Persondatapolitik for behandling af personoplysninger i Børnecancerfonden

Vedtaget af Børnecancerfonden den 25.05.2018

Indholdsfortegnelse

1 Baggrund

Der er i EU og Danmark indført nye regler med "Europa-Parlamentets og Rådets forordning (EU) 2016/679" for håndtering af personoplysninger. Reglerne er på mange områder en videreførelse af eksisterende lovgivning, men på nogle områder er reglerne strammet væsentligt.

2 Formål

Formålet med denne persondatapolitik er at fastlægge rammerne for behandling af personoplysninger i Børnecancerfonden. Endvidere har persondatapolitikken til formål at sikre en løbende kontrol med efterlevelsen af krav i gældende lovgivning.

3 Omfang

Denne persondatapolitik finder anvendelse i hele Børnecancerfonden, samt for samarbejdspartnere, der udfører opgaver på vores vegne. Politikken sætter rammerne for, hvordan vi behandler personoplysninger om kunder, medarbejdere, leverandører, samarbejdspartnere og andre.

4 Roller og ansvar

Nedenstående skema giver et overblik over roller og ansvar i Børnecancerfonden. Ledelse og medarbejdere er forpligtede til at handle i henhold til nedenstående i forhold til efterlevelse af gældende regler for beskyttelse af personoplysninger.

Gruppe / funktion	**Roller og ansvar**
Øverste ledelsesniveau/ Direktionen	Det er den øverste ledelse/direktionen, der har det endelige ansvar for, at Børnecancerfonden efterlever gældende regler for beskyttelse af personoplysninger, herunder Persondataforordningen. Den øverste ledelses/direktionens rolle er at foretage dokumenterede ledelsesmæssige beslutninger om beskyttelsen af personoplysninger i Børnecancerfonden.
Daglig leder	Den daglige leder er ansvarlig for, at formålene med behandling af personoplysninger, samt at retningslinjerne til understøttelse af politikken, er kommunikeret klart og tydeligt til medarbejderne.
Databeskyttelsesrådgiver (DPO)	I de fleste tilfælde skal private virksomheder *ikke* udpege en databeskyttelsesrådgiver. Kun private virksomheder, der som deres kerneaktivitet behandler følsomme oplysninger eller oplysninger om strafbare forhold i et stort omfang eller foretager regelmæssig og systematisk overvågning af personer i stort omfang, er forpligtede til at udpege en databeskyttelsesrådgiver. Følgende tre betingelser skal alle være opfyldt: 1. Behandling af personoplysninger skal være virksomhedens *kerneaktivitet* 2. Der skal behandles personoplysninger i et *stort omfang* 3. Behandlingsaktiviteten består i *regelmæssig* og *systematisk overvågning* af personer eller behandlingen vedrører *følsomme oplysninger* eller oplysninger om *strafbare forhold* Børnecancerfondens kerneaktivitet er at yde støtte til: • Lægevidenskabelig og anden forskning • Uddannelses- og mødeaktiviteter og

	• Oplysnings- og informationsvirksomhed Vedrørende børnecancer, samt at yde støtte til foranstaltninger for cancersyge børn og deres pårørende. Der behandles personoplysninger i det omfang der modtages ansøgninger om støtte, udarbejdes støtteprojekter og formidles dokumentation om fondens aktiviteter, hvilket er i et stort omfang, samt oplysninger om medarbejdere i Fonden. Behandlingsaktiviteten er regelmæssig og systematisk og kan indeholde oplysninger om både følsomme forhold, herunder om børn, i stort omfang. Børnecancerfonden har ikke nødvendigvis pligt til at udpege en DPO, da pkt. 1 ikke er opfyldt. Men da Fonden behandler følsomme oplysninger i stort omfang, herunder om børn har Fonden ønsket at sikre overblikket over og efterlevelsen af databeskyttelsesreglerne ved at udpege en DPO.
Systemejer	Systemejeren har ansvaret for driften og vedligeholdelse af div. Systemer, der behandler personoplysninger.
Dataejer	Dataejere er medarbejdere, der ikke er leder, men som har en koordinerende rolle i forhold til at implementere de sikkerhedstiltag, det er vurderet, der er behov for i forhold til beskyttelsen af personoplysninger. De er ligeledes ansvarlige for de personoplysninger, der behandles.
Medarbejdere	Medarbejdere, der behandler personoplysninger, er ansvarlige for at gøre sig bekendt med formålene med behandlingen og de retningslinjer, der er relevante for udførelsen af deres arbejde.

5 Ansvarlighed

Vi udviser altid ansvarlighed, når vi behandler personoplysninger. Det gør vi bl.a. ved at dokumentere:

- de beslutninger, vi træffer
- de foranstaltninger og aktiviteter, vi udfører
- de retningslinjer og kontroller, vi implementerer om behandlingen af personoplysninger.

Endvidere sørger vi aktivt for at holde os opdaterede i henhold til denne politik, samt kravene i underliggende bilag og retningslinjer som der henvises til i teksten.

6 Klassifikation og grundprincipperne for behandling af personoplysninger

Formålet er at sætte de overordnede rammer for, hvordan vi behandler personoplysninger forsvarligt. Persondataforordningens artikel 5 og 9

6.1 Klassifikation af personoplysninger

I Børnecancerfonden har vi truffet beslutning om at klassificere personoplysninger, når vi behandler personoplysninger.

Klassifikationen har bl.a. betydning, når vi vurderer, hvilket behandlingsgrundlag der gør en behandling lovlig, idet vi sondrer mellem behandling af almindelige, almindelige fortrolige og følsomme personoplysninger. Endvidere benytter vi klassifikationen, når vi vurderer,

designer og implementerer tekniske og organisatoriske sikkerhedsforanstaltninger og kontroller for at beskytte personoplysningerne.

6.2 Grundprincipperne for behandling af personoplysninger

Vi behandler personoplysninger i henhold til de gældende regler i forordningen på området. Det betyder bl.a., at vi kun behandler personoplysninger til lovlige, rimelige og legitime formål, som vi kan dokumentere.

Vi indsamler, opbevarer og behandler kun personoplysninger, der er nødvendige for opfyldelsen af det angivne formål for behandlingen. Vi sørger derfor aktivt for at minimere indsamlingen og behandlingen af personoplysninger til det, der er absolut nødvendigt.

Vi begrænser behandlingen af personoplysninger, så vi ikke behandler dem på en måde, der er uforeneligt med det oprindelige formål. Endvidere sikrer vi, at personoplysningerne ikke opbevares i et længere tidsrum end det, der er nødvendigt for at opfylde formålet med behandlingen. Når personoplysningerne ikke længere er nødvendige, sikrer vi, at de enten slettes i henhold til vores regler om sletning, eller at der træffes andre tekniske og organisatoriske foranstaltninger som fx anonymisering, således at den registrerede ikke længere kan identificeres ud fra oplysningerne.

Såfremt personoplysningerne er urigtige eller ufuldstændige/mangelfulde i forhold til de formål, hvortil de behandles, sørger vi for at rette, opdatere eller slette disse.

6.3 Lovlig behandling af personoplysninger

Formålet er at sikre, at vi kun behandler personoplysninger lovligt. Persondataforordningens artikel 6-10

Vi sikrer os, at der er et lovligt grundlag, når vi behandler personoplysninger. Mindst ét af følgende grundlag for behandling af personoplysninger skal dermed gøres gældende.

Grundlagene for almindelige personoplysninger som benyttes hos Børnecancerfonden er:

- **Samtykke** – den registrerede, forældre eller værge har givet samtykke til behandling af personoplysninger.
- **Kontrakt** – behandlingen er nødvendig for at kunne opfylde eller indgå en kontrakt, som den registrerede er en del af.
- **Retlig forpligtelse** – behandlingen er nødvendig for at overholde en retlig forpligtelse.
- **Interesseafvejning** – behandlingen er nødvendig for at forfølge en legitim interesse.

Grundlagene for følsomme personoplysninger (afviger fra grundlagene for almindelige personoplysninger) som benyttes hos Børnecancerfonden er:

- **Samtykke** – den registrerede eller dennes forældre eller værge har givet udtrykkeligt samtykke til behandling af personoplysninger.
- **Arbejds-, sundheds- og socialretlige forpligtelser og rettigheder** – behandlingen er nødvendig for at overholde en organisations eller den registreredes arbejds-, sundheds-, og socialretlige forpligtelser og specifikke rettigheder.
- **Stiftelser og sammenslutninger uden gevinst for øje** – behandlingen foretages af en organisation, der arbejder uden gevinst for øje.
- **Offentliggjort af registrerede** – den registrerede har selv offentliggjort personoplysningerne.
- **Samfundsmæssig interesse** – behandlingen er nødvendig for at kunne udføre en opgave, som er i samfundets interesse.

Samtykke
Såfremt behandlingen foretages på baggrund af et indhentet samtykke fra den registrerede, dennes forældre eller værge, sikrer vi, at samtykket er afgivet frivilligt og er formuleret i et let forståeligt sprog, så den registrerede ikke er tvivl om, hvad der gives samtykke til. Endvidere sikrer vi, at samtykket er afgivet ved en aktiv handling, således at den registrerede fx skal klikke ok, skrive under eller lign. for at acceptere samtykket.

Herudover sikrer vi, at den registrerede bliver oplyst om, at samtykket altid kan trækkes tilbage.

7 Overførsel af personoplysninger til lande uden for EU og EØS (tredjelande)

Formålet er at sikre, at der ikke overføres personoplysninger til lande uden for EU/EØS, uden at vi har et lovligt grundlag herfor. Persondataforordningens artikel 44-50

Vi overfører kun personoplysninger til lande uden for EU og EØS (Det Europæiske Økonomiske Samarbejde), såfremt vi har et lovligt, rimeligt og legitimt grundlag herfor, og vi kan sikre et tilstrækkeligt beskyttelsesniveau. På nuværende tidspunkt overfører Børnecancerfonden data til lande uden for EU med hjemmel i EU-US Privacy Shield.

8 Fortegnelser over behandlingsaktiviteter

Formålet er at sikre, at vi fører de nødvendige fortegnelser over behandlingsaktiviteter, som kan stilles til rådighed for Datatilsynet ved eventuelle tilsyn. Endvidere er formålet at sikre, at der foreligger et grundlag for vurdering af risikoen ved behandling af de registreredes personoplysninger. Persondataforordningens artikel 30

Vi fører en fortegnelse over de behandlinger af personoplysninger, vi foretager, og sørger for at holde fortegnelsen opdateret. Fortegnelsen anvendes bl.a. som en del af dokumentationspligten, såfremt Datatilsynet kommer på tilsyn, samt som grundlag for vurdering af risici for den registrerede ved behandling af dennes personoplysninger.

9 Den registreredes rettigheder

Formålet er at sikre, at behandlingen af personoplysninger tilgodeser den registreredes ret til at kontrollere hvornår, hvordan og i hvilket omfang dennes personoplysninger bliver behandlet, samt hvem den registrerede ønsker, har adgang til sine personoplysninger. Persondataforordningens artikel 12-23

Vi sikrer den registreredes rettigheder ved bl.a. at behandle dennes personoplysninger på en åben og oplyst måde. Det betyder, at vi oplyser den registrerede om, at vi behandler dennes personoplysninger, samt om hvordan, så den registrerede har mulighed for at gøre sine rettigheder gældende.

Herudover hjælper vi den registrerede med at udøve sine rettigheder, og vi håndterer den registreredes anmodning om at gøre sine rettigheder gældende, hvad enten vi skal efterkomme den registreredes anmodning eller ej. Når vi kommunikerer med den registrerede, gør vi det i en kortfattet form og i et klart og letforståeligt sprog.

Nedenfor er listet, hvilke rettigheder vi hjælper den registrerede med, såfremt de anmoder om det:

- Indsigt i de behandlinger af personoplysninger, vi foretager om denne
- Berigtigelse, såfremt personoplysningerne er forkerte eller mangelfulde
- Sletning af de personoplysninger vi behandler
- Begrænsning af behandlingen af personoplysninger
- Udlevering af personoplysninger eller overførsel internt eller til eksternt selskab
- Behandling af indsigelse mod behandling af personoplysninger.

Vi videregiver ikke personoplysninger til samarbejdspartnere eller andre eksterne organisationer, medmindre den registrerede har givet samtykke til dette, eller vi er retligt forpligtet til at videregive personoplysningerne. Hvis du vil gøre brug af ovennævnte rettigheder kan du kontakte os på: kontakt@boernecancerfonden.dk, tlf. 3555 4833 eller pr. brev til Børnecancerfonden, Ramsingsvej 7, 2500 Valby.

Ansøgere om støtte oplyses endvidere om deres rettigheder på Børnecancerfondens hjemmeside https://boernecancerfonden.dk/

10 Dataansvarlig og databehandler

Formålet er at sikre, at det er afklaret, hvorvidt vi er dataansvarlige eller databehandlere i forhold til alle behandlinger af personoplysninger. Endvidere er formålet at sikre, at der er overblik over, hvilke databehandlere der benyttes, og at der er indgået databehandleraftaler med dem.

Persondataforordningens artikel 24-29

Når vi behandler personoplysninger, vurderer vi, hvornår vi er dataansvarlig, databehandler eller har delt ansvar (fælles dataansvarlige).

10.1 Dataansvarlig

Såfremt vi er dataansvarlige, sikrer vi, at alle databehandlere, vi benytter, kan stille de fornødne sikkerhedsgarantier for behandling af personoplysninger. Endvidere sikrer vi, at de er instrueret i, hvordan de må behandle personoplysninger på vores vegne, samt at der er indgået en databehandleraftale, der lever op til kravene i de gældende regler.

10.2 Databehandler

Såfremt vi er databehandlere, sikrer vi, at vi kun behandler personoplysninger under instruks fra den dataansvarlige.

Endvidere sikrer vi, at vi ikke gør brug af andre databehandlere (underdatabehandlere), uden at vi har fået dette godkendt af den dataansvarlige.

Såfremt vi har fået en skriftlig godkendelse fra den dataansvarlige, sikrer vi, at vi underretter den dataansvarlige, såfremt vi planlægger at udskifte anvendte databehandlere, eller indgå aftaler med nye, således at den dataansvarlige får mulighed for at gøre indsigelse mod sådanne ændringer.

Såfremt den dataansvarlige har godkendt, at vi bruger andre databehandlere (underdatabehandlere), sikrer vi, at de minimum lever op til de krav, som den dataansvarlige har stillet os.

10.3 Fælles dataansvarlige

Hvis vi er fælles dataansvarlige med en anden organisation, sikrer vi, at vi har fastlagt det delte ansvar i forhold til overholdelse af gældende regler på området. Vi sikrer endvidere, at de forpligtelser, vi har over for den registrerede, overholdes, herunder hvem der gør oplysningerne tilgængelige for den registrerede, samt at dette sker på en åben og oplyst

måde. Den registrerede kan dog frit vælge, hvilken dataansvarlig denne vil udøve sine rettigheder overfor.

11 Registreredes risikovurdering

Formålet er at identificere potentielle risici for den registrerede ved behandling af dennes personoplysninger.

Når vi behandler personoplysninger, vurderer vi risiciene for den registrerede ved behandlingen af dennes personoplysninger. Vi foretager vurderingen på baggrund af de behandlingsaktiviteter, vi foretager, herunder anvendte systemer, således at vi får et samlet overblik over risiciene. Risiciene er beregnet og identificeret på baggrund af en mulig konsekvens for den registrerede ved behandlingen af dennes personoplysninger, samt sandsynligheden for at konsekvensen indtræffer.

Risikovurderingen dokumenteres periodisk og ad hoc ved behov og godkendes af det øverste ledelsesniveau hos Fonden.

12 Konsekvensanalyse

Formålet er at sikre, at der foretages en konsekvensanalyse forud for behandling af personoplysninger, der sandsynligvis indebærer høj risiko for den registrerede, for dermed at identificere tiltag, der kan reducere denne risiko.

Persondataforordningens artikel 35+36

Hvis det er vurderet i registreredes risikovurdering, at en type behandling af personoplysninger sandsynligvis vil indebære høj risiko for de registreredes rettigheder eller frihedsrettigheder, udfører vi en konsekvensanalyse. Konsekvensanalysen skal hjælpe med at fastlægge de foranstaltninger, vi påtænker, kan imødegå disse risici. Såfremt de påtænkte tekniske og organisatoriske sikkerhedsforanstaltninger ikke kan imødegå risiciene i tilstrækkelig omfang, rådfører vi os hos Datatilsynet, inden vi foretager behandling af personoplysningerne.

13 Behandlingssikkerhed

Formålet er at sikre, at der er tilstrækkelig sikkerhed ved behandling af personoplysninger, som afdækker de identificerede risici i risiko- og konsekvensanalysen.

Persondataforordningens artikel 32 og 25

Vi sikrer, at der opretholdes et tilstrækkeligt sikkerhedsniveau både teknisk og organisatorisk ved behandling af personoplysninger.

13.1 Sikkerhedsstyring

På baggrund af den udarbejdede risikoanalyse og konsekvensanalyse definerer vi, hvilket sikkerhedsniveau og hvilke sikkerhedstiltag, der skal være implementeret for at sikre et tilstrækkeligt beskyttelsesniveau, når vi behandler personoplysninger.

I den forbindelse overvejer vi følgende forhold:

- Brugen af pseudonymisering, kryptering og anonymisering.
- Sikring af fortrolighed og integritet.
- Systemernes tilgængelighed og modstandsdygtighed (robusthed).
- Muligheden for at kunne genskabe tilgængelighed og adgang til behandlede personoplysninger inden rimelig tid (backup).

- De identificerede risici, som behandling af personoplysninger indebærer, såsom hændelig eller ulovlig tilintetgørelse, tab, ændring eller uautoriseret videregivelse af eller adgang til de behandlede personoplysninger, som kan føre til fysisk, materiel eller immateriel skade.

Vi revurderer løbende proceduren for sikkerhedstiltag, og ved ændringer testes og evalueres sikkerheden, for at sikre at sikkerhedsniveauet fortsat er tilstrækkeligt.

13.2 Privacy by design/default

Vi sikrer os, at løsninger, der anvendes til behandling af personoplysninger, er designet, således at de reducerer graden af indgriben i den registreredes privatliv.

Endvidere sikrer vi, at løsninger, der anvendes til behandling af personoplysninger, har sikkerhedsindstillingerne slået til som standard, således at der ikke indhentes eller behandles flere personoplysninger, end hvad der er nødvendig til behandlingens formål, samt at personoplysninger ikke opbevares i længere tid end nødvendigt.

Herudover sikrer vi, at personoplysninger ikke stilles til rådighed for andre, uden der har været en fysisk person involveret, hvilket betyder, at udlevering af personoplysninger til andre ikke må ske automatisk, fx som følge af en proces.

14 Brud på persondatasikkerheden

Formålet er at sikre, at brud på persondatasikkerheden håndteres korrekt, herunder at der sker anmeldelse til Datatilsynet, og at den registrerede underrettes, såfremt bruddet har høj konsekvens for den registrerede.

Persondataforordningens artikel 33 og 34

14.1 Anmeldelse til Datatilsynet

Såfremt der skulle ske et brud på persondatasikkerheden, anmelder vi det uden unødig forsinkelse og senest 72 timer, efter vi har opdaget det, til Datatilsynet. Hvis det er usandsynligt, at bruddet indebærer en risiko for de registreredes rettigheder eller frihedsrettigheder, er vi ikke forpligtet til at anmelde det.

14.2 Underretning til den registrerede

Hvis bruddet sandsynligvis vil indebære høj risiko for de registreredes rettigheder eller frihedsrettigheder, underretter vi endvidere de registrerede om bruddet uden unødig forsinkelse og oplyser om, hvad konsekvensen for dem er.

15 Kontakten til Datatilsynet

Formålet er at sikre, at eventuelle tilsyn og henvendelser fra Datatilsynet håndteres korrekt, herunder at Datatilsynet får den rette dokumentation.

Persondataforordningens kapitel VI

Såfremt Datatilsynet skulle foretage tilsyn eller rette henvendelse til Børnecancerfonden, sikrer det øverste ledelsesniveau, at de får den efterspurgte og rette information, herunder fortegnelserne over behandlingsaktiviteter.

Endvidere sikrer vi, at vi til enhver tid overholder de tidsfrister, som Datatilsynet måtte stille i forbindelse med et tilsyn eller en henvendelse.