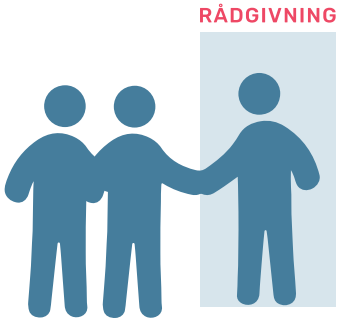
Rådgivnings Danmark

VEJLEDNING TIL RÅDGIVNINGER OM DATABESKYTTELSES-FORORDNINGEN OG -LOVEN

Revideret udgave februar 2023

Til sociale rådgivningstilbud der er medlem af RådgivningsDanmark

GUIDE



INDHOLD

INDLEDNING

Denne vejledning er udarbejdet til sociale rådgivningstilbud, der er medlem af Rådgivnings-Danmark. Formålet med vejledningen er at sikre en fælles forståelse på tværs af rådgivningsfeltet af, hvad reglerne om behandling af personoplysninger betyder for branchen samt understøtte RådgivningsDanmarks medlemsorganisationer i at leve op til lovgivningen.

I 2016 blev databeskyttelsesforordningen vedtaget af EU. Forordningen er direkte gældende i Danmark og er suppleret af en dansk databeskyttelseslov. Tilsammen afløser disse de tidligere regler.

Mange af databeskyttelsesforordningens begreber, principper og regler er allerede kendt fra den gamle lovgivning. Forordningen indeholder imidlertid også en række nyskabelser, der har til formål at styrke beskyttelsen af personoplysninger. Databeskyttelsesforordningen gælder både for offentlige myndigheder samt private virksomheder og organisationer. Foreninger og rådgivningstilbud skal som udgangspunkt betragtes som private aktører i forhold til forordningen. Der vil dog også være nogle med status af offentlig instans, fx foreninger der har driftsoverenskomster med kommuner.

Overordnet lægger forordningen vægt på, at man har gjort sig fornuftige overvejelser om, hvilke personoplysninger man behandler, samt hvorfor og hvordan man behandler dem. Disse overvejelser skal kunne dokumenteres over for Datatilsynet. Forordningen giver på en del områder mulighed for at vælge de løsninger, der giver mening i den enkelte rådgivning – og er inden for lovens rammer naturligvis. Der er altså ikke nødvendigvis kun én rigtig måde at gøre tingene på.

Med denne vejledning ønsker RådgivningsDanmark at give et overblik over de væsentligste databeskyttelsesregler og problemstillinger, som har betydning på forenings- og rådgivnings-området. Vejledningen beskriver reglerne i hovedtræk og er derfor ikke udtryk for en fuldstændig gennemgang af databeskyttelsesforordningens og lovens bestemmelser. Man kan med fordel orientere sig i Datatilsynets vejledninger om forordningen, der ligger på tilsynets hjemmeside og løbende bliver opdateret. Se links til sidst i vejledningen.

REVIDERET UDGAVE

Dette er første reviderede udgave af vejledningen. Den vil løbende blive opdateret i takt med, at Datatilsynet træffer afgørelser, og ny viden opstår.

Revideringen gælder blandt andet:

- **CPR-numres status**
  CPR-numre har status af en fortrolig oplysning – hverken almindelig eller følsom oplysning - og er særskilt reguleret i databeskyttelsesloven.

- **Krav om krypterede mails**
  E-mails med fortrolige eller følsomme oplysninger skal sendes via krypteret mail.

- **Anmeldelsesordning og fortegnelseskrav**
  Kravet om en intern fortegnelses erstatter i nogle tilfælde den tidligere anmeldelsesordning hos Datatilsynet. Anmeldelsesordningen er således bevaret i databeskyttelsesloven, når der er tale om behandling efter artikel 9, stk. 2, litra g – behandling af følsomme oplysninger er nødvendig af hensyn til væsentlige samfundsinteresser.

- **Behandling af fotos**
  Det er lovligt at offentliggøre billeder af genkendelige personer – fx bestyrelsesmedlemmer og frivillige – uden at indhente samtykke, da Datatilsynet ikke længere skelner mellem situations- og portrætbilleder.

DEFINITION AF RELEVANTE BEGREBER

Personoplysninger
Enhver form for information, der kan henføres til bestemte personer, også selv om dette forudsætter kendskab til et personnummer, registreringsnummer eller lignende, betegnes personoplysninger. Oplysninger om en persons fysik, psyke, økonomiske, sociale eller kulturelle identitet er personoplysninger. Også oplysninger i form af fx et billede, et fingeraftryk eller en IP-adresse er personoplysninger.

Selv om oplysninger som navn eller IP-adresse er erstattet af en kode, er det stadig en person-oplysning, hvis koden med nogen rimelige hjælpemidler kan føres tilbage til den oprindelige oplysning. Dette betegnes også pseudonymisering, se side 6.

Datatilsynet har udarbejdet "Generel informationspjece om Databeskyttelsesforordningen", hvor ovenstående blandt andet er beskrevet.

Almindelige personoplysninger
De personoplysninger, der ikke falder ind under kategorien "følsomme personoplysninger", betegnes "almindelige personoplysninger". Almindelige personoplysningerne skal – ligesom følsomme oplysninger – behandles med fortrolighed, omtanke og efter de gældende regler. Almindelige personoplysninger kan fx være identifikationsoplysninger som navn og adresse, oplysninger om økonomiske og sociale forhold, sygedage, familieforhold, foto eller andre lignende ikke-følsomme oplysninger.

I den lovgivning, der gik forud for den nuværende, er blandt andet sygedage og væsentlige sociale problemer betragtet som følsomme personoplysninger. I forordningen betragtes de som almindelige personoplysninger.

Følsomme personoplysninger
Oplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering betragtes som følsomme personoplysninger. Listen her er udtømmende, det vil sige, at alle andre personoplysninger er almindelige.
CPR-nummer har status af en fortrolig oplysning, der er særskilt reguleret i databeskyttelsesloven.

Oplysninger om strafbare forhold
Oplysninger om strafbare forhold kan være en oplysning om, at en person har begået en bestemt lovovertrædelse, men det kan fx også være en oplysning om, at en person har adresse i et fængsel. Med andre ord er der tale om en oplysning om strafbare forhold, hvis det ud fra oplysningen kan udledes, at en person har begået noget strafbart. Regler om behandling af oplysninger om strafbare forhold er særskilt reguleret i data-beskyttelsesloven § 8.

En identificerbar person
Når en person kan direkte eller indirekte identificeres, betegnes vedkommende identificerbar. Det gælder også, selvom det kun er muligt for særligt indviede at forstå, hvem oplysningen vedrører, eller selvom der skal flere enkeltstående oplysninger til for at identificere vedkommende. En person er ikke identificerbar, hvis oplysningerne om vedkommende er fuldstændig anonymiserede.

Dataansvarlig
Den dataansvarlige er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der alene eller sammen med andre afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger.

Databehandler
En databehandler er en fysisk eller juridisk person, en offentlig myndighed, en institution eller et andet organ, der behandler personoplysninger på den dataansvarliges vegne.

Behandling af personoplysninger
Enhver håndtering af alle former for personoplysninger med eller uden brug af elektronisk databehandling. Det kan fx være indsamling, registrering, systematisering, opbevaring eller videregivelse af oplysninger. Behandling kan også være offentliggørelse af oplysninger på en hjemmeside, fx en liste over ansatte, fotos af frivillige eller sletning af oplysninger.

Pseudonymisering
Behandling af personoplysninger på en måde, så oplysningerne ikke længere kan henføres til en bestemt person uden brug af supplerende oplysninger, betegnes pseudonymisering. Oplysninger om navn eller IP-adresse, som er erstattet af en kode, der kan føres tilbage til den oprindelige oplysning, er eksempler på pseudonymisering. Pseudonymisering er blot én blandt flere sikkerhedsforanstaltninger, som forordningen beskriver.

Samtykke
Et samtykke er en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvor personen ved erklæring eller klar bekræftelse indvilliger i, at vedkommendes personoplysninger bliver behandlet, fx indsamlet, gemt eller videregivet.

Fortegnelse over behandlingsaktiviteter
Langt de fleste dataansvarlige og databehandlere er forpligtet til at føre en fortegnelse over behandling af personoplysninger. Kravet om at føre en fortegnelse er en intern forpligtelse. Det betyder blandt andet, at man kun efter anmodning skal sende sin fortegnelse til Datatilsynet. Fortegnelseskravet erstatter i nogle tilfælde den hidtil gældende anmeldelsesordning. Dog er dele af anmeldelsesordningen bevaret og beskrevet i databeskyttelsesloven.

HVILKE PERSONERS OPLYSNINGER BEHANDLER EN RÅDGIVNING?

Rådgivningstilbud behandler personoplysninger om en række forskellige målgrupper. Der vil for det første være tale om behandling af oplysninger om ansatte og frivillige samt i nogle tilfælde oplysninger om medlemmer. Disse oplysninger vil typisk bestå af almindelige personoplysninger som navn, adresse og CPR-numre, og måske af følsomme personoplysninger, fx helbredsoplysninger.

Der vil for det andet være tale om behandling af personoplysninger om brugere af rådgivningen. Dét at henvende sig i et rådgivningstilbud karakteriseres ikke som udgangspunkt som en følsom oplysning i forordningen. Dog betragtes helbredsmæssige – fysiske som mentale – oplysninger som følsomme, så hvis rådgivningen primært omhandler dette, vil selve henvendelsen ofte være en følsom oplysning i sig selv. Hvis brugere henvender sig til rådgivninger, hvor deres personoplysninger er fuldstændig anonymiserede, betegnes de som ikke-identificerbare, og registrering af fx brugernes køn og alder, betragtes ikke som en behandling af personoplysninger. Hvis brugerne henvender sig i fortrolige rådgivninger, hvor de fx aftaler en ny tid og i den forbindelse opgiver deres navn, telefonnummer og måske CPR-nummer, er deres oplysninger derimod personhenførbare og er således omfattet af lovgivningen.

KRYPTEREDE OPLYSNINGER KAN VÆRE PERSONHENFØRBARE

Vær opmærksom på, at krypterede oplysninger, fx et telefonnummer eller en IP-adresse, sjældent er at betragte som fuldstændig anonymiserede oplysninger, da det ofte vil være muligt for teleudbyderen at finde brugernes oprindelige kontaktoplysninger, fx hvis politiet beder udbyderen gøre det. Disse oplysninger betegnes som pseudonymiserede og skal behandles derefter.

I praksis betyder det, at telefon-, chat- og SMS-rådgivninger i en del tilfælde behandler personoplysninger, når de registrerer og gemmer forskellige baggrundsoplysninger, anonyme brugere giver i forbindelse med rådgivning. Generiske oplysninger, fx køn og alder, vil i sig selv ikke være personhenførbare oplysninger, selvom de kombineres med hinanden. Kombineres køn og alder derimod med fx et telefonnummer eller en IP-adresse, kan oplysningerne tilsammen være personhenførbare.

ANBEFALING: FÅ OVERBLIK OVER BEHANDLING AF PERSONOPLYSNINGER

Skab overblik over de personoplysninger, der bliver behandlet i rådgivningen, ved at stille jer selv nogle grundlæggende spørgsmål:

- Hvilke målgrupper behandler I personoplysninger for? Fx ansatte, frivillige og brugere.
- Hvilke typer – almindelige, fortrolige og følsomme – personoplysninger behandler I?
- Hvordan foregår indsamlingen af personoplysninger?
- Hvor bliver data gemt, og hvor gammel er den data, I har liggende?
- Til hvilket formål bliver personoplysningerne behandlet?
- Hvorfor har I lov til at behandle oplysningerne, med andre ord hvad er jeres behandlingshjemmel? Er det fx nødvendigt for at opfylde en kontrakt, fordi I har en legitim interesse i at behandle oplysningerne, eller fordi I har indhentet samtykke?
- Hvilke typer teknologier anvender I? Fx digitale databaser eller analoge arkivsystemer.
- Hvilken behandling finder sted? Fx opbevaring eller videregivelse til andre?
- Hvem har adgang til oplysningerne? Fx ansatte eller eksterne samarbejdspartnere.

KRAV OM BEHANDLINGSFORTEGNELSE

Forordningen stiller krav om, at langt de fleste dataansvarlige og databehandlere skal føre interne fortegnelser over deres behandling af personoplysninger. Fortegnelsespligten fremgår af databeskyttelsesforordningens artikel 30 og erstatter i et vist omfang anmeldelsespligten i den gamle lovgivning. Formålet med fortegnelsen er at kunne dokumentere, at behandlingen af personoplysninger overholder forordningens regler.

Foreninger og rådgivninger skal i langt de fleste tilfælde udarbejde en behandlingsfortegnelse. Fx kræver regelmæssig behandling af personoplysninger, såsom behandling i forbindelse med personaleadministration, og behandling af følsomme personoplysninger en fortegnelse.

Se Datatilsynets "Vejledning om fortegnelse", der indeholder en skematisk oversigt over, hvem der er forpligtet til at udarbejde en fortegnelse, og en skabelon til en behandlingsfortegnelse.

HVEM ER ANSVARLIG FOR BEHANDLING AF PERSONOPLYSNINGER?

Det har stor betydning for både interne procedurer samt eventuelle sanktioner fra Datatilsynet ved tilsyn, hvem der er dataansvarlig for behandling af personoplysninger. Det kan samtidig være relativt kompliceret at afgøre i større organisationer, hvor der kan være langt til de enkelte afdelinger. Der er en lang række kriterier i spil, når ansvaret som dataansvarlig, selvstændig databehandler eller databehandler skal placeres. Det har blandt andet betydning, hvorvidt enheden har selvstændig vedtægt, ledelse, økonomi og CVR-nummer.

Det er den dataansvarlige, der har ansvaret for at sikre, at der bliver gennemført passende tekniske og organisatoriske foranstaltninger for at sikre, at behandlingen af personoplysninger er i overensstemmelse med forordningen. For store foreninger kan der være langt fra hoved-administrationen til det konkrete – måske endda lokale – rådgivningstilbud. Her skal man være særligt opmærksom på, hvorvidt rådgivningstilbuddet kan betragtes som en selvstændig enhed og dermed som dataansvarlig eller selvstændig databehandler.

Forordningens artikel 24 og 25 beskriver, at det er den dataansvarliges ansvar at foretage passende tekniske og organisatoriske foranstaltninger i forbindelse med behandling af personoplysninger under hensyntagen til det aktuelle tekniske niveau, implementerings-omkostninger med mere.

Hvis foreningen både selv er opdragsgiver til behandling af personoplysninger og desuden selv behandler oplysningerne, er foreningen både dataansvarlig og -behandler. Man vil i de tilfælde blot omtale foreningen som dataansvarlig, og det er ikke nødvendigt at indgå databehandleraftaler med sig selv.

NÅR MAN ER FLERE DATAANSVARLIGE OM BEHANDLING AF PERSONOPLYSNINGER

Forordningens artikel 26 beskriver de situationer, hvor to eller flere aktører i fællesskab fastlægger formålene med behandling af personoplysninger. Et eksempel kunne være et samarbejde mellem en kommune og en forening om borgere, der skal støttes i at komme i beskæftigelse, eller et samarbejde mellem to organisationer om en undersøgelse af børns oplevelse med mobning. Parterne vil i de tilfælde typisk være fælles dataansvarlige.

De dataansvarlige skal på en gennemsigtig måde fastlægge deres respektive ansvar for overholdelse af forpligtelserne i henhold til forordning. Det kan man med fordel gøre i forlængelse af kontrakten for samarbejdet. Det væsentligste indhold af aftalen mellem de dataansvarlige i relation til forordningen skal være tilgængelig for de personer, hvis oplysninger bliver behandlet.

RÅDGIVNINGER MED DRIFTSOVERENSKOMSTER SKAL HAVE EN DPO

I forordningens artikel 37 omtales en databeskyttelsesrådgiver (på engelsk Data Protection Officer - DPO), som skal være uvildig og uafhængig og sikre, at organisationens behandling af personoplysninger er i overensstemmelse med forordningen. Foreninger er forpligtet til at have en DPO, hvis de betragtes som offentlige.

Selvejende institutioner med en driftsoverenskomst eller lignende partnerskab med en kommune betragtes som offentlige og skal derfor have en DPO. I de tilfælde vil man have mulighed for at udpege en fælles DPO med en anden selvejende institution omfattet af samme lovgivning eller fx den kommune, som foreningen har driftsoverenskomst med, i det omfang kommunen yder sekretariatsbistand til institutionen.

Læs den fulde definitionen af, hvornår man er en offentlig myndighed i Datatilsynets "Vejledning om databeskyttelsesrådgivere".

ANBEFALING: UDPEG EN ANSVARLIG FOR BEHANDLING AF PERSONOPLYSNINGER

Uanset om foreningen har en DPO, bør man udpege en ansvarlig for behandling af person-oplysninger. Det er vigtigt, at vedkommende får frigjort tid til at sætte sig ind i lovgivningen og løbende følge op på de interne processer. Vedkommendes kontaktoplysninger skal fremgå af foreningens privatlivspolitik.

Det vil aldrig være en enkeltperson, der er dataansvarlig, selvom foreningen har udpeget en medarbejder med ansvar for behandling af personoplysninger. Den dataansvarlige er altid en organisation, fx hovedorganisationen eller en selvstændig enhed.

OM DATABEHANDLERE

Der vil være mange situationer, hvor den dataansvarlige har brug for at inddrage eksterne aktører til at behandle personoplysninger for sig. Det kan fx være, at en forening har brug for at hyre et konsulentfirma til at undersøge brugernes tilfredshed med rådgivningen eller har brug for en nyhedsbrevs- eller en chatudbyder til at levere digitale ydelser til rådgivningen og dens frivillige eller brugere. Når en ekstern aktør behandler personoplysninger på vegne af den dataansvarlige, bliver denne betegnet databehandler.

Det er den dataansvarlige, der har ansvaret for at sikre, at databehandlere træffer de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger i forhold til at beskytte personoplysninger.

Den dataansvarlige skal sikre dette ved at indgå databehandleraftaler med de eksterne aktører. Databehandleraftaler skal pålægge den eksterne aktør at sikre de nødvendige sikkerhedsforanstaltninger, så behandlingen lever op til kravene i forordningen og lovgivningen. Læs Datatilsynets "Vejledning om dataansvarlige og databehandlere" og se skabelon til en databehandleraftale.

VÆR OPMÆRKSOM PÅ DATABEHANDLERE UDEN FOR EU/EØS

Man skal være opmærksom på, om man bruger databehandlere lokaliseret i lande uden for EU/EØS området. Da forordningen kun gælder for lande inden for EU/EØS området, er det den dataansvarliges ansvar at sikre, at databehandlere uden for kan garantere, at der forefindes lovligt grundlag for overførsel af personoplysninger. Det er lovligt, hvis virksomheden uden for EU/EØS lever op til EU's Privacy Shield eller EU Model Clauses. Amerikanske Mailchimp, som mange bruger til at udsende nyhedsbrev, er et eksempel på en virksomhed, der er EU-U.S. Privacy Shield certificeret.

HVORNÅR MÅ PERSONOPLYSNINGER BEHANDLES?

Reglerne for, hvornår personoplysninger må behandles, afhænger af en konkret vurdering af, om betingelserne for at behandle personoplysninger er opfyldt.

IKKE-PERSONHENFØRBARE OPLYSNINGER

Behandling, fx registrering og opbevaring, af ikke-personhenførbare oplysninger er ifølge forordningen ikke omfattet af lovgivningen. Med andre ord er det ikke behandling af personoplysninger, hvis en anonym rådgivning alene registrerer fx fremmødte brugeres alder og køn. Det er dog god skik at orientere brugere, hvis man registrerer generiske, ikke-personhenførbare oplysninger, og forklare til hvilket formål.

Vær opmærksom på, at oplysninger om brugere, der henvender sig via digitale rådgivnings-tjenester, sjældent vil kunne betegnes fuldstændig anonymiserede, men derimod som pseudonymiserede oplysninger, se side 6.

GRUNDLÆGGENDE PRINCIPPER FOR BEHANDLING

De grundlæggende principper for, hvornår personoplysninger må behandles, findes i forord-ningens artikel 5 og er desuden beskrevet i Datatilsynets "Generelle informationspjece om forordningen". Disse skal altid være overholdt, uanset hvilket retligt grundlag man som rådgivning har for at behandle personoplysninger. Principperne er:

Lovlighed, rimelighed og gennemsigtighed
Den dataansvarlige skal overholde reglerne for behandling af oplysninger og skal give let tilgængelig information om behandlingen af oplysninger. Det indebærer blandt andet, at den person, der behandles oplysninger om, som udgangspunkt skal have oplyst, hvem der er ansvarlig for behandlingen af oplysninger, og hvad der er formålet med behandlingen.

Formålsbegrænsning
Når der indsamles oplysninger, skal den dataansvarlige gøre sig klart, hvilke formål oplysningerne indsamles til, og det skal være saglige formål. Man må ikke indsamle oplysninger med den begrundelse, at det måske senere kan vise sig nyttigt at være i besiddelse af oplysningerne. Samtidig åbner forordningen op for, at formålet godt kan ændre sig, så længe det er foreneligt med det oprindelige. Statistik, forskning og kvalitetssikring vil typisk blive vurderet som et foreneligt formål.

Det er i første omgang den organisation eller myndighed, der indsamler oplysninger, som skal vurdere, om en bestemt indsamling af oplysninger er saglig. Derudover kan formålets saglighed blandt andet bedømmes ud fra, om indsamlingen sker i forbindelse med løsningen af en opgave, som det er naturligt for organisationen at løse. Endelig har det betydning for vurderingen af indsamlingens saglighed, at den registrerede er oplyst herom.

Dataminimering
Behandlingen af personoplysninger skal begrænses til det, der er nødvendigt for at opfylde formålet. Det betyder også, at man bør rydde op i og slette data, så snart data ikke længere har et sagligt og nødvendigt formål.

Rigtighed
Oplysningerne skal være rigtige og ajourførte, og hvis oplysningerne viser sig at være urigtige, skal de som udgangspunkt slettes eller berigtiges. Dette princip stiller krav til etablering af interne procedurer og retningslinjer, der sikrer ajourføring, fx løbende oprydning og retningslinjer for sletning.

Opbevaringsbegrænsning
Personoplysninger skal slettes eller gøres anonyme, når det ikke længere er nødvendigt for den dataansvarlige at have oplysningerne. Det er i første omgang op til den enkelte dataansvarlige at vurdere, hvor længe det er nødvendigt at opbevare oplysningerne ud fra det formål, som oplysningerne oprindelig blev indsamlet til.

Integritet og fortrolighed
Oplysninger skal beskyttes mod uautoriseret eller ulovlig behandling, ligesom det skal sikres, at oplysninger ikke går tabt eller bliver beskadiget. Dette princip stiller krav til de sikkerhedsmæssige foranstaltninger omkring behandlingen af personoplysninger.

SPECIELLE LOVBESTEMMELSER GÅR FORUD FOR DATABESKYTTELSESFORORDNINGEN

Speciel lovgivning, fx straffeloven, serviceloven og skattereglerne, går altid forud for forordningens generelle bestemmelse om databeskyttelse. Med andre ord kan der aldrig opstå regelkonflikt mellem andre lovbestemmelser og forordningen.

I praksis betyder det fx, at arbejdsgivers pligt til indberetning af løn til SKAT er reguleret af skattereglerne og ikke af forordningen – og skulle der være en konflikt imellem bestemmelserne i forordningen, vil det altid være skattereglerne, der går forud.

RETLIGT GRUNDLAG FOR BEHANDLING AF ALMINDELIGE PERSONOPLYSNINGER

Behandling af almindelige personoplysninger er beskrevet i artikel 6 og er kun lovlig, hvis mindst én – gerne flere – af de oplistede forhold gør sig gældende. De mest relevante retlige grundlag for rådgivningsfeltet er fremhævet.

a) **Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.**
Hvis man som rådgivning ønsker at indsamle og opbevare kontaktoplysninger på en pårørende til de ansatte eller frivillige i en rådgivning, som kan kontaktes i tilfælde af en krisesituation, bør man indhente samtykke hertil.

Hvis en rådgivning ønsker at sende en påmindelse per SMS om en aftale til sine brugere, vil det typisk også være relevant at indhente brugerens samtykke til at modtage sådan én. Her skal man huske, at samtykket skal være specifikt, det vil sige, at samtykket ikke giver carte blanche til at sende alle mulige informationer, fx om nye åbningstider, men kun til at sende en reminder om en aftale.

b) **Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.**
I forbindelse med ansættelse, indmeldelse eller at melde sig som frivillig er det nødvendigt at behandle en række almindelige personoplysninger som navn, telefonnummer og i nogle tilfælde bankoplysninger for at kunne opfylde kontrakten mellem parterne.

I de fleste rådgivninger er det en forudsætning for at blive ansat eller frivillig, at man underskriver en tavshedspligtserklæring, der også gælder efter ansættelsens ophør. Med andre ord er det nødvendigt at indsamle og opbevare disse erklæringer for at kunne indgå kontrakt med ansatte eller aftale med frivillige. Kravet om en tavshedspligtserklæring kan med fordel desuden fremgå af andre formelle dokumenter, fx af ansættelseskontrakten eller foreningens vedtægter.

c) **Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.**
Langt de fleste retlige forpligtelser, en rådgivning har i forbindelse med behandling af personoplysninger, vil være reguleret af anden lovgivning, fx skattereglerne, bogføringsloven eller serviceloven. Man kan i de tilfælde med fordel omtale både de relevante lovgivninger og denne hjemmel i privatlivspolitikken og behandlingsfortegnelsen.

d) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.
Vil sjældent være aktuelt for rådgivninger.

e) **Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.**
Dette retlige grundlag kan være relevant for mange rådgivninger på det sociale område, hvis behandling af personoplysninger er i samfundets interesse, fordi rådgivningerne løfter vigtige sociale opgaver. Fx kan det være relevant for en rådgivning at notere og opbevare oplysninger om brugeres økonomiske forhold i forbindelse med økonomisk rådgivning, der kræver en opfølgende samtale i rådgivningen.

f) **Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.**
Dette behandlingsgrundlag kaldes også for "interesseafvejningsreglen". Fx har rådgivningskoordinatoren en legitim interesse i at kunne rundsende et vagtskema blandt de frivillige i en rådgivning. Husk her at overveje, hvilke personoplysninger, der er relevante at rundsende, fx er hjemmeadresse sjældent relevant. Ligeledes har en rådgivning en legitim interesse i at registrere og opbevare mailadresser på de personer, som tilmelder sig rådgivningens nyhedsbrev, indtil de ikke længere ønsker at modtage det. Rådgivningen kan også have en legitim interesse i, at de frivilliges foto hænger i rådgivningen, så alle kan se, hvem der er frivillig, og fx hvem der er på vagt. Billedet må naturligvis hverken udstille, udnytte eller krænke den eller de personer, som er på billedet.

Dette behandlingsgrundlag er også aktuelt, når en bruger søger gældsrådgivning eller retlig bistand, hvor det oftest er relevant at gemme oplysninger om vedkommendes økonomiske situation eller sag for at kunne gennemføre en meningsfyldt opfølgende samtale.

RETLIGT GRUNDLAG FOR BEHANDLING AF FØLSOMME PERSONOPLYSNINGER

Behandling af følsomme personoplysninger er som udgangspunkt forbudt. Forordningens artikel 9 beskriver imidlertid en række undtagelser til forbuddet:

a) **Den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål.**
I rådgivninger, der behandler følsomme oplysninger om deres brugere, og hvor der foregår en eller anden form for journalføring, fx fordi brugerne er i et forløb, kan det være relevant at indhente samtykke fra brugeren til at notere og opbevare personoplysninger.

b) **Behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder.**
Langt de fleste retlige forpligtelser, en rådgivning har i forbindelse med behandling af følsomme personoplysninger, vil være reguleret af anden lovgivning, fx sygedagpengeloven

eller straffeloven. Man kan i de tilfælde med fordel omtale både de relevante lovgivninger og denne hjemmel i privatlivspolitikken og behandlingsfortegnelsen.

c) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke. Vil sjældent være aktuelt for rådgivninger.

d) **Behandling foretages af en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i organets legitime aktiviteter og med de fornødne garantier, og på betingelse af at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at personoplysningerne ikke videregives uden for organet uden den registreredes samtykke.**
Dette retlige grundlag er blandt andet relevant for foreninger, hvor medlemskab i sig selv er en følsom personoplysning, såsom foreninger af religiøs karakter. Hvis foreningen fx gerne vil rundsende en deltagerliste til deltagerne i et konkret arrangement, kan dette retlige grundlag anvendes. Husk her at overveje, hvilke personoplysninger, der er relevante at rundsende, fx er telefonnummer måske ikke relevant i denne sammenhæng.

e) **Behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede.**
Hvis et medlem af en sygdomsrelateret forening medvirker i en artikel om sin sygdomshistorik i foreningens fagblad, der bliver udsendt til en stor medlemsskare og lagt online, har vedkommende selv offentliggjort disse oplysninger, og behandling kan derfor finde sted.

f) Behandling er nødvendig for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol.
Vil sjældent være aktuelt for rådgivninger.

g) **Behandling er nødvendig af hensyn til væsentlige samfundsinteresser.**
Dette retlige grundlag kan være relevant for mange rådgivningstilbud på det sociale område og sundhedsområdet, hvis behandling af følsomme personoplysninger er i samfundets interesse, fordi rådgivningerne løfter vigtige sociale opgaver. Fx kan det være relevant for en rådgivning at indsamle og opbevare en brugers helbredsmæssige oplysninger i forbindelse med rådgivning om livet med sygdom til en opfølgende samtale i rådgivningen.

Dette behandlingsgrundlag skal kombineres med en behandlingstilladelse fra Datatilsynet. Det er reguleret i databeskyttelseslovens § 7, stk. 4. Læs mere herom side 17. Se Rådgivnings-Danmarks "Guide til behandling af personoplysninger ifm. telefonisk og digital rådgivning" (2019).

h) Behandling er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester.
Vil sjældent være aktuelt for rådgivninger.

i) Behandling er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, fx beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr.
Vil sjældent være aktuelt for rådgivninger.

j) **Behandling er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1.**
Det kan fx være nødvendigt at indsamle og opbevare kvantitative og kvalitative følsomme personoplysninger, hvis et rådgivningstilbud forsker i eller skriver videnskabelige artikler om en helbredsmæssig problematik.

Selvom én af ovenstående betingelser er opfyldt, må behandlingen kun finde sted, så længe den ikke strider imod de grundlæggende principper i forordningens artikel 5, se side 12.

SØG TILLADELSE TIL BEHANDLING AF FØLSOMME OPLYSNINGER HOS DATATILSYNET

Når en rådgivning har brug for at behandle følsomme oplysninger, fx helbredsmæssige oplysninger om brugere, skal der findes et retligt grundlag for behandlingen i forordningens artikel 9, stk. 2. Hvis det retlige grundlag er "Behandling er nødvendig af hensyn til væsentlige samfundsinteresser", jf. artikel 9, stk. 2 litra g, skal Datatilsynet give tilladelse til behandlingen. Alternativt kan et samtykke fra brugeren være en mulighed.

Indhentelse af tilladelse fra Datatilsynet fremgår ikke eksplicit af forordningen, men derimod af databeskyttelseslovens § 7, stk. 4.

Tilladelse indhentes ved at kontakte Datatilsynet. Der findes ingen skabelon eller formular hertil. RådgivningsDanmark har udarbejdet en guide om indhentelse af tilladelse, "Guide til behandling af personoplysninger ifm. telefonisk og digital rådgivning" (2019).

BEHANDLING AF PERSONOPLYSNINGER TILLAGT HØJERE GRAD AF BESKYTTELSE

CPR-numre og oplysninger om strafbare forhold har karakter af en særlig fortrolig oplysning og er reguleret i databeskyttelsesloven § 8. Det betyder, at disse typer oplysninger skal være bedre beskyttet end almindelige personoplysninger, som fx et telefonnummer.

KRYPTEREDE MAILS SKAL BENYTTES VED FØLSOMME ELLER FORTROLIGE OPLYSNINGER

Datatilsynet stiller krav om, at e-mails med følsomme eller fortrolige oplysninger skal krypteres. Det betyder blandt andet, at e-mails, der indeholder CPR-numre, skal sendes via en krypteret forbindelse, ligesom rådgivninger, der tilbyder rådgivning per e-mail og beskæftiger sig med helbredsmæssige oplysninger, skal benytte sig af krypteret mail.

SAMTYKKET

Et samtykke kan både afgives mundtligt, skriftligt og digitalt. Det afgørende er, at det er frivilligt, specifikt, informeret og utvetydigt. Ellers kan det ikke anvendes som retligt grundlag for behandling af almindelige og følsomme personoplysninger. Det betyder blandt andet, at samtykket ikke bliver givet stiltiende eller underforstået. Fx er en forhåndsafkrydset boks i en digital meddelelse ikke udtryk for et utvetydigt samtykke – man skal altså aktivt selv sætte fluebenet.

I en del tilfælde vil det være muligt at finde et andet retligt grundlag end samtykke til behandling, og i de tilfælde bør man ikke benytte samtykke, men fx bestemmelsen om, at behandling er nødvendig for at opfylde en kontrakt, jf. artikel 6, stk. 1, litra b, eller er nødvendig af hensyn til væsentlige samfundsinteresser, jf. artikel 9, stk. 2, litra g. Det er også vigtigt at huske, at et samtykke ikke giver carte blanche til at behandle personoplysninger, præcis som man ønsker. Artikel 5, de grundlæggende principper for behandling, skal altid overholdes.

SAMTYKKE MÅ ALDRIG VÆRE EN BETINGELSE

Et samtykke må aldrig være en betingelse for at modtage en ydelse, deltage eller lignende, for så er det ikke længere et frivilligt samtykke.

Fx må et samtykke ikke danne grundlag for at blive frivillig i et rådgivningstilbud eller modtage rådgivning. Hvis en frivillig ikke vil give samtykke til, at vedkommendes private mailadresse bliver lagt på hjemmesiden, vil det være svært at argumentere sagligt for, at vedkommende – af den grund – ikke kan være frivillig. Hvis det derimod er en forudsætning for at blive frivillig at give sin mailadresse til rådgivningskoordinatoren, for at denne kan tilrettelægge rådgivningen, er et samtykke ikke det korrekte retlige grundlag for at indsamle mailadressen. I det tilfælde vil interesseafvejningsreglen finde anvendelse, fordi rådgivningstilbuddet forfølger en legitim interesse, når den indsamler mailadresser til koordineringen af de frivilliges arbejde.
Se Datatilsynets "Vejledning om samtykke", der også indeholder en tjekliste.

Samtykket skal være indhentet, før behandling af oplysninger begynder, og det skal være personhenførbart, det vil sige, det skal være tydeligt, hvem der har givet samtykke, ellers fungerer det ikke som et samtykke. En anmodning om samtykke skal desuden være let tilgængelig og forståelig. For rådgivninger kan det betyde, at man sprogligt skal versionere samtykket til de forskellige målgrupper. Fx én version til ansatte og frivillige og en anden til brugere af rådgivningen.

Et samtykke kan til enhver tid trækkes tilbage, jf. artikel 7, stk. 3. Hvis dét sker, må den data-ansvarlige ikke længere behandle de oplysninger, der er blevet givet på grundlag af samtykket. Derfor skal den registrerede også vide – inden vedkommende giver samtykke – at vedkommende kan trække samtykke tilbage og hvordan.

ANBEFALING: DOKUMENTÉR MUNDTLIGE SAMTYKKER SKRIFTLIGT

Hvis det ikke er muligt at få et skriftligt samtykke fra brugere af en rådgivning, fx i telefonrådgivninger, er det rådgivernes ansvar at dokumentere, at brugerne har givet et mundtligt frivilligt, specifikt, informeret og utvetydigt samtykke til behandling af deres personoplysninger.

For at kunne løfte bevisbyrden for et mundtligt samtykke bør rådgivninger dokumentere de interne procedurer for indhentelse af mundtlige samtykker i behandlingsfortegnelsen. Med andre ord bør man beskrive, hvordan rådgiverne oplyser brugerne om deres rettigheder, hvordan rådgiverne bliver oplært i at give de lovbestemte oplysninger til brugerne, og hvordan rådgiverne registrerer samtykket.

SÆRLIGE REGLER FOR BØRNS SAMTYKKE

Børn skal efter databeskyttelsesforordningen have en særlig beskyttelse, fordi de er mindre bevidste om de risici og konsekvenser, der kan være forbundet med behandling af personoplysninger. Beskyttelsen handler særligt om børns personoplysninger med henblik på markedsføring eller informationstjenester, fx online spil og sociale medier. Aldersgrænsen for, hvornår børn selv kan give samtykke, er fastsat til 13 år herhjemme.

Der er dog formuleret en undtagelse fra denne regel, når det gælder forebyggende eller rådgivende tjenester, der tilbydes direkte til børn. Disse tjenester er ikke omfattet af kravet om samtykke, idet børn i alle aldre skal kunne henvende sig til rådgivningstilbud uden forældremyndighedsindehaverens samtykke.

DEN REGISTREREDES RETTIGHEDER

Når personoplysninger bliver indsamlet, skal den dataansvarlige give den registrerede information om en række rettigheder. Neden for er gengivet de mest relevante i rådgivningsregi. Se kapitel 3 i forordningen for den registreredes samlede rettigheder eller læs Datatilsynets "Vejledning om de registreredes rettigheder".

- **Retten til at få besked om, at der behandles personoplysninger (artikel 13 om oplysningspligt)**
  Den registrerede har ret til at modtage oplysning om, hvem der er dataansvarlig, eventuelle andre modtagere af oplysningerne, hvor længe oplysningerne bliver opbevaret, indsigtsretten, retten til berigtigelse, retten til sletning samt retten til at trække samtykke tilbage og klagemulighed til tilsynsmyndighed.

- **Retten til at få indsigt i sine personoplysninger (artikel 15 om indsigtsret)**
  Den registrerede har ret til få at vide, hvis vedkommendes personoplysninger bliver behandlet, og ret til at få adgang til disse oplysninger samt en række informationer om grundlaget for behandlingen.

- **Retten til at få urigtige personoplysninger berigtiget (artikel 16 om ret til berigtigelse)**
  Den registrerede har ret til at få urigtige oplysninger om sig selv berigtiget eller suppleret af den dataansvarlige.

- **Retten til at få oplysninger rettet eller slettet (artikel 17 om ret til sletning)**
  Den registrerede kan bede om at få oplysninger rettet, hvis de er forkerte. Desuden har man i visse tilfælde ret til at få personoplysninger slettet. Det kan fx være, hvis oplysningerne ikke længere er nødvendige til at opfylde det/de formål, hvortil de blev indsamlet, hvis et samtykke, som er nødvendigt for behandlingen, trækkes tilbage eller hvis behandlingen er ulovlig.

- **Retten til at gøre indsigelse mod at personoplysninger anvendes til direkte markedsføring (artikel 21 om ret til indsigelse)**
  Den registrerede har til enhver tid ret til at protestere mod behandling af sine personoplysninger til markedsføring.

- **Retten til at gøre indsigelse mod automatiske individuelle afgørelser, herunder profilering (artikel 22 om automatiske afgørelser og profilering)**
  Den registrerede har ret til ikke at være underlagt afgørelser, der berører vedkommende i væsentlig grad, og som alene er truffet på grundlag af edb-behandling af oplysninger, der er bestemt til at vurdere bestemte personlige forhold, såsom erhvervsevne, kreditværdighed, pålidelighed, adfærd osv.

ANBEFALING: LEV OP TIL OPLYSNINGSPLIGTEN MED EN PRIVATLIVSPOLITIK

Den registreredes rettigheder kan være beskrevet i foreningens privatlivspolitik, som med fordel kan udleveres til nye medarbejdere sammen med ansættelseskontrakten og til frivillige, når de begynder i rådgivningen.

Det kan være sværere for rådgivninger at leve op til deres oplysningspligt overfor brugere af rådgivningstilbud. Det er det, dels fordi brugernes kontakt til rådgivningen typisk er meget løs, dels fordi det ikke er hensigtsmæssigt fra et brugerperspektiv at starte rådgivningssamtalen med en gennemgang af en række juridiske rettigheder. En måde at komme denne problematik i møde på er med en tekst på rådgivningens hjemmeside inklusiv kontaktoplysninger på den dataansvarlige og link til rådgivningens privatlivspolitik for brugere. Dette er ud fra en forventning om, at brugerne orienterer sig dér, inden de kontakter rådgivningen.

Ovenstående overvejelser og procedurer skal beskrives i behandlingsfortegnelsen, hvis en sådan haves.

SIKKERHEDSFORANSTALTNINGER

Forordningens artikel 32 omtaler en række sikkerhedsforanstaltninger, som foreninger bør tage stilling til, når de behandler personoplysninger.

Artikel 32, stk. 1 giver mulighed for, at den enkelte forening og rådgivning lever op til forordningen under hensyntagen til dens aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang og formål. I praksis betyder det, at der bliver stillet mindre vidtgående krav til små foreningers tekniske og organisatoriske sikkerhedsforanstaltninger end til store nationale virksomheders.

EKSEMPLER PÅ TILPASNING TIL RESSOURCER

Afvejning af ressourcer

En rådgivning har et ældre IT-system, hvis sikkerhed bliver gennemgået, og det viser sig, at systemet ikke på alle områder er tidssvarende. Implementeringsomkostningerne ved at bringe hele systemet på niveau vurderes til at blive uforholdsmæssigt store i forhold til den begrænsede datamængde og typen af data, der ligger i systemet. Her kan den dataansvarlige i stedet arbejde for at imødekomme behovet for større sikkerhed ved hjælp af organisatoriske foranstaltninger. Der er altså ingen forpligtelse til at efterkomme sikkerhedskravene alene rent teknisk, hvis der kan etableres et sikkerhedsniveau, der giver mening i forhold til behandlingens karakter, omfang og formål, gennem organisatoriske foranstaltninger.

Eksempel på en organisatorisk foranstaltning

En organisatorisk foranstaltning kan fx være, at man begrænser de ansatte og frivilliges adgang til personoplysninger, så det kun er bestemte personer, der har adgang til bestemte personoplysninger. Eller det kan være, at man ændrer intervallet af, hvor ofte passwords skal skiftes.

ANBEFALING: TJEK IT-SIKKERHEDEN

Rådet for Digital Sikkerhed har i samarbejde med Erhvervsstyrelsen udarbejdet et værktøj – **www.startvaekst.virk.dk/sikkerhedstjekket** – der kan hjælpe organisationer med at få et overblik over deres IT-sikkerhed. Ved at svare på en række spørgsmål får man et fingerpeg om, hvor fokus bør være i organisationens fremadrettede sikkerhedsindsats.

ANBEFALING: OPBEVAR PERSONOPLYSNINGER FORSVARLIGT

Rådgivninger opbevarer en række personoplysninger om blandt andet ansatte, frivillige og brugere. Personoplysninger, herunder samtykker, skal opbevares sikkert og forsvarligt. Jo mere følsomme oplysningerne er, jo højere sikkerhed skal der være omkring behandlingen.

Man kan fx opbevare personoplysninger:
- i et aflåst arkivskab eller lignende. Overvej og beskriv hvem, der har adgang til nøglen.
- som indscannede dokumenter i mappe på server, der kun kan tilgås med en kode. Overvej og beskriv hvem, der har brug for at kende koden.
- i et digitalt journaliseringssystem, hvor en administrator kan give ansatte og frivillige adgang til de mapper, der har relevans for den enkelte.

Man bør *ikke* opbevare personoplysninger:
- på nettet, hvor oplysningerne kan findes ved en google søgning.
- i frit tilgængelige skuffer, mapper og lignende, hvor alle kan tilgå dem.
- på en computer, som mange personer har fri adgang til.
- i online cloud-systemer medmindre udbyderen angiver, at virksomheden lever op til databeskyttelsesforordningen – er *compliant*, som det også hedder – og er sikker på, at udbyderen har et passende sikkerhedsniveau.

ANBEFALING: BEGRUND VALG OMKRING FORANSTALTNINGER

Brug behandlingsfortegnelsen til at begrunde, hvorfor konkrete beslutninger om sikkerhed er truffet i forhold til tilgængelige ressourcer i rådgivningen.
Hvis I fx opbevarer personoplysninger på frivillige i et aflåst arkivskab fremfor i et digitalt journaliseringssystem, bør I beskrive, at det valg er truffet fx under hensyntagen til rådgivningens mulighed for at indkøbe et digitalt system, herunder de økonomiske ressourcer.

UDARBEJDELSE AF POLITIKKER

PRIVATLIVSPOLITIK

Der er ikke krav om udarbejdelse af en privatlivspolitik, men det er en god måde at leve op til sin oplysningsforpligtelse overfor alle registrerede – fx ansatte, frivillige og brugere.

Det er vigtigt at være entydig i beskrivelser og afgrænsninger af hvem, der udgør de forskellige målgrupper, fx hvordan henholdsvis medlemmer og brugere defineres. Derudover bør man sikre, at foreningens vedtægter og privatlivspolitik er forbundet og er let tilgængelige på rådgivningens hjemmeside.

ANBEFALING: FÅ HJÆLP TIL AT UDARBEJDE EN PRIVATLIVSPOLITIK

Privacy Kompasset er et digitalt værktøj udarbejdet af Erhvervsstyrelsen og Datatilsynet og er et godt sted at starte, når man skal lave sin privatlivspolitik. På baggrund af besvarelserne af en række spørgsmål om organisationens behandling af personoplysninger genererer værktøjet en tjekliste over, hvad man skal arbejde videre med.
Find værktøjet: www.startvaekst.virk.dk/privacykompasset

SIKKERHEDSPOLITIK

Databeskyttelsesforordningen stiller ikke formelt krav om, at organisationer, der behandler personoplysninger, har en decideret sikkerhedspolitik. Man skal dog under alle omstændigheder beskrive, fx i privatlivspolitikken, hvilke organisatoriske og IT-relaterede sikkerhedsforanstaltninger, man har truffet.

TI GODE RÅD OM IT-SIKKERHED

1. Hold IT-systemer og programmer opdaterede.
2. Installér en sikkerhedspakke med firewall, antivirusprogram og et spamfilter.
3. Indstil sikkerhedsniveau i browsere, så ansatte og frivillige bliver spurgt, inden filer og programmer bliver overført til deres computere.
4. Hav adgangskode til og eventuel kryptering af foreningens trådløse netværk.
5. Brug gode og sikre kodeord, der som standard udskiftes jævnligt.
6. Udvis sikker adfærd på internettet, fx ved besøg på hjemmesider, installering af nye programmer og modtagelse af mails fra ukendte afsendere.
7. Hav styr på USB-stick. Undgå at bruge samme USB-stick i privat og arbejdsmæssig sammenhæng, husk løbende at slette indhold og brug kun USB-stick fra pålidelige kilder.
8. Tag backups og undgå at gemme data lokalt på computeren, fx på skrivebordet.
9. Begræns antallet af brugerkonti med administratorrettigheder.
10. Lås computeren, når den forlades.

SLETTEPOLITIK

Rådgivninger bør løbende gennemgå behandlede personoplysninger, fx oplysninger der er gemt eller bliver videregivet. Gennemgangen er en anledning til at ajourføre, anonymisere eller slette oplysninger. Gennemgangen kan med fordel tage udgangspunkt i rådgivningens slettepolitik og kan fx foregå to gange om året.

Kravene til sletning er relativt svære at gennemskue i forordningen. Den primære overvejelse, når det gælder sletning eller ej af personoplysninger, er, at der skal være et sagligt formål med at opbevare oplysningerne. Og derudover skal man være opmærksom på, at det retlige grundlag for at gemme oplysningerne, fx opfyldelse af en kontrakt, forfølgelse af en legitim interesse eller samtykke, er på plads.

Der er nogle typer personoplysninger, som en forening – og alle andre – er forpligtet til at gemme. Det gælder fx oplysninger, der skal bogføres til SKAT og lignende. Der er derimod en hel masse oplysninger, man som ansat og frivillig som udgangspunkt ikke har lov til at gemme i længere tid. Det gælder fx e-mails, lister over gamle frivillige og fotos af tidligere ansatte.

Derfor skal rådgivninger udarbejde en slettepolitik, som giver nogle rettesnore for, hvilke typer personoplysninger, der bør slettes og med hvilken frekvens, og hvilke oplysninger der er et sagligt formål med at gemme og hvor længe. Slettefrister vil fremgå af behandlingsfortegnelsen og kan også med fordel indgå i privatlivspolitikken.

BEHANDLING AF BESTYRELSESREFERATER

Almindelige personoplysninger, fx navn, om personer, der varetager et tillidshverv i foreningen, fx en bestyrelsespost, er at betragte som allerede offentliggjorte og må derfor gerne behandles. Omvendt må følsomme personoplysninger om ansatte eller andre ikke fremgå af bestyrelsesreferater. Typisk vil det desuden fremgå af foreningens vedtægter, hvorvidt medlemmer af foreningen har adgang til referaterne.

TJEKLISTE

Når I kan svare JA til nedenstående spørgsmål, er I nået et godt stykke af vejen. At svare JA er ikke ensbetydende med at være i mål med alle procedurer og dokumenter. Det betyder derimod, at I har gjort jer en række vigtige overvejelser over jeres behandling af personoplysninger og dokumenterer disse overvejelser og valg.

- Har I taget stilling til, hvem der er henholdsvis dataansvarlig for behandling af person-oplysninger, og hvem der er databehandler?
- Har I indgået databehandleraftaler?
- Har I taget stilling til, om I skal have en DPO. Hvis I ikke skal have det, har I så en medarbejder, der er ansvarlig for databeskyttelse?
- Har I taget stilling til, om I skal søge tilladelse til behandling af følsomme oplysninger hos Datatilsynet?
- Har I taget stilling til, om I videregiver CPR-numre eller følsomme oplysninger per mail og derfor skal anvende krypteret mail?
- Har I udarbejdet behandlingsfortegnelse(r)?
- Lever I op til jeres oplysningspligt overfor de registrerede, fx med en privatlivspolitik på hjemmesiden?

NYTTIGE LINKS

LOVGIVNING

Databeskyttelsesforordningen
http://eur-lex.europa.eu/legal-content/DA/TXT/PDF/?uri=0J:L:2016:119:FULL&from=DA

Databeskyttelsesloven
https://www.ft.dk/samling/20171/lovforslag/L68/som_vedtaget.htm

VEJLEDNINGER OG GUIDES

Datatilsynet generelt om databeskyttelse
www.datatilsynet.dk/generelt-om-databeskyttelse/

Datatilsynets vejledninger og skabeloner
www.datatilsynet.dk/generelt-om-databeskyttelse/vejledninger-og-skabeloner/

Find blandt andet vejledning om
- Fortegnelse
- Samtykke
- Dataansvarlige og databehandlere
- Ofte stillede spørgsmål om frivillige foreningers behandling af personoplysninger fra Justitsministeriet.

Find blandt andet skabelon til
- Standard-databehandleraftale
- Iagttagelse af oplysningspligten
- Aftale om fælles dataansvar.

Datatilsynets og Erhvervsstyrelsens digitale værktøj Privacy Kompasset
https://startvaekst.virk.dk/privacykompasset

CfSA's guide om foreningers behandling af personoplysninger
https://frivillighed.dk/guides/regler-for-persondata-i-foreninger

DGI og DIF's Vejledning til idrætsforeninger om persondata
https://www.dif.dk/da/forening/raad-og-viden-om-idraetsudvikling/gl_jura_og_raadgivning

EGNE NOTER

Vejledning til rådgivninger om

databeskyttelsesforordningen og -loven

Læs mere

På **www.raadgivingsdanmark.dk**
Følg RådgivningsDanmark på **LinkedIn** og **Twitter**
eller tilmeld dig **nyhedsbrevet**.

Rådgivnings
Danmark

Email: info@raadgivningsdanmark.dk
Telefon: 61 31 70 28