NOTAT

Bilag I Kommunernes 10 højest prioriterede GDPR-problemstillinger

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Indhold

1. Dataansvarskonstruktioner

1.1. Skema vedrørende dataansvarskonstruktioner

Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?**	**Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?**	**Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?**
Det er fortsat uklart i en lang række situationer, hvem der i givne samarbejds- og leverandørsituationer er dataansvarlig henholdsvis databehandler, og	Art. 4, nr. 7 og 8 og art. 26, stk. 1	Kommunerne efterlyser mere vejledning med flere konkrete eksempler, som også ikke GDPR-kyndige kan bruge.	DPO´erne er i mange kommuner blevet inddraget i spørgsmålet. En række DPO´er har udarbejdet egne vejledninger

hvornår der eventuelt er tale om en fælles dataansvarskonstruktion.		Gerne løbende udbygning af Datatilsynets vejledning. Det foreslås også, at Datatilsynet træffer flere afgørelser på området for at lægge en mere tydelig linje.	og retningslinjer til deres kommuner. De kommunalt ansatte og DPO´erne er ikke i alle tilfælde nødvendigvis enige om vurderingen af spørgsmålet.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

1.2. Bemærkninger

Løsningsforslag
Kommunerne efterlyser mere vejledning med flere konkrete eksempler, som også ikke GDPR-kyndige kan bruge. Gerne løbende udbygning af Datatilsynets vejledning, hvor tjekspørgsmålene også ønskes forbedret samt udbygning af vejledningen i forhold til fælles dataansvarskonstruktionen. Det foreslås også, at Datatilsynet træffer flere afgørelser på området for at lægge en mere tydelig linje.

KL foreslår desuden, at Justitsministeriet går i dialog med erhvervslivets parter om at finde løsninger på, at mange af kommunernes private leverandører opleves ofte ikke at have de juridiske kompetencer til at foretage den juridiske vurdering af dataansvarskonstruktionen.

Såfremt der fortsat er uklarhed omkring reglerne efter en yderligere vejledningsindsats i de kommende år, vil det være hensigtsmæssigt at overveje, hvorvidt definitionerne af henholdsvis "dataansvarlig" og "databehandler", jf. artikel 4, nr. 7 og 8, og i forlængelse heraf artikel 26 om fælles dataansvarlige, bør revideres, eventuelt i kombination med en revision af artikel 28 om databehandlere.

Uddybning
Kommunerne giver udtryk for, at der fortsat bruges alt for mange resurser i kommunerne på at afklare, hvem der er dataansvarlig henholdsvis databehandler. Eller om der eventuelt er tale om en fælles dataansvarskonstruktion. DPO´erne forsøger at hjælpe med svar og awareness-aktiviteter, typisk vejledninger, men det er meget tidskrævende, og det havde været bedre, hvis reglerne havde været mere enkle.

Definitionerne i art. 4, nr. 7 og 8 (og art. 26) er svære at anvende i praksis. Hvem der "afgør, til hvilke formål og med hvilke hjælpemidler der må foretages behandling af personoplysninger" er i mange tilfælde ikke en hjælp ift. at udpege den dataansvarlige, idet både den dataansvarlige og databehandleren jo har (hver sit) formål med behandlingen.

De konkrete eksempler i Datatilsynets vejledning om dataansvarlige og databehandlere fremhæves som gode, men der efterlyses mange flere eksem-

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

pler og afklaringer. Tjekspørgsmålene i vejledningen opleves ikke som brugbare. Spørgsmålene er tvetydige og de resultater, man når frem til ved at bruge spørgsmålene, er ikke nødvendigvis korrekte. Der efterlyses derfor en bedre spørgeramme som støtte for de konkrete vurderinger, som kommunerne skal foretage. Vejledningen opleves desuden ikke som tilstrækkelig i forhold til at afklare fælles dataansvarskonstruktioner. Her efterlyses også mere detaljeret vejledning om konstruktionen. Gerne suppleret med flere eksempler. Kommunerne påpeger det også som et generelt problem, at Datatilsynet ikke udtaler sig konkret om fastlæggelsen af dataansvaret i konkrete sager, der ikke er klagesager.

Kommunerne nævner en lang række områder, hvor det giver udfordringer at afklare dataansvarsforholdet. Generelt opleves reglerne som svært anvendelige, når ydelsen omhandler noget andet end drift af en it-løsning:

- Private botilbud, som har en kontrakt med kommunen
- Børnehus-konstruktionen, som er fastlagt ved lov, men hvor ressortministeriet ikke vil bistå i forhold til afklaringen af dataansvaret
- De mange aktører på beskæftigelsesområdet, fx en leverandør, som kommunen måtte bestille til at udføre en opgave hjemlet i beskæftigelseslovgivningen (fx vejlednings- og opkvalificeringsforløb efter LAB-lovens § 91)
- Ældreplejeområdet og tilbud til voksne med særlige behov
- Social- og seniorområdets aftaler med private aktører
- Skolefotografering
- Sprogtolkning
- Leverandører til kommunerne som modtager personoplysninger om borgere fra kommunen for at kunne levere deres ydelser, fx hjælpemidler
- Ingeniørvirksomheder og landinspektørfirmaer, der udfører opgaver for teknisk forvaltning
- Leverandører der er pålagt en vis form for ”afrapportering", fx at angive borgerens cpr-nummer i de fakturaer, leverandøren sender til kommunen
- Aftaler vedrørende tjenesteydelser, hvor kommunerne har eksterne rådgivere, mentorer mv. til borgere
- Statslige og regionale it-løsninger og projekter, hvor kommunerne skal indgå, fx statslige portaler for at videregive oplysninger om fx rotter, fælles it-løsninger til telemedicin, sårjournaler, fælles kvalitetsudviklingsprojekter mv.
- I forhold til samarbejde med andre offentlige myndigheder, særligt styrelser, hvor der er stor forskel på, hvordan dataansvarskonstruktioner vurderes.
- Fx opleves det, at styrelser vælger, at der skal være en fælles dataansvarskonstruktion – også selv kommunen ikke er med til at fastsætte formålet med en given behandling.

I forhold til kommunernes mange private leverandører opleves det ofte, at disse ikke har de juridiske kompetencer til at foretage den juridiske vurdering af dataansvarskonstruktionen. Ofte betyder det, at kommunerne bliver presset til at indgå databehandleraftaler med deres leverandører – også i tilfælde, hvor databehandlerkonstruktionen ikke er den rigtige. Her foreslår KL, at Justitsministeriet går i dialog med erhvervslivets parter om udfordringen.

Flere kommuner peger helt generelt på, at det ville være en hjælp, hvis regelsættet omkring dataansvarlige og databehandler blev forenklet. Såfremt

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

der fortsat er uklarhed omkring reglerne efter en yderligere vejledningsindsats i de kommende år, vil det være hensigtsmæssigt at overveje, hvorvidt definitionerne af henholdsvis "dataansvarlig" og "databehandler", jf. artikel 4, nr. 7 og 8, og i forlængelse heraf artikel 26 om fælles dataansvarlige, bør revideres, så det bliver lettere at vurdere, hvornår der er tale om dataansvarskonstruktioner, der kræver indgåelse af databehandleraftaler eller aftaler om fælles dataansvar. Eventuelt i kombination med en revision af artikel 28 om databehandlere, hvor det kunne præciseres, at hvorvidt der er tale om en databehandlerkonstruktion afhænger af, hvilken ydelse, der skal leveres. – Sådan, at der kun er tale om en databehandlerkonstruktion, hvis databehandleren ingen egen interesse har i oplysningerne.

2. Databehandleraftaler med staten

2.1. Skema vedrørende databehandleraftaler med staten

Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?**	**Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?**	**Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?**
Når kommunerne samarbejder med staten om løsningen af forskellige opgaver, fx borger.dk-siden, vil kommunerne i mange tilfælde blive bedt om at indgå databehandleraftaler mellem den enkelte kommune og staten, som ikke afspejler det reelle dataansvarsforhold. Ligeledes skal alle kommunerne hver især bruge ressourcer på at gennemlæse og forholde	Art. 4, nr. 7 og 8 og art. 28	Kommunerne har foreslået overvejet, om problemstillingen kan løses via særskilt lovhjemmel til, at der ikke skal indgås databehandleraftaler, når staten er aftaleparten. Ligeledes foreslås juridisk afklaring af området herunder, om der reelt bør benyttes aftaler om fælles dataansvar i samarbejdet mellem stat og kommuner frem for en databehandlerkonstruktion. Alle databehandleraftaler mellem kommunerne og staten foreslås i stedet reguleret af	I de fleste kommuner er DPO´en ikke inddraget i problemsstillingen, idet kommunerne reelt ikke oplever at have anden handlemulighed end at indgå databehandleraftalerne med staten.

sig til aftalerne, desuagtet, at kommunerne ikke oplever at have nogen indflydelse på aftalernes indhold.		bekendtgørelser, "andet retligt dokument", jf. artikel 28, stk. 3.	

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

2.2. Bemærkninger

Løsningsforslag
Kommunerne har foreslået, at der ses på, om der kan etableres lovhjemmel til, at der ikke skal indgås databehandleraftaler, når staten er aftaleparten, idet kommunerne reelt oplever ikke at have indflydelse på indretningen og behandlingen af data i de pågældende løsninger.

Hvis dette ikke er muligt, foreslås alle databehandleraftaler mellem kommunerne og staten reguleret af bekendtgørelser, "andet retligt dokument", jf. artikel 28, stk. 3, sådan, at den enkelte kommune ikke skal anvende unødige resurser på at forholde sig til aftaler, som de ikke har nogen indflydelse på. I den forbindelse foreslås det, at der ses på, om fælles dataansvar er en mere juridisk korrekt model frem for, at kommunerne er dataansvarlige for statslige myndigheder. Generelt efterlyser kommunerne mere ensretning/oprydning/afklaring af området for dataansvarsaftaler med staten.

Uddybning
Det giver udfordringer for kommunerne, at statslige myndigheder, som fastsætter reglerne for kommunernes behandling af personoplysninger, i databehandleraftaler mellem kommunerne og de statslige myndigheder juridisk defineres som "databehandlere", som kommunerne skal indgå databehandleraftaler med, instruere og føre tilsyn med. Kommunerne oplever, at definitionen af databehandlere, "... der behandler personoplysninger på den dataansvarliges vegne", jf. art. 4, nr. 8, ikke afspejler det reelle setup, når der samarbejdes med staten. Kommunen står formelt som dataansvarlig på trods af, at den enkelte kommune ikke har nogen indflydelse på hverken formål eller hjælpemidler og dermed reelt ikke kan siges at være dataansvarlig, jf. art. 4, nr. 7. Den statslige myndighed træffer beslutningen om en given it-løsning, og kommunen er forpligtet til at anvende denne. Aftalerne opleves derfor reelt som meningsløse og af proformakaraktér.

En uhensigtsmæssig konsekvens af aftalerne er ligeledes, at kommunerne i rollen som dataansvarlige reelt ikke har mulighed for at stille krav til it-sikkerheden i løsningerne. I sidste ende kan dette have konsekvenser for sikkerheden omkring borgernes data.

Aktuelle eksempler, som kommunerne nævner, er indberetningen af Utilsigtede hændelser (Sundhedsdatastyrelsen), Danmarks Adresseregister (DAR), Borger.dk (Digitaliseringsstyrelsen) og Unilogin (Styrelsen for IT og Læring), klageportaler, Professionshøjskolernes Praktikportal, EGU-portalen, FMK (Fælles medicinkort), geoDk-data, BBR, Byg Og Miljø, Danmarks Miljøportal, Husdyrgodkendelse.dk, Jupiter - Danmarks geologiske & hydrologiske database, KMD ESR (Ejendoms-stamregistret), DSPD, Telesår, FUT, system for trivselsmåling, systemet ”ydelsesrefusion", Det Fælles Data-

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

grundlag under STAR, den nye telemedicinske løsning, de lovpligtige indberetninger til hhv. NAB og SMDB (rusmiddelområdet), undersøgelser, der udarbejdes for/sammen med statslige myndigheder.

I nogle situationer oplever kommunerne at blive opfattet som databehandlere for de statslige myndigheder desuagtet, at kommunerne har myndighedsansvaret for opgaven ved lov. Det giver heller ikke mening for kommunerne. Det gælder fx ift. kommunernes udstedelse af NemID og ift. Miljøportalen. Generelt påpeger kommunerne behov for en ensretning/oprydning/afklaring af området for dataansvarsaftaler med staten. Gerne via særskilt vejledning om området.

Det er ligeledes unødvendigt forbrug af kommunernes resurser, at alle kommunerne hver især skal bruge tid på at gennemlæse og forholde sig til enslydende aftaler, desuagtet, at kommunerne ikke oplever at have nogen indflydelse på aftalernes indhold, herunder kunne stille individuelle krav til aftalerne. Det er i følge kommunerne et godt eksempel på en problemstilling, hvor kommunerne bruger mange resurser uden, at det giver øget datasikkerhed for borgerne. Det er oplagt, at alle databehandleraftaler mellem kommunerne og staten, såfremt disse ikke kan afløftes via lovgivning, reguleres centralt via bekendtgørelser sådan, at den enkelte kommune ikke skal anvende unødige resurser på at forholde sig til aftaler, som de ikke har nogen indflydelse på.

3. Overførsel til tredjelande/Schrems II-dommen

3.1. Skema vedrørende overførsel til tredjelande/Schrems II-dommen

Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?**	**Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?**	**Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?**
Reglerne for overførsler af personoplysninger til tredjelande, fx via cloud-løsninger, er besværlige at arbejde med – særligt i lyset af Schrems II-dommen.	Art. 46, stk. 2, litra c	Kommunerne opfordrer til, at der nationalt eller i EU-regi centralt foretages en vurdering af forholdene i alle relevante tredjelande. At staten presser på for, at der i EU-regi hurtigst muligt bliver aftalt en ny ordning, som er-	Enkelte kommuner har inddraget DPO´en i spørgsmålet, men oplevelsen er generelt, at problemet ikke kan løses af den enkelte kommune alene.

		statning for Privacy Shield-ordningen. Opdateret vejledning om reglerne for overførsler til tredjelande efterlyses.	

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

3.2. Bemærkninger

Løsningsforslag
Kommunerne opfordrer til, at der nationalt eller i EU-regi centralt foretages en vurdering af forholdene i alle relevante tredjelande, herunder tredjelandenes lovgivning sådan, at det ikke er en opgave som hver enkelt dataansvarlig pålægges. Der opfordres ligeledes til, at staten presser på for, at der i EU-regi hurtigst muligt bliver aftalt en ny ordning, som erstatning for Privacy Shield-ordningen.
Generelt efterlyses der opdateret vejledning om reglerne for overførsler til tredjelande.

Uddybning
Reglerne for overførsler af personoplysninger til tredjelande, fx via cloud-løsninger, er besværlige at arbejde med – særligt i lyset af Schrems II-dommen. Da kommunerne som følge af dommen ikke længere kan anvende den såkaldte "Privacy Shield"-ordning som gyldigt overførselsgrundlag for overførsler af data til USA, skal alle kommunerne til hver især at indgå supplere standardkontraktaftaler med deres leverandører. En opgave, der før var afløftet via Privacy Shield-ordningen. Desuden stilles Schrems II-dommen krav om, at kommunerne udover at indgå standardkontraktaftaler skal foretage en vurdering af forholdene i det tredjeland, som kommunerne ønsker at overføre data til. Krav som det i praksis ikke er muligt eller hensigtsmæssigt, at man som dataansvarlig kommune alene skal opfylde. Der stilles krav om, at man som dataansvarlig skal vurdere, hvorvidt lovgivningen i de enkelte tredjelande respekterer de krav til beskyttelse af data, som EU-lovgivningen stiller. Og hvis det ikke er tilfældet, skal man ligeledes analysere, hvilke supplerende foranstaltninger der skal aftales med leverandøren.

Kommunerne opfordrer til, at der nationalt eller i EU-regi centralt foretages en vurdering af forholdene i alle relevante tredjelande, herunder tredjelandenes lovgivning sådan, at det ikke er en opgave som hver enkelt dataansvarlig pålægges. Ligeledes opfordres der til, at en sådan vurdering ligeledes omfatter vurderingen af, hvilke supplerende foranstaltninger der eventuelt yderligere skal aftales med leverandører i de enkelte tredjelande. Sådan at resurceforbruget forbundet med at anvende standardkontrakterne begrænses mest muligt for alle dataansvarlige, der ønsker at overføre data til tredjelande. I forhold til USA opfordrer kommunerne til, at staten presser på for, at der i EU-regi aftales en ny ordning med USA til erstatning for Privacy Shield-ordningen. Sådan at kommunerne ikke skal anvende resurser på at indgå supplerende standardkontrakter ved overførsler til USA.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Generelt påpeger kommunerne også behovet for nye og konkrete vejledninger om reglerne for overførsler til tredjelande.

4. Aftaler med tech-giganterne, bl.a. Facebook

4.1. Skema vedrørende aftaler med tech-giganterne, bl.a. Facebook

Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?**	**Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?**	**Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?**
Det er ikke muligt for kommunerne at indgå retvisende aftalegrundlag (databehandleraftale eller aftale om fælles dataansvar) med de store tech-giganter, herunder Facebook, da disse opererer med standardvilkår.	Art. 26 og art. 28	Kommunerne ser behov for, at staten eller EU tager ejerskab til problematikken. Det foreslås bl.a., at der kunne etableres en enhed, nationalt eller på EU-niveau, som løbende vurderer sikkerheden hos de store spillere (f.eks. Facebook, Apple, Zoom, Amazon, Google m.fl.). Der efterlyses desuden meget klarere, gerne risikobaseret, vejledning fra Datatilsynet og/eller Justitsministeriet om, hvordan kommunerne bør forholde os til tech-giganterne i praksis, indtil der er fundet en brugbar løsning på tech-giganternes standardvilkår.	I nogle kommunern har dialogen med DPO´en betydet, at der er blevet udarbejdet organisatoriske tiltag i form af procedurer for anvendelse af sociale medier, hvor der opfordres til at minimere brugen af personoplysninger på Facebook. I andre kommuner har DPO´en anbefalet, at sociale medier ikke anvendes.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

4.2. Bemærkninger

Løsningsforslag
Kommunerne ser behov for, at staten eller EU ved EU-Kommissionen eller Det Europæiske Databeskyttelsesråd tager ejerskab til problematikken og lægger kollektivt pres på de store tech-giganter. Det foreslås bl.a., at der kunne etableres en enhed, nationalt eller på EU-niveau, som løbende vurderer sikkerheden hos de store spillere (f.eks. Facebook, Apple, Zoom, Amazon, Google m.fl.).

Kommunerne efterlyser desuden meget klarere, gerne risikobaseret, vejledning fra Datatilsynet og/eller Justitsministeriet om, hvordan kommunerne bør forholde os til tech-giganterne i praksis, indtil der er fundet en brugbar løsning på tech-giganternes standardvilkår.

Uddybning
Det er ikke muligt for kommunerne at komme til at indgå retvisende dataansvarsaftaler (databehandleraftaler eller aftaler om fælles dataansvar) med de store tech-giganter som Facebook, Google og Microsoft. Tech-giganterne udarbejder alene standardvilkår for brugen af deres løsninger, som de offentliggør på deres hjemmesider, og der er ikke mulighed for, at den enkelte kommune kan justere i disse vilkår, selvom aftalerne ikke afspejler de dataansvarlige kommuners ønsker til behandlingen af data.

For så vidt angår Facebooks databehandlervilkår lever de fx ikke op til kravene til indholdet af en databehandleraftale. Vilkårene har nogle indholdsmæssige mangler, men væsentligst er, at formålet med en databehandleraftale er at skabe klarhed over databehandlerens rolle og, at denne kun kan behandle oplysninger på vegne af de dataansvarlige. Aftalen skal således tydeliggøre, at databehandleren ikke selv kan definere, til hvilket formål og med hvilke midler, der skal ske behandling af personoplysninger. Facebooks databehandlervilkår skaber tvivl om, hvilken rolle Facebook reelt påtager sig. Kommunerne gives som dataansvarlige reelt ikke nogen instruktionsbeføjelse, i stedet må kommunerne acceptere behandlinger og vilkår, fx i forhold til sletning og brugen af data, som Facebook definerer. Hermed skabes der tvivl om databehandlerens rolle og forpligtelser.

Tech-giganternes brug af standardvilkår gør det uklart for kommunerne, hvorvidt de kan anvende tech-giganternes løsninger. Og flere kommuner udarbejder egne retningslinjer for fx brugen af Facebook, hvor der opfordres til at minimere, eventuelt undlade, brugen af personoplysninger på Facebook, indtil der er afklaring af området.

I forhold til tech-giganterne oplever kommunerne at være "den lille" uanset, at de juridisk har rollen som dataansvarlige for borgernes data. KL har også tidligere været i dialog om problematikken med både Datatilsynet, Justitsministeriet og Facebook selv uden, at der blev opnået et resultat. Kommunerne peger på, at det er en problemstilling, som der er behov bliver løst af staten eller i EU-regi og, at der bør lægges kollektivt pres på de store tech-giganter. Det foreslås bl.a., at der kunne etableres en enhed, nationalt eller på EU-niveau, som løbende vurderer sikkerheden hos de store spillere (f.eks. Facebook, Apple, Zoom, Amazon, Google m.fl.).

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Kommunerne efterlyser desuden meget klarere vejledning fra Datatilsynet og/eller Justitsministeriet om, hvordan kommunerne bør forholde os til tech-giganterne i praksis, indtil der er fundet en brugbar løsning på tech-gigan-ternes standardvilkår. Vejledning, der alene refererer reglerne om, at der er krav om indgåelse af dataansvarsaftaler er ikke reel vejledning for kommu-nerne. I forlængelse heraf bemærker kommunerne, at et totalt ophør med at anvende sociale medier, herunder Facebook, er urealistisk. Kommunerne fo-reslår, at der kan ses på konkret vejledning, der tager udgangspunkt i en risi-kobaseret tilgang herunder, at der tages højde for, at de fleste borgere ac-cepterer risikoen i forhold til privat brug af sociale medier.

5. Bagatelgrænse for anmeldelse af sikkerhedsbrud

5.1. Skema vedrørende bagatelgrænse for anmeldelse af sikker-hedsbrud

Konkret beskri-velse af problem-stillingen	**Hvilken databeskyt-telsesretlig regel knytter problemstil-lingen sig til?**	**Hvilke databeskyt-telsesretlige over-vejelser har man gjort sig som led i løsningen af pro-blemstillingen?**	**Har problemstillin-gen været drøftet med en DPO (data-beskyttelsesrådgi-ver)? Hvad blev re-sultatet af drøftel-sen?**
Det er uklart, i hvil-ket omfang der re-elt er sikkerheds-brud, som ikke skal anmeldes.	Art. 33, stk. 1	At der fastlægges en højere bagatel-grænse, der er no-get højere grad end i dag afspejler databeskyttelses-forordningens risi-kobaserede tilgang til arbejdet med datasikkerhed. En-ten via revision af national vejledning eller på sigt revi-sion af artikel 33, stk. 1. Evt. hvor stikprøvekontroller af hændelseslog-gen erstatter an-meldelsesordnin-gen. En udbygning af Datatilsynets vej-ledning med flere kommunale ek-sempler, der gør det mere klart, hvornår der ikke behøver at blive	Kommunerne an-vender i et vist om-fang DPO´erne til sparring ift. vurde-ringen af risici for-bundet med et sik-kerhedsbrud.

		foretaget anmeldelse som følge af en vurdering af det samlede aktuelle risikobillede.	

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

5.2. Bemærkninger

Løsningsforslag

Kommunerne foreslår, at Datatilsynets vejledning om håndtering af brud på persondatasikkerheden udbygges med flere kommunale eksempler, der gør det mere klart, hvornår der ikke behøver at blive foretaget anmeldelse af sikkerhedsbrud som følge af en vurdering af det samlede, aktuelle risikobillede. Og at der i den forbindelse fastlægges en bagatelgrænse, der er noget højere end i dag og afspejler databeskyttelsesforordningens risikobaserede tilgang til arbejdet med datasikkerhed.

På sigt kan kommunernes erfaringer med anmeldelse af bagatelagtige sikkerhedsbrud bringes i spil i forbindelse med en eventuel revision af reglerne i databeskyttelsesforordningen med henblik på, i art. 33, stk. 1, at få hævet barren for, hvornår der skal ske anmeldelse. Som alternativ til anmeldelsesordningen kunne det i samme forbindelse overvejes i stedet at etablere en ordning, hvor der foretages stikprøvekontroller af kommunernes hændelseslog i forbindelse med håndtering af sikkerhedsbrud.

Uddybning
Kommunerne bruger mange resurser på at anmelde sikkerhedsbrud til Datatilsynet. Ofte sikkerhedsbrud som kommunerne oplever som i småtingsafdelingen, men som anmeldes for at være på den sikre side i forhold til overholdelse af reglerne. Kommunerne tilkendegiver, at det føles som spild af tid og meradministration, der reelt ikke giver mere datasikkerhed. Kommunerne opfordrer til, at deres (og Datatilsynets) tid og resurser i stedet fokuseres på de mere alvorlige brud på sikkerheden. Særligt i lyset af, at kommunerne oplever at indberette sikkerhedsbrud, der i en lang række tilfælde alligevel blot umiddelbart afsluttes hos Datatilsynet med et svar til den enkelte kommune om, at hændelsen ikke står mål med de resurser, som de skal bruge på opgaven.

Derfor efterlyser kommunerne fastlæggelsen af en bagatelgrænse i Datatilsynets vejledning om håndtering af brud på persondatasikkerheden, der er noget højere end i dag og afspejler databeskyttelsesforordningens risikobaserede tilgang til arbejdet med datasikkerhed. Kommunerne oplever, at Datatilsynet reelt ikke ser nogen nedre grænse for, hvad der skal anmeldes.

Et brud på persondatasikkerheden skal ikke anmeldes til Datatilsynet, hvis det er usandsynligt, at bruddet indebærer en risiko for fysiske personers rettigheder eller frihedsrettigheder, jf. art. 33, stk. 1. Og ifølge Datatilsynets vejledning, er det det samlede aktuelle risikobillede, der er afgørende for, om der skal ske anmeldelse af et brud på persondatasikkerheden til Datatilsynet. Det er dog kommunernes oplevelse, at denne risikovurdering ikke i dag er tilstrækkeligt afspejlet i Datatilsynets mundtlige rådgivning af kommunerne, hvorefter nærmest alle sikkerhedsbrud skal anmeldes.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Da formuleringen af art. 33, stk. 1, er formuleret meget snævert, idet anmeldelse kun kan udelades, såfremt det er *usandsynligt*, at bruddet indebærer en risiko, kan kommunernes erfaringer med anmeldelse af bagatelagtige sikkerhedsbrud på sigt bringes i spil i forbindelse med en eventuel revision af reglerne i databeskyttelsesforordningen. Som alternativ til anmeldelsesordningen kunne det også overvejes i stedet at etablere en ordning, hvor foretage stikprøvekontroller af kommunernes hændelseslog i forbindelse med håndtering af sikkerhedsbrud.

Indtil en eventuel revision efterlyser kommunerne, at Datatilsynets vejledning udbygges med flere kommunale eksempler, der gør det mere klart, hvornår der ikke skal indgives anmeldelse som følge af en vurdering af det samlede risikobillede.

Som konkrete eksempler på sikkerhedsbrud, som kommunerne bruger tid på at anmelde nævnes:
- Dokumenter med personoplysninger glemt i printeren eller et møderum
- Medarbejdere, der arbejder i "åbent rådhus"-lokaler og glemmer at lukke for deres computere i et kortere tidsrum – fx ved en tur til printeren.

Herudover gør kommunerne opmærksom på, at formularerne til brug for anmeldelse ikke er optimale, bl.a. er der ikke mulighed for at kunne tilføje til eksisterende anmeldelser og formularerne stiller krav om indtastning af oplysninger som ikke altid er relevant i den givne situation.

6. Oplysningspligten i artikel 13 og 14

6.1. Skema vedrørende oplysningspligten

Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?**	**Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?**	**Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?**
Uklarhed med hensyn til, hvordan og i hvilke tilfælde oplysningspligten skal opfyldes. Hvornår er der tale om et nyt formål, og hvor bredt må formålet være? Samt hvor specifikt skal oplysningspligten gives?	Art. 13 og 14	Kommunerne efterlyser uddybning af Datatilsynets eksisterende vejledning om registreredes rettigheder med flere konkrete eksempler, gerne med kommunal relevans, som også ikke GDPR-kyndige kan bruge.	DPO har ofte været inddraget i spørgsmålet, men uden at finde løsninger på spørgsmålene.

Endvidere er oplysningspligten overfor bipersoner fortsat en udfordring for kommunerne.			

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

6.2. Bemærkninger

Løsningsforslag
Kommunerne efterlyser en udbygning af Datatilsynets vejledning om registreredes rettigheder i afsnittet om oplysningspligten med flere konkrete eksempler, gerne med kommunal relevans, som ikke GDPR-kyndige også kan bruge.

Uddybning
Generelt oplever kommunerne de største udfordringer med oplysningspligten i forhold til de øvrige regler om registreredes rettigheder.

På trods af kommunernes viden om formålet med oplysningspligten er kommunerne i flere situationer bekymrede for, at reglerne ikke altid skaber den ønskede åbenhed og gennemsigtighed om behandlingen af personoplysninger, men mange gange desværre opleves af borgerne som unødvendig og ligegyldig spamming fra kommunerne.

Det fremgår af Datatilsynets vejledning, at oplysningspligten som udgangspunkt kun skal opfyldes én gang også ved løbende indsamlinger. Oplysningspligten skal derfor kun opfyldes på ny, hvis oplysningerne anvendes til nye formål, som der ikke tidligere er oplyst om. Oplysningspligten skal ikke opfyldes igen ved løbende indsamlinger til samme formål.

Det indebærer, at der kan være forskel på tilfælde, hvor en borger i en enkeltstående sag fx søger om et hjælpemiddel eller søger om en byggetilladelse, og på den anden side et forløb, hvor et barn begynder i skole, en ældre borger flytter på plejehjem eller en medarbejder begynder i et ansættelsesforhold, hvor der løbende indsamles oplysninger af forskellig karakter.

Kommunerne oplever desværre, at Datatilsynets vejledning ikke medvirker til at hjælpe kommunerne med at navigere indenfor oplysningspligten, så kommunerne kan balancere hensynet til både borgere og kommuner, jf. art. 1 i forordningen, og som derigennem sikrer borgerne gennemsigtighed (men ikke ligegyldig spamming) og forvaltningens effektivitet (som også gavner borgerne).

Konkret oplever kommunerne endvidere, at gennemførelse af oplysningspligten i forhold til udsatte grupper af borgere ofte kan være vanskelig, da denne gruppe af borgere har svært ved at forstå indholdet af oplysningspligten, og tit bliver unødigt bekymret, når kommunen giver dem de konkrete oplysninger.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Kommunerne oplever videre, at det kan være vanskeligt at afklare, hvor specifikt formålene skal angives i oplysningspligten. Er det for generelt, er der principielt en risiko for, at oplysningspligten ikke opfyldes, og er det "for præcist", er der risiko for, at oplysningspligten skal gentages for ofte overfor borgeren.

Bestemmelsen om formålsbestemthed i art. 5. stk.1, litra b, giver i praksis anledning til stor tvivl hos kommunerne – også i forhold til opfyldelse af oplysningspligten.

Kommunerne er i tvivl om, hvor brede formål de kan arbejde med. Spørgsmålet har desuden den praktiske betydning, at behandling til et nyt formål, udløser en ny oplysningspligt. Dette fører ifølge kommuner ofte til, hvad der kan opleves som spamming af borgerne. Dette hænger også sammen med, at det af administrative årsager er mere enkelt at sende en "fuld" oplysningspligt end at skulle vurdere konkret, om borgeren kender enkelte af oplysningerne, og derfor kun skal oplyses om en delmængde af oplysningspligtsoplysningerne.

Tvivlen opstår videre i fx ansøgningssager, hvor det er uklart for kommunerne, hvornår det er tilstrækkeligt at henvise til særlovgivning fx serviceloven og, hvor der skal ske henvisning til databeskyttelsesforordningen og databeskyttelsesloven.

Mange kommuner oplever desuden, at oplysningspligten overfor bipersoner er udfordrende. Vejledningen om registreredes rettigheder nævner, at man i videre omfang end i forhold til andre registrerede vil kunne anvende undtagelserne til oplysningspligten, da opfyldelse af oplysningspligten her ofte vil være umulig eller kræve en – relativt set i forhold til beskedne rolle, bipersonen spiller i sagen – uforholdsmæssigt stor indsats. Denne del af vejledningen kan med fordel udbygges med konkrete eksempler med udgangspunkt i den kommunale virkelighed.

Løsningsforslag:

- KL anbefaler, at der sker en væsentlig udbygning af Datatilsynets vejledning om registreredes rettigheder med flere konkrete eksempler, gerne med kommunal relevans, som ikke GDPR-kyndige også kan bruge
- KL anbefaler videre, at der i Datatilsynets vejledning om registreredes rettigheder tages højde for, at formål ikke defineres så snævert, at oplysningspligts-oplysninger skal gives hver gang personoplysninger videregives, og som tager højde for:
    - Dels at der i forvejen inden for de forskellige fagområder er bestemmelser, der sikrer, at borgerne bliver involveret og informeret, fx i den sociale retssikkerhedslovs § 1, nr. 1 og § 4, officialprincippet, partshøringsbestemmelsen i forvaltningslovens § 19, regler på folkeskoleområdet om skole/hjem-samarbejde m.m.
    - Dels at de områder, som kommunerne dækker, spænder over alt fra enkeltsager som fx ansøgning om et hjælpemiddel til flerårige forløb som fx 5-6 år i integreret institution eller 10 år i folkeskolen. I forbindelse med forløb bør formålet kunne afgrænses, så det dækker hele forløbet.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

7. Samspillet mellem GDPR, forvaltningsretlige regler og sektorlovgivning

7.1. Skema vedrørende samspillet mellem GDPR, forvaltningsretlige regler og sektorlovgivning

Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?**	**Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?**	**Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?**
Uklarhed med hensyn til om en behandling er nødvendig af hensyn til myndighedsudøvelse eller en behandling i samfundets interesse fører til at mange kommuner tyr til samtykke	Art. 6, stk. 1, litra a og e, samt artikel 6, stk. 2-3 (og art. 9)	Kommunerne er opmærksomme på, at løsningen skal findes i fortolkningen af nødvendighedskravet i art. 6, stk. 1, litra e (og art. 5, stk. 1, litra c).	DPO bliver overordnet set inddraget i problemstillinger af denne karakter, men DPO'en er som udgangspunkt ikke specialist i hverken forvaltningsret eller sektorlovgivning og kan derfor ikke vejlede (nogle DPO'ere mener godt, at de kan).

7.2. Bemærkninger

Løsningsforslag
Kommunerne efterlyser centralt udarbejdet konkret vejledning med virkelighedsnære eksempler særligt på sundheds-, social- og beskæftigelsesområdet, men også i forhold til brug af billeder. SSP-vejledningen, som Justitsministeriet har udgivet, er et eksempel på en sådan vejledning.

Hvis uklarheden ikke kan afhjælpes med vejledning, må det overvejes at få præciseret nødvendighedskravet i en kommende evaluering af databeskyttelsesforordningen på europæisk plan.

Uddybning
Der er en udbredt tvivl om afgrænsningen af behandlingsgrundlaget i art. 6, stk. 1, litra e (1. og 2. led) og det hertil knyttede nødvendighedskrav (som også findes i art. 5, stk. 1, litra b om dataminimeringsprincippet). Det gælder både i forbindelse med udveksling af oplysninger inden for samme forvaltning, mellem forvaltninger og mellem myndigheder – navnlig inden for sundheds-, social- og beskæftigelsesområdet, men også i forbindelse med brug

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

af billeder i kommunernes kommunikationsarbejde, herunder på sociale platforme, og i forbindelse med dagligdagen i kommunale skoler og institutioner.

Reglerne stiller krav om, at borgernes personoplysninger – medmindre det sker på grundlag af samtykke – kun må behandles, når det er nødvendigt. Det er uklart, hvad der menes med "nødvendigt". Datatilsynet har fx afvist, at det var nødvendigt at bruge matematisk beregnede fingeraftryk som tidsregistrering, fordi man kunne bruge andre, mindre indgribende metoder, fx en portvagt, selv om denne løsning er meget dyrere og bureaukratisk. I andre tilfælde synes kravet om nødvendighed at være opfyldt, selv om der er alternativer. Fx mener Datatilsynet, at det vil være OK at benytte fotos af børn i garderoben i en daginstitution, selv om børnene også vil kunne finde deres pladser fx ved hjælp af dyremotiver.

Kommunerne anfører, at medarbejderne på grund af tvivl om nødvendighedskravet tyr til at bede om samtykke til behandlingen.

Problemstillingen afspejler også en tvivl, der udspringer af muligheden for nationalt at fastsætte mere specifikke regler i henhold til art. 6, stk. 2-3, når dette mere specifikke retsgrundlag selv indeholder regler om samtykke.

Løsningsforslag:
- Der bør udarbejdes central og klar vejledning, der tydeliggør at behandlingsgrundlaget for den sagsbehandling kommunerne udfører på grundlag af forvaltningsloven og den sociale retssikkerhedslov, herunder disse loves samtykkebestemmelser, er artikel 6, stk. 1, litra e om samfundsinteresse og myndighedsudøvelse og ikke artikel 6, stk. 1, litra a.
- Der bør udarbejdes central og klar vejledning om forståelsen af nødvendighedskravet. Det er KL's opfattelse, at nødvendighedskravet for offentlige myndigheder bør forstås bredt som et krav om saglighed.
- Det bør udarbejdes central og klar vejledning med tydelig angivelse af samspillet mellem hjemlerne i forordningen, de forvaltningsretlige regler og sektorlovgivningen, og således at samspillet mellem regelsættene illustreres med praksisnære eksempler i stil med SSP-vejledningen. Eksemplerne skal belyse samspillet mellem regelsættene både i forbindelse med udveksling af oplysninger inden for og uden for den kommunale enhedsforvaltning. Efterspørgslen på vejledning er særligt udtalt for så vidt angår udveksling af oplysninger i krydsfeltet mellem sundheds-, social- og beskæftigelsesområdet.
- Der bør udarbejdes vejledning, der med en anden tydelighed end s. 215 i betænkningen om GDPR fastslår med hvilken hjemmel i art. 9, forbuddet mod behandling af følsomme oplysninger kan afløftes i forbindelse med faktisk forvaltningsvirksomhed.
- Der er behov for mere konkret vejledning om brug af billeder i den kommunale sektor

Kommunerne har individuelt suppleret med flere konkrete eksempler, som kan føres tilbage til ovenstående problematikker.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

8. Dokumentations-/påvisningskravet

8.1. Skema vedrørende dokumentations-/påvisningskravet

Konkret beskrivelse af problemstillingen	Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?	Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?	Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?
Det er uklart, hvilke og hvor mange foranstaltninger den dataansvarlige skal iagttage for at leve op til kravet om at kunne påvise ansvarlighed ift. overholdelsen af behandlingsprincipperne.	Art. 5, stk. 2	Kommunerne efterlyser konkretisering og uddybning af påvisningskravet via mere vejledning.	I nogle kommuner har problemstillingen været drøftet med kommunens DPO uden, at det nødvendigvis har givet den fornødne afklaring, idet der mangler vejledning om problemstillingen.

8.2. Bemærkninger

Løsningsforslag
Kommunerne efterlyser konkretisering og uddybning af påvisningskravet via mere vejledning.

Uddybning
Det er uklart, hvilke og hvor mange foranstaltninger den enkelte dataansvarlige kommune skal iagttage for at leve op til kravet om at kunne påvise ansvarlighed ift. overholdelsen af behandlingsprincipperne. Kommunerne bruger tid og resurser på at diskutere indholdet af kravet om accountability.

Hvilke dokumentationskrav fordrer bestemmelsen? Kommunernes opgavevaretagelse, herunder håndtering af persondata, er allerede i vidt omfang detaljeret reguleret ved lov. Dvs. håndteringen sker allerede "lovligt, rimeligt og på en gennemsigtig måde", til "legitime formål" og med korrekte og relevante data, der gemmes så længe, der er administrativt eller arkivmæssigt formål, jf. art. 5, stk. 1, litra a-e. Det virker i udgangspunktet som unødvendigt bureaukrati for kommunerne at bruge tid på at skrive ned, at man gør det, man er pålagt i medfør af loven.

Kommunerne efterlyser konkretisering og uddybning af påvisningskravet via mere vejledning sådan, at det undgås, at kommunerne indfører unødvendige procedurer, og at der sker overimplementering af kravet. I den forbindelse bør det ligeledes afklares, hvorvidt der stilles de samme dokumentationskrav til allerede eksisterende behandlingsaktiviteter, der har fundet sted i mange år forud for databeskyttelsesforordningens ikrafttræden, eller om kravet

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

alene gælder i forhold til "nye" behandlingsaktiviteter, som kommunerne har iværksat efter, at databeskyttelsesforordningen trådte i kraft.

Ved en eventuel revision af GDPR kunne man overveje at erstatte de mange dokumentationskrav med andre modeller til sikring af, at reglerne overholdes. Fx ved spørge de registrerede/borgerne og de kommunalt ansatte om de føler sig oplyste og trygge i forhold til kommunens databehandlinger.

9.Tilsyn med databehandlere

9.1. Skema vedrørende tilsyn med databehandlere

Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?**	**Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?**	**Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?**
Det er uklart, hvad der reelt er genstanden for tilsynet med databehandlere. Det er uklart, hvordan kommunerne i praksis kan føre fælles tilsyn med deres leverandører. Der er uklart, hvornår kommunerne kan nøjes med skriftlige tilsyn med deres databehandlere, og hvornår der kræves fysisk tilsyn Og i fald et skriftligt tilsyn er nok, hvilke krav, der så er til et sådant? Og hvordan gennemføres et fysisk tilsyn i fald, der er krav herom?	Art. 28, stk. 3, litra h	Opdatering og udbygning af Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere, gerne med tjeklister og/eller tilsynsskabeloner.	Flere kommuner har drøftet spørgsmålet med deres DPO.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

9.2. Bemærkninger

Løsningsforslag
Kommunernes efterspørger mere vejledning om tilsynsopgaven via en opdatering og udbygning af Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere, gerne med tjeklister og/eller tilsynsskabeloner.

Uddybning
Generelt har kommunerne en lang række spørgsmål til, hvordan kommunerne lever op til kravet om følge op på, at deres databehandlere overholder kravene i databeskyttelsesforordningens artikel 28, jf. artikel 28, stk. 3, litra h, forudsætningsvis. Kommunerne efterspørger, at Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere udbygges med svar på kommunernes spørgsmål. Til brug herfor har KL i maj 2019 fremsendt notat til Datatilsynet med de spørgsmål, som kommunerne ønsker afklaret i forhold til tilsynopgaven. Kommunerne afventer fortsat en opdatering af Datatilsynets vejledende tekst.

Kommunerne ønsker afklaring på, hvad der reelt er tilsynets genstand, og KL vil derfor foreslå, at vejledningen tydeliggør kommunernes minimumsforpligtelse i forhold til tilsynsforpligtelsen – særligt fordi KL ligesom Datatilsynet har set eksempler på, at ekstern revision ser behov for at påse forhold, der ikke er relevante i forhold til de sikkerhedsforanstaltninger, som er aftalt i den enkelte databehandleraftale. Vil det være tilstrækkeligt, at det påses, at de sikkerhedsforanstaltninger, som konkret er aftalt i databehandleraftalen, er blevet gennemført? Eller vil det ligeledes skulle påses, at databehandleren overholder alle dele af databehandleraftalen, jf. artikel 28, stk. 3, litra a-h, herunder om databehandleren, jfl. litra c, generelt har indrettet sig i overensstemmelse med artikel 32, dvs. således, at der skal føres tilsyn med sikkerhedsforanstaltninger, der ikke nødvendigvis har noget at gøre med de behandlinger, som foretages i medfør af databehandleraftalen?

Det ønskes ligeledes afklaret i forhold til tilsynets genstand, om der foreligger en forpligtelse til at skulle påse, at databehandleren overholder alle krav i artikel 28, fx, at databehandleren har indgået de nødvendige databehandleraftaler med eventuelle underdatabehandlere, jf. artikel 28, stk. 4, og, at disse aftaler indeholder de samme forpligtelser som aftalen med databehandleren?

Kommunerne efterlyser også afklaring af, under hvilke forudsætninger kommunerne kan gå sammen om at føre tilsyn med deres leverandører. Er det når kommunerne har købt samme it-løsning, anvender it-løsningen til samme formål, eller vil man kunne føre fælles tilsyn blot de aftalte sikkerhedsforanstaltninger er de samme? Og vil kommunerne kunne "dele" en tilsynsrapport fra fx et eksternt revisionsfirma, sådan at én kommunes tilsyn med en leverandør "genanvendes" af andre kommuner?

Kommunerne efterlyser også afklaring af, hvornår de kan nøjes med skriftlige tilsyn med deres databehandlere, og hvornår der kræves fysisk tilsyn med databehandlerne. Og i fald et skriftligt tilsyn er nok, hvilke krav, der så er til et sådant? Beder man blot leverandøren om at bekræfte, at de overhol-

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

der de sikkerhedsforanstaltninger, som de allerede én gang via databehandleraftalen har forpligtet sig til at gennemføre? Eller skal der spørges nærmere ind til status på gennemførslen af sikkerhedsforanstaltningerne? Og ændrer risikoovervejelserne på, hvor "dybdeborende" spørgsmålene skal være? Ligeledes ønskes afklaret, hvordan et fysisk tilsyn gennemføres i fald, der er krav herom, bl.a. hos cloud-leverandører?

Kommunerne efterlyser som hjælp til gennemførelse af tilsynet af deres databehandlere, at Datatilsynets vejledende tekst udbygges med tjeklister og/eller tilsynskabeloner.

10. Risikovurderinger og sikkerhedsforanstaltninger

10.1. Skema vedrørende risikovurderinger og sikkerhedsforanstaltninger

Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?**	**Hvilke databeskyttelsesretlige overvejelser har man gjort sig som led i løsningen af problemstillingen?**	**Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?**
Det er uklart, hvad der konkret skal til for at overholde artikel 32 om behandlingssikkerhed. Det fremgår ikke af bestemmelsen, hvad der er ”passende” sikkerhedsforanstaltninger, jf. artikel 32.	Art. 32	Kommunerne efterlyser støtte til arbejdet med fastlæggelse af sikkerhedsniveauet via mere vejledning med flere konkrete eksempler. Udover vejledning efterlyses et konkret risikovurderingsværktøj med udførlig hjælp til at gennemføre risikovurderinger, fx med en spørgeramme i forhold til de forhold, der skal overvejes.	Flere kommuner har drøftet spørgsmålet med deres DPO.

10.2. Bemærkninger

Løsningsforslag
Kommunerne efterlyser støtte til arbejdet med fastlæggelse af sikkerhedsniveauet via mere vejledning med flere konkrete eksempler.

Dato: 9. oktober 2020

Sags ID: SAG-2020-03947
Dok. ID: 2987141

E-mail: KAHH/LPJ@kl.dk
Direkte: 3370 3261

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Udover vejledning efterlyses et konkret risikovurderingsværktøj med udførlig hjælp til at gennemføre risikovurderinger, fx med en spørgeramme i forhold til de forhold, der skal overvejes.

Uddybning
Databeskyttelsesforordningens artikel 32 stiller krav om, at kommunerne skal gennemføre tekniske og organisatoriske sikkerhedsforanstaltninger, der passer til de risici, der er forbundet med givne behandlinger af persondata. Eftersom fastlæggelsen af sikkerhedsniveauet beror på en vurdering af de konkrete risici, fremgår det ikke af bestemmelsen, hvad der er "passende" sikkerhedsforanstaltninger. Det er en udfordring, at alle kommuner er forpligtede til at foretage risikovurderinger af alle behandlinger og herefter vælge passende sikkerhedsforanstaltninger til at håndtere de identificerede risici. Det er ressourcekrævende, og det kan blive dyrt at forsøge at tilvejebringe noget, der er godt nok, når der ikke står nogen steder, hvad der er tilstrækkeligt. Fx kan det være svært at vide, hvad der efter artikel 32 er "passende" foranstaltninger til sikring af personoplysninger, som fx oplysninger om beboere på et bosteds aktiviteter på en aktivitetstavle, særligt fordi aktiviteterne i visse tilfælde kan indikere helbredsforhold. Eller hvorvidt papirer med personoplysninger skal være i aflåst skab, i aflåst alarmeret lokale eller i bankboks. Der skal udarbejdes en risikovurdering, som skal tage hensyn til en lang række forhold, førend der kan foretages selv helt almindelige behandlinger af oplysninger.

Kommunerne efterlyser støtte til arbejdet med fastlæggelse af sikkerhedsniveauet for deres behandlinger af persondata via mere vejledning med flere konkrete eksempler på, hvad der vurderes at være "passende" sikkerhedsforanstaltninger i givne situationer og hvorfor. Er TLS-kryptering fx en tilstrækkelig sikkerhedsforanstaltning til forsendelse af alle typer personoplysninger? Og hvilken foranstaltninger kan anbefales til behandlingen af almindelige henholdsvis følsomme personoplysninger? Ligeledes efterspørges vejledning om, i hvilket omfang givne risikovurderinger kan "genbruges". Udover vejledning efterlyses et konkret risikovurderingsværktøj med udførlig hjælp til at gennemføre risikovurderinger, fx med en spørgeramme i forhold til de forhold, der skal overvejes.