HOVEDSTADENS BEREDSKAB

POLITIK FOR DATABESKYTTELSE

27-08-2018

Sagsnr.

2018-0005556

Dokumentnr.

2018-0005556-2

1 Formål

For at varetage beredskabets opgaver på optimal vis, er det nødvendigt at behandle en række almindelige, fortrolige og følsomme personoplysninger fra medarbejdere og borgere.

Behandlingen af personoplysninger kan som følge af persondataretlige krav have direkte indflydelse på Hovedstadens Beredskabs økonomi, omdømme og borgernes tillid til organisationen. Derfor er det essentielt, at Hovedstadens Beredskab fastsætter retningslinjer for behandling af personoplysninger og sikrer, at alle dele af Hovedstadens Beredskabs organisation er bekendt med retningslinjerne. Politik for databeskyttelse skal medvirke til at sikre dette.

2 Anvendelsesområde

Politikken gælder for samtlige behandlinger af personoplysninger, der udføres eller planlægges af Hovedstadens Beredskab.

Politikken fastlægger de overordnede definitioner, regler og vejledninger for at sikre, at Hovedstadens Beredskabs ansatte håndterer og beskytter personoplysninger i overensstemmelse med lovgrundlaget og de registreredes forventninger.

3 Referencer

Politikken tager afsæt i lovgrundlaget, først og fremmest Databeskyttelsesforordningen og Databeskyttelsesloven.

Databeskyttelsespolitikken supplerer it-sikkerhedspolitikken for Hovedstadens Beredskab og er derudover rammesættende for interne regler om databeskyttelse.

4 Definitioner

Personoplysninger: Enhver form for information om en identificeret eller identificerbar fysisk person. Ved identificerbar menes: Direkte eller indirekte identifikation gennem f.eks. navn, tjenestenummer, j.nr., nummerplade etc.

Følsomme personoplysninger:[1] Personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt 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.

Behandling betyder enhver aktivitet eller række af aktiviteter, som personoplysninger gøres til genstand for. Dette inkluderer f.eks.

[1] I databeskyttelsesforordningen 2016/679 kaldes disse oplysninger for "særlige kategorier at personoplysninger", se artikel 9, stk. 1.

indsamling, registrering, organisering, opbevaring, tilpasning, ændring, genfinding, søgning, brug, videregivelse ved transmission eller overladelse, sammenstilling, begrænsning, sletning eller tilintetgørelse.

Registrerede personer eller 'de registrerede' er fysiske personer, primært medarbejdere og borgere, hvis personoplysninger behandles af Hovedstadens Beredskab.

5 Vision og mål for beskyttelse af personoplysninger

Hovedstadens Beredskabs overordnede vision i forhold til beskyttelsen af personoplysninger er:

> *"Hovedstadens Beredskab har en klar ambition om at opnå en høj grad af gennemsigtighed i forhold til organisationens behandling af persondata - både manuelt og digitalt.*
>
> *Det er essentielt at medarbejdere, samarbejdspartnere og borgere kan regne med, at it-sikkerheden er høj, og at personoplysninger ikke behandles til andre formål end de højest nødvendige.*
>
> *Dette sikres ved at koncentrere ressourcerne om de områder, der indebærer den højeste risiko i forhold til databeskyttelsesforordningen og it-sikkerhed generelt, og ved at skabe en kultur internt i Hovedstadens Beredskab, hvor privatlivsbeskyttelse konsekvent har en høj prioritet."*

Det er Hovedstadens Beredskabs klare overbevisning, at ovenstående vision kan nås, hvis nærværende databeskyttelsespolitik efterleves.

Hovedstadens Beredskabs mål med denne databeskyttelsespolitik er at opretholde organisationens integritet og troværdighed i forhold til behandlingen af personoplysninger.

6 Roller og ansvar

Alle ansatte skal sikre, at persondatabeskyttelsespolitikken overholdes i deres daglige arbejde samt i de aktiviteter og processer, som de har ansvaret for.

Databeskyttelsesrådgiveren (herefter DPO'en) overvåger Hovedstadens Beredskabs overholdelse af lovgrundlaget og denne politik for persondatabeskyttelse. DPO'en overvåger også om politikken er effektiv og tilstrækkelig i forhold til lovgrundlaget og udviklingen i dette.

DPO'en er Hovedstadens Beredskabs interne og eksterne kontaktpunkt i forhold til sager om beskyttelse af personoplysninger.

DPO'en rådgiver Hovedstadens Beredskab og ansatte i forhold til eksisterende eller planlagte aktiviteter, som involverer personoplysninger. DPO'en rådgiver også de registrerede om deres rettigheder i forhold til Hovedstadens Beredskabs behandling af personoplysninger.

DPO'en kan kontaktes på dpo@hbr.dk og tlf. 33 43 13 55.

Databeskyttelsesrådgiverens forretningspartnere er bindeled mellem de forskellige forretningsområder og DPO'en og bistår DPO'en i overvågning og rådgivning af organisationen i forhold til behandling af personoplysninger.

Ledelsen er ansvarlig for Hovedstadens Beredskabs aktiviteter, inkl. behandling af personoplysninger og deres overensstemmelse med lovgrundlaget. Ledelsen træffer de nødvendige beslutninger og passende foranstaltninger i forhold til persondatabeskyttelsespolitikkens effektivitet og tilstrækkelighed.

Databeskyttelsesrådgiverens og forretningspartnernes roller og ansvar skal være beskrevet i funktionsbeskrivelser eller tilsvarende.

7 Databehandlingsprincipper

Hovedstadens Beredskabs behandling af personoplysninger skal altid være i overensstemmelse med de grundprincipper, der er beskrevet i dette afsnit og som følger af lovgrundlaget[2]. Principperne er:

1. Lovlig, rimelig og gennemsigtig behandling
2. Formålsbegrænsning
3. Dataminimering
4. Integritet, fortrolighed og tilgængelighed
5. Opbevaringsbegrænsning

7.1 Lovlig, rimelig og gennemsigtig behandling

Hovedstadens Beredskab foretager kun behandling af personoplysninger, når behandling er baseret på et lovligt grundlag. Der gælder forskellige regler afhængigt af om der er tale om almindelige personoplysninger, følsomme personoplysninger eller cpr-numre og oplysninger om strafbare forhold.

7.1.1 Behandling af almindelige personoplysninger

Jf. persondataretten er en behandling lovlig, når mindst ét af følgende grundlag er til stede:

[2] Se artikel 5 i databeskyttelsesforordningen 2016/679.

- ***Offentlig myndighedsudøvelse***: Behandlingen er nødvendig for at udføre en opgave, som er en del af Hovedstadens Beredskabs myndighedsudøvelse.
- ***Retlig forpligtelse***: Behandlingen er nødvendig for at overholde Hovedstadens Beredskabs forpligtelser.

  Dette kan fx være i tilfælde, hvor Hovedstadens Beredskab skal videregive oplysninger om en ansat til skattemyndighederne.
- ***Kontraktretlig forpligtelse***: Behandlingen er nødvendig til brug for opfyldelse af en kontrakt, som den registrerede er part i, eller ved gennemførelse af kontraktuelle indledende aktiviteter.

  OBS: Det er kun de aktiviteter, som er nødvendige for at opfylde kontrakten, der er dækket af denne grund. F.eks. er behandling af ansattes bankkontodetaljer nødvendig for lønudbetaling og dermed opfyldelse af ansættelseskontrakten, mens videoovervågning af ansatte ikke er.
- ***Samtykke***: En behandling er lovlig, når der foreligger en frivillig, specifik, informeret og utvetydig indvilgelse i, at personoplysninger der vedrører den registrerede, gøres til genstand for behandling.

  OBS: Fordi samtykket skal være frivilligt, er det sjældent hensigtsmæssigt at anvende i ansættelsesmæssig sammenhæng, hvor der kan være tvivl om en ansats mulighed for at afvise en anmodning om behandling af personoplysninger.[3]
- ***Legitim interesse***: Behandlingen er nødvendig for, at Hovedstadens Beredskab eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesse eller grundlæggende rettigheder og frihedsrettigheder går forud herfor.
- ***Vitale interesser***: Behandlingen er nødvendig for at beskytte en fysisk persons liv, og ingen andre grundlag for behandling anvendes.

Hovedstadens Beredskab opretholder gennemsigtighed vedrørende sine aktiviteter, især når disse kan påvirke fysiske personers rettigheder eller frihedsrettigheder[4]. Gennemsigtigheden kommer især til udtryk i organisationen ved, at det er nemt for de registrerede at gennemskue

[3] Se DT vejledning, November 2017 og WP 259 (udkast)

[4] Se evt. Artikel 29-gruppens notat om gennemsigtighed: https://www.datatilsynet.dk/fileadmin/user_upload/dokumenter/Vejledninger/wp260_gennemsigtighed_en.pdf

hvorfor de afgiver deres personoplysninger, og hvad de bliver brugt til. Derudover sikrer Hovedstadens Beredskab, at enhver behandling er rimelig i forhold til formålet med behandlingen.

7.1.2 Behandling af følsomme personoplysninger

Hovedstadens Beredskab behandler i visse situationer en række følsomme personoplysninger. Eftersom lovgivningen stiller skærpede krav ved behandlingen af følsomme personoplysninger, sikrer Hovedstadens Beredskab at sådanne oplysninger kun behandles, hvis mindst én af følgende omstændigheder er til stede:

- ***Retlig forpligtelse:*** Behandlingen er nødvendig og udtrykkeligt tilladt i medfør af lov
- ***Samtykke:*** Den registrerede har givet sit udtrykkelige samtykke til behandlingen
- ***Egen offentliggørelse:*** Den registrerede har tydeligvis offentliggjort disse personoplysninger (forstået som offentliggørelse til den brede befolkning, og ikke blot eksempelvis når der uopfordret indsendes oplysninger til Hovedstadens Beredskab)
- ***Vitale interesser:*** En fysisk persons vitale interesser er i spil, og den registrerede er ikke i fysisk eller juridisk stand til at give samtykke til behandlingen.

7.1.3 Behandling af CPR-numre og oplysninger om strafbare forhold

I de tilfælde, hvor Hovedstadens Beredskab behandler CPR-numre eller oplysninger om en persons strafbare forhold finder de behandlingsprincipper, der er fastsat i denne sektion ligeledes anvendelse. Hovedstadens Beredskab behandler udelukkende disse oplysninger, når der hjemmel til dette i lovgrundlaget.

7.2 Formålsbegrænsning

Hovedstadens Beredskab indsamler og behandler kun personoplysninger til begrænsede, veldefinerede/udtrykkeligt angivne og legitime formål. Hovedstadens Beredskab kan herudover viderebehandle personoplysninger, hvis det sker til formål, der har hjemmel i en lov eller databeskyttelsesforordningen.

Formålets omfang samt formålet ved en eventuel viderebehandling fastsættes *inden* personoplysninger indsamles. Hvis Hovedstadens Beredskab viderebehandler personoplysninger til et nyt formål, sikrer Hovedstadens Beredskab at der ligeledes eksisterer et lovgrundlag til den nye behandling – eksempelvis et nyt samtykke – og at den nye

behandling ligeledes står i et rimelig forhold til formålet med behandlingen.

7.3 Dataminimering

Hovedstadens Beredskabs ledere og medarbejdere sørger for kun at behandle de personoplysninger, som er nødvendige for at varetage organisationens formål.

7.4 Integritet, fortrolighed og tilgængelighed

I overensstemmelse med it-sikkerhedspolitikken er det Hovedstadens Beredskabs princip at sikre oplysninger og behandlingssystemer ift.:

Fortrolighed, dvs. at modtagelse af eller adgang til personoplysninger er begrænset til dem, som skal udføre behandlingen og at dette er sikret gennem passende administrative, tekniske og fysiske sikkerhedsforanstaltninger.

Integritet, dvs. at personoplysningers rigtighed og fuldstændighed bevares gennem hele behandlingen, og at oplysninger er beskyttet mod uautoriserede ændringer eller hændeligt tab, tilintetgørelse eller beskadigelse. Hvis det eksempelvis konkluderes – eller der har været mistanke om – at visse personoplysninger har været manipuleret eller ikke er korrekte, tages der rimelige skridt for at sikre, at oplysningerne bliver ajourført, berigtiget eller slettet.

Tilgængelighed, dvs. at personoplysninger altid er tilgængelige for dem, som har rettigheder dertil. Hovedstadens Beredskab opretholder robusthed i de systemer, som bruges ved behandling af personoplysninger, og gennemfører passende foranstaltninger for at være i stand til at retablere systemers tilgængelighed og integritet i tilfælde af fysiske eller tekniske hændelser.

7.5 Opbevaringsbegrænsning

Hovedstadens Beredskab opbevarer kun oplysninger, der kan identificere en fysisk person, så længe de er nødvendige for behandling til et bestemt og specificeret formål.

Opbevaringsperioder fastsættes så tidligt som muligt for de enkelte behandlingsaktiviteter.

Når der ikke længere er et formål med at behandle personoplysningerne, slettes de eller anonymiseres, så en fysisk person ikke længere kan identificeres ved brug af disse oplysninger. I nogle tilfælde kan der dog være pligt til fortsat opbevaring af oplysningerne; fx i kraft af arkivlovgivningen.

8 Risikovurdering og afbødning af risici

8.1 Sikkerhedsniveauet tilpasses risici

Hovedstadens Beredskab har implementeret en række basale tekniske, administrative og organisatoriske foranstaltninger til beskyttelse af data.

Risici for de registreredes rettigheder og frihedsrettigheder varierer imidlertid i sandsynlighed og konsekvens i forhold til behandlingens karakter, omfang, sammenhæng og formål.

Eksempler:

Oplysningers omfang: isolerede oplysninger om en persons navn og adresse indebærer lavere risici for den registrerede, end hvis de er forbundet med personens helbredsoplysninger.

Behandlingsaktiviteter: indsamling af de registreredes oplysninger i en database i Hovedstadens Beredskab indebærer lavere risici for de registrerede end videregivelse eller overførsel af disse oplysninger til andre virksomheder og myndigheder.

Hovedstadens Beredskab tilpasser derfor beskyttelsesniveauet for personoplysninger til de faktiske risici, som knytter sig til de forskellige behandlingsaktiviteter.

Hovedstadens Beredskab behandler ikke personoplysninger, hvis risiciene er for høje, medmindre Hovedstadens Beredskab er retligt forpligtet til at udøve behandlingen.

8.2 Indledende risikovurdering og konsekvensanalyser (DPIA)

Når Hovedstadens Beredskab overvejer eller planlægger at foretage behandling af personoplysninger, vurderes indledningsvist hvilke risici behandlingen kan have og om behandlingen kan have konsekvenser for de registreredes rettigheder og frihedsrettigheder. Herudfra afgøres om behandlingen af de pågældende personoplysninger kræver særlige kontrol- eller sikkerhedsforanstaltninger.

Risikovurderingen kan omfatte flere lignende eller forbundne behandlingsaktiviteter, og skal derfor nødvendigvis ikke foretages på alle aktiviteter hver for sig. Imidlertid er det centralt, at vurderingen udføres *før* behandlingen iværksættes, og at DPO'en involveres.

Viser en indledende risikovurdering, at en bestemt type behandling sandsynligvis vil indebære høje risici, skal en konsekvensanalyse gennemføres (også kaldet DPIA – "data protection impact analysis").

Der skal foreligge retningslinjer for gennemførelse af risikovurderinger og konsekvensanalyser til understøttelse af politikken.

8.3 Opfølgning på risikovurderinger

Hovedstadens Beredskab fastsætter en proces for jævnlig test og vurdering af effektiviteten, tilstrækkeligheden og nødvendigheden af behandlingernes tekniske og organisatoriske sikkerhedsforanstaltninger.

Risikovurderinger skal gentages eller ajourføres, hvis der sker en markant ændring i behandlingsformålet- eller betingelserne. En fornyet risikovurdering af enhver behandlingsaktivitet foretages under alle omstændigheder senest tre år efter den seneste risikovurdering.

8.4 Databeskyttelse i design og standardindstillinger

Ved vurdering af hvilke sikkerhedsforanstaltninger, der er nødvendige til at forebygge og minimere risici og overholde behandlingsprincipperne i sektion 7, spiller databeskyttelse gennem design og standardindstillinger en væsentlig rolle.

Det betyder i praksis, at processer, systemer, it-infrastruktur, skabeloner osv. så vidt muligt skal være designet og sat op til at sikre behandlingsprincipperne nævnt i sektion 7, herunder være gennemtænkt i forhold til at minimere brugen af personoplysninger og begrænse risici for de registrerede.

9 Gennemsigtighed i behandling

9.1 Tilgang til gennemsigtighed i behandling af personoplysninger

Hovedstadens Beredskab gennemfører og opretholder gennemsigtighed i enhver behandling af personoplysninger og omkring behandlingsaktiviteter.

Som udgangspunkt formidler Hovedstadens Beredskab derfor rettidige og fuldstændige oplysninger om deres behandlingsaktiviteter med passende undtagelse i forhold til fortrolige oplysninger eller retlig tavshedspligt. Hovedstadens Beredskab imødekommer og understøtter de registreredes udøvelse af deres rettigheder.

Denne tilgang sikrer, at de registrerede er bevidste omkring, hvilke oplysninger der bliver behandlet af Hovedstadens Beredskab og grunden hertil, samt tilgængelige klage- eller berigtigelsesmidler. Hovedstadens Beredskabs gennemsigtighedsregler, procedurer og principper, understøtter Hovedstadens Beredskabs kontrol over behandlingsaktiviteters overensstemmelse med lovgrundlaget og databeskyttelsespolitik samt de registreredes rimelige forventninger.

Gennemsigtighed gennem behandling og omkring behandlingsaktiviteter betyder også, at Hovedstadens Beredskab kan påvise overensstemmelse med lovgrundlag og databeskyttelsespolitik til myndigheder og registrerede.

9.2 Kommunikation med de registrerede

Hovedstadens Beredskabs kommunikation med de registrerede gennemføres i en kortfattet, gennemsigtig, letforståelig og lettilgængelig form og i et klart og enkelt sprog. Hovedstadens Beredskab kommunikerer skriftligt med de registrerede og så vidt muligt elektronisk.

OBS: Hvor mundtlig oplysning kræves af de registrerede, skal Hovedstadens Beredskab i alle tilfælde være i stand til at påvise, hvilken information der blev givet og at denne var i overensstemmelse med lovgrundlaget og databeskyttelsespolitikken.

9.3 De registreredes rettigheder

De registrerede personer har i kraft af lovgivningen følgende rettigheder i forhold til Hovedstadens Beredskabs behandling af deres personoplysninger:

Oplysningspligt: Hovedstadens Beredskab oplyser de registrerede, når deres personoplysninger indsamles og om formålet dermed. Hovedstadens Beredskab oplyser desuden de registrerede når formålet med behandlingen, eller selve behandlingsaktiviteten, ændres.[5]

Ret til indsigt i Hovedstadens Beredskabs behandling, dvs. bekræftelse af, at den registreredes personoplysninger bliver behandlet, beskrivelse af denne behandling, information om vedkommendes rettigheder samt kopi af de personoplysninger, som behandles.

Ret til berigtigelse af urigtige personoplysninger eller til fuldstændiggørelse af ufuldstændige oplysninger.

Ret til sletning eksempelvis; i tilfælde hvor personoplysninger, som ikke (længere) er nødvendige til Hovedstadens Beredskabs formål; hvor et samtykke trækkes tilbage af registrerede; eller hvor den registrerede gør indsigelser mod behandlingen mv.

Ret til begrænsning af behandling af personoplysninger, mens Hovedstadens Beredskab vurderer en anmodnings gyldighed, eller i stedet for sletning.

Ret til dataportabilitet i det omfang Hovedstadens Beredskab har behandlingsaktiviteter, der er omfattet af denne ret. Retten finder nemlig ikke anvendelse på behandling der er nødvendig for udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.

[5] Se eventuelt WP260 (udkast)

Ret til indsigelse mod en behandling udført af Hovedstadens Beredskab med grundlag i Hovedstadens Beredskabs myndighedsudøvelse, retlige forpligtelse eller legitime interesse. I disse tilfælde vurderer Hovedstadens Beredskab, om der eksisterer vægtige legitime grunde til at fortsætte behandlingen.

Underretningspligt: Hovedstadens Beredskab underretter personoplysningernes eksterne modtagere om enhver berigtigelse, sletning eller begrænsning, der er udført eller registreredes anmodning herom.

Der kan ske ændringer i disse rettigheder, som følge af ændringer i lovgrundlaget. Det gælder især i forhold til behandlingsaktiviteter, som udgår fra Hovedstadens Beredskabs myndighedsudøvelse eller retlige forpligtelser.

Der skal foreligge en proces for håndtering af anmodninger om udøvelse af rettigheder.

10 Styring af personoplysninger

10.1 Fortegnelse over behandlingsaktiviteter

Hovedstadens Beredskab er forpligtet til at føre en fortegnelse over sine behandlingsaktiviteter. Denne fortegnelse understøtter Hovedstadens Beredskabs styring med de aktiviteter, som vedrører personoplysninger og aktiviteternes overensstemmelse med loven og denne databeskyttelsespolitik.

Hovedstadens Beredskabs behandlingsfortegnelse beskriver de forskellige kategorier af behandlingsaktiviteter, inkl. kategorier af oplysninger, registrerede og modtagere, information om overførsler til tredjelande (ikke-EU lande) og, hvor muligt, forventet opbevaringsperiode og de tekniske og organisatoriske sikkerhedsforanstaltninger vedrørende behandlingen.

10.2 Overførsel/videregivelse af personoplysninger

Hovedstadens Beredskab er ansvarlig for beskyttelsen af de personoplysninger, der behandles af selskabet. Derfor vil Hovedstadens Beredskab som udgangspunkt ikke videregive eller give adgang til personoplysninger til 3. parter, medmindre der findes en hjemmel til og er et konkret formål med overførslen/videregivelsen.

10.3 Eksterne databehandlere

Hovedstadens Beredskab overfører/overlader kun personoplysninger til en ekstern behandler – fx et privat selskab eller en offentlig myndighed – når behandlingsvilkårene er fastsat i en kontrakt (databehandleraftale) eller i lovgrundlaget.

Derudover fører Hovedstadens Beredskab passende kontroller med sine eksterne databehandlere for at sikre, at disse overholder de fastsatte behandlingsvilkår.

11 Brud på persondatasikkerhed

Hvis der sker et hændeligt eller intentionelt brud på sikkerheden, som fører til at personoplysningers fortrolighed, integritet eller tilgængelighed kompromitteres, er der tale om et brud på persondatasikkerheden.

Et persondatabrud kan føre til alvorlige konsekvenser for de registreredes rettigheder og frihedsrettigheder og Hovedstadens Beredskabs integritet og troværdighed.

Hovedstadens Beredskab vil ved et eventuelt persondatabrud analysere hændelsen og implementere forebyggende og korrigerende tiltag, der kan afbøde konsekvenserne af bruddet og minimere sandsynligheden for at det sker igen. Hovedstadens Beredskab bestræber sig samtidig på at værne de registrerede mod de mulige farer og risici, som følger af et persondatabrud.

Ansatte, som bliver bekendt med eller har mistanke om et persondatabrud i Hovedstadens Beredskab, skal anmelde dette hurtigst muligt.

12 Overtrædelse af retningslinjerne

Personoplysninger må kun behandles i overensstemmelse med denne politik, og kun efter instruks fra Hovedstadens Beredskab. Overtrædelse af politikken kan få ansættelsesretlige konsekvenser.

13 Godkendelse og ikrafttræden

HovedMED har godkendt databeskyttelsespolitikken på møde den 13. september 2018 og politikken træder i kraft umiddelbart herefter. Bestyrelsen orienteres efterfølgende om politikken på møde den 14. november.

Databeskyttelsespolitikken revideres i HovedMED på begæring af enten arbejdsgiver- eller medarbejderside.

Politikken kan opsiges med tre måneders varsel med henblik på genforhandling. Hvis parterne ikke er enige om en ny politik, kan arbejdsgiversiden udstikke de nødvendige retningslinjer.