POLITIK

24. MAJ 2018

Behandling af persondata

- gældende for landsforeningen Røde Kors

Version 0.8
Politikken er godkendt af hovedbestyrelsen den 7. juni 2018

DENNE POLITIK ANGIVER, HVORDAN VI MÅ OG SKAL BEHANDLE PERSONDATA OM DEM, SOM VI ARBEJDER FOR OG SAMMEN MED.

INDHOLD

1 Introduktion 3

2 Formål og ansvar 3

3 Behandling af persondata 4

3.1 Definition af persondata 5

3.2 Hjemmel (lovlig behandling) 5

3.3 Sådan gør du 6

3.4 De registreredes rettigheder 7

3.5 Behandling af HR-data 8

3.6 Sletning af persondata 8

3.7 Brug af billeder og video 9

3.8 Overførsler til tredjelande 9

4 Aftaler med leverandører som behandler persondata 10

5 Behandlingssikkerhed 10

Bilag

Bilag 1: Overvejelser ved behandling af persondata

Bilag 2: Eksempler på brug af hjemmel

Bilag 3: Klassificering af data

Bilag 4: Oversigt over retningslinjer

1 INTRODUKTION

Alle mennesker har ret til, at deres personlige oplysninger beskyttes. Personlige oplysninger eller persondata spænder lige fra navn, adresse og billeder til cpr.nr. og religiøs overbevisning. I Røde Kors modtager, opbevarer og anvender vi persondata på mange personer. Det er vigtigt for Røde Kors' virke og omdømme, at alle disse personer trygt kan regne med, at vi behandler deres persondata i overensstemmelse med gældende lovgivning[1].

Politikken introducerer en række nye begreber – du kan få et samlet overblik og se, hvad begreberne dækker over i bilag 1. Her introduceres hovedbegreberne kort:

Persondata (oplysninger) er data, som gør, at en person kan identificeres. I Røde Kors er persondata typisk navn, kontaktoplysninger, e-mail mv., men kan også omfatte persondata af mere følsom karakter som f.eks. helbredsoplysninger.

Behandling er alt det, vi gør med persondata, dvs. når vi indsamler, gemmer, læser, ændrer, søger og videregiver data.

Beskyttelse handler om ethvert menneskes ret til at bestemme, hvilke persondata vedkommende vil dele – og med hvem data skal deles med. Det betyder, at når vi indsamler persondata, så må vi kun anvende dem til det, vi har aftalt med personen. Dvs. at dem, vi behandler persondata om, (**de registrerede**) skal oplyses om, hvordan vi behandler deres data.

2 FORMÅL OG ANSVAR

Formålet med denne politik er at fastsætte rammen for, hvordan persondata må og skal behandles i Røde Kors samt give en henvisning til, hvordan behandlingen kan udføres.

Det overordnede dataansvar for behandling af persondata i Røde Kors (dataansvarlig[2]) ligger hos Landsforeningen Røde Kors (herefter 'Røde Kors') og omfatter dermed alt behandling af persondata i Røde Kors-afdelingerne med tilhørende aktiviteter og på landskontoret, herunder kontorer i udlandet, det psykosociale center og asylafdelingen. Det betyder, at i praksis er landskontoret ved generalsekretæren dataansvarlig.

Ungdommens Røde Kors anses som selvstændig dataansvarlig, da de er en selvstændig juridisk enhed. Ungdommens Røde Kors er således ansvarlig for deres behandling af persondata, og de har derfor deres egen persondatapolitik og retningslinjer.

Denne politik samt de dertilhørende retningslinjer gælder for alle i Røde Kors, som behandler persondata, dvs. både frivillige og ansatte. Med ansatte menes alle ledere og medarbejdere ansat i Røde Kors-afdelinger og på landskontoret, herunder ansatte i asylafdelingen, det psykosociale center og delegater.

Ansvaret for at udforme og efterleve politikken er placeret hos ledergruppen på landskontoret, som består af general- og vicegeneralsekretæren samt afdelingsledere. Afdelingsledere har til opgave at

[1] Gældende lovgivning er EU's persondataforordning med virkning fra 25. maj 2018 samt supplerende dansk persondatalovgivning. Til dagligt omtales forordningen også som GDPR (General Data Protection Regulation).
[2] Se definition i bilag 1.

sikre, at politikken udbredes til de frivillige og ansatte, som behandler persondata, og føre kontrol med, at den efterleves.

Sanktioner for ikke at overholde gældende lovgivning eller læk af persondata i form af bøde eller kritik fra Datatilsynet håndteres af Landsforeningen Røde Kors som overordnet dataansvarlig.

Persondatakontaktperson; er en person udnævnt fra hver Røde Kors-afdelingsbestyrelse, der har et særligt blik på persondata og behandlingen heraf, og som kan hjælpe afdelingen med at sikre, at den behandling, som foregår i den enkelte Røde Kors-afdeling, sker i overensstemmelse med denne politik og de tilhørende retningslinjer.

Frivillige; skal efterleve politikken og de tilhørende retningslinjer, som de præsenteres for dem i form af håndbøger og vejledninger. Hvis der opstår problemer, skal den frivillige drøfte sagen med persondatakontaktpersonen i egen afdeling eller afdelingsformanden og derefter medvirke til, at der handles på sagen.

Medarbejdere; skal være orienteret i og efterleve politikken samt de underliggende retningslinjer. Hvis der opstår uklarheder, skal medarbejderen drøfte sagen med nærmeste leder og derefter medvirke til, at der handles på sagen.

Nærmeste leder; skal sikre, at medarbejderne har kendskab til politikken samt underliggende retningslinjer. Hvis medarbejdere mod forventning ikke efterlever de gældende retningslinjer, skal nærmeste leder tage de nødvendige forholdsregler for at sikre, at de gældende retningslinjer fremadrettet overholdes.

Røde Kors' databeskyttelsesrådgiver (DPO[3]); skal tilse, at Røde Kors overholder persondataforordningen samt nærværende persondatapolitik.

Der vil løbende blive udviklet retningslinjer og praktiske vejledninger, der skal understøtte, at både ansatte og frivillige kan overholde persondatapolitikken (se bilag 4). Persondatapolitikken og retningslinjer vil blive publiceret forskellige steder, alt efter hvilken enhed i Røde Kors man hører til, dvs. det kan være www.mitrødekors.dk eller intranettet hos asyl, Hovedstadens Røde Kors eller på landskontoret. I politikken vil der blive refereret til intranettet, som en samlet betegnelse for alle enheder.

Spørgsmål til politikken eller retningslinjer, som ikke kan besvares af din leder eller afdelingens persondatakontaktperson, sendes til DPO'en på DPO@rodekors.dk.

3 BEHANDLING AF PERSONDATA

I dette afsnit gennemgås de overvejelser du skal foretage, hver gang du planlægger at behandle persondata. Mange af de behandlinger, som vi foretager i Røde Kors, beskrives i retningslinjer og håndbøger, men du skal også selv være i stand til at bedømme, om den behandling, du planlægger, overholder gældende regler.

Er du i tvivl, om du må foretage en behandling, eller om igangværende behandling overholder gældende regler, er det vigtigt, at du spørger din leder, persondatakontaktpersonen eller DPO'en.

[3] DPO står for Data Protection Officer. Røde Kors behandler i stort omfang følsomme persondata, og derfor skal Røde Kors ifølge EU's persondataforordning have en DPO.

3.1 Definition af persondata

Persondata (oplysninger) er som nævnt data, som gør, at en person kan identificeres. Der er mange oplysninger om en person, som regnes for persondata. I Røde Kors behandler vi i stort omfang både almindelige og følsomme oplysninger. Forskellen mellem almindelige og følsomme persondata er, at de følsomme persondata skal vi passe ekstra godt på, bl.a. stilles der ekstra krav til behandlingssikkerheden. Du kan læse mere om behandlingssikkerhed i afsnit 5.

Af oversigten nedenfor fremgår, hvilke data der regnes for almindelige, og hvilke der regnes for følsomme persondata.

Almindelige persondata	Navn, adresse, arbejds- og privattelefon, mobil nr., arbejdsområde, e-mail, IP-adresse, titel, ansættelsesdato, CV, ansøgning, eksamen, bil, bolig, familieforhold, tjenstlige forhold, sygedage, gæld, skat, økonomi, andre rent private forhold, væsentlige sociale forhold
Følsomme persondata	Race, etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data med henblik på entydig identifikation, helbredsoplysninger, seksuelle forhold eller orientering, straffedomme, lovovertrædelser, cpr.nr og id.nr. på en asylansøger

Persondata kan være en kombination af data, hvor de hver for sig ikke identificerer en person, men hvor kombinationen af data gør, at personen kan identificeres. F.eks. er det ikke muligt at identificere en person ud fra titlen 'afdelingsformand', men hvis det kombineres med afdelingens navn bliver personen identificerbar, selvom personens navn ikke nævnes.

3.2 Hjemmel (lovlig behandling)

Vi må gerne behandle alle de persondata, som Røde Kors har et legitimt formål med at behandle, både almindelige og følsomme persondata – så længe vi har hjemmel til behandlingen. Hjemmel er et juridisk begreb, som angiver, om det er lovligt at gennemføre en planlagt behandling af persondata.

Når du indsamler persondata i Røde Kors, skal det altså ske med et legitimt formål, og du skal sikre dig, at behandlingen er lovlig, dvs. at du har hjemmel til behandlingen.

Der findes flere forskellige hjemler, som ligger til grund for, om en behandling er lovlig. For hver behandling vælges den hjemmel, som passer på formålet. Er der ikke en hjemmel, der understøtter det, du ønsker at opnå, kan behandlingen ikke gennemføres.

Du har hjemmel til behandlingen (lovlig behandling), når du

- skal opfylde en aftale med den registrerede (**kontraktlig forpligtelse**)
- skal overholde en retlig forpligtelse (**lovgivning**)
- skal behandle persondata som en del af den opgave, som Røde Kors skal løse (**legitim interesse**)
- har et **samtykke** fra den, hvis data du behandler
- er i en nødsituation, hvor du er nødt til at gennemføre behandlingen for at beskytte den registreredes eller andres **vitale interesse**
- skønner at behandlingen er i **samfundets interesse**.

Til eksempel har vi brug for at vide, hvem Røde Kors' medlemmer er. Formålet er, at vi skal vide, hvem der har stemmeret i foreningen, og fra hvem vi kan opkræve medlemsgebyr. For at vi kan opfylde vores formål, er vi derfor nødt til at have et register over alle medlemmers kontaktoplysninger. Vi finder hjemlen i legitim interesse, da behandlingen indgår som en del af den opgave, som Røde Kors skal løse. Det er altså vores legitime interesse at foretage registreringen, så længe medlemmet ønsker at være medlem.

Du kan finde yderligere information om de ovenfornævnte hjemler i bilag 2 samt eksempler på, hvordan de kan bruges. Bemærk at hvis du bruger samtykke som hjemmel til den planlagte behandling, så skal samtykket opfylde en række krav.

Et samtykke skal være frivilligt, specifikt, utvetydigt samt afgivet på et informeret grundlag, så den registrerede kan gennemskue, hvad der siges ja til. Et samtykke er ikke gyldigt, hvis det er umuligt for personen at sige nej. Samtykket skal gives senest på det tidspunkt, hvor data indsamles.

Som udgangspunkt skal det være muligt at kunne dokumentere et samtykke. Hvis der er behov for at bruge et samtykke i en proces hvor det ikke er muligt at dokumentere samtykket, skal processen afklares i samarbejde med DPO'en, før behandlingen sættes i gang.

Du kan læse mere om, hvordan samtykke indhentes og dokumenteres i 'Retningslinjer for at indhente samtykke'. Her kan du også finde eksempler på samtykke og en skabelon til at indhente dette. Du finder retningslinjer og skabelon på intranettet.

Processer, hvor vi behandler persondata i Røde Kors, er beskrevet i 'Fortegnelsen', som du kan finde på intranettet. Her er de overordnede formål og hjemmel for behandlingsprocesserne beskrevet.

3.3 Sådan gør du

Når du planlægger at behandle persondata, er der en række overvejelser, som du skal have tænkt igennem, før du begynder behandlingen:

a. Hvad er dit formål med behandlingen?
b. Hvilke persondata har du brug for?
c. Hvad gør, at behandlingen er lovlig (hjemmel)?
d. Hvem skal have adgang til de persondata, du indsamler?
e. Hvor skal persondata gemmes?
f. Hvor længe skal de persondata, du har indsamlet, gemmes/hvornår skal de slettes?

Når du går i gang med at indsamle persondata, skal du huske, at de personer, som du behandler persondata om, skal oplyses om behandlingen. Du kan læse mere om oplysningspligten i afsnit 3.4.

Et eksempel på ovenstående proces er, at

a. En frivillig i en Røde Kors Butik vil lave en fødselsdagsliste over frivillige i butikken.
b. Den frivillige har brug for navn og fødselsdato.
c. Hjemmel får den frivillige ved at spørge de andre frivillige, om de har lyst til at stå på listen – der indhentes altså et samtykke.
d. Alle frivillige der arbejder i Røde Kors butikken
e. Listen hænges op på opslagstavlen i baglokalet.
f. Listen opdateres, når der kommer nye frivillige, eller når nogen stopper i butikken. Gamle lister slettes elektronisk, og papirudgaven destrueres.

Ved indsamlingen af navn og fødselsdato fra de frivillige i butikken oplyser den frivillige om, at listen vil blive hængt op på opslagstavlen i baglokalet, og dermed kan den ses af alle, som kommer i lokalet, samt at de til enhver tid kan blive slettet fra listen, altså trække deres samtykke tilbage.

Når du indsamler data, skal du sørge for kun at indsamle de persondata, du har brug for. Modtager du flere oplysninger, end du har brug for, så bed vedkommende om fremadrettet at begrænse mængden af data og slet de overflødige data.

Allerede når du indsamler persondata, skal du tænke over, hvor længe du har brug for at gemme dem. Det skal du fordi, når formålet med at behandle data er ophørt, eller der ikke længere er hjemmel til behandlingen, så skal de slettes. Du kan læse mere om sletning af data i afsnit 3.6.

Når du gemmer data elektronisk, skal du også tænke over, hvem som skal have adgang til de data, du behandler; hvis det f.eks. drejer sig om en deltagerliste til en familielejr, så er det kun dem, som er med til at arrangere kurset, som har brug for at se deltagerlisten. Det kan virke rimeligt uskyldigt, at en deltagerliste bliver delt med uvedkommende, men hvis man ser på det fra den registreredes side, så er det ikke sikkert, at den registrerede ønsker, at andre skal have kendskab til, at man har deltaget i en familielejr.

Det er vigtigt at have en systematik i forhold til lagring af persondata, så du hele tiden ved, hvor data befinder sig, i tilfælde af at den registrerede beder om indsigt, ønsker at få rettet data eller at få egne persondata slettet. Følsomme og fortrolige oplysninger skal være låst inde eller gemmes i et system med begrænset adgang. Kun de personer, som ud fra dine overvejelser jfr. ovenfor skal kunne tage del i behandlingen, må få adgang til de gemte data.

Vi skal altså altid sikre os, at vi har de registreredes rettigheder for øje.

3.4 De registreredes rettigheder

Formålet med forordningen er altså ikke at forhindre os i at behandle persondata, men derimod at sikre, at behandlingen er lovlig, sker under hensyntagen til de registreredes rettigheder, samt at de registrerede bliver informeret om, hvordan vi behandler deres persondata på en letforståelig måde.

De registreredes ret til at bestemme over egne persondata er specificeret i seks rettigheder, som de registrerede kan gøre brug af, nemlig retten til at:

- vide at egne persondata behandles (oplysningspligt)
- kende hvilke persondata, der er registreret (indsigtsret)
- få rettet persondata, hvis de er forkerte (retten til berigtigelse)
- få persondata slettet (retten til at blive glemt)
- gøre indsigelse mod at persondata bruges til direkte markedsføring eller profilering
- flytte persondata til en anden organisation.

Retten til at vide at persondata behandles, altså Røde Kors' oplysningspligt, løser vi overordnet set ved, at der på hjemmesiden rodekors.dk er en privatlivspolitik, som du skal henvise til skriftligt eller mundtligt, når du indsamler data.

Er der noget, som den registrerede skal have oplyst om behandlingen, som ikke fremgår af privatlivspolitikken, skal du selv sørge for at oplyse den registrerede om det. I forhold til eksemplet ovenfor, med en frivillig som ønsker at lave en fødselsdagsliste over frivillige i butikken, så fremgår den om-

talte fødselsdagsliste ikke af privatlivspolitikken, da det ikke er muligt at omtale hver enkelt behandling af persondata i privatlivspolitikken. Derfor skal de frivillige, der siger ja tak til at stå på listen, oplyses specifikt om, hvordan deres persondata behandles, altså som nævnt ovenfor bliver navne og fødselsdage skrevet på en liste og hængt op i baglokalet i butikken.

Når en registreret henvender sig for at få rettet sine data, skal du sikre dig, at dette sker, og at det sker alle de steder, hvor vi har registreret personens data. Den registrerede kan også bede om at få sine persondata slettet. Beder den registrerede om indsigt eller om at blive slettet, og er du i tvivl om, hvordan denne opgave skal løses, så tag fat i din leder, persondatakontaktperson i din afdeling eller DPO'en. Bemærk at Røde Kors kun har en måned til at berigtige eller slette data fra den dato, den registrerede henvender sig. Du kan læse mere om sletning af data i afsnit 3.6.

Når en registreret beder om indsigt, har de ret til at få adgang til alle de oplysninger, du og andre i Røde Kors har registreret på vedkommende. Derfor er det vigtigt, at du ikke gemmer persondata, som du ikke hjemmel til.

Ønsker en person at flytte sine persondata til en anden organisation, og du er i tvivl om, hvordan det kan foregå, så kontakt DPO'en.

3.5 Behandling af HR-data

I Røde Kors behandler vi persondata om ansatte og ansøgere til stillinger og frivilligjobs.

I forhold til ansatte er det lovlige grundlag til behandlingen, at vi har indgået en kontrakt. Hvad behandlingen nærmere går ud på, og hvordan den foregår, fremgår af Røde Kors' 'privatlivspolitik for behandling af persondata om ansatte'.

I forhold til frivillige er det lovlige grundlag til behandlingen, at vi har indgået en Røde Kors-aftale. Hvad behandlingen nærmere går ud på, og hvordan den foregår, fremgår af Røde Kors' 'privatlivspolitik', som findes på www.rodekors.dk.

Hvis ansatte får tilsendt ansøgning og CV uden om Røde Kors' HR-systemer til håndtering af ansøgere, skal disse altid sendes til HR, som sikrer den rette behandling af ansøgers persondata. Modtagne ansøgninger og CV'er må ikke opbevares mere end seks måneder, medmindre der indhentes samtykke hertil.

Informationer modtaget fra ansøgere til frivilligjobs må ikke gemmes mere end seks måneder, medmindre der indhentes samtykke hertil.

3.6 Sletning af persondata

Som nævnt må du kun gemme persondata, så længe behandlingen er lovlig og foregår i overensstemmelse med det oprindelige formål. Når du ikke længere har en gyldig grund til at gemme data, skal de slettes.

Har du brug for at gemme data til statistik, f.eks. hvor mange familier der deltog i en aktivitet, og hvor mange børn familien har, så kan du vælge at anonymisere listen ved at fjerne alle informationer, som gør, at vi kan identificere de registrerede. Dermed kommer listen til at bestå af en anonym betegnelse, f.eks. familie 1 med tre børn, familie 2 med et barn, osv. Det vigtige ved anonymisering er at være opmærksom på, at i en bestemt kontekst kan en kombination af oplysninger stadig medføre,

at en person kan identificeres, selvom navn og kontaktoplysninger er fjernet. Hvis det er tilfældet, skal flere data anonymiseres, for at det er lovligt at gemme data.

Hvis en person beder om at få slettet sine persondata, skal vedkommendes persondata slettes i alle systemer, mails og fysiske mapper, hvor vedkommende er registreret. Dog kan man ikke blive slettet, hvis registreringen har hjemmel i lovgivning eller opfyldelse af en kontrakt.

For personer, som er registreret mere end et sted og i flere systemer, kan det være en omfattende øvelse at slette vedkommendes data, da de kan være registreret i flere Røde Kors-afdelinger og på landskontoret. Er du i tvivl om, hvordan opgaven kan løses, så spørg din leder eller DPO'en. Bemærk at Røde Kors kun har en måned til at udføre denne opgave.

Husk at printet materiale, som indeholder følsomme persondata, skal destrueres på en forsvarlig måde f.eks. ved makulering.

Vær opmærksom på at Røde Kors har en aftale med Rigsarkivet om overlevering af historiske data. Er du i tvivl om, hvilke historiske data som skal overleveres til Rigsarkivet så spørg DPO'en.

3.7 Brug af billeder og video

I Røde Kors bruger vi billeder og video til at kommunikere med på hjemmesider, mitrødekors.dk, sociale medier, foldere, præsentationer m.v.

Et billede eller en video anses for at være persondata, når det er muligt at identificere blot én person på billedet eller videoen, og dermed er brugen af billedet eller videoen underlagt reglerne for behandling af persondata.

Det betyder, at vi skal sikre os, at vi har et specifikt formål og hjemmel til at bruge billedet eller videoen, inden vi går i gang. Du kan læse i 'Retningslinjer for brug af billeder og video', hvordan du sikrer dig, at du må bruge billedet eller videoen. Du kan finde disse retningslinjer på intranettet.

3.8 Overførsler til tredjelande

Forordningen har strenge regler for, hvornår persondata må behandles uden for EU/EØS[4], samt hvordan det skal foregå. Formålet er at sikre, at persondata kun deles udenfor EU/EØS, når der kan opnås samme niveau af sikkerhed i behandlingen af persondata, som hvis behandlingen foregår inden for EU/EØS. Overførsler til lande uden for EU/EØS omtales som tredjelandsoverførsler.

I Røde Kors udveksler vi løbende persondata med delegater, andre Røde Kors-selskaber, samarbejdspartnere, donorer m.v. på tværs af landegrænser. Når det drejer sig om såkaldte sikre lande udenfor EU/EØS, skal vi foretage de samme overvejelser som ved enhver anden behandling af persondata inden for EU/EØS; altså forholde os til hvad formålet er med behandlingen, og om vi har et lovligt grundlag for at gennemføre behandlingen. Der er kun få lande udenfor EU/EØS, som regnes for sikre lande som f.eks. Schweiz[5]. Bemærk, at USA og Australien ikke regnes for sikre lande pt.

---

[4] EØS er et økonomisk samarbejde mellem EU og Norge, Island og Liechtenstein.
[5] EU-Kommissionen genovervejer løbende hvilke lande, der er sikre. Lige nu er følgende tredjelande klassificeret som sikre: Andorra, Argentina, Færøerne, Guernsey, Isle of Man, Israel, Jersey, New Zealand, Schweiz og Uruguay.

Skal du overføre persondata til såkaldte usikre tredjelande, altså udenfor EU/EØS, skal du først orientere dig i 'Retningslinjer for tredjelandsoverførsler' på intranettet. Her fremgår om den ønskede behandling er lovlig. Det samme gælder, hvis du vil overføre persondata fra et tredjeland til EU/EØS.

Hvis behandlingen af persondata ikke omhandler en EU-borger, og udvekslingen af data foregår mellem to lande udenfor EU/ØES, gælder forordningen ikke for denne overførelse. Af etiske grunde vil Røde Kors selvfølgelig altid forsøge at sikre, at behandling af persondata om ikke-EU borgere uden for EU/EØS foregår på så sikker en måde som muligt. Dog må de forhold, som Røde Kors arbejder under i f.eks. en katastrofesituation, vurderes op imod behovet for at kunne beskytte persondata i den pågældende situation.

4 AFTALER MED LEVERANDØRER SOM BEHANDLER PERSONDATA

Vi skal indgå en aftale med alle de leverandører, som behandler persondata for Røde Kors, en såkaldt databehandleraftale. Denne aftale skal indgås i tillæg til hovedaftalen med leverandøren. Typisk vil en sådan leverandør være en it-leverandør, men det kan også være et telemarketingbureau eller en kommune. Formålet med at indgå en databehandleraftale er, at vi skal give databehandleren en instruks om, hvad de må gøre med de persondata, de behandler på vegne af os.

Når du indgår en aftale med en ny leverandør, som behandler persondata, skal du samtidig sørge for, at der bliver udarbejdet en databehandleraftale.

Der er en række krav til, hvad en databehandleraftale skal indeholde. I 'Vejledning om databehandleraftaler' kan du læse mere om processen for at indgå databehandleraftaler, hvilken information aftalen skal indeholde, og hvordan vi efterfølgende fører tilsyn med aftalerne. På intranettet kan du finde skabeloner på dansk og engelsk til databehandleraftaler. Bemærk at databehandleraftaler altid skal kvalitetssikres af DPO'en, før de underskrives.

5 BEHANDLINGSSIKKERHED

I Røde Kors er vores behandling af persondata underlagt vores 'Informationssikkerhedspolitik', hvor det fremgår, hvordan information er klassificeret i Røde Kors, og hvad det betyder for behandlingen af informationer. Du kan få et hurtigt overblik over klassificering i Bilag 3. Formålet med klassificeringen er at hjælpe frivillige og ansatte til at håndtere information korrekt i forhold til gældende lovgivning og interne retningslinjer.

Det er serviceejers[6] ansvar at sikre, at de systemer, som vedkommende er ansvarlig for, lever op til disse krav.

Som tidligere nævnt stilles der ekstra krav til behandlingssikkerheden af følsomme persondata, som f.eks. cpr.nr. og helbredsoplysninger. Disse data må kun deles på e-mail, hvis en Røde Kors e-mail anvendes. Frivillige, hvor deling af følsomme persondata indgår i opgaven, skal derfor have en Røde kors e-mail, før opgaven varetages[7].

---

[6] Serviceejer er en afdelingsleder, som har ansvaret for et IT-system. I asylafdelingen anvendes begrebet systemejer.
[7] Alle frivillige i Røde Kors har mulighed for at få en Røde Kors e-mailadresse, også frivillige som ikke behandler personfølsomme data. Er du frivillig og ønsker at få en Røde Kors e-mailadresse, så send en mail til helpdesk@rodekors.dk.

Sendes følsomme data til en ekstern person, f.eks. en myndighed, skal mailen sendes som 'Sikker Mail', hvorved informationerne krypteres, og dermed mindskes risikoen væsentligt for, at uvedkommende kan få adgang til disse data. Du kan se en vejledning til, hvordan du kan sende sikker mail på intranettet.

Røde Kors må ikke opfordre den registrerede til at sende f.eks. cpr.nr. på mail til Røde Kors, men hvis vedkommende vælger at gøre det, er det for egen risiko.

Du må ikke dele fortrolige person- og forretningsdata via systemer, som Røde Kors ikke har mulighed for at kontrollere adgangen til, og som ikke overholder password-politikken, jfr. klassificeringen af data angivet i informationssikkerhedspolitikken. Sådanne systemer er f.eks. dropboks eller google drev.

Hvis uautoriserede har fået adgang til registreredes persondata, er Røde Kors forpligtet til at anmelde sikkerhedsbruddet til Datatilsynet og de registrerede, inden 72 timer fra bruddet er opdaget. Derfor skal en frivillig eller ansat, som bliver opmærksom på uautoriseret adgang til persondata enten eksternt eller internt, straks meddele det til nærmeste leder og DPO'en.

Bilag 1: DEFINITIONER

Nedenfor følger definitioner af udvalgte begreber anvendt i hovedteksten.

Persondata (oplysninger)
Persondata som gør, at en person kan identificeres, direkte eller indirekte, alene eller i kombination. Forskellen mellem almindelige og følsomme persondata er, at de følsomme persondata skal vi passe ekstra godt på, bl.a. stilles der ekstra krav til behandlingssikkerheden. Du kan læse mere om behandlingssikkerhed i afsnit 5.

Almindelige persondata	Navn, adresse, arbejds- og privattelefon, mobil nr., arbejdsområde, e-mail, IP-adresse, titel, ansættelsesdato, CV, ansøgning, eksamen, bil, bolig, familieforhold, tjenstlige forhold, sygedage, gæld, skat, økonomi, andre rent private forhold, væsentlige sociale forhold
Følsomme persondata	Race, etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssige tilhørsforhold, genetiske data, biometriske data med henblik på entydig identifikation, helbredsoplysninger, seksuelle forhold eller orientering, straffedomme, lovovertrædelser og cpr.nr

Behandling
Enhver aktivitet eller række af aktiviteter som involverer brug af persondata, dvs. at se, læse, indsamle, registrere, systematisere, gemme, søge, bruge, videregive eller slette.

Registrerede
Alle de personer som vi registrer persondata om.

Beskyttelse
Alle har ret til at bestemme, hvilke persondata vedkommende vil dele – og med hvem data skal deles med – medmindre der en hjemmel, som angiver noget andet, fx lovgivning som kræver, at indtægter angives til Skat. Det betyder, at når vi indsamler persondata, så må vi kun anvende dem til det, vi har aftalt med personen. Dvs. at dem, vi behandler persondata om (**de registrerede**), skal oplyses om, hvordan vi behandler deres data (oplysningspligten).
Persondata, som indgår i kategorien af følsomme persondata, stiller forordningen strengere krav til, hvordan de skal behandles. Sikkerhed omkring behandling af persondata fremgår af afsnit 5.

Hjemmel
Hjemmel er et juridisk begreb, som angiver, om det er lovligt at gennemføre en planlagt behandling af persondata. Se bilag 2 med eksempler på hjemmel.

Oplysningspligt
Pligten til at fortælle den registrerede hvordan vi behandler vedkommendes persondata. Registrerede kan læse om, hvordan Røde Kors behandler persondata på www.rodekors.dk under 'privatlivspolitik'.

Dataansvarlig
Den som er ansvarlig for, hvordan data behandles i Røde Kors, dvs. den som bestemmer ud fra hvilke formål og med hvilke hjælpemidler, vi behandler persondata.

Databehandler

Den leverandør eller offentlige myndighed der behandler persondata på den dataansvarliges vegne.

Fortegnelsen
Fortegnelsen er den måde hvorpå, at Røde Kors skal dokumentere over for Datatilsynet, hvilke persondata vi behandler og hvordan det foregår. Fortegnelsen afløser den anmeldelsespligt til Datatilsynet, som den tidligere persondatalovgivning krævede. Du kan finde en oversigt over fortegnelsen samt de enkelte fortegnelser på intranettet.

EU's Persondataforordning
Europa-Parlamentets og -Rådets Forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med Behandling af persondata og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF med tilhørende regulering.

Databeskyttelsesloven
Den lov, som forventes at blive vedtaget på baggrund af forslag til lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af persondata og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) fremsat den 25. oktober 2017.

Bilag 2: EKSEMPLER PÅ BRUG AF HJEMMEL

Nedenfor gennemgås eksempler på hvordan en hjemmel fastlægges, og hvilken behandling vi derefter kan foretage. Hjemmel er et juridisk begreb, som angiver, om det er lovligt at gennemføre en planlagt behandling af persondata.

Opfylde en aftale med den registrerede (kontraktlig forpligtet)
En kontraktlig forpligtelse kan være en aftale med en leverandør, en Røde Kors-aftale med en frivillig eller en ansættelseskontrakt. Når en kontrakt er indgået, har vi ret til at behandle de persondata, som kontrakten omfatter, indtil kontrakten udløber.

Ønsker en frivillig ikke at være frivillig i Røde Kors længere, er der ikke hjemmel til at behandle personens data, medmindre der findes en anden hjemmel. Er en frivillig f.eks. bidragsyder, er vi forpligtet til at gemme personens data i fem år ifølge bogføringsloven. Man kan altså godt være forpligtet til at slette en persons oplysninger et sted, mens man skal gemme dem et andet sted.

En donoraftale er også en kontraktlig forpligtelse, og en sådan aftale kan kræve, at persondata skal gemmes i op til syv år efter sidste betaling, for at Røde Kors kan dokumentere, hvordan de donerede midler er brugt.

Overholde en retlig forpligtelse (lovgivning)
Vi er forpligtet til at behandle persondata, som angivet i anden lovgivning end persondataforordningen. Til eksempel kræver sundhedsloven, at journaler gemmes i ti år, hvilket omfatter f.eks. sundhedsklinikkerne og samarittjenesten. Røde Kors er desuden forpligtet til at indberette udbetalt løn til Skat, og til at bogføre indtægter og udgifter, selvom det involverer behandling af persondata.

Den behandling, som kræves af en lovgivning, kan den person, som det omhandler, ikke sige nej til. Bemærk at fordi man er retlig forpligtet til at behandle persondata med det formål at følge loven, giver det os ikke ret til at bruge de data til andre formål.

Behandle persondata ud fra Røde Kors' legitime interesse
Legitim interesse handler om, når en behandling af data er nødvendig for at gennemføre en opgave, som er i Røde Kors' interesse. F.eks. når vi registrerer medlemmer. Hvis ikke vi kunne få lov til at registrere medlemmer, ville medlemmet ikke kunne stemme til generalforsamlingen, og vi ville ikke kunne opkræve medlemsgebyr. Det er altså vores legitime interesse at foretage registreringen, så længe medlemmet ønsker at være medlem.

Et andet eksempel er uddeling af julehjælp. Det er helt legitimt, at vi registrerer hvem, der har søgt om julehjælp, så vi på dagen ved, hvem julehjælpen skal deles ud til. Men vi må ikke efterfølgende bruge listen over modtagere til julehjælp til at sende en invitation ud om deltagelse i en anden aktivitet. Ønsker man at informere modtagere af julehjælp om andre tilbud i Røde Kors, skal man altså gøre det samtidig med, at julehjælpen uddeles.

Det er legitimt, at vi registrerer indsamlere til landsindsamlingen, hvordan skal vi ellers vide, hvem der skal samle ind på dagen. Det er også legitim interesse at spørge indsamlerne fra sidste år, om de vil samle ind igen. Men er det mere end tre år siden, en indsamler sidst har samlet ind, er der ikke længere en tilknytning til Røde Kors, som gør, at man må spørge dem igen.

Samtykke
Samtykke kan anvendes, når vi ikke kan finde anden hjemmel til den behandling, vi gerne vil gennemføre.

Et samtykke kan anvendes, når vi gerne vil bruge et billede med en identificerbar person til vores hjemmeside eller anden form for kommunikation. Du kan læse mere om brug af billeder i Retningslinjer for brug af billeder og video.

Et samtykke kan også bruges, hvis du er i kontakt med en gruppe personer i en sammenhæng og gerne vil kontakte dem i en anden sammenhæng. F.eks. hvis du gerne vil have lov til at kontakte modtagere af julehjælp, når der skal afholdes familielejr. Så kan du bede om deres samtykke til at kontakte dem, når der inviteres til familielejr. Du kan læse mere om samtykke i afsnit 3.5.

Vital interesse
Denne hjemmel vil kun være brugbar i få situationer, som f.eks. hvis en samarit skal behandle en bevidstløs person, hvor det ikke er muligt at bede om samtykke til behandling af persondata.

Samfundets interesse
Der vil kun være få tilfælde, hvor hjemmel til behandling af persondata kan findes i hjemlen 'samfundets interesse'. Det kan f.eks. være forskning af sådan en karakter, at samfundets interesse overskygger de registreredes rettigheder. Brug af denne hjemmel må kun ske, hvis det specifikt er angivet som hjemmel i Fortegnelsen, i en af de til denne politik tilhørende retningslinjer eller efter nærmere aftale med DPO'en.

Bilag 3: KLASSIFICERING AF DATA I RØDE KORS

Kategori	Typer	
	Forretningsdata	*Persondata*
Offentlig Der er ingen fortrolighed og ingen begrænsninger på hvem, der må få adgang	Ingen forretningskritiske data Eksempelvis offentliggjorte regnskaber og informationer om Røde Kors, som kan findes på hjemmesiden, mv.	Hvis materialet indeholder persondata, skal der være hjemmel til at offentliggøre disse (via lovgivning, kontrakt eller samtykke). Eksempelvis billeder på hjemmesider og personlige historier i foldere.
Intern Informationer, som vedkommer alle eller udvalgte frivillige og/eller ansatte, men ikke offentligheden	Forretningsdata, som ikke ønskes delt udenfor organisationen pt. Eksempelvis interne mails, notater og rapporter	Hvis persondata registreres eller deles, skal der være hjemmel til denne håndtering (via lovgivning, kontrakt eller samtykke). Eksempelvis registrering af persondata i databaser.
Fortrolig Data, som kun vedkommer få udvalgte frivillige og/eller ansatte i Røde Kors, og som andre ikke må få adgang til	Forretningskritiske data Eksempelvis interne mails, notater og rapporter med en høj grad af fortrolighed	Hvis følsomme persondata registreres eller deles, skal der være hjemmel til denne håndtering (via lovgivning, kontrakt eller samtykke). Eksempelvis følsomme oplysninger på deltagere i aktiviteter og projekter, frivillige og ansatte (cpr.nr., helbredsmæssige, religiøse og økonomiske oplysninger, race og etnicitet, mv.)

Bilag 4: OVERSIGT OVER RETNINGSLINJER

Nedenfor fremgår de retningslinjer som er nævnt i denne Politik.

- Retningslinjer for brug af billeder og video
- Retningslinjer for indhentning af samtykke
- Retningslinjer for tredjelandsoverførsler
- Retningslinjer for indhentning af databehandleraftaler
- Retningslinjer for frivilliges håndtering af persondata indgår i håndbøger for aktiviteter og andre relevante vejledninger