DATATILSYNET

Viborg Kommune
Prinsens Allé 5
8800 Viborg

Sendt via Digital Post

5. august 2019

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

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

J.nr. 2018-423-0022
Dok.nr. 55934
Sagsbehandler
Amanda Lærke Vad

Tilsyn med behandling af personoplysninger

Viborg Kommune var blandt de offentlige myndigheder, som Datatilsynet i efteråret 2018 udvalgte til tilsyn efter databeskyttelsesloven[1] og databeskyttelsesforordningen[2].

Datatilsynets planlagte tilsyn med Viborg Kommune fokuserede navnlig på kommunens efterlevelse af de krav, som knytter sig til anvendelse af databehandlere.

Efter anmodning fra Datatilsynet havde Viborg Kommune inden tilsynsbesøget sendt en liste over, hvilke databehandlere kommunen gør brug af. Viborg Kommune havde – efter anmodning herom fra tilsynet – ligeledes sendt en kopi af samtlige af kommunens databehandleraftaler.

Tilsynsbesøget fandt sted den 8. november 2018.

På baggrund af hvad Datatilsynet har konstateret i forbindelse med tilsynsbesøget, finder Datatilsynet grundlag for sammenfattende at konkludere:

1. At Viborg Kommune i flere tilfælde ikke har levet op til kravene i databeskyttelsesforordningens artikel 28, stk. 3, herunder ved
    a. at kommunen for så vidt angår 5 af kommunens databehandlere ikke har indgået databehandleraftaler der – som et minimum – indeholder en beskrivelse af de forpligtelser, som er nævnt i artikel 28, stk. 3,
    b. at kommunen i flere tilfælde ikke i tilstrækkelig grad har forholdt sig til, hvordan forpligtelserne i artikel 28, stk. 3, skal opfyldes af parterne i praksis,

[1] 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).
[2] 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).

   c. at kommunen ikke på en tilstrækkelig klar måde har instrueret samtlige databehandlere i, hvilken behandling af personoplysninger, der skal foretages på vegne af kommunen.
2. At Viborg Kommune ikke har ført løbende tilsyn med behandlingen af personoplysninger hos – i hvert fald – 3 af kommunens databehandlere.
3. At Viborg Kommune ikke har ført løbende tilsyn med behandlingen af personoplysninger hos kommunens underdatabehandlere.

Efter en gennemgang af sagen finder Datatilsynet samlet set grundlag for at udtale **alvorlig kritik** af, at Viborg Kommune ikke har efterlevet databeskyttelsesforordningens krav i forbindelse med brugen af databehandlere, jf. databeskyttelsesforordningens artikel 28, stk. 3, og artikel 5, stk. 2, jf. artikel 5, stk.1.

Datatilsynet finder endvidere grundlag for at meddele Viborg Kommune **påbud** om at indgå databehandleraftaler, som lever op til kravene i forordningens artikel 28, stk. 3, med følgende databehandlere:

1. Applikator ApS, CVR.nr.: 32325750 (Vagtplanlægning)
2. Region Midtjylland (Defactum, Kommunale hjerterehabiliteringsdatabase)
3. Edora A/S, CVR.nr.: 27518184 (WorkForcePlanner)
4. SmartTID ApS, CVR.nr.: 35375562 (SmartTID STU)
5. Socialstyrelsen (De Utrolige År)

Påbuddet meddeles i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra d.

Fristen for efterlevelse af påbuddet er den **30. september 2019**. Datatilsynet skal anmode om senest samme dato at modtage en bekræftelse på, at påbuddet er efterlevet.

Ifølge databeskyttelseslovens § 41, stk. 2, nr. 5, straffes med bøde eller fængsel i op til 6 måneder den, der undlader at efterkomme et påbud meddelt af Datatilsynet i medfør af databeskyttelsesforordningens artikel 58, stk. 2.

Datatilsynet skal herudover anmode Viborg Kommune om en redegørelse for de databeskyttelsesretlige overvejelser, som kommunen har gjort sig på baggrund af tilsynsbesøget. Redegørelsen bedes være Datatilsynet i hænde senest den **30. september 2019**.

Datatilsynet skal endelig anmode Viborg Kommune om at sende en konkret og detaljeret plan for, hvordan kommunen fremadrettet vil føre det fornødne tilsyn med kommunens databehandlere og underdatabehandlere. Planen bedes være Datatilsynet i hænde senest den **15. oktober 2019**.

Ved valget af sanktion har Datatilsynet fundet det formildende, at de fem databehandleraftaler, som Viborg Kommune – på tidspunktet for tilsynsbesøget

– ikke havde nået at indgå/opdatere, alene udgør en lille del af kommunens samlede antal på omkring 130 databehandleraftaler. Datatilsynet har således taget det med i sine betragtninger, at kommunen skulle nå at have indgået/opdateret et stort antal databehandleraftaler inden den 25. maj 2018, hvor databeskyttelsesforordningen fandt anvendelse, og at indgåelse og forhandling af databehandleraftaler generelt kan være en omfattende og tidskrævende proces.

I forhold til Viborg Kommunes tilsyn med databehandlere har Datatilsynet lagt vægt på det oplyste om, at kommunen på generelt plan fører et risikobaseret tilsyn med de behandlinger, der foretages af kommunens databehandlere, selvom stikprøverne viste, at kommunens tilsyn var mangelfuldt.

En nærmere gennemgang af Datatilsynets konklusioner følger nedenfor.

1. Indgåelse af databehandleraftaler, ansvarlighedsprincippet og de generelle principper for behandling af personoplysninger

1.1. Relevante regler

Af databeskyttelsesforordningens artikel 28, stk. 3, følger det, at en databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, der er bindende for databehandleren med hensyn til den dataansvarlige, og der fastsætter genstanden for og varigheden af behandlingen, behandlingens karakter og formål, typen af personoplysninger og kategorierne af registrerede samt den dataansvarliges forpligtelser og rettigheder. Denne kontrakt eller dette andet retlige dokument skal navnlig omfattet de krav til databehandleren, som fremgår af forordningens artikel 28, stk. 3, litra a-g.

Det skal efter databeskyttelsesforordningens artikel 28, stk. 3, litra a, bl.a. fremgå af en databehandleraftale, at databehandleren kun må behandle personoplysninger efter dokumenteret instruks fra den dataansvarlige, herunder for så vidt angår overførsel af personoplysninger til et tredjeland eller en international organisation, medmindre det kræves i henhold til EU-ret eller medlemsstaternes nationale ret, som databehandleren er underlagt; i så fald underretter databehandleren den dataansvarlige om dette retlige krav inden behandling, medmindre den pågældende ret forbyder en sådan underretning af hensyn til vigtige samfundsmæssige interesser.

Af databeskyttelsesforordningens artikel 29 følger det, at databehandleren og enhver der udfører arbejde for den dataansvarlige eller databehandleren, og som har adgang til personoplysninger, kun må behandle disse oplysninger efter instruks fra den dataansvarlige, medmindre det kræves i henhold til EU-retten eller medlemsstaternes nationale ret.

Det skal efter databeskyttelsesforordningens artikel 28, stk. 3, litra d, endvidere fremgå af en databehandleraftale, at databehandleren skal opfylde de betingelser, der er omhandlet i artikel 28, stk. 2 og 4, for at gøre brug af en anden databehandler (underdatabehandler).

Af databeskyttelsesforordningens artikel 28, stk. 2, følger det, at databehandleren ikke må gøre brug af en anden databehandler (underdatabehandler) uden forudgående specifik eller generel skriftlig godkendelse fra den dataansvarlige. I tilfælde af generel skriftlig godkendelse skal databehandleren underrette den dataansvarlige om eventuelle planlagte ændringer vedrørende tilføjelse eller erstatning af andre databehandlere og derved give den dataansvarlige mulighed for at gøre indsigelse mod sådanne ændringer.

Af artikel 28, stk. 4, følger det, at hvis en databehandler gør brug af en anden databehandler (underdatabehandler) i forbindelse med udførelse af specifikke behandlingsaktiviteter på vegne af den dataansvarlige, pålægges denne anden databehandler de samme databeskyttelsesforpligtelser som dem, der er fastsat i kontrakten eller et andet retligt dokument mellem den dataansvarlige og databehandleren som omhandlet i stk. 3, gennem en kontrakt eller et andet retligt dokument i henhold til EU-retten eller medlemsstaternes nationale ret, hvorved der navnlig stilles de fornødne garantier for, at de vil gennemføre de passende tekniske og organisatoriske foranstaltninger på en sådan måde, at behandlingen opfylder kravene i denne forordning. Hvis denne anden databehandler ikke opfylder sine databeskyttelsesforpligtelser, forbliver den oprindelige databehandler fuldt ansvarlig over for den dataansvarlige for opfyldelsen af denne anden databehandlers forpligtelser.

Det følger endvidere af databeskyttelsesforordningens artikel 5, stk. 1, litra a og f, at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede, og at oplysningerne skal 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 og organisatoriske foranstaltninger.

Herudover følger det af databeskyttelsesforordningens artikel 5, stk. 2, at den dataansvarlige er ansvarlig for og skal kunne påvise, at artikel 5, stk. 1, overholdes.

Databeskyttelsesforordningens artikel 5, stk. 2, indeholder således et ansvarlighedsprincip, som betyder, at den dataansvarlige bl.a. skal sikre og kunne påvise, at personoplysninger behandles til lovlige og rimelige formål, og at oplysningerne behandles på en måde, som sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger – også når den dataansvarlige beder en anden part (en databehandler) om at behandle oplysningerne på sine vegne.

Den dataansvarlige må herefter – for at leve op til sine forpligtelser i forbindelse med brugen af databehandlere – udarbejde en databehandleraftale, som regulerer de områder, der er nævnt i artikel 28, stk. 3, og forholde sig til, hvordan disse forpligtelser skal opfyldes i praksis.

Den dataansvarlige skal ligeledes – på en tilstrækkelig klar måde – instruere databehandleren i, hvilken behandling af personoplysninger, der skal foretages på vegne af den dataansvarlige. Dette vil i praksis betyde, at den data-

ansvarlige skal have et overblik over behandlingen og være i stand til at dokumentere, hvilke behandlingsaktiviteter databehandleren er instrueret i at foretage, herunder hvilke aktiviteter den dataansvarlige har godkendt i forhold til eventuelle overførsler til tredjelande eller internationale organisationer, anvendelse af underdatabehandlere mv.

Eksistensen af en tilstrækkelig tydelig instruks er – efter Datatilsynets opfattelse – en forudsætning for, at den dataansvarlige har overblikket og kontrol med behandlingen, når denne overlades til en databehandler, samt for at kunne fastslå, hvornår en databehandler evt. handler uden for rammerne af den aftalte instruks.

Det er ligeledes vigtigt, at den dataansvarlige er opmærksom på, om det fremgår af aftalen, at databehandleren også anvender oplysningerne til egne formål. Hvis den dataansvarlige godkender en databehandleraftale, hvori det fremgår – enten af databehandleraftalen, af hovedaftalen eller andre aftalevilkår – at databehandleren anvender oplysningerne til egne formål, vil der efter tilsynets opfattelse være tale om en videregivelse af personoplysninger, som vil kræve en særskilt videregivelseshjemmel i databeskyttelsesforordningens kapitel 2.

Hvis der videregives personoplysninger til databehandleren, kan dette med fordel reguleres i et særskilt tillæg til aftalen, så databehandlerens behandling til egne formål ikke blandes sammen med den behandling, som foretages på vegne af den dataansvarlige. Det bør således være tydeligt, hvornår databehandleren er underlagt instruks fra den dataansvarlige, og hvornår databehandleren er selvstændigt ansvarlig for behandlingen af personoplysninger.

1.2. Overholdelse af reglerne hos Viborg Kommune

1.2.1. Databehandleraftaler i proces eller under opdatering

Datatilsynet spurgte under tilsynsbesøget ind til, om Viborg Kommune har indgået gyldige databehandleraftaler med alle sine databehandlere, eller om der er aftaler, som endnu ikke er indgået eller opdateret, så de lever op til minimumskravene i databeskyttelsesforordningen.

Datatilsynet henviste i den forbindelse til, at det fremgår af den fremsendte liste over databehandlere, at der er 19 databehandleraftaler, som er i proces, eller som er ved at blive opdateret.

Viborg Kommune bemærkede hertil, at der i de konkrete tilfælde eksisterer databehandleraftaler, men at disse endnu ikke er opdateret i forhold til de nye krav. Kommunen oplyste ligeledes, at det skal vurderes, om nogle af disse databehandleraftaler blot skal ophøre, for eksempel i de tilfælde, hvor der ikke er tale om en databehandlerkonstruktion, eller hvor behandlingen er ophørt.

Viborg Kommune har efter tilsynsbesøget ved e-mail af 11. december 2018 sendt en opdateret liste over kommunens databehandleraftaler. Det fremgår heraf, at kommunen mangler at indgå gyldige databehandleraftaler med fem af kommunens databehandlere.

Datatilsynet spurgte under gennemgangen af de konkrete databehandleraftaler ligeledes ind til nedenstående punkter.

1.2.2. Typen af personoplysninger, der behandles på kommunens vegne
Under gennemgangen af de konkrete databehandleraftaler fandt Datatilsynet eksempler på, at det ikke fremgik af aftalen, hvilke specifikke typer af personoplysninger, som behandles på vegne af kommunen. Nogle aftaler indeholdt således en mere generel angivelse af, at der er tale om behandling af personoplysninger i henhold til databeskyttelsesforordningen eller lign.

Datatilsynet bemærkede hertil, at det generelt bør fremgår mere tydeligt, hvilke typer af personoplysninger, som overlades til databehandleren.

Datatilsynet erklærede sig i den forbindelse dog enige i, at det i visse særlige situationer kan være vanskeligt på forhånd at fastslå, hvilke nærmere typer af personoplysninger, der er omfattet af aftalen. Det kan eksempelvis være tilfældet ved behandling af personoplysninger i relation til en e-mailserver eller en skytjeneste, hvor der vil blive behandlet mange forskellige typer af oplysninger, f.eks. fordi en kommune skal anvende tjenesten til at opbevare sager fra flere forskellige fagområder.

I en sådan situation må man – efter Datatilsynets opfattelse – så specifikt som muligt forsøge at angive, hvilke typer af personoplysninger, der er genstand for behandling. Det vil dog selvsagt bero på en konkret vurdering, hvor specifikt det er muligt i databehandleraftalen at angive typen af personoplysninger.

Datatilsynet bemærkede på tilsynsbesøget, at det under alle omstændigheder bør fremgå klart, om der behandles oplysninger af følsom eller fortrolig karakter, idet dette vil have en betydning for eksempelvis fastlæggelsen af sikkerhedsforanstaltninger og den dataansvarliges løbende tilsyn med behandlingen hos databehandleren.

1.2.3. Proceduren for kommunens godkendelse eller indsigelse over for brugen af nye underdatabehandlere
Datatilsynet spurgte på tilsynsbesøget nærmere ind til proceduren for kommunens godkendelse af underdatabehandlere.

Under gennemgangen af de specifikke aftaler spurgte Datatilsynet således ind til, om det er nærmere aftalt, hvordan og hvornår kommunen skal underrettes om planlagte ændringer – når kommunen har givet en generel godkendelse til anvendelse af underdatabehandlere – herunder om kommunen reelt har mulighed for kunne nå at gøre indsigelse mod eventuelle ændringer.

Datatilsynet kunne på baggrund af kommunens besvarelser konstatere, at der i flere tilfælde ikke var taget stilling til, hvordan og hvornår databehandleren skal underrette kommunen om sådanne ændringer.

I ét af de tilfælde, hvor parterne i databehandleraftalen havde taget stilling til den praktiske gennemførsel af underretningen, kunne det endvidere konstateres, at tidsperioden mellem underretningen og den planlagte anvendelse af underdatabehandleren var aftalt til en så kort tidsperiode, at kommunen i praksis ikke ville kunne nå at gøre indsigelse mod anvendelsen.

Datatilsynet bemærkede i den forbindelse, at det – efter tilsynets opfattelse – ikke vil være i overensstemmelse med kravene i databeskyttelsesforordningens artikel 28, stk. 2, at en databehandler videreoverlader behandlingen eller dele af behandlingen til en underdatabehandler, før den dataansvarlige reelt har haft mulighed for at gøre indsigelse mod dette. Datatilsynet oplyste endvidere, at det er tilsynets umiddelbare opfattelse, at den dataansvarlige aktivt skal underrettes om ændringer vedrørende tilføjelse eller erstatning af underdatabehandlere.

1.2.4. Dokumenteret instruks og databehandlerens behandling af personoplysninger til egne formål
Datatilsynet spurgte under tilsynsbesøget generelt ind til, hvordan kommunen vurderer, om en dokumenteret instruks er tilstrækkelig tydelig.

Kommunen oplyste hertil, at databehandleren typisk beskriver den behandling, som foretages, da databehandleren er ekspert i den ydelse, som leveres, men at kommunen forholder sig aktivt til den beskrivelse af behandlingen, som databehandleren har udarbejdet.

Datatilsynet spurgte herefter ind til, hvilke overvejelser kommunen har gjort sig i forhold til de tilfælde, hvor det fremgår af en databehandleraftale, at databehandleren ligeledes vil anvende oplysninger til egne formål, herunder om kommunen er opmærksom på denne situation.

Datatilsynet oplyste i den forbindelse, at tilsynet tidligere har erfaret/set eksempler på databehandleraftaler, hvoraf det fremgår mere eller mindre tydeligt, at databehandleren også bruger oplysningerne til egne formål.

Kommunen oplyste, at de ikke havde oplevet sådanne situationer, og at kommunen i modsat fald ville have reageret på dette.

Efter de generelle spørgsmål spurgte Datatilsynet ind til kommunens overvejelser i forhold til instruksen i nogle af de udvalgte databehandleraftaler.

Databehandler 1
Datatilsynet spurgte ind til, om kommunen har gjort sig nogle overvejelser i forhold til, at databehandleren anvender personoplysninger til egne formål. Datatilsynet henviste i den forbindelse til aftalens bilag 3 (instruks), hvor det fremgår, at:

”*Kommunen og kommunens lærere skal være opmærksom på, at [databehandler] anvender udvalgte oplysninger til egne formål. [Databehandler] anvender f.eks. oplysninger om brugeradfærd til at kunne målrette den bru-*

gerorienterede dialog samt til at optimere vores produkter og tjenesteydelser. [Databehandler] vil derfor behandle udvalgte oplysninger i forbindelse med nyhedsbreve, markeds- og produktundersøgelser samt service- og produktorienteringer".

Kommunen oplyste hertil, at kommunen ikke har været opmærksom på dette ved indgåelsen af aftalen, og derfor ikke har forholdt sig aktivt til databehandlerens anvendelse af personoplysningerne til egne formål.

Adspurgt oplyste kommunen, at de således heller ikke har undersøgt, hvilke specifikke personoplysninger som databehandleren anvender til egne formål, ligesom at kommunen ikke har forholdt sig til, om der foreligger en videregivelseshjemmel.

Kommunen bekræftede herefter, at det ikke er tydeligt for kommunen, hvornår databehandleren handler på kommunes vegne, og hvornår de handler på egne vegne. Kommunen oplyste, at de ville følge op på dette efter tilsynsbesøget.

Databehandler 2
Datatilsynet spurgte på tilsynsbesøget nærmere ind til punkt 2 i ydelsesbeskrivelsen (et bilag til databehandleraftalen), hvoraf det fremgår, at databehandleren er berettiget til løbende at ændre i ydelsesbeskrivelsen, som bl.a. indeholder punkter vedrørende beskrivelse af genstanden for aftalen, typen af personoplysninger, formålet med behandlingen, sikkerhedsforanstaltninger, anvendelsen af underdatabehandlere og overførsler til tredjelande.

Det fremgår ligeledes af ydelsesbeskrivelsen, at databehandleren skal varsle ændringer i denne i "så betids", at kommunen kan nå at gøre indsigelse mod ændringerne. Kommunen har herefter 30 dage til at gøre indsigelse. Hvis kommunen ikke gør indsigelse inden for 30 dage, vil databehandleren anse ændringerne for at være accepteret af kommunen.

Datatilsynet satte i den forbindelse spørgsmålstegn ved, om en manglende indsigelse fra kommunen vil kunne udgøre en dokumenteret instruks i forhold til behandlingen hos databehandleren.

Databehandler 3
I forhold til databehandleraftalen med *databehandler 3*, bemærkede Datatilsynet, at det – efter tilsynets opfattelse – er uklart, hvilken behandling databehandleren foretager på vegne af kommunen, og hvad databehandleren eventuelt gør som selvstændig dataansvarlig.

Kommunen bemærkede hertil, at databehandleren opbevarer personoplysningerne på vegne af kommunen, og at databehandleren er et såkaldt datalager.

Datatilsynet bemærkede, at det ud fra vilkårenes indhold – og de mange tilknyttede dokumenter – umiddelbart er uklart, om databehandleren er andet

end et datalager, og at det – efter tilsynets opfattelse – er svært at gennemskue den behandling, der foretages.

Kommunen oplyste under tilsynsbesøget, at kommunen var enig i, at det er en "labyrint" at finde rundt i de mange dokumenter, som vilkårene henviser til, og bekræftede, at kommunen ikke har læst alle dokumenterne.

Viborg Kommune har efter tilsynsbesøget henvist til nedenstående afsnit i forhold til præcisering af instruksen.

"Behandling af kundedata, ejerskab
Kundedata bruges eller på anden vis behandles kun for at levere Onlinetjenester til Kunden, herunder formål i forbindelse med levering af sådanne tjenester. [Databehandler] bruger ikke eller på anden vis behandler Kundedata eller udleder oplysninger derfra til reklamemæssige eller lignende kommercielle formål. Som mellem parterne, beholder Kunden alle rettigheder, ejendomsret og interesse i og til Kundedata. [Databehandler] erhverver ingen rettigheder i Kundedata, bortset fra de rettigheder, som Kunden tildeler [databehandler] med henblik på at levere Onlinetjenester til Kunden. Dette afsnit har ingen indflydelse på [databehandlers] rettigheder til software eller tjenester, som [databehandler] tildeler Kunden licens til."

og

"Roller og ansvarsområder for behandler og registeransvarlig
Kunder og [databehandler] accepterer, at Kunden er registreringsansvarlig for Personlige data, og [databehandler] er behandleren af sådanne data, undtagen når (a) Kunden fungerer som behandler af Personlige data, i hvilket tilfælde [databehandler] er en underbehandler, eller (b) andet fremgår i de vilkår, der er specifikke for Onlinetjenesterne. [Databehandler] behandler kun Personlige data efter dokumenterede instruktioner fra Kunden. Kunde accepterer, at dennes volumenlicensaftale (herunder Vilkår for Onlinetjenester) sammen med Kundens brug og konfiguration af funktioner i Onlinetjenesterne er Kundens fyldestgørende og endelige dokumenterede instruktioner til [databehandler] vedrørende behandlingen af Personlige data. Alle yderligere eller ændrede instruktioner skal aftales i henhold til ændringsprocessen for Kundens volumenlicensaftale. I det tilfælde, hvor Persondataforordningen gælder, og Kunden er en behandler, garanterer Kunden over for [databehandler], at Kundens instruktioner, herunder udnævnelse af [databehandler] som en behandler eller underbehandler, er godkendt af den relevante registeransvarlige."

og

"Bevarelse og sletning af data
I hele den periode, hvor Kundens abonnement er aktivt, har Kunden mulighed for at få adgang til og udtrække og slette Kundedata, der er gemt på hver Onlinetjeneste.

[Databehandler] bevarer Kundedata, som forbliver gemt på Onlinetjenesterne (undtagen gratis prøveversioner og LinkedIn-tjenester), på en konto med begrænset funktionalitet i 90 dage efter udløb eller ophør af Kundens abonnement, så Kunden kan udtrække dataene. Når opbevaringsperioden på 90 dage slutter, deaktiverer [databehandler] Kundens konto og sletter Kundedataene og Personlige data inden for yderligere 90 dage, medmindre [databehandler] har tilladelse til eller er pålagt i henhold til gældende lov at bevare sådanne data eller er blevet godkendt til det i denne aftale.

Onlinetjenesten må ikke understøtte opbevaring eller udtrækning af software, der leveres af Kunden. [Databehandler] har ingen ansvarsforpligtelser i forbindelse med sletning af Kundedata eller Personlige data som beskrevet i dette afsnit."

Efter en gennemlæsning af ovenstående afsnit står det stadig ikke Datatilsynet klart, hvilken behandling af personoplysninger, databehandleren foretager på vegne af Viborg Kommune.

1.2.5. Kommunens overblik over brug af underdatabehandlere og overførsel af personoplysninger til tredjelande
Datatilsynet spurgte under tilsynsbesøget flere gange ind til kommunens overblik i forhold til konkrete databehandleres brug af underdatabehandlere, hvorvidt kommunen havde accepteret overførsel af personoplysninger til tredjelande i de konkrete tilfælde, og om kommunen havde sikret sig, at der eksisterede et gyldigt overførselsgrundlag for eventuelle overførsler.

Viborg Kommune kunne i flere tilfælde ikke svare på ovennævnte spørgsmål, og det var tydeligt for Datatilsynet, at kommunen mangler overblik.

1.3. Sammenfatning
Det er i forhold til punkt 1 sammenfattende Datatilsynets opfattelse, at Viborg Kommune ikke har levet op til databeskyttelsesforordningens artikel 28, stk. 3.

Datatilsynet har herved lagt vægt på, at Viborg Kommune for så vidt angår 5 af kommunens databehandlere ikke har indgået databehandleraftaler der – som et minimum – indeholder en beskrivelse af de forpligtelser, som er nævnt i artikel 28, stk. 3, og i flere tilfælde heller ikke i tilstrækkelig grad har forholdt sig til, hvordan forpligtelserne i artikel 28, stk. 3, skal opfyldes af parterne i praksis.

Herudover har Datatilsynet lagt vægt på, at Viborg Kommune – i forhold til samtlige af de gennemgåede databehandlerafter – ikke på en tilstrækkelig klar måde har instrueret databehandlerne i, hvilken behandling af personoplysninger, der skal foretages på vegne af kommunen. Dette tydeliggøres særligt af kommunens manglende overblik over, hvad de har accepteret i forhold til brugen af underdatabehandlere og overførsel af personoplysninger til tredjelande. For så vidt angår en af de gennemgåede databehandleraftaler var det ligeledes Datatilsynets opfattelse, at kommunen ikke var opmærksom på, at

de havde accepteret databehandlerens brug af personoplysninger til egne formål, og at kommunen heller ikke havde vurderet, om der var den fornødne videregivelseshjemmel til en sådan accept.

2. Tilsyn med behandlingen af personoplysninger hos kommunens databehandlere

2.1. Relevante regler

Af databeskyttelsesforordningens artikel 5, stk. 1, følger bl.a., at personoplysninger skal behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede, og at oplysningerne skal 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 og organisatoriske foranstaltninger.

Herudover følger det af databeskyttelsesforordningens artikel 5, stk. 2, at den dataansvarlige er ansvarlig for og skal kunne påvise, at artikel 5, stk. 1, overholdes.

Artikel 5, stk. 2, indeholder et ansvarlighedsprincip, som – efter Datatilsynet opfattelse – betyder, at den dataansvarlige skal sikre og kunne påvise, at personoplysninger behandles til lovlige og rimelige formål, og at oplysningerne behandles på en måde, som sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger – også når den dataansvarlige beder en anden part (en databehandler eller underdatabehandler) om at behandle oplysningerne på sine vegne.

Manglende opfølgning på den behandling af personoplysninger, der sker hos databehandlere og underdatabehandlere, vil – efter Datatilsynets opfattelse – som udgangspunkt betyde, at den dataansvarlige ikke kan sikre eller påvise behandlingens overholdelse af de generelle principper for behandling af personoplysninger, herunder at oplysningerne behandles på en lovlig, rimelig og gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«), samt at oplysningerne 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«).

Den dataansvarlig må således føre et (større eller mindre) tilsyn med, at den indgåede databehandleraftaler overholdes, herunder bl.a. at databehandleren har gennemført de aftalte tekniske og organisatoriske sikkerhedsforanstaltninger.[3]

2.2. Overholdelse af reglerne hos Viborg Kommune

[3] Læs mere herom i Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere, som kan findes på tilsynets hjemmeside.

Datatilsynet spurgte under tilsynsbesøget ind til, om kommunen generelt fører tilsyn med databehandlernes overholdelse af kravene i databehandleraftalen, herunder hvor ofte og hvordan der føres tilsyn.

Viborg Kommune oplyste, at kommunen har en risikobaseret tilgang til databeskyttelse, og at kommunen generelt stiller krav om en revisionserklæring fra databehandleren. Nogle af erklæringerne skal kommunen selv aktivt gå ind og hente på leverandørens hjemmeside, andre får kommunen tilsendt fra databehandleren.

Datatilsynet spurgte ind til, om der føres tilsyn på andre måder end via indhentelse/modtagelse af revisionserklæringer.

Hertil oplyste kommunen, at i tilfælde, hvor det ikke kan lade sig gøre at indhente/modtage en revisionserklæring, foretager kommunen i stedet en oplysningsindsamling ved telefonisk drøftelse med den konkrete databehandler, hvor der tages udgangspunkt i emnerne fra ISAE 3000.

Adspurgt herom oplyste Viborg Kommune, at kommunen ikke har dokumenteret de tilsyn, hvor kommunen har indsamlet oplysninger ved telefonisk drøftelse med databehandlerne, eksempelvis ved journalisering af et telefonnotat.

Adspurgt oplyste Viborg Kommune endvidere, at kommunen generelt bruger revisionserklæringerne ISAE 3402 og ISAE 3000, når de fører tilsyn med håndteringen af personoplysninger hos databehandleren. Kommunen bekræftede, at disse erklæringer primært vedrører behandlingssikkerheden hos databehandleren.

2.2.1. Stikprøvekontrol
Under tilsynsbesøget foretog Datatilsynet ligeledes stikprøvekontrol af, om Viborg Kommune havde indhentet revisionserklæringer i forhold til behandlingen af personoplysninger hos tre konkrete databehandlere.

Datatilsynet kunne på baggrund af stikprøvekontrollerne konstatere, at Viborg Kommune ikke i nogen af de udvalgte stikprøver kunne fremvise dokumentation for indhentelse af revisionserklæringer, eller udøvelse af andre former for løbende tilsyn med behandlingen hos databehandleren.

Datatilsynet har noteret sig, at Viborg Kommune efter tilsynsbesøget har fremsendt indhentede revisionserklæringer fra de tre pågældende databehandlere og dokumentation for, at kommunen har forholdt sig til indholdet af disse.

2.3. Sammenfatning
Det er i forhold til punkt 2 sammenfattende Datatilsynets opfattelse, at Viborg Kommune ikke i tilstrækkelig grad har levet op til databeskyttelsesforordningens artikel 5, stk. 2, jf. stk. 1.

Datatilsynet har herved lagt vægt på, at Viborg Kommune ikke har ført løbende tilsyn med behandlingen af personoplysninger hos – i hvert fald – de 3 af kommunens databehandlere, som Datatilsynet havde udvalgt til stikprøvekontrol, og at kommunen således ikke har sikret sig eller kunne påvise behandlingernes overholdelse af de generelle principper i forordningens artikel 5, stk. 1.

3. Tilsyn med behandlingen af personoplysninger hos kommunens underdatabehandlere

3.1. Relevante regler
Der henvises til denne udtalelses punkt 2.1.

3.2. Overholdelse af reglerne hos Viborg Kommune
Datatilsynet spurgte under tilsynsbesøget indtil, om kommunen generelt følger op på, om behandlingen hos eventuelle underdatabehandlere sker i overensstemmelse med de vilkår, som følger af kommunens aftale med databehandleren.

Viborg Kommune oplyste i den forbindelse, at kommunen skal godkende anvendelsen af underdatabehandlere enten ved en generel eller specifik godkendelse.

Datatilsynet oplyste hertil, at godkendelsen af eventuelle underdatabehandlere ikke i sig selv udgør et (løbende) tilsyn med behandlingen af personoplysninger hos underdatabehandleren. Datatilsynet spurgte på den baggrund nærmere ind til, hvordan kommunen sikrer sig, at behandlingen hos underdatabehandleren er i overensstemmelse med databehandleraftalen og forordningen.

Kommunen henviste til kædeansvaret, hvor databehandleren hæfter for underdatabehandlerens overtrædelser af databehandleraftalen.

Viborg Kommune oplyste herefter, at kommunen på den baggrund ikke fører tilsyn med behandlingen hos underdatabehandlerne.

Datatilsynet erklærede sig enig i, at tilsynet med behandlingen af personoplysninger hos underdatabehandleren ofte vil foregå gennem databehandleren, men at dette ikke i sig selv fritager den dataansvarlige fra – i et større eller mindre omfang – at orientere sig om, hvorvidt behandlingen i sin helhed lever op til forordningens regler.

Datatilsynet spurgte herefter, om kommunen sikrer sig – for eksempel ved indsættelse af et krav herom i databehandleraftalen − at databehandleren fører det relevante tilsyn med underdatabehandleren.

Viborg Kommune oplyste hertil, at kommunen anvender revisionserklæringer, som i et vist omfang berører databehandlerens tilsyn med underdatabehandleren. Kommunen bekræftede dog, at det ikke generelt indgår som et krav i

kommunens databehandleraftaler, at databehandleren skal føre det fornødne tilsyn med eventuelle underdatabehandlere.

Datatilsynet bemærkede, at tilsynet med behandlingen hos underdatabehandlerne eksempelvis kan ske ved, at kravet om databehandlerens tilsyn med underdatabehandlerne indsættes i databehandleraftalen, og at databehandleren herefter fremsender dokumentation for det udførte tilsyn til den dataansvarlige eller gør det let for den dataansvarlige selv at indhente information herom.

Adspurgt bekræftede kommunen, at de ikke kan være sikre på, om databehandleren fører tilsyn med underdatabehandleren, idet dette ikke er aftalt i databehandleraftalen, og idet kommunen ikke har fulgt op på, om det rent faktisk sker.

Kommunen bemærkede dog, at de generelt har tillid til, at deres leverandører har styr på behandlingen hos eventuelle underdatabehandlere.

3.3. Sammenfatning

Det er i forhold til punkt 3 sammenfattende Datatilsynets opfattelse, at Viborg Kommune ikke har levet op til databeskyttelsesforordningens artikel 5, stk. 2, jf. stk. 1, ved ikke i tilstrækkelig grad at have fulgt op på den behandling af personoplysninger, som finder sted hos kommunens underdatabehandlere.

Datatilsynet har herved lagt vægt på, at Viborg Kommune ikke har sikret sig, at der føres et løbende tilsyn med behandlingen af personoplysninger hos underdatabehandlerne, eksempelvis ved at indsætte dette som et krav i databehandleraftalen og herefter aktivt følge op på, om der rent faktisk føres tilsyn, og hvad disse tilsyn viser om behandlingen. Viborg Kommune har således ikke sikret sig eller kunne påvise behandlingernes overholdelse af de generelle principper i forordningens artikel 5, stk. 1.

4. Konklusion

På baggrund af hvad Datatilsynet har konstateret i forbindelse med tilsynsbesøget, finder Datatilsynet grundlag for sammenfattende at konkludere:

1. At Viborg Kommune i flere tilfælde ikke har levet op til databeskyttelsesforordningens artikel 28, stk. 3, herunder ved
    a. at kommunen for så vidt angår 5 af kommunens databehandlere ikke har indgået databehandleraftaler der – som et minimum – indeholder en beskrivelse af de forpligtelser, som er nævnt i artikel 28, stk. 3,
    b. at kommunen i flere tilfælde ikke i tilstrækkelig grad har forholdt sig til, hvordan forpligtelserne i artikel 28, stk. 3, skal opfyldes af parterne i praksis,
    c. at kommunen ikke på en tilstrækkelig klar måde har instrueret samtlige databehandlere i, hvilken behandling af personoplysninger, der skal foretages på vegne af kommunen.

2. At Viborg Kommune ikke har ført løbende tilsyn med behandlingen af personoplysninger hos – i hvert fald – 3 af kommunens databehandlere.
3. At Viborg Kommune ikke har ført løbende tilsyn med behandlingen af personoplysninger hos kommunens underdatabehandlere.

Efter en gennemgang af sagen finder Datatilsynet samlet set grundlag for at udtale **alvorlig kritik** af, at Viborg Kommune ikke har efterlevet databeskyttelsesforordningens krav i forbindelse med brugen af databehandlere, jf. databeskyttelsesforordningens artikel 28, stk. 3, og artikel 5, stk. 2, jf. artikel 5, stk.1.

Datatilsynet finder endvidere grundlag for at meddele Viborg Kommune **påbud** om at indgå databehandleraftaler, som lever op til kravene i forordningens artikel 28, stk. 3, med følgende databehandlere:

1. Applikator ApS, CVR.nr.: 32325750 (Vagtplanlægning)
2. Region Midtjylland (Defactum, Kommunale hjerterehabiliteringsdatabase)
3. Edora A/S, CVR.nr.: 27518184 (WorkForcePlanner)
4. SmartTID ApS, CVR.nr.: 35375562 (SmartTID STU)
5. Socialstyrelsen (De Utrolige År)

Påbuddet meddeles i medfør af databeskyttelsesforordningens artikel 58, stk. 2, litra d.

Fristen for efterlevelse af påbuddet er den **30. september 2019**. Datatilsynet skal anmode om senest samme dato at modtage en bekræftelse på, at påbuddet er efterlevet.

Ifølge databeskyttelseslovens § 41, stk. 2, nr. 5, straffes med bøde eller fængsel i op til 6 måneder den, der undlader at efterkomme et påbud meddelt af Datatilsynet i medfør af databeskyttelsesforordningens artikel 58, stk. 2.

Datatilsynet skal herudover anmode Viborg Kommune om en redegørelse for de databeskyttelsesretlige overvejelser, som kommunen har gjort sig på baggrund af tilsynsbesøget. Redegørelsen bedes være Datatilsynet i hænde senest den **30. september 2019**.

Datatilsynet skal endelig anmode Viborg Kommune om at sende en konkret og detaljeret plan for, hvordan kommunen fremadrettet vil føre det fornødne tilsyn med kommunens databehandlere og underdatabehandlere. Planen bedes være Datatilsynet i hænde senest den **15. oktober 2019**.

Ved valget af sanktion har Datatilsynet fundet det formildende, at de fem databehandleraftaler, som Viborg Kommune – på tidspunktet for tilsynsbesøget – ikke havde nået at indgå/opdatere, alene udgør en lille del af kommunens samlede antal på omkring 130 databehandleraftaler. Datatilsynet har således taget det med i sine betragtninger, at kommunen skulle nå at have indgået/op-

dateret et stort antal databehandleraftaler inden den 25. maj 2018, hvor databeskyttelsesforordningen fandt anvendelse, og at indgåelse og forhandling af databehandleraftaler generelt kan være en omfattende og tidskrævende proces.

I forhold til Viborg Kommunes tilsyn med databehandlere har Datatilsynet lagt vægt på det oplyste om, at kommunen på generelt plan fører et risikobaseret tilsyn med de behandlinger, der foretages af kommunens databehandlere, selvom stikprøverne viste, at kommunens tilsyn var mangelfuldt.

5. Afsluttende bemærkninger
Datatilsynet skal for god ordens skyld bemærke, at tilsynet forventer at offentliggøre denne udtalelse på tilsynets hjemmeside om én uge.

Med venlig hilsen

Katrine Valbjørn Trebbien
Souschef, tilsynsenheden