Koncern IT
Økonomiforvaltningen

Orientering til Økonomiudvalget (ØU) til aflæggerbordet - anvendelse af Sharepoint i Københavns Kommune

11. november 2019

Sagsnummer
2019-0284883

Dokumentnummer
2019-0284883-5

Baggrund

Datatilsynet er via et anonymt tip den 12. december 2018 blevet orienteret om, at ansatte i KEID i Københavns Kommune (KK) har benyttet Sharepoint til deling af filer, hvori fortrolige personoplysninger om kommunens medarbejdere indgår. Af det anonyme tip fremgik skærmbilleder fra Sharepoint, hvor der i fire konkrete filer var oplysninger om navngivne medarbejdere og deres CPR-numre.

Sharepoint blev introduceret i 2018 ifm. introduktionen af Office365 og erstatter de oprindelige fildrev, der bruges til lagring af dokumenter, billeder mm.

Datatilsynet har i samarbejde med KK undersøgt forholdene, og d. 16. oktober 2019 har kommunen modtaget Datatilsynets endelige afgørelse, hvor tilsynet udtaler *alvorlig kritik* af KK.

Datatilsynet lægger i sin afgørelse vægt på, at KK ikke havde etableret de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger, ligesom den etablerede logning samt KK's interne sikkerhedsretningslinjer ikke anses for at udgøre en passende sikkerhedsforanstaltning.

Problemstilling

Datatilsynet anfører, at den allerede etablerede logning og de interne oplyste retningslinjer om, at følsomme og fortrolige oplysninger ikke må opbevares i endelig dokumentform på fællesdrev i mere end 30 dage, ikke i sig selv kan anses for at udgøre en passende sikkerhedsforanstaltning i den konkrete sag.

Datatilsynet er på den baggrund af den opfattelse, at de personoplysninger sagen omhandler, skal fjernes fra Sharepoint og overføres til kommunens sagsbehandlingssystem.

Løsning

KEID har taget initiativ til at flytte de pågældende dokumenter til eDoc samt sikret, at kun relevante medarbejdere har adgang til den pågældende Sharepoint-mappe. Parallelt med sagen er der igangsat en række yderligere tiltag, som skal styrke den generelle sikkerhed i Sharepoint:

- I januar 2019 nedsatte It-kredsen en Office 365-styregruppe, som har til formål at sikre en tæt koordinering mellem forvaltningerne i forbindelse med oprydning og styring af rettigheder på Sharepoint.
- Der er i fællesskab mellem forvaltningerne udarbejdet en række principper for brugen af Sharepoint, herunder politikker samt procedurer for oprettelse af sites og dokumenter.
- Derudover er der udarbejdet procedurer for dataklassifikation af dokumenter samt tildeling af rettigheder og ejerskab til sites i Sharepoint.

Koncern IT
Strategi og Analyse
Borups Allé 177
2400 København NV

EAN-nummer
5798009809056

- Der er i perioden fra marts til oktober 2019 udarbejdet et it-understøttet governance-system, som kan automatisere håndteringen af ovennævnte principper.
- Forvaltningerne er i gang med at udarbejde detailplaner for oprydning af de forvaltningsspecifikke forvaltningssites på Sharepoint.
- Fra og med september 2019 gennemfører KIT en stikprøvevis logopfølgning samt kontrol af adgangsrettigheder på Sharepoint.

Videre proces
På baggrund af de initiativer, som KK har igangsat, har Datatilsynet oplyst, at sagen anses som afsluttet og at man ikke vil foretage sig yderligere.

KK har løbende været i dialog med kommunens Data Protection Officer (DPO) om sagen. Bl.a på baggrund af nedsættelsen af styregruppen, der skal sikre oprydning og rettighedsstyring af Sharepoint, vil DPO'en ikke foretage sig yderligere i sagen.

Bilag
Bilag 1. Udtalelse fra Datatilsynet.

DATATILSYNET

Københavns Kommune
Rådhuspladsen 1
1599 København V

Sendt med Digital Post

15. oktober 2019

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200

E-mail dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2019-432-0018
Dok.nr. 98860
Sagsbehandler
Pernille Walther

Anvendelse af SharePoint i Københavns Kommune

Datatilsynet vender hermed tilbage til sagen, hvor tilsynet ved e-mail af 12. december 2018 ved et anonymt tip blev orienteret om, at Københavns Kommune benytter cloud platformen SharePoint til deling af filer, hvori personoplysninger, herunder fortrolige personoplysninger om kommunens medarbejdere, indgår, og at der ved disse delinger videregives fortrolige personoplysninger om kommunens medarbejdere til uvedkommende.

1. Afgørelse

Efter en gennemgang af sagen finder Datatilsynet grundlag for at udtale **alvorlig kritik** af, at Københavns Kommunes behandling af personoplysninger ikke er sket i overensstemmelse med databeskyttelsesforordningens artikel 32[1].

Nedenfor følger en nærmere gennemgang af sagen og en begrundelse for Datatilsynets afgørelse.

2. Sagsfremstilling

På baggrund af en anonym henvendelse modtaget den 12. december 2018 besluttede Datatilsynet at undersøge Københavns Kommunes anvendelse af SharePoint.

Af det anonyme tip fremgik screenshots fra http://kksky.sharepoint.com, hvor der af thumbnails for fire konkrete filer fremgår oplysninger om navngivne personer og deres CPR-numre. Navnene på de fire filer var:

1. "031218 Jødisk Jul.xlsx"
2. "021218 Juletræstænding.xlsx"
3. "041218 ITUC.xlsx"
4. "291117 THM Julefest (10.000).xlsx"

Ved brev af 7. januar 2019 til Københavns Kommune anmodede Datatilsynet om at få oplyst, om Københavns Kommune behandler eller har behandlet

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

oplysninger om sine medarbejdere i SharePoint på adressen https://kk-sky.share-point.com, herunder i gruppen "ark-2371-rådhusservice", og i givet fald om der er sket utilsigtet videregivelse af personoplysninger fra platformen som følge af utilstrækkelig adgangskontrol.

Endvidere anmodede Datatilsynet om oplysninger om bl.a. Københavns Kommunes hjemmel til at behandle personoplysninger om sine medarbejdere i SharePoint, samt om de trufne sikkerhedsforanstaltninger i forhold til at sikre, at personoplysninger ikke kommer til uvedkommendes kendskab.

Ved brev af 1. februar 2019 fremkom Københavns Kommune med en udtalelse i sagen. Supplerende oplysninger blev fremsendt den 28. februar og 18. marts 2019.

2.1. Københavns Kommunes bemærkninger

Københavns Kommune har oplyst blandt andet, at der i SharePoint behandles en række ansættelsesrelaterede oplysninger om kommunens medarbejdere, herunder eksamensbeviser, CV, stamdata, CPR-numre, tro- og loveerklæringer, børne- og straffeattester, it-autorisationer, fotos, lægeerklæringer, refusion for sygdom, vagtplaner mv.

Københavns Kommune har redegjort for det retlige grundlag for at behandle de ovennævnte oplysninger i form af almindelige personoplysninger, CPR-numre, børne- og straffeattester og helbredsoplysninger. Københavns Kommune har i den forbindelse henvist til henholdsvis databeskyttelseslovens § 7, stk. 2, § 11, stk. 1, og § 12, stk. 1-3, samt forordningens artikel 6, stk. 1, litra a og litra e, samt artikel 9, stk. 2, litra a og b.

Det fremgår endvidere af redegørelsen fra Københavns Kommune, at SharePoint-folderen "ark-2371-rådhusservice" er et fællesdrev for en koncernenhed i kommunens økonomiforvaltning. Folderen indeholder et stort antal filer i en folderstruktur indeholdende forskellige dokumenter som f.eks. rådhusarrangementer, vagtplaner og andet materiale af almen interesse for medarbejderne.

Filerne indeholder oplysninger af praktisk karakter f.eks. om medarbejdernes vagter, arbejdsopgaver, timeforbrug, og anvendes til planlægning af et arrangement, udarbejde vagtplaner, afregning af (over)arbejde m.m. samt udsendelse af faktura til kunden (uden indhold af personoplysninger). Filerne indeholder således oplysninger om navne og CPR-nummer på de medarbejdere, som har været involveret i afviklingen af et arrangement.

Københavns Kommune har anført, at dokumentet "031218 Jødisk Jul.xlsx", ikke indeholder oplysninger om personer og deres religiøse overbevisning, men alene oplysninger om medarbejdernes vagter og overarbejde, og at betegnelsen "Jødisk Jul" alene referer til arrangements navn.

Københavns Kommune har endvidere oplyst, at der er etableret differentieret brugeradgang til alle SharePoint foldere. Tildeling af adgangsrettigheder sker

konkret baseret på den enkelte medarbejders opgaveportefølje til varetagelse af vedkommendes arbejdsopgaver.

Om adgang til folderen "ark-2371-rådhusservice", herunder de fire omhandlede filer, har Københavns Kommune oplyst, at ca. 560 (pr. februar 2019) medarbejdere har adgangsrettigheder til folderen på overordnet niveau. Det er kommunens vurdering, at de pågældende som led i deres ansættelse har (forskellige) saglige arbejdsbetingede formål med at have adgang til folderen. De generelle adgangsrettigheder til hele folderen er imidlertid 'brudt' i forhold til 79 underfoldere, hvor der er varierende adgangsrettigheder.

Foranlediget af nærværende sag har Københavns Kommune besluttet at begrænse adgangen til de medarbejdere, som vurderes at have hyppigt behov for at tilgå filerne. Medarbejdere, som alene i sjældnere tilfælde har behov for adgang, vil blive håndteret f.eks. ved ad hoc tildeling af adgangsrettigheder. Kommunen har endvidere taget initiativ til at flytte de pågældende dokumenter til kommunens journalsystem.

Om øvrige trufne sikkerhedsforanstaltninger har Københavns Kommune endvidere oplyst, at der blandt andet foretages logning af alle anvendelser af personoplysninger, herunder også af thumbnails, og at der er fastsat interne regler om opbevaring af fortrolige og følsomme personoplysninger i endelig dokumentform på fællesdrevet i maksimalt 30 dage, ligesom der er foretaget og planlægges foretaget en yderligere filoprydning for at dataminimere.

Idet Københavns Kommune ikke med sikkerhed har kunnet identificere de oplysninger, som den anonyme henvendelse til Datatilsynet vedrører, har Københavns Kommune ikke kunnet vurdere, om der i forhold til de konkrete oplysninger er sket en utilsigtet videregivelse.

Københavns Kommune har endvidere oplyst, at der efter en gennemgang af logfiler ikke ses at være sket en utilsigtet videregivelse af oplysninger i form af oversigter over personale til brug for fintælling i forbindelse med valg. Dokumenterne er imidlertid nu blevet flyttet til kommunens journalsystem. Tilsvarende gælder i forhold til vagtrapporterne, der indeholder oplysninger om, at medarbejdere har forladt arbejdet på grund af sygdom mv.

3. Begrundelse for Datatilsynets afgørelse

Datatilsynet lagt til grund, at Københavns Kommune både behandler ikke-følsomme oplysninger, fortrolige oplysninger og følsomme oplysninger i SharePoint, og at dette sker med hjemmel i databeskyttelsesforordningen og databeskyttelsesloven.

Det følger af databeskyttelsesforordningens artikel 32, stk. 1, at den dataansvarlige og databehandleren under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gen-

nemfører passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici.

Efter en gennemgang af sagen finder Datatilsynet, at Københavns Kommune ikke i tilstrækkelig grad havde iagttaget databeskyttelsesforordningens artikel 32, stk. 1, således at kommunen havde etableret de fornødne tekniske og organisatoriske foranstaltninger med henblik på et passende sikkerhedsniveau.

Datatilsynet har herved lagt vægt på, at flere medarbejdere, end hvad der må anses for at have været nødvendigt, har haft adgang til de omhandlede filer, og at Københavns Kommune har haft en omfattende mængde filer i SharePoint, herunder filer med oplysninger af fortrolig og følsom karakter.

Datatilsynet har endvidere lagt vægt på, at den etablerede logning og de oplyste interne retningslinjer om, at følsomme og fortrolige oplysninger ikke må opbevares i endelig dokumentform på fælles drev i mere end 30 dage, ikke i sig selv i den pågældende sag i tilstrækkelig grad kan anses for at udgøre en passende sikkerhedsforanstaltning.

Med henblik på at iagttage databeskyttelsesforordningens artikel 32, stk. 1, er det således Datatilsynets opfattelse, at personoplysninger, der behandles i SharePoint, hurtigst muligt – efter en risikovurdering – skal overføres til Københavns Kommunes sagsbehandlingssystem.

Efter en samlet vurdering af sagens oplysninger finder Datatilsynet grundlag for at udtale **alvorlig kritik** af Københavns Kommunes behandling af oplysninger om medarbejdere i SharePoint.

4. Afsluttende bemærkninger
Datatilsynet anser hermed sagen for afsluttet og foretager sig herefter ikke yderligere i sagen.

Med venlig hilsen

Pernille Walther

Bilag: Retsgrundlag.

Bilag: Retsgrundlag

Uddrag af Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse).

Artikel 2. Denne forordning finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikke-automatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register.

Artikel 5. Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)
b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)
c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)
d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)
e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)
f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

Stk. 2. Den dataansvarlige er ansvarlig for og skal kunne påvise, at stk. 1 overholdes (»ansvarlighed«).

Artikel 6. Behandling er kun lovlig, hvis og i det omfang mindst ét af følgende forhold gør sig gældende:

a) Den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.
b) Behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.
c) Behandling er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
d) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser.
e) Behandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
f) Behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

Første afsnit, litra f), gælder ikke for behandling, som offentlige myndigheder foretager som led i udførelsen af deres opgaver.

Artikel 9. Behandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt.

Stk. 2. Stk. 1 finder ikke anvendelse, hvis et af følgende forhold gør sig gældende:

a) Den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål, medmindre det i EU-retten eller medlemsstaternes nationale ret er fastsat, at det i stk. 1 omhandlede forbud ikke kan hæves ved den registreredes samtykke.
b) Behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder, for så vidt den har hjemmel i EU-retten eller medlemsstaternes nationale ret eller en kollektiv overenskomst i medfør af medlemsstaternes nationale ret, som giver fornødne garantier for den registreredes grundlæggende rettigheder og interesser.
c) Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke.

d) Behandling foretages af en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i organets legitime aktiviteter og med de fornødne garantier, og på betingelse af at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at personoplysningerne ikke videregives uden for organet uden den registreredes samtykke.
e) Behandling vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede.
f) Behandling er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol. g) Behandling er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.
g) Behandling er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson og underlagt de betingelser og garantier, der er omhandlet i stk. 3.
h) Behandling er nødvendig af hensyn til samfundsinteresser på folkesundhedsområdet, f.eks. beskyttelse mod alvorlige grænseoverskridende sundhedsrisici eller sikring af høje kvalitets- og sikkerhedsstandarder for sundhedspleje og lægemidler eller medicinsk udstyr på grundlag af EU-retten eller medlemsstaternes nationale ret, som fastsætter passende og specifikke foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder, navnlig tavshedspligt.
i) Behandling er nødvendig til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, på grundlag af EU-retten eller medlemsstaternes nationale ret og står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.

Artikel 32. Under hensyntagen til det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige og databehandleren passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der passer til disse risici, herunder bl.a. alt efter hvad der er relevant:

a) pseudonymisering og kryptering af personoplysninger
b) evne til at sikre vedvarende fortrolighed, integritet, tilgængelighed og robusthed af behandlingssystemer og -tjenester
c) evne til rettidigt at genoprette tilgængeligheden af og adgangen til personoplysninger i tilfælde af en fysisk eller teknisk hændelse
d) en procedure for regelmæssig afprøvning, vurdering og evaluering af effektiviteten af de tekniske og organisatoriske foranstaltninger til sikring af behandlingssikkerhed.

Stk. 2. Ved vurderingen af, hvilket sikkerhedsniveau der er passende, tages der navnlig hensyn til de risici, som behandling udgør, navnlig ved hændelig eller ulovlig tilintetgørelse, tab, ændring, uautoriseret videregivelse af eller adgang til personoplysninger, der er transmitteret, opbevaret eller på anden måde behandlet.

Stk. 3. Overholdelse af en godkendt adfærdskodeks som omhandlet i artikel 40 eller en godkendt certificeringsmekanisme som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af kravene i nærværende artikels stk. 1.

Stk. 4. Den dataansvarlige og databehandleren tager skridt til at sikre, at enhver fysisk person, der udfører arbejde for den dataansvarlige eller databehandleren, og som får adgang til personoplysninger, kun behandler disse efter instruks fra den dataansvarlige, medmindre behandling kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

Uddrag af Lov nr. 502 af 23. maj 2018 om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

§ 11, stk. 1. Offentlige myndigheder kan behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer.

§ 12. Behandling af personoplysninger i forbindelse med ansættelsesforhold omfattet af artikel 6, stk. 1, og artikel 9, stk. 1, i databeskyttelsesforordningen kan finde sted, hvis behandlingen er nødvendig for at overholde den dataansvarliges eller den registreredes arbejdsretlige forpligtelser eller rettigheder som fastlagt i anden lovgivning eller kollektive overenskomster.

Stk. 2. Behandling af oplysninger som nævnt i stk. 1 må også finde sted, hvis behandlingen er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, som udspringer af anden lovgivning eller kollektive overenskomster, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder går forud herfor.

Stk. 3. Behandling af personoplysninger i ansættelsesforhold kan finde sted på baggrund af den registreredes samtykke i overensstemmelse med artikel 7 i databeskyttelsesforordningen.