DATATILSYNET

Randers Kommune
Laksetorvet 1
8900 Randers C

Sendt med 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. 2018-423-0021
Dok.nr. 102860
Sagsbehandler
Zenia Dinesen

Tilsyn med Randers Kommunes behandling af personoplysninger

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

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

Efter anmodning fra Datatilsynet havde Randers Kommune inden tilsynsbesøget sendt en liste over, hvilke databehandlere kommunen gør brug af. Randers Kommune sendte ligeledes en kopi af samtlige af kommunens databehandleraftaler.

Tilsynsbesøget fandt sted den 9. november 2018.

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

1. At Randers Kommune i mange tilfælde ikke har levet op til kravene i databeskyttelsesforordningens artikel 28, stk. 3, herunder ved
    a. at kommunen for så vidt angår 68 af kommunens databehandlere ikke har indgået databehandleraftaler, der – som et minimum – indeholder en beskrivelse af de forpligtelser, som er nævnt i forordningens artikel 28, stk. 3,
    b. at kommunen i enkelte 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 Randers Kommune har ført løbende tilsyn med behandlingen af personoplysninger hos de af kommunens databehandlere, som Datatilsynet havde udvalgt til stikprøvekontrol.
3. At Randers Kommune ikke i alle tilfælde 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 Randers 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 skal anmode Randers 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 Randers 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 kommunen skulle nå at have indgået/opdateret et stort antal databehandleraftaler (210 aftaler) inden den 25. maj 2018, hvor databeskyttelsesforordningen fandt anvendelse, og at indgåelse og forhandling af databehandleraftaler generelt kan være en omfattende og tidskrævende proces.

Herudover har Datatilsynet fundet det formildende, at kommunen havde et klart overblik over, hvor kommunen manglede at få indgået databehandleraftaler, og hvor det var nødvendigt at opdatere databehandleraftalernes indhold. Datatilsynet fik på tilsynsbesøget et indtryk af, at Randers Kommune generelt har iværksat en række tiltag i forhold til at sikre efterlevelsen af de regler, der knytter sig til brugen af databehandlere, og at de fundne mangler i høj grad skyldes den lange implementeringstid af de iværksatte tiltag.

Datatilsynet har endelig fundet det formildende, at der for så vidt angår 28 databehandlere forelå (gamle) aftaler, som i et vist omfang regulerede databehandlerens behandling af personoplysninger, og at kommunen efter tilsynsbesøget har fået indgået alle relevante databehandleraftaler.

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 dataansvarlige 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 Randers Kommune

1.2.1. Databehandleraftaler i proces eller under opdatering

Datatilsynet spurgte under tilsynsbesøget ind til, om Randers 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 68 – ud af omkring 210 – databehandleraftaler, som er i proces, eller som er ved at blive opdateret, herunder 40 databehandleraftaler som er i proces med leverandøren, og 28 databehandleraftaler som er ved at blive opdateret i overensstemmelse med kravene i databeskyttelsesforordningen.

Randers Kommune bekræftede, at der i alle 68 tilfælde er tale om situationer, hvor behandlingen af personoplysninger er påbegyndt.

Randers Kommune oplyste i forlængelse heraf, at kommunen – i forbindelse med implementeringen af databeskyttelsesforordningen – har gjort meget ud af at få et overblik over, hvor kommunen mangler at få indgået databehandleraftaler, og hvor det er nødvendigt at opdatere databehandleraftalernes indhold, men at kommunen som følge af det høje antal databehandleraftaler ikke var nået helt i mål med dette.

Herudover oplyste Randers Kommune, at kommunen har haft et efterslæb i forhold til gamle kontrakter, hvor leverandører som led i deres ydelser har behandlet personoplysninger på vegne af kommunen, men hvor der ikke har været indgået databehandleraftaler. I forbindelse med opfølgningen på gamle kontrakter har kommunen erfaret, at det kan være svært efterfølgende at få leverandører til at underskrive en databehandleraftale, når kommunen allerede gør brug af leverandørens ydelse.

Kommunen har som følge heraf iværksat, at kommunens it-contract manager skal gennemgå alle nye kontrakter med henblik på at sikre, at der ikke skrives under på kontrakter, uden at der samtidig er en databehandleraftale klar til underskrift, hvis den pågældende leverandør behandler personoplysninger på vegne af kommunen.

Ved e-mail af 1. maj 2019 har Randers Kommune oplyst, at kommunen har fået indgået databehandleraftaler med de pågældende leverandører i overensstemmelse med kravene i databeskyttelsesforordningen. Kommunen har samtidig anført, at de manglende databehandleraftaler – efter kommunens vurdering – ikke har betydet en forøget sikkerhedsmæssig risiko.

1.2.2 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 to tilfælde ikke var taget konkret stilling til, hvordan og hvornår databehandleren skal underrette kommunen om sådanne ændringer.

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.

Randers Kommune oplyste på tilsynsbesøget, at kommunen fremadrettet i sine databehandleraftaler vil være opmærksom på at tydeliggøre, hvordan og hvornår kommunen skal underrettes om planlagte ændringer i forhold til anvendelsen af underdatabehandlere.

1.2.3. 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, at kommunen ikke førhen har haft samme opmærksomhed på udformningen af instrukser til databehandleren, og at kommunen har noget arbejde i at skulle gennemgå indholdet af databehandleraftalerne med henblik på at vurdere, om den givne instruks er tilstrækkelig tydelig.

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 anvender 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 det altid fremgår af kommunens databehandleraftaler, at databehandleren udelukkende må anvende personoplysningerne i overensstemmelse med de formål, som fremgår af aftalen, og derved ikke til egne formål.

Datatilsynet henledte senere opmærksomheden på en af de konkrete databehandleraftaler og 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 brugerorienterede 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*".

Randers Kommune oplyste hertil, at kommunen ikke har været opmærksom på dette ved indgåelsen af den pågældende aftale 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, og at kommunen heller 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 vil følge op på dette efter tilsynsbesøget.

1.2.4. Overblik over databehandlerens brug af underdatabehandlere
Under gennemgangen af to af de konkrete databehandleraftaler, konstaterede Datatilsynet, at databehandleraftalen ikke indeholdt oplysninger om, hvorvidt databehandleren gjorde brug af underdatabehandlere. Datatilsynet spurgte på den baggrund ind til, om kommunen i disse to tilfælde var bekendt med, om databehandleren gjorde brug af underdatabehandlere.

Randers Kommune oplyste i forhold til begge databehandleraftaler, at kommunen ikke havde kendskab til, om databehandlerne gør brug af underdatabe-

handlere, men at dette ville blive reguleret i en ny databehandleraftale, som var i proces med databehandleren.

I en af de andre konkrete databehandleraftaler fremgår det vedrørende databehandlerens brug af underdatabehandlere, at den dataansvarlige kan finde information om underdatabehandlere, herunder om underdatabehandlerens behandling af personoplysninger og lokation, på databehandlerens hjemmeside. Datatilsynet spurgte på den baggrund ind til, om kommunen havde et overblik over hvor mange underdatabehandlere, der anvendes, og hvor i verden personoplysningerne behandles.

Randers Kommune oplyste hertil, at kommunen ikke har et overblik over dette. Adspurgt oplyste kommunen endvidere, at kommunen ikke har set nogen af de pågældende underdatabehandleraftaler, og at det ligeledes er uklart for kommunen, om databehandleren fører det relevante tilsyn med underdatabehandlerne, idet kommunen ikke har fulgt op på dette.

1.3. Sammenfatning

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

Datatilsynet har herved lagt vægt på, at Randers Kommune for så vidt angår 68 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 Randers Kommune – i forhold til nogle af de gennemgåede databehandleraftaler – ikke på en tilstrækkelig klar måde har instrueret databehandlerne i, hvilken behandling af personoplysninger, der skal foretages på vegne af kommunen. Dette viste sig ved, at kommunen i to tilfælde ikke havde overblik over, hvad de har accepteret i forhold til brugen af underdatabehandlere. 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 Randers Kommune

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.

Randers Kommune oplyste, at kommunen konsekvent stiller krav om revisorerklæringer, der lever op til branchestandarderne (eksempelvis ISAE 3000 eller ISAE 3402) fra sine databehandlere. Adspurgt oplyste kommunen endvidere, at kommunen ikke har prioriteret ressourcer til at udføre fysisk tilsyn hos sine databehandlere.

Adspurgt oplyste Randers Kommune, at kommunens IT-afdeling står for at følge op på, at kommunen rent faktisk modtager de relevante revisionserklæringer fra databehandlerne, og at IT-afdelingen i den forbindelse har udarbejdet en oversigt over status for opfølgning på de enkelte databehandleraftaler.

---

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

Herudover oplyste Randers Kommune, at IT-afdelingen forholder sig aktivt til indholdet af en revisionserklæring og vurderer, om denne giver tilstrækkelig information om behandlingssikkerheden. Når kommunen modtager en revisionserklæring fra en databehandler, journaliseres erklæringen i kommunens journalsystem, og der vedlægges et dokument på sagen, hvor kommunen anfører sine eventuelle bemærkninger hertil. Randers Kommune fremviste i den forbindelse et eksempel på et sådant dokument.

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

Datatilsynet kunne på baggrund af stikprøvekontrollerne konstatere, at Randers Kommune har indhentet revisionserklæringer hos de to konkrete databehandlere, og at Randers Kommune kunne fremvise dokumentation for indhentelse af revisionserklæringerne, og at kommunen havde forholdt sig til indholdet af disse.

I forhold til den tredje konkrete databehandler oplyste kommunen, at databehandlingen var ophørt, og at den pågældende databehandleraftale således ikke længere var aktuel.

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

Datatilsynet har herved lagt vægt på, at Randers Kommune kunne påvise, at kommunen havde ført tilsyn med behandlingen af personoplysninger hos de af kommunens databehandlere, som Datatilsynet havde udvalgt til stikprøvekontrol. Randers Kommune kunne således fremvise dokumentation for indhentelse af revisionserklæringerne, og at kommunen havde forholdt sig til indholdet af disse.

3. Tilsyn med behandlingen af personoplysninger hos kommunens underdatabehandlere

3.1. Relevante regler
Der henvises til udtalelsens punkt 2.1.

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

Randers Kommune oplyste i den forbindelse, at det typisk indgår som et krav i kommunens databehandleraftaler, at databehandleren har ansvaret for at føre det relevante tilsyn med underdatabehandleren, men at kommunen fører stikprøvekontrol med, om databehandlerne rent faktisk har ført tilsyn med underdatabehandlerne.

Kommunen oplyste endvidere, at kommunen forholder sig aktivt til indholdet af de revisionserklæringer, de modtager fra deres databehandlere. Hvis kommunen har bemærkninger til erklæringerne vedrørende underdatabehandlerens overholdelse af reglerne, sørger databehandleren for at videreformidle kommunens bemærkninger til underdatabehandleren.

Datatilsynet gennemgik herefter en af de konkrete databehandleraftaler, hvor det fremgår, at databehandleren gør brug af 16 underdatabehandlere, og spurgte i den forbindelse ind til, om kommunen foretager nogen form for tilsyn med behandlingen hos de angivne underdatabehandlere.

Randers Kommune oplyste hertil, at kommunen ikke har ført nogen form for tilsyn med behandlingen hos de 16 underdatabehandlere, men at kommunen forventer og har tillid til, at den pågældende databehandler har styr på dette. Kommunen har efter tilsynsbesøget bemærket, at det fremgår af databehandlerens revisionserklæring, at databehandleren løbende fører tilsyn hos underdatabehandlerne, herunder ved at indhente revisionserklæringer fra disse. Datatilsynet lægger imidlertid fortsat til grund, at Randers Kommune ikke har forholdt sig til, om den pågældende databehandler rent faktisk har ført tilsyn hos underdatabehandlerne, og hvad resultatet af disse tilsyn i givet fald viser om underdatabehandlerens behandling af personoplysninger.

Ved gennemgangen af en af de andre konkrete aftaler, hvor kommunen ikke havde et overblik over antallet af underdatabehandlere, oplyste kommunen, at det var uklart for kommunen, om den pågældende databehandler fører det relevante tilsyn med underdatabehandlerne, og at kommunen ikke har fulgt op på dette.

Datatilsynet spurgte herudover ind til, om Randers Kommune generelt følger op på, om databehandleren – i overensstemmelse med aftalen – har sikret sig det fornødne overførselsgrundlag i forbindelse med overførsler til eventuelle underdatabehandlere i tredjelande.

Randers Kommune oplyste i den forbindelse, at kommunen – når de indgår databehandleraftaler – forsøger at sikre og dokumentere, at der er et gyldigt overførselsgrundlag, hvis der i de konkrete tilfælde overføres personoplysninger til tredjelande. Kommunen oplyste dog samtidig, at dette ikke altid har været kommunens praksis.

3.3. Sammenfatning

Det er i forhold til punkt 3 sammenfattende Datatilsynets opfattelse, at Randers Kommune ikke har levet op til databeskyttelsesforordningens artikel 5, stk. 2, jf. stk. 1, ved ikke – for så vidt angår enkelte af de gennemgåede data-

behandleraftaler – at have fulgt op på den behandling af personoplysninger, som finder sted hos de pågældende underdatabehandlere.

Datatilsynet har herved lagt vægt på, at Randers Kommune i to tilfælde ikke har fulgt op på, om databehandleren rent faktisk fører tilsyn hos underdatabehandlerne, og hvad disse tilsyn viser om behandlingen. Randers Kommune har således ikke sikret sig eller kunne påvise disse behandlingers 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:

4. At Randers Kommune i mange tilfælde ikke har levet op til kravene i databeskyttelsesforordningens artikel 28, stk. 3, herunder ved
    a. at kommunen for så vidt angår 68 af kommunens databehandlere ikke har indgået databehandleraftaler, der – som et minimum – indeholder en beskrivelse af de forpligtelser, som er nævnt i forordningens artikel 28, stk. 3,
    b. at kommunen i enkelte 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.
5. At Randers Kommune har ført løbende tilsyn med behandlingen af personoplysninger hos de af kommunens databehandlere, som Datatilsynet havde udvalgt til stikprøvekontrol.
6. At Randers Kommune ikke i alle tilfælde 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 Randers 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 skal anmode Randers 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 Randers 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 kommunen skulle nå at have indgået/opdateret et stort antal databehandleraftaler (210 aftaler) inden den 25. maj 2018, hvor databeskyttelsesforordningen fandt anvendelse, og at indgåelse og forhandling af databehandleraftaler generelt kan være en omfattende og tidskrævende proces.

Herudover har Datatilsynet fundet det formildende, at kommunen havde et klart overblik over, hvor kommunen manglede at få indgået databehandleraftaler, og hvor det var nødvendigt at opdatere databehandleraftalernes indhold. Datatilsynet fik på tilsynsbesøget et indtryk af, at Randers Kommune generelt har iværksat en række tiltag i forhold til at sikre efterlevelsen af de regler, der knytter sig til brugen af databehandlere, og at de fundne mangler i høj grad skyldes den lange implementeringstid af de iværksatte tiltag.

Datatilsynet har endelig fundet det formildende, at der for så vidt angår 28 databehandlere forelå (gamle) aftaler, som i et vist omfang regulerede databehandlerens behandling af personoplysninger, og at kommunen efter tilsynsbesøget har fået indgået alle relevante databehandleraftaler.

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