finder på dds.dk/persondata. Når den er udfyldt, vil I have et bedre overblik over, hvilke persondata I håndterer i grupperne og enhederne, og på hvilke områder I evt. ikke overholder forordningens krav, ex i forhold til sletning af data og kontroller.

## Persondata i cloud-løsninger og mails

Når vi opbevarer og deler persondata, skal vi altid have den registrerede for øje og bl.a. overveje risikoen for at personens oplysninger kommer i uvedkommendes hænder og hvad det vil betyde for den registrerede.

Når vi bruger gratisløsninger så som Dropbox og Google, har vi ikke de samme muligheder for selv at styre, hvor vores data ligger, og vi kan have svært ved at kontrollere eller dokumentere, at data opbevares korrekt og sikkert.

Forsøg derfor at begrænse jeres deling af persondata i de gratis cloud-løsninger, hvor I har svært ved selv at kontrollere data.

Brug med fordel skyen til at dele aktiviteter, løbsbeskrivelser, huskelister, processer, oversigter, tjeklister, opskrifter, arrangementsbeskrivelser, årshjul, generel dokumentation, osv. og hold personoplysninger i Medlemsservice eller betalingsløsninger, hvor sikkerheden er højere og I har nemmere ved at styre, hvem der har adgang til de relevante dokumenter.

**Overvej følgende inden I deler persondata i skyen:**

- Har I mulighed for selv at vælge hvor din data opbevares (inden for EU)?
- Kan I følge med i, hvem der tilgår de forskellige dokumenter?
- Kan I begrænse adgangen til bestemte mapper og dokumenter, så ikke alle har adgang til alt?

**Ønsker I at fortsætte med at gemme og dele persondata i cloud-løsninger, kan I hurtigt og nemt mindske risikoen for den registrerede gennem følgende tiltag:**

- Sørg for at der er adgangskontrol/-begrænsning til systemet/mappen
- Hav en procesbeskrivelse for hvordan I sikrer opdatering af adgange (herunder også at fjerne adgange igen)
- Lav en begrundelse for hvem der har adgang (det skal kun være relevante personer)
- Overvej hvad I deler (og om det er hensigtsmæssigt)
- Opret abonnementer med professionelle profiler/mails (forsøg at undgå privatabonnementer)
- Sæt en kode på de Excel-ark der deles.

Det samme gælder jeres spejdermails, som indeholder masser af personoplysninger og derfor også er omfattet af forordningen. Der ligger en opgave i at få et overblik over, hvad man har liggende og få slettet den data, som ikke længere tjener et formål.

Fremadrettet kan man gennem retningslinjer forsøge at begrænse mængden af følsomt indhold i mails og andre kommunikationsformer, der bruges i grupperne og enhederne.

**I kan tage udgangspunkt i følgende råd:**

- Vi sender som udgangspunkt ikke følsomme og fortrolige oplysninger over mail, ex. helbredsoplysninger og CPR-numre. Vi opfordrer heller ikke andre til at sende det til os. Sender folk alligevel følsomme oplysninger til os, sletter vi dem umiddelbart efter vi har behandlet dem. Sørg også for at slette eller anonymisere persondata, hvis du skal besvare mails med fortrolige eller følsomme personoplysninger.
- Kan vi ikke komme uden om at sende personfølsomme eller fortrolige oplysninger på mail, vedhæfter vi det i et dokument, som vi låser med en kode. Koden sendes pr. sms eller overleveres til rette vedkommende over telefonen.
- Cc og del kun mails med kollegaer og andre, der også skal involveres i behandlingen af persondata – eller slet/anonymisér persondata, før du videresender mailen.

## Tjekliste

- ✓ Lav en fortegnelse over jeres behandling af persondata. Brug Excel ark-skabelonen fra dds.dk/persondata – og sørg for at opdatere den.

- ✓ Indhent databehandleraftaler med leverandører og relevante samarbejdspartnere. Husk at korpset har lavet en standardskabelon til databehandleraftaler.

- ✓ Lav retningslinjer for, hvordan I arbejder med persondata i gruppen:
  - ☐ Sørg for at have en procedure for hvordan I håndterer en forespørgsel fra medlemmerne/de frivillige (registrerede) og sikr jer, at I kan reagere rettidigt
  - ☐ Fortæl jeres frivillige hvordan i håndterer persondata i gruppen og enheden, så I sikrer, at jeres regler følges i praksis
  - ☐ Sørg for at få lavet nogle sletteregler for persondata og jeres mails
  - ☐ Lav en tjekliste til hvordan I fører kontrol med, at data bliver slettet og at I har styr på adgangsrettigheder, så I sikrer jer, at det bliver gjort og at I kan dokumentere det
  - ☐ Aftal hvordan I håndterer og dokumenterer et eventuelt brud på datasikkerheden.

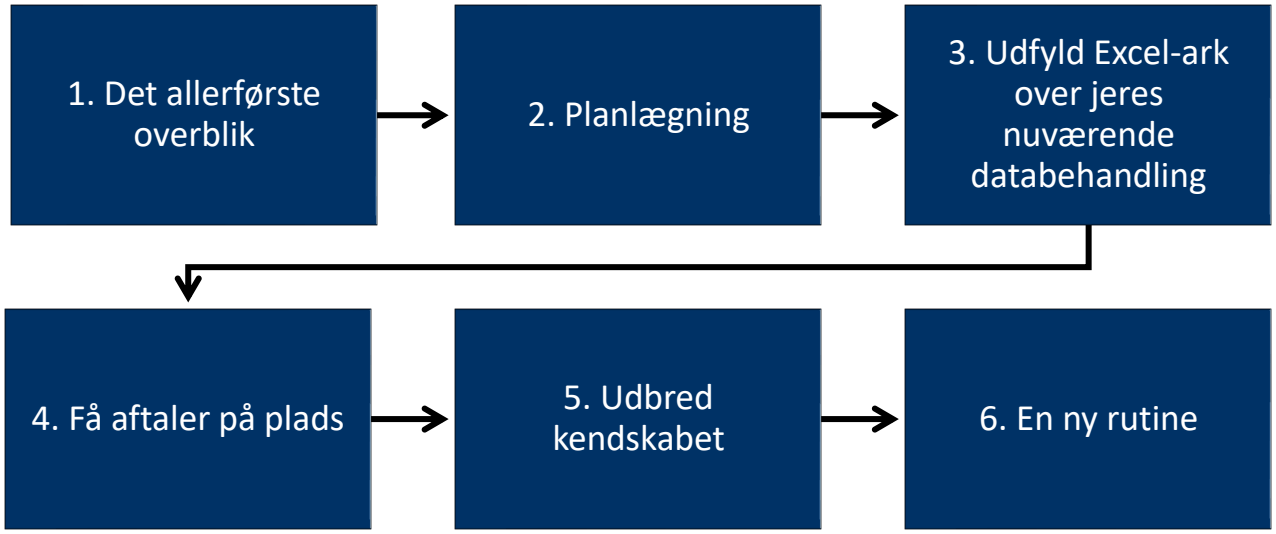
- ✓ Pas godt på persondata:
  - ☐ Sæt adgangsbegrænsning på dokumenter og systemer, så alle ikke har adgang til alt
  - ☐ Hav adgangskoder på computere og forny dem løbende
  - ☐ Lad ikke fortrolige papirer ligge fremme – lås dem inde i skuffe/skab
  - ☐ Del kun persondata med frivillige med de fornødne rettigheder
  - ☐ Benyt ikke et netværk uden kode.

- ✓ Gennemgå jeres tilmeldingsformularer og sikr jer, at I kun beder om oplysninger i har brug for til det bestemte formål, så i ikke indsamler en masse unødvendige oplysninger.

- ✓ Lav en årlig oprydning både på computeren og i hytten, så I sikrer jer, at I ikke ligger inde med en masse data, I ikke har ret til at behandle. Husk opslagstavlerne.

## Kom godt i gang

Her får du seks trin til, hvordan I kan gribe opgaven med at passe godt på persondata an i gruppen og enheden.




1. **Det allerførste overblik**
   Her overvejer I (snakker om), hvordan I behandler persondata i dag. Denne fase skal munde ud i et overblik over, hvor stor en opgave I står overfor. Da det er meget forskelligt, hvor meget kendskab I har haft til den nuværende persondatalov og arbejdet efter reglerne, vil dette variere meget fra enhed til enhed.

2. **Planlægning**
   Herefter udarbejder I en køreplan for bedre persondatasikkerhed i gruppen. Hvem er tovholder på projektet? Hvor meget tid kan I sætte af til projektet? Hvornår begynder I?

3. **Udfyld Excel ark over nuværende databehandling**
   I giver jer nu i kast med at kortlægge jeres håndtering af persondata i gruppen. Hertil kan I bruge den skabelon, som korpset stiller til rådighed. Resultatet af denne fase er bl.a. et overblik over, hvor I ikke lever op til reglerne og det giver jer et billede af, hvilke tiltag I skal sætte i gang. Det er også i denne fase, at I prioriterer, hvad I skal starte med.

4. **Få aftaler på plads**
   I denne fase sikrer I jer det juridiske grundlag for at kunne behandle persondata, udarbejder retningslinjer og sikrer jer en passende dokumentation. Det inkluderer bl.a. indhentning af databehandleraftaler, aftaler om henvendelse fra registrerede og ved databrud, opsætning af sletteregler og kontroller og evt. oplæg til justering af IT-sikkerhed.

### 5. Udbred kendskabet

I denne fase udbreder I kendskabet til persondataforordningen i hele gruppen eller enheden. I sætter jeres medspejdere ind i de nye regler og ikke mindst, hvordan I har valgt at efterleve dem hos jer. Hvordan I gør dette, er op til jer selv og jeres fantasi, men det er en vigtig fase, idet der bliver samlet op på arbejdet med persondataforordningen, den data I behandler og de nye regler skal 'efterprøves i praksis'.

### 6. En ny rutine

Nu er det vigtigt, at I sikrer jer, at jeres nye regler for håndtering af persondata efterleves internt i enheden (gennem kontroller) og at jeres processer og datahåndtering opdateres, når der ex indgås nye samarbejdsaftaler eller lign. Det er også i denne fase, at vi for alvor lærer, hvordan forordningens regler skal forstås i praksis, når Datatilsynet starter sine kontroller og der falder afgørelser i persondatasager. De afgørelser skal vi huske at tilpasse vores egen praksis efter. Her står korpset naturligvis klar med råd og anbefalinger.

# FAQ

### ”Hvad betyder det, at vi er selvstændige dataansvarlige?”

Svar: Det betyder bl.a. at I selv skal påvise et dataansvar herunder leve op til dokumentationskravet, som er beskrevet nærmere i denne vejledning. Den juridiske vurdering af vores selvstændige dataansvar bygger bl.a. på følgende faktorer: I korpset, grupperne og enhederne har man egne medlemmer tilknyttet, egne bestyrelser, selvstændige økonomier, egne leverandører, eget CVR og kan søge tilskud uafhængigt af korpsene. Det er altså den fortolkning, at man er medlem af en lokalforening, som er organiseret i en landsorganisation, som man dermed er medlem af også, gennem lokalforeningen.

### ”Hvordan ved jeg, hvem der er vores databehandlere?”

Svar: Dem som behandler personoplysninger på vegne af en dataansvarlig, er databehandlere, ex. Medlemsservice, Dropbox, Google men også regnskabssystemer og mailudbydere kan være databehandlere. Korpset er databehandler for grupper og enheder ved indhentelse af børneattester.
En god tommelfingerregel er, at kan du bede din databehandler om at slette den data der behandles på dine vegne helt, er det en databehandler, modsat en selvstændig dataansvarlig som ex. SKAT.

### ”Er vi ansvarlige for at Medlemsservice lever op til reglerne?”

Svar: I er ansvarlige for at dokumentere jeres håndtering af persondata i Medlemsservice og for at have en gyldig dataaftale med korpset, som har en aftale med Medlemsservice I/S, hvori reglerne for samarbejdet er ridset op. I/S’et står som korpsets, gruppernes og enhedernes databehandler på mål for at medlemssystemet overholder forordningens regler. Dataaftalen blev udsendt i april 2018 og indeholder både en aftale om fællesdataansvar for de oplysninger der behandles i Medlemsservice og en databehandleraftale mellem korpset og grupper/enheder i forhold til indhentning af børneattester.

Korpset har udarbejdet en privatlivspolitik for medlemskab i korpset, grupperne og enhederne.

Vær opmærksomme på, at bruger jeres gruppe eller enhed ikke den online indmeldelsesformular i Medlemsservice, skal I selv opdatere jeres formularer i forhold til bl.a. at henvise til korpsets persondatapolitik.

### ”Hvordan lever vi op til den registreredes ret til at blive glemt/slettet?”

Svar: I behandlingen af den data, I selv administrerer (uden for Medlemsservice), skal I slette oplysninger, hvis I bliver bedt om det – MEN – kun hvis der ikke er andre (evt. retlige) forpligtelser, I skal leve op til.

Eksempel: Et medlem ringer og beder om at blive meldt ud og at al data skal slettes. I denne konkrete sag kan I ikke bare slette alle medlemmets data, da I jf. bogføringsloven har pligt til at gemme oplysninger i op til 5 år + indeværende.

### ”Hvad er reglerne for brug af billeder på hjemmesider og sociale medier?”

Svar: Portrætbilleder skal du altid indhente samtykke for at bruge[2]. Situationsbilleder kan du som udgangspunkt anvende, uden at du har spurgt om tilladelse. Situationsbilleder er billeder, hvor det primære motiv/formål er at vise en situation – fx spejdere der laver en aktivitet. Det gør ikke noget, at man kan gen-

[2] Datatilsynet ændrede i september 2019 praksis i forhold til offentliggørelse af billeder på nettet. Hvor offentliggørelse af portrætbilleder tidligere har krævet et udtrykkeligt samtykke lægges der nu op til, at en offentliggørelse af portrætbilleder uden samtykke fra den berørte person beror på en helhedsvurdering af billedet og formålet med offentliggørelsen. Man satte i sin tid Medlemsservice op til at kunne håndtere samtykke til portrætbilleder og det står uændret efter Datatilsynets nye vurdering af den grund, at det for mange af jer, er rart med et overblik over de spejdere, der ikke ønsker deres billeder offentliggjort, hvilket de naturligvis stadig har ret til at frabede sig.

kende personer på situationsfotoet, når blot det er klart, at hensigten med billedet mere er at vise situationen end den enkelte person. Personen/personerne på billedet må ikke føle sig udstillet, så overvej om der kan være en chance for, at en spejder vil finde billedet pinligt - billederne skal være harmløse.

Billeder må aldrig bruges til andet formål end det, de er indsamlet til uden forudgående samtykke.
(Se link til Datatilsynets regler på området under afsnittet 'Læs mere').

### "Hvornår skal vi have samtykke?"

Svar: Forsøg kun at bruge samtykke som behandlingsgrundlag, når der ikke er andre hjemler for behandlingen. Samtykke kan nemlig være et svært grundlag at arbejde med, da det til enhver tid kan tilbagekaldes.

### "Skal vi have samtykke for at indhente oplysninger om allergier og lign. i forbindelse med ture og arrangementer?"

Svar: Helbredsoplysninger er følsomme og kræver derfor i langt de fleste tilfælde et udtrykkeligt samtykke. Det samtykke indhentes allerede ved indmeldelse, så I skal ikke indhente det på hvert enkelt arrangement. I er dog stadig forpligtede til at slette oplysningerne, når I ikke længere har brug for dem.

### "Hvornår er en spejder gammel nok til selv at afgive samtykke?"

Svar: Den danske lovgivning lægger op til, at man som 13-årig kan give samtykke. Det er dog en forudsætning, at samtykket er formuleret i et klart og simpelt sprog. Datatilsynets praksis har holdt sig til 15 år, men helt konkret er der tale om en vurdering af modenheden. Er en spejder derfor under 13 år gammel, skal forælder/værge samtykke til at der indsamles helbredsoplysninger og tages billeder til kommunikation om spejder i trykte, digitale og sociale medier herunder Facebook.

### "Hvordan håndterer jeg cpr-numre i forbindelse med indhentelse af børneattester?"

Svar: Når du som medlemsansvarlig vil indhente en børneattest på en leder i Medlemsservice, behøver du ikke have de sidste fire chifre i medlemmets personnummer. Læs mere om hvordan du nemt og sikkert indhenter børneattester her.

### "Skal vores frivilliges data behandles anderledes end medlemmernes?"

Svar: Nej. Indhenter I oplysninger på de få af jeres frivillige der (endnu) ikke er medlem af korpset, skal I sørge for kun at indhente de oplysninger, der er nødvendige i forbindelse med deres virke i gruppen og enheden. I skal overholde oplysningspligten som for medlemmer og deres oplysninger gemmes forsvarligt af vejen i aflåst skuffe/skab og bl.a. opdateres, udleveres og slettes ved anmodning fra den frivillige.

### "Hvad er reglerne for deling af oplysninger internt i gruppen i forbindelse med afholdelse af ture/arrangementer/lejre?"

Svar: I må gerne dele oplysninger internt i gruppen eller enheden. I er dog stadig forpligtet til at sikre jer, at kun relevant data deles med relevante personer, som har de fornødne rettigheder til at se den info, I deler. Ex har et madhold meget sjældent brug for at se de tilmeldtes kontaktinfo og lign. men kun eventuelle tilpasninger i kosten, så her vil det give mening at redigere lidt i listen, inden den deles med madholdet. Fjerner I personoplysningerne helt og efterlader kun kommentar til kost, kan listen deles frit.

Printer I lister/stamkort ud i forbindelse med ture, skal I sørge for at få dem makuleret igen umiddelbart efter endt tur. Sker dette ikke, skal I argumentere for, hvordan de håndteres efterfølgende og at det er i overensstemmelse med forordningen. Et godt fif er at fremsøge oplysningerne på mobilversionen af Medlemsservice i stedet for at printe dem.

### ”Må jeg videregive oplysninger til aktører uden for gruppen/enheden, ex i forbindelse med en tur?”

Eksempel: I skal på sommerlejr i England og har i den forbindelse brug for at dele pasoplysninger med flyselskabet. I vil også gerne sende jeres venskabsgruppe nogle af spejdernes oplysninger i forbindelse med koordinering af aktiviteter.

Svar: I dette tilfælde informerer I ved tilmelding spejderne om, hvilke oplysninger der deles med flyselskabet og venskabsgruppen og hvad formålet med delingen er.

Deler I persondata uden for gruppen og enheden, skal I altså huske at informere om det på forhånd. Står I en situation, hvor I efter tilmelding finder ud af, at I er nødt til at dele oplysningerne eksternt, skal I indhente samtykke inden de deles.

### ”Er referater omfattet af persondataforordningen?”

Svar: Referater fra jeres møder indeholder også persondata, så overvej hvor de gemmes og om de alle egner sig til offentliggørelse.

## Læs mere

- dds.dk/persondata
  Herunder bl.a.:
  - Vejledninger
  - Skabeloner
  - Aftaledokumenter
  - Generel info om forordningen
  - Sammendrag af GDPR-nyhedsbreve fra korpset

- Generelt om databeskyttelse på Datatilsynets hjemmeside

  Herunder bl.a.:

  - Hvad er personoplysninger og hvornår må du behandle dem?
  - Ofte stillede spørgsmål
  - Vejledninger, ex
    - Samtykke
    - Dataansvarlige og databehandlere
    - Vejledning om fortegnelse
    - Registreredes rettigheder

  - Datatilsynets råd om brug af billeder på internettet

- Billigere software og digitale løsninger til frivillige foreninger

- Regler for foreningers brug og behandling af personoplysninger (Center for frivilligt socialt arbejde)