7. APRIL 2020

DATABESKYTTELSESRETLIGE PROBLEMSTILLINGER I RELATION TIL COVID-19

AF ANDERS VALENTINER-BRANTH, RASMUS BLAABJERG, OLE HASSELGAARD OG ULRICH C. TYNDESKOV

I forbindelse med den aktuelle COVID-19-pandemi opstår der også en række forskellige spørgsmål af databeskyttelsesretlig karakter, herunder eksempelvis i forhold til anvendelse af elektroniske opkaldstjenester i sagsbehandlingen, bekæmpelse og kortlægning af COVID-19-pandemien, behandling af oplysninger om medarbejdere, behandlingssikkerhed ved brug af hjemmearbejdspladser og håndtering af databehandleres (herunder f.eks. hostingleverandører) konkurs. Det er relevant for både offentlige myndigheder, faglige organisationer, private virksomheder og andre typer af dataansvarlige at forholde sig til disse spørgsmål.

Anvendelse af elektroniske opkaldstjenester i sagsbehandlingen

Blandt andet offentlige myndigheder, private virksomheder og faglige organisationer er på baggrund af COVID-19-pandemien i højere grad gået over til at anvende hjemmearbejdspladser og til at afholde møder, konferencer og lignende digitalt. Som følge heraf gøres der i vidt omfang brug af forskellige former for elektroniske opkaldstjenester til at kommunikere internt i organisationerne såvel som eksternt til andre, f.eks. i forbindelse med sagsbehandlingen.

Kendetegnende for de fleste typer af elektroniske opkaldstjenester er, at de etablerer en forbindelse på internettet mellem afsender og modtager. Afsender og modtager kan via denne forbindelse kommunikere skriftligt eller mundtligt (herunder også ved brug af video) med hinanden. Eksempler på sådanne elektroniske opkaldstjenester er Microsoft Teams, Skype, Zoom og Facebook Messenger.

Der kan være gode praktiske grunde til, at en medarbejder finder det nemmere at optage en samtale mv., f.eks. fordi medarbejderen i den offentlige forvaltning herefter ikke er forpligtet til at tage notater om samtalen.

Vælger en medarbejder imidlertid at lagre sådanne oplysninger digitalt, vil der være tale om, at personoplysninger (en persons stemme eller et billede af personen udgør en personoplysning), der med den digitale lagring vil være undergivet elektronisk behandling. I givet fald skal alle reglerne i databeskyttelsesforordningen og databeskyttelsesloven iagttages af den dataansvarlige.

Det bemærkes, at i det omfang en transmission via en opkaldstjeneste ikke er forbundet med optagelse eller anden lagring, vil der efter omstændighederne kunne være tale om elektronisk behandling af en så flygtig karakter, at databeskyttelsesforordningens og lovens bestemmelser ikke finder anvendelse. Der kan i den forbindelse eksempelvis henvises til Kristian Korfits Nielsen og Anders Lotterup i den nye og meget anbefalelsesværdige bog: Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer (side 253-254 og 260-261).

Vælger den enkelte medarbejder at lagre samtalerne mv., vil den dataansvarlige derimod f.eks. med sikkerhed skulle leve op til reglerne om de registreredes rettigheder i databeskyttelsesforordningens kapitel III, herunder at de registrerede skal gives information om behandlingen, ligesom de registrerede efter omstændighederne kan have ret til indsigt, indsigelse, sletning eller lignende.

Derudover skal man også sikre sig, at man har hjemmel til at foretage den pågældende behandling, f.eks. i databeskyttelsesforordningens artikel 6 om behandling af almindelige personoplysninger (hvis der i samtalen bliver nævnt oplysninger, der er følsomme oplysninger, vil der i givet fald også skulle være hjemmel til at behandle sådanne oplysninger), ligesom de almindelige behandlingsprincipper i artikel 5 skal overholdes, således at der f.eks. ikke indsamles flere personoplysninger end nødvendigt, og at oplysningerne slettes, når det ikke længere er nødvendigt at opbevare dem af hensyn til formålet. Højesteret har i U 2019.3878 H taget stilling til en om optagelse af sådanne samtaler, hvor Højesteret også kommer ind på betydningen af straffelovens § 263, stk. 2, 2. pkt.

Hvis man som dataansvarlig også er omfattet af forvaltningslovens og offentlighedslovens regler, skal man herudover blandt andet være opmærksom på, at borgerne efter omstændighederne kan have ret til aktindsigt i de pågældende optagede oplysninger.

Allerede fordi det er vanskeligt fuldstændigt at sikre, at der ikke konkret bliver lagret enkelte samtaler mv., anbefaler vi her ud over at man som dataansvarlig sikrer sig, at anvendte opkaldstjenester har de fornødne sikkerhedsforanstaltninger på plads (jf. herom i afsnittet "Behandlingssikkerhed ved brug af hjemmearbejdspladser" nedenfor).

Bekæmpelse og kortlægning af COVID-19-pandemien

En række offentlige myndigheder såvel som private virksomheder har været med til at iværksætte initiativer til kortlægning og bekæmpelse af COVID-19-pandemien, f.eks. gennem hjemmesider, apps, spørgeskemaer mv. Disse initiativer kan være meget forskellige, men det er fælles for mange af initiativerne, at de indebærer indsamling af personoplysninger, herunder f.eks. om sygdomssymptomer og eventuelt også om bevægelsesmønstre for relevante persongrupper.

Selv om sådanne initiativer kan være med til at understøtte sundhedsmyndighedernes arbejde med at kortlægge og bekæmpe pandemien, skal man som dataansvarlig, der vil iværksætte et sådant projekt, være opmærksom på de grænser, der følger af de databeskyttelsesretlige regler.

Datatilsynet fremhæver i en nyhed den 2. april 2020, at sådanne initiativer kan være lovlige, men at det modsatte også kan være tilfældet.

Som dataansvarlig skal man f.eks. overveje, om man har hjemmel til behandlingen af de pågældende personoplysninger. Overordnet vil det være sådan, at jo mere fortrolige eller følsomme personoplysningerne er, desto snævrere er adgangen til at behandle dem i forbindelse med bekæmpelse og kortlægning af COVID-19-pandemien.

Det er vores opfattelse, at man som udgangspunkt ikke uden et samtykke, der lever op til reglerne i databeskyttelsesforordningen, vil kunne behandle følsomme helbredsoplysninger fra de registrerede til at kortlægge eller bekæmpe COVID-19-pandemien, hvis man ikke er pålagt en retlig forpligtelse hertil, f.eks. i medfør af sundhedslovgivningen, eller hvis der ikke er tale om statistiske eller videnskabelige undersøgelser af væsentlig samfundsmæssig betydning, jf. databeskyttelseslovens § 10, stk. 1.
Man skal også være opmærksom på de almindelige behandlingsprincipper i databeskyttelsesforordningens artikel 5, herunder f.eks. at der ikke indsamles flere personoplysninger end nødvendigt til formålet, at man ikke senere viderebehandler personoplysningerne til et formål, som er uforeneligt med det oprindelige formål (f.eks. markedsføring), ligesom personoplysningerne skal slettes, når de ikke længere er nødvendige til det formål, hvortil de blev indsamlet.

Derudover skal blandt andet også de databeskyttelsesretlige krav til behandlingssikkerheden i databeskyttelsesforordningens artikel 32 iagttages. Eksempel vil et i øvrigt positivt og velment tiltag med f.eks. gode lægefaglige råd og vejledning via de sociale medier kunne indebære uhensigtsmæssig offentliggørelse af enkeltpersoners helbredsoplysninger med deraf følgende risiko for overtrædelse af de databeskyttelsesretlige regler, f.eks. i form af et brud på persondatasikkerheden.

Datatilsynets nyhed af 2. april 2020 kan læses her.

Behandling af personoplysninger om medarbejdere
Et centralt spørgsmål er, i hvilket omfang arbejdsgivere efter de databeskyttelsesretlige regler er berettigede til at behandle (herunder indsamle, lagre og videregive) oplysninger om medarbejdere, hvis det relaterer sig til COVID-19-pandemien – eksempelvis hvis det sker med henblik på at mindske smitterisikoen på arbejdspladsen.

Behandling af almindelige personoplysninger
De typer af personoplysninger, som arbejdsgivere i den forbindelse potentiel kan komme i berøring med og have behov for at behandle, strækker over et bredt spektrum og kan f.eks. udgøre personoplysninger om, at en medarbejder:

- Har opholdt sig i et land, som Udenrigsministeriet kategoriserer som et risikoområde,
- Er i hjemmekarantæne som følge af et sådant ophold eller lignende, eller
- Er syg (uden nogen angivelse af årsag eller præcisering).

Datatilsynet har i en nyhed den 5. marts 2020 udtalt, at arbejdsgiverens ret til at modtage henholdsvis medarbejderens pligt til at afgive sådanne oplysninger som udgangspunkt afhænger af ansættelsesretlige og sundhedsretlige regler.
Datatilsynet udtaler i den forbindelse, at hvis det ikke er i strid med de pågældende regelsæt at behandle sådanne personoplysninger – som ikke kan kategoriseres som helbredsoplysninger – vil det heller ikke være i strid med de databeskyttelsesretlige regler at behandle dem, så længe det er nødvendigt at foretage den pågældende behandling, jf. nærmere herom nedenfor i afsnittet "Behandling af helbredsoplysninger".

Behandling af helbredsoplysninger
Et hertil relateret spørgsmål er, i hvilket omfang arbejdsgivere kan behandle helbredsoplysninger om medarbejdere, f.eks. en oplysning om at en medarbejder er blevet smittet med COVID-19. Dette er et relevant spørgsmål, fordi databeskyttelsesforordningen stiller nogle særlige krav til behandling af følsomme personoplysninger, herunder helbredsoplysninger.

I den nyhed fra Datatilsynet, som vi omtaler ovenfor, giver tilsynet udtryk for, at det er tilsynets opfattelse, at en arbejdsgiver efter omstændighederne kan behandle sådanne helbredsoplysninger, f.eks. af hensyn til, at ledelsen og kolleger skal kunne træffe nødvendige forholdsregler, hvorved der må forstås eksempelvis forholdsregler til at forebygge eller afværge en opstået smitterisiko eller lignende.

Tilsynet understreger, at behandling af helbredsoplysninger (ligesom behandlingen af andre typer af personoplysninger) skal begrænses til det nødvendige, og at man som arbejdsgiver derfor bør overveje, om der er god grund til at behandle oplysningerne, om formålet kan opnås uden at behandle oplysningerne, og om og det er nødvendigt at nævne navnet på den person, som den pågældende foranstaltning mv. vedrører.

Opdatering og kommunikation af privatlivspolitikker, oplysningstekster mv.
Vi anbefaler, at man som arbejdsgiver i nødvendigt omfang sørger for at opdatere sine privatlivspolitikker, oplysningstekster mv., så disse tekster afspejler den pågældende behandlingsaktivitet – herunder at der kan ske behandling af medarbejdernes helbredsoplysninger til brug for administrationen af arbejdsforholdet – hvis dette ikke allerede fremgår af privatlivspolitikker, oplysningstekster mv. Vi anbefaler også, at sådanne opdateringer bliver kommunikeret til medarbejderne i overensstemmelse med databeskyttelsesforordningens krav.

Datatilsynets nyhed af 5. marts 2020 kan læses her.

Behandlingssikkerhed ved brug af hjemmearbejdspladser

Som følge af COVID-19-pandemien arbejder mange medarbejdere for tiden via fjernopkobling fra hjemmearbejdspladser. Databeskyttelsesforordningen indeholder ikke et forbud mod at anvende hjemmearbejdspladser, men det er centralt, at man som dataansvarlig implementer passende sikkerhedsforanstaltninger, når medarbejderne anvender hjemmearbejdspladser, jf. forordningens artikel 32.
Datatilsynet har den 16. marts 2020 offentliggjort en nyhed, hvor tilsynet giver en række råd til at sikre kravene til behandlingssikkerhed i forbindelse med hjemmearbejdspladser.

Tilsynet fremhæver blandt andet, at man som arbejdsgiver skal fastlægge og udmelde nogle klare retningslinjer for hjemmearbejdet. Tilsynet kommer ikke nærmere ind på, hvad sådanne retningslinjer kan indeholde, men efter vores opfattelse kan det være relevant at tage stilling til f.eks. opbevaring og afskaffelse af fysiske dokumenter (jf. nærmere herom nedenfor), anvendelse af arbejdscomputere på offentlige steder, krav til adgangskoder, anvendelse af digitale tjenester til at afholde møder eller til udveksling af filer, elektronisk lagring af dokumenter mv.

Særligt i forhold til anvendelse af digitale tjenester (f.eks. Microsoft Teams, Skype, Dropbox eller Google Cloud) er det vores opfattelse, at man som arbejdsgiver bør sikre sig, at der indgås databehandleraftaler med de digitale tjenester i det omfang, at disse behandler personoplysninger på vegne af arbejdsgiveren som dataansvarlig, og at man er særligt opmærksom på tjenestens behandlingssikkerhed, herunder at de ikke videregiver personoplysninger fra f.eks. videomøder eller i dokumenter til tredjeparter.

Tilsynet fremhæver endvidere, at det bør sikres, at der anvendes en sikker adgang til arbejdspladsens fagsystemer, f.eks. VPN, direkte opkobling eller andre sikre tjenester, ligesom medarbejdere så vidt muligt bør benytte arbejdspladsens centrale fagsystem, når de arbejder, og at det bør sikres, at adgangskontrol, dokumentversionering, backup mv. er på plads.

Derudover fremhæver tilsynet, at det bør sikres, at hvis der anvendes papirdokumenter, som indeholder personoplysninger, skal sådanne dokumenter opbevares og skaffes af vejen på betryggende vis. Tilsynet kommer ikke nærmere ind på, hvad der menes hermed, men efter vores opfattelse vil det efter omstændighederne f.eks. kunne være relevant, at fysiske dokumenter opbevares aflåst, og at visse typer af medarbejdere får udleveret makulatorer til brug for destruktion af følsomme dokumenter.

Datatilsynet knytter også nogle bemærkninger til de særlige problemstillinger, der kan opstå, hvis en medarbejder får et akut behov for at lagre dokumenter på medarbejderens egen enhed (f.eks. en privat bærbar computer) i stedet for på arbejdspladsens fagsystemer. Tilsynet fremhæver blandt andet, at enheden eller filen skal krypteres, at ingen andre (heller ikke børn) må have adgang til enheden, at det skal sikres, at der sker dokumentversionering samt at dokumentet lægges ind i fagsystemet så snart, dette er muligt, og at den lokale fil herefter straks slettes.

Datatilsynet henviser også til nogle sikkerhedsråd fra Center for Cybersikkerhed af 15. marts 2020. Center for Cybersikkerhed fremhæver her blandt andet, at man som arbejdsgiver bør være opmærksom på det øgede trusselsbillede som følge af pandemien, f.eks. ved, at it-kriminelle udnytter situationen ved brug af ransomware, phishing mv. Dette indebærer også, at organisationens medarbejdere bør orienteres om dette øgede trusselsbillede.

Center for Cybersikkerhed fremhæver desuden, man som arbejdsgiver bør sikre sig, at den automatiske opdatering af medarbejdernes arbejdscomputere fungerer, når de arbejder hjemmefra, eller at medarbejderne alternativt jævnligt mindes om, at de skal opdatere deres systemer.

Datatilsynets nyheds af 16. marts 2020 kan læses her og Center for Cybersikkerheds nyhed af 15. marts 2020 kan læses her.

Håndtering af databehandleres konkurs

I forbindelse med COVID-19-pandemien er mange virksomheder verden over desværre blevet hårdt ramt økonomisk, og mange vil formentlig gå konkurs. Dette stiller en række særlige krav til håndtering af personoplysninger, som en konkursramt virksomhed som databehandler behandler på vegne af en dataansvarlig.

Et eksempel kan være en kommune eller en privat virksomhed, der anvender en leverandør, som står for en hostingløsning, og som nu er gået konkurs.

I et sådant tilfælde – navnlig hvis den konkursramte databehandler på vegne af den dataansvarlige opbevarer personoplysninger, som den dataansvarlige ikke selv er i besiddelse af – bør den dataansvarlige hurtigst muligt sørge for at anmode databehandleren (eller konkursboet) om øjeblikkeligt at tilbagelevere de behandlede personoplysninger og slette enhver kopi heraf og om at orientere den dataansvarlige, når alle disse skridt er foretaget. Foretagelse af disse skridt kan være med til at sikre, at de behandlede personoplysninger ikke går tabt eller videregives til uvedkommende.

Det samme kan gøre sig gældende i det tilfælde, hvor en databehandler, som er gået konkurs, har anvendt en underdatabehandler til at foretage den pågældende behandling på vegne af databehandleren (og dermed på vegne af den dataansvarlige).

Et eksempel herpå kan være en fagforening, som får leveret en hostingløsning af en leverandør, som nu er gået konkurs. Den pågældende leverandør har så anvendt en underleverandør til at foretage back-up eller en afgrænset del af den pågældende hosting.

Her bør man også som dataansvarlig hurtigst muligt rette henvendelse til underdatabehandleren og sikre sig, at de ovenstående skridt gennemføres.

Hvis den dataansvarlige og databehandleren har indgået deres databehandleraftale på Datatilsynets tidligere gældende standarddatabehandleraftale, bør den dataansvarlige her være særligt opmærksom på aftalens pkt. 7.8, hvorefter databehandleren i sin aftale med underdatabehandleren skal indføje den dataansvarlige som begunstiget tredjemand i tilfælde af databehandlerens konkurs, således at den dataansvarlige kan indtræde i databehandlerens rettigheder over for underdatabehandleren, f.eks. så den dataansvarlige kan instruere underdatabehandleren om at foretage sletning eller tilbagelevering af oplysninger.

ANDERS VALENTINER-BRANTH

ADVOKAT (H)

AVB@NNLAW.DK

Mobil: 53 88 41 48

RASMUS BLAABJERG

ADVOKAT (L)

RBL@NNLAW.DK

Mobil: 26 19 77 47

OLE HASSELGAARD

ADVOKAT

OHA@NNLAW.DK

Mobil: 41 27 12 48

ULRICH C. TYNDESKOV

ADVOKATFULDMÆGTIG

UCT@NNLAW.DK

Mobil: 21 86 06 82