

BILAG 2: GDPR-udfordringer og løsninger

KL har i forbindelse med den nationale evaluering af databeskyttelsesreglerne sendt en lang række problemstillinger, som KL tidligere er blevet spurgt om i forhold til GDPR, i skriftlig høring hos alle kommuner mhp. at afklare, om problemstillingerne var udtryk for generelle problemstillinger. I det omfang kommunerne har svaret bekræftende, fremgår problemstillingerne af skemaet nedenfor.

I høringen af kommunerne opfordrede KL ligeledes de enkelte kommuner til at fremkomme med yderligere GDPR-udfordringer, som den enkelte kommune måtte opleve. Det har kommunerne gjort. Rækker markeret med * er udtryk for disse problemstillinger.

	Konkret beskrivelse af problemstillingen	Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?	Har I overvejet, hvordan man kan løse problemet? (Fx via ændring af reglerne, mere vejledning, nye centrale, organisatoriske tiltag etc.)	Har problemstillingen været drøftet med en DPO (databeskyttelsesrådgiver)? Hvad blev resultatet af drøftelsen?
		(Alle henvisninger er til databeskyttelsesforordningen medmindre andet er anført).		
1.	Behandlingen af personoplysninger inden for det sundhedsfaglige område er reguleret af flere forskellige regelsæt. Både GDPR, retssikkerhedsloven, forvaltningsloven, serviceloven og sundhedsloven er i spil. Da der har været så megen opmærksomhed på GDPR, herunder kravet om, at borgerne (i nogle tilfælde) skal afgive samtykke til behandlingen af deres oplysninger, opstår der meget let misforståelser om, hvilke regler der gælder i hvilke sammenhænge.	Hele forordningen (Art. 6, stk. 1, litra e, art. 6, stk. 2-3 og art. 6, stk. 1, litra a)	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).
2.	Det er uklart, hvornår der er tale om behandlinger, som ikke er omfattet af reglerne, fordi der er tale om rent personlige eller familiemæssige aktiviteter?	Art. 2, stk. 2, litra c	Synes ikke på grundlag af høringssvarene at give anledning til udbredt tvivl. Nogle angiver, at der fortsat er behov for eksempler på grænsetilfælde.	DPO'en ses at have været involveret i de kommuner, der er stødt på problematikken.
3.	At afklare ud fra definitionen, hvem der er "dataansvarlig", giver mange udfordringer. 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. Fx er det uklart hvem, der er dataansvarlig ifm. skolefotografering. Er både skole og fotograf dataansvarlige? Er skolen databehandler for fotografen ifm. formidling af kontakt til forældrene?	Art. 4, nr. 7	Kommunerne efterlyser mere vejledning med flere konkrete eksempler, som også ikke GDPR-kyndige kan bruge. Gerne løbende udbygning af Datatilsynets vejledning. Det foreslås også, at Datatilsynet træffer flere afgørelser på området for at lægge en mere tydelig linje.	DPO'erne er i mange kommuner blevet inddraget i spørgsmålet. En række DPO'er har udarbejdet egne vejledninger og retningslinjer til deres kommuner. De kommunalt ansatte og DPO'erne er ikke i alle tilfælde nødvendigvis enige om vurderingen af spørgsmålet.
4.	Det har givet udfordringer, at statslige myndigheder, der fastsætter reglerne for kommunernes behandling af personoplysninger, juridisk defineres som "databehandlere", som kommunerne skal indgå databehandleraftaler med og føre tilsyn med. Kommunerne oplever, at definitionen, "... der behandler personoplysninger på den dataansvarliges vegne", jf. art. 4, nr. 8, i mange tilfælde ikke afspejler det reelle setup.	Art. 4, nr. 8	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 fremfor en databehandlerkonstruktion.	I de fleste kommuner er DPO'en ikke inddraget i problemstillingen, idet kommunerne reelt ikke oplever at have anden handlemulighed end at indgå databehandleraftalerne med staten.

	Kommunen står formelt som dataansvarlig og forudsættes at skulle føre tilsyn med (og bestemme over/instruere) statslige myndigheder, men sådan fungerer det ikke i praksis: Kommunerne har reelt ikke indflydelse på, hvordan den tekniske løsning er indrettet; dette bestemmer den statslige myndighed, og kommunen er forpligtet til at anvende systemet. Aktuelle eksempler er indberetningen af utilsigtede hændelser (Sundhedsdatastyrelsen), og Unilogin (Styrelsen for IT og Læring).		Alle databehandlaftaler mellem kommunerne og staten foreslås i stedet reguleret af bekendtgørelser, "andet retligt dokument", jf. artikel 28, stk. 3.	
5.	Viderebehandling/genanvendelse af personoplysninger, som borgeren allerede har afleveret til kommunen ifm. en sag, må ikke være "uforenelig" med det oprindelige formål, hvortil oplysningerne er indsamlet. Det kan være svært at vide, hvad der er foreneligt og ikke foreneligt. Eksempel: Videreanvendelse af en elevproduktion (tegning/maleri) i forbindelse med en årbog eller på skolens hjemmeside.	Art. 5, stk. 1, litra b og art. 6, stk. 4	Bestemmelsen om formålsbestemthed i art. 5, stk. 1, litra b, giver i praksis anledning til stor tvivl. 1) Hvor brede formål kan man arbejde med? Spørgsmålet har også 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. Løsningsforslag: - KL anbefaler, at der udarbejdes vejledning, der tager højde for, at formål ikke defineres så snævert, at oplysningspligtsoplysninger skal gives hver gang, personoplysninger videregives, og som tager højde for: o 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. o 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. 2) Hvornår foreligger der ikke-uforenelighed. Testen i art. 6, stk. 4, er vanskelig at afgrænse og der er meget få fortolkningsbidrag (der bidrager med andet end en gentagelse af bestemmelsens ordlyd). Det er vanskeligt at forstå, hvilke videreanvendelser der kræver en "§ 5, stk. 3"-bekendtgørelse (databeskyttelsesloven), eller en lov, der lever op til artikel 23, og hvilke videreanvendelser, der	Kommunernes DPO'ere bliver løbende inddraget, men ikke i alle tilfælde. Enkelte nævner at formulere formål tilpas bredt, så oplysningspligten ikke indtræffer i unødigt hyppigt omfang. Enkelte nævner awareness-kampagner men også at det er ressourcekrævende og at det ville være at foretrække, hvis reglerne var mere enkle.

			<p>kan finde sted på grundlag af ikke-uforenelighedstesten i art. 6, stk. 4.</p> <p>Justitsministeriet har udarbejdet en vejledning om udveksling (og dermed videreanvendelse) af oplysninger i SSP-samarbejdet.</p> <p>Løsningsforslag:</p> <ul style="list-style-type: none"> - Vejledninger i stil med SSP-vejledningen kunne med fordel udarbejdes på en lang række andre områder (navnlig vedrørende udveksling af oplysninger internt og på tværs af sundheds-, social- og beskæftigelsesforvaltningerne). 	
6.	<p>Sondringen mellem overdragelse og videregivelse og viderebehandling. Hvornår er der tale om hhv overdragelse, videregivelse og viderebehandling i forskellige situationer.</p> <p><i>Hermed menes:</i></p> <ul style="list-style-type: none"> - <i>overdragelse = til databehandler</i> - <i>videregivelse = til tredjemand (selvstændig dataansvarlig)</i> - <i>viderebehandling = til nyt formål inden for den dataansvarliges organisation.</i> <p>Eksempler:</p> <ul style="list-style-type: none"> - oplysninger fra afgivende til modtagende skole - oplysninger fra dagtilbud og skole - oplysninger fra skole til folkekirke - oplysninger fra skole til aflastnings- eller plejefamilier - oplysninger om navn/adresse på barns skole eller dagtilbud eller om barnets forhold i skole/dagtilbud til forælder, der ikke har del i forældremyndigheden, men som har orienteringsret i medfør af forældreansvarslovens § 23 - oplysninger til politiet - oplysninger mellem sundhedsplejerske og skole - oplysninger til leverandør af praktisk hjælp i borgerens hjem - oplysninger til mentor/coach o.lign. i relation til sygefravær mv. - oplysninger til konsulent-virksomhed i relation til ydelesesforløb (fleksjob eller virksomhedspraktik) - oplysninger til konsulentvirksomhed i relation til beskæftigelsesindsats for unge.* 	Art. 5, stk. 1, litra b og art. 6 stk. 2-3	<p>Der er behov for øget opmærksomhed på samspillet mellem databeskyttelsesreglerne og forvaltningretten mv., fx formålsberænsningsprincippet sammen med officialsprincippet, herunder betydning af, hvis der er tale om en ansøgningssag (FVL § 29).</p>	Ingen bemærkninger
7.	<p>Eksempler på formål (abstraktionsniveau) ift. fortegnelser efterlyses, og er formålsafgrænsningen den samme i fortegnelsen som ifm. oplysningspligten? *</p>	art. 5, stk. 1, litra b og art. 30		Ingen bemærkninger
8.	<p>Dataminimeringsprincippet stiller krav om, at behandling af personoplysninger kun må ske i det omfang,</p>	Art. 5, stk. 1, litra c	<p>Grundlæggende den samme problematik som nr. 1 om sundhedslovgivning m.v.</p>	Enkelte har angivet at have inddraget DPO'en.

	oplysningerne er "tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles". Det er uklart, hvorvidt de behandlinger af personoplysninger, som kommunerne udfører for at løse de opgaver, de er pålagt i medfør af lovgivningen, kan være ulovlige i medfør af dataminimeringsprincippet. Fx kunne man jo i princippet sige, at det at vise den enkelte borgers aktiviteter, med navns nævnelse på en tavle, på et bosted, ikke er nødvendigt i forhold til bostedets behandlingsformål, som er at gøre borgeren i stand til at klare sig i eget hjem, eventuelt med støtte.			
9.	<p>Det er uklart, hvor mange foranstaltninger den dataansvarlige skal iagttage for at leve op til kravet om at kunne påvise ansvarlighed ift. overholdelsen af behandlingsprincipperne. Hvilke dokumentationskrav fordrer bestemmelsen?</p> <p>Kommunernes opgavevaretagelse, herunder håndtering af persondata, er allerede i vidt omfang detaljeret reguleret ved lov. Det virker derfor som unødvendigt ekstraarbejde for kommunerne at bruge tid på at skrive ned, at man gør det, man er pålagt i medfør af loven.</p> <p>Det er desuden uklart, hvorvidt Datatilsynet stiller de samme dokumentationskrav i forhold til "nye" behandlingsaktiviteter, som kommunen måtte iværksætte efter databeskyttelsesforordningen trådte i kraft, som ift. til allerede eksisterende behandlingsaktiviteter, der har fundet sted i mange år?</p>	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.
10.	Der er tvivl om, hvilken hjemmel (samtykke eller myndighedsudøvelse), der skal anvendes til behandling af billeder i den kommunale administration. Fx billeder af medarbejdere på udflugt, børn der leger i børnehaven etc. Og vil man kunne sige, at behandlingen er "nødvendig"?	Art. 6	<p>Problemstillingen er inddraget under bemærkningerne til pkt. 1 (samspil mellem GDPR og faglovgivning inkl. generelle forvaltningsretlige regler).</p> <p>Man kan læse ud af besvarelserne, at der bliver brug megen tid på håndtering af spørgsmål om brug af billeder – behandlingshjemmel og hvornår der skal slettes ved tilbagetrækning af samtykke eller indsigelser – og også håndtering af oplysningspligten.</p>	DPO'en er blevet involveret i stort omfang. De fleste har ikke uddybet yderligere, men enkelte angiver, at det til stadighed er en meget ressourcekrævende og svær opgave. Løsninger findes konkret, men det er ikke altid de samme løsninger. Det skaber usikkerhed om, hvad der er rigtigt.
11.	<p>Tvivl om behandlingsgrundlag og hjemmel ved samarbejde med civilsamfundet (herunder foreninger, lokalråd og landdistriktsråd) og understøttelse af samskabelse er blevet besværliggjort, fx:</p> <ul style="list-style-type: none"> ○ Landdistriktsrådet fik tidligere lister over tilflyttere ud, så de kunne besøge nye borgere og tage godt imod dem. Det må vi ikke længere. ○ Tidligere havde vi oversigt over foreninger og adresser med navn på formændene på hjemmesiden, så alle kunne finde dem, og de kunne finde hinanden. Det må vi heller ikke uden individuelt samtykke. 	Art. 6		Ingen bemærkninger

	<ul style="list-style-type: none"> ○ Må vi eksempelvis offentliggøre fx foreninger, vandværksformænd og lodsejere på hjemmesiden? * 			
12.	Brug af billeder: Det er uklart, hvornår der skal indhentes samtykke samt, hvornår vi som kommune må bruge billeder ifm. fx kommunikationsopgaver. Der kan vejledningen godt gøres en del tydeligere.*	Art. 6		Ingen bemærkninger
13.	Det uklart, hvad der er hjemlen for behandling af personoplysninger om medarbejdere ifm. medarbejderaktiviteter (kagelister, lister over deltagere i sportsaktiviteter på arbejdspladsen mv.). Vil man kunne bruge artikel 6, stk. 1, litra e, om "samfundsinteresse" eller "offentlig myndighedsudøvelse", eller er disse aktiviteter ikke omfattet af GDPR-reglerne, da der er tale om private/personlige aktiviteter, jf. forordningens artikel 2, stk. 2, litra c?	Art. 6 (og art. 2, stk. 2, litra c)	<p>Der er efter Datatilsynets svar på benspændskataloget ikke tvivl i kommunerne om, at man gerne må have disse lister, men det er fortsat uklart, om behandlingsgrundlaget er myndighedsudøvelse/samfundsinteresse – eller om det er ok, fordi det falder uden for GDPR. Dette er også afspejlet i kommunernes besvarelse. Nogle anfører samfundsinteresse som behandlingsgrundlag, nogle anfører, at det falder uden for GDPR, og nogle mener, at behandlingsgrundlaget er DBL § 12. Endelig er der nogle, der blot konstaterer, at Datatilsynet har konkluderet, at man gerne må have sådanne lister, men at tilsynet ikke har begrundet svaret.</p> <p>Principielt er problemstillingen medtaget under pkt. 1, idet der også i dette eksempel er tvivl om afgrænsningen af behandlingshjemlen i art. 6, stk. 1, litra e.</p>	Flere har angivet at have inddraget DPO'en, men har ikke uddybet dennes involvering.
14.	Det er uklart, om man som dataansvarlig må videregive oplysninger om, hvem der deltager i et arrangement, til de pågældende deltagere, herunder udsende deltagerlister – og i givet fald hvad hjemlen er hertil?	Art. 6	<p>Høringssvarene viser, at der er usikkerhed om hvorvidt behandlingsgrundlaget er myndighedsudøvelse/samfundsinteresse eller samtykke. Problemstillingen er grundlæggende den samme som anført i forbindelse med punkt 1 – altså afgrænsning af art. 6, stk. 1, litra e, og i den forbindelse fortolkningen af nødvendighedskravet.</p> <p>Flere konstaterer, at Datatilsynet har svaret, men at behandlingshjemlen ikke er angivet.</p> <p>Ved tvivl om rækkevidden af behandlingshjemlen i art. 6, stk. 1, litra e, herunder forståelsen af nødvendighedskravet, tyr mange til samtykke som behandlingsgrundlag med de krav til oplysning og dokumentation, dette indebærer.</p> <p>I den forbindelse bidrager Datatilsynets vejledning om samtykke til tvivl om, hvornår samtykke er relevant som behandlingsgrundlag. I eksempel 2 i vejledningen, angives samtykke som (eksempel på) behandlingsgrundlag for behandling af medarbejdernes billeder i en intern digital telefonbog. Dette er ikke hensigtsmæssigt, når Datatilsynet i sin praksis har anerkendt, at en sådan behandling ikke kræver et</p>	Mange angiver ikke noget om DPO. De der angiver, at DPO'en er inddraget, har i de fleste tilfælde ikke angivet noget særligt. Enkelte har en generel bemærkning om, at DPO'en inddrages og forsøger at give svar og løsninger.

			<p>databeskyttelsesretligt samtykke. Det bidrager endvidere til tvivl, når det i vejledningen om samtykke hedder:</p> <p><i>"I visse situationer, hvor den registreredes afvisning af at give samtykke er uden betydning for myndighedens sagsbehandling af en ydelse eller tilladelse til den registrerede, vil behandling kunne ske på grundlag af samtykke. Det kan eksempelvis gælde, hvis en borger ønsker at acceptere kommunens tilbud om at modtage oplysninger på e-mail eller SMS om afhentning af storskrald eller oplysning om forsinkede anlægsarbejder i lokalområdet."</i></p> <p>Det er KL's opfattelse, at en kommune under henvisning til art. 6, stk. 1, litra e, "i samfundets interesse" kan rette henvendelse til borgere om en sådan sms-service, og at borgerne vil kunne takke ja eller nej, uden at behandlingsgrundlaget ændres/skifter til samtykke.</p>	
15.	<p>Behandling af ikke-følsomme oplysninger, som fx oplysninger på en aktivitetstavle om de aktiviteter man skal deltage i, kræver, at man som kommune foretager en vurdering af, om en behandling af personoplysninger er "nødvendig", jf. artikel 6, stk. 1, litra e. Det er uklart, hvad der er "nødvendige" behandlinger.</p>	Art. 6, stk. 1, litra e	<p>Mange henviser til, at problemstillingen er besvaret i Datatilsynets svar på benspændskataloget. Høringssvarene viser dog også, at der i et vist omfang er usikkerhed omkring, hvordan nødvendighedsvurderingen skal angribes.</p> <p>Grundlæggende er problemstillingen den samme, som der er redegjort for i punkt. 1 – altså afgrænsning af art. 6, stk. 1, litra e og i den forbindelse fortolkningen af nødvendighedskravet.</p>	Mange angiver ikke noget om DPO. De der angiver, at DPO'en er inddraget, har i de fleste tilfælde ikke angivet noget særligt.
16.	<p>Offentliggørelse af navn og adresse på borgere, som har haft byggesager hos kommunen, kræver, at man som kommune foretager en vurdering af, om behandlingen, her offentliggørelsen, af personoplysningerne er "nødvendig", jf. artikel 6, stk. 1, litra e. Det kan være uklart, hvad der er nødvendigt i denne sammenhæng.</p> <p>Formålet med at offentliggøre byggesager er at hjælpe nye ejere af boliger med at få kendskab til deres boligs "historie". Om det i den forbindelse er "nødvendigt" at offentliggøre navne og adresser på borgere, der har været involveret i byggesagerne (ansøgere, arkitekter, advokater m.fl.) kan være svært at vurdere. Nogle gange vil det være relevant/nødvendigt, andre gange ikke. Og relevansen bliver mindre og mindre jo ældre byggesagerne bliver, og betyder det så, at kommunerne er forpligtede til at slette i navne og adresser efter en given årrække?</p>	Art. 6, stk. 1, litra e	<p>Høringssvarene viser, at kommunerne ikke er i tvivl om, at der ikke må offentliggøres fortrolige oplysninger i byggesagsarkiver. Høringssvarene viser også, at der er tvivl om, hvordan nødvendighedskravet – både i art. 6, stk. 1, litra e og i art. 5, stk. 1, litra c – skal afgrænses. Flere peger på, at problemstillingen er den samme for så vidt angår offentliggørelse af høringssvar og offentliggørelse af dagsordener til kommunalbestyrelsesmøder m.v.</p> <p>Grundlæggende er problemstillingen den samme, som der er redegjort for i punkt. 1.</p>	Mange angiver ikke noget om DPO. De der angiver, at DPO'en er inddraget, har i de fleste tilfælde ikke angivet noget særligt. Enkelte har angivet, at der har været en grundig dialog med DPO'en om løsninger.
17.	<p>Må der ske offentliggørelse af høringssvar fra borgere, som indeholder personoplysninger, i forbindelse med en politisk behandling.*</p>	Art. 6	<p>Ifølge Datatilsynets svar på KLS benspænd har vi fået oplyst: <i>Så længe der er tale om almindelige oplysninger som navn og adresse, må kommunerne – ligesom f.eks. Folketinget – offentliggøre høringssvarene.</i></p> <p>Men vi mangler fortsat et svar på, hvilken lovhjemmel der siger, at vi må gøre det, da vi bliver udfordret på det af fx borgere, som ikke altid er tilfredse med, at vi har offentliggjort deres</p>	Ingen bemærkninger

			personoplysninger. Der holder det ikke helt at sige "Når Folketinget må det, så må vi også".	
18.	<p>GDPR er svært at forstå:</p> <ul style="list-style-type: none"> • Det er svært at forstå hvor langt et givent behandlingsgrundlag mv. egentligt strækker og, hvor grænsen så går. <ul style="list-style-type: none"> ○ Hvordan det defineres som en del af det at drive kommune og, hvornår det bliver "nice-to-have". * ○ 	Art. 6, stk. 1, litra e		Ingen bemærkninger
19.	<p>Det er uklart, om kommunerne umiddelbart må behandle billeder (herunder tage billeder samt lægge dem på Facebook) i medfør af databeskyttelsesforordningens artikel 6, stk. 1, litra e. I det Datatilsynets vejledning kræver, at kommunerne skal foretage en vurdering af, om billederne indeholder følsomme oplysninger, der kræver indhentning af <u>samtykke</u> fra de afbillede. Det ser ikke i vejledningen ud til, at kommunerne kan anvende anden hjemmel i artikel 9 (hjemlen til behandling af følsomme oplysninger) til behandling af billeder med følsomt indhold ifm. udførelsen af <u>faktisk forvaltningsvirksomhed</u> end ved at indhente samtykke. At administrere samtykker – indhentning, specificering, tilbagetrækning mv. er administrativt tunge processer.</p> <p>Det er ligeledes uklart, hvoraf det følger, at kommunerne også, når billeder lægges på Facebook, skal foretage en vurdering af, om de afbillede personer kan føle sig krænkede, udnyttede eller udstillede.</p>	Art. 6, stk. 1, litra e og art. 9	<p>Grundlæggende er problemstillingen den samme, som der er redegjort for i punkt. 1.</p> <p>Høringssvarene viser, at det er uklart, hvornår der efter reglerne stilles krav om samtykke ifm. brug af billeder – og om samtykket i givet fald er et samtykke efter art. 6, stk. 1, litra a, eller om behandlingsgrundlaget for en offentlig myndighed skal findes i art. 6, stk. 1, litra e, i kombination med princippet i artikel 5, stk. 1, litra a, om lovlighed, rimelighed eller gennemsigtighed, således at dette princip konkret begrænser muligheden for frit at anvende billeder uden accept; og således at accepten i denne sammenhæng alene udgør en garanti for den registrerede og ikke et behandlingsgrundlag i form af samtykke med hvad dertil hører, jf. art. 4, nr. 11).</p>	DPO'en er i flere tilfælde blevet involveret, men høringssvarene viser også, at der mangler brugbare løsninger.
20.	<p>Det er tungt at administrere, at fx film, der viser børn i en børnehave, som er behandlet (optaget) til ét formål, ikke umiddelbart kan anvendes til andre formål uden en nærmere juridisk vurdering af sammenhængen mellem det første behandlingsformål og det andet formål. Selv om vurderingen af sammenhængen/foreneligheden mellem de forskellige behandlingsformål er udfoldet i artikel 6, stk. 4, litra a-e, er bestemmelsen stadig tung og svært at administrere efter. Det samme er kravet i artikel 6, stk. 4, om, at der skal ske en vurdering af, om genanvendelsen er en "nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til de mål, der er omhandlet i artikel 23, stk. 1".</p>	Art. 6, stk. 4	<p>De fleste er af den opfattelse, at det er helt rimeligt, at man skal genoverveje rimelighed ved videreanvendelse til et nyt formål. Enkelte giver udtryk for, at det er en tung procedure lokalt, fordi videreanvendelse skal godkendes af en jurist.</p>	Flere angiver at have involveret DPO'en, men der er ikke bortset fra enkeltstående besvarelser uddybende bemærkninger om involveringen.
21.	<p>Der er generelle usikkerheder om (gen)anvendelse af data inden for enhedsforvaltningen, når der ikke er tale om ansøgningssager (med det deraf følgende samtykkekrav).</p> <p>Litteraturen lægger til grund, at data indsamlet i én forvaltning kan genanvendes i en anden forvaltning, når blot formålene er ikkeforenelige, men det giver alligevel anledning til jævnlig tvivl om, hvordan ikke-uforeneligheden skal fortolkes ved genanvendelse af</p>	Art. 6 og art. 9 [art. 6, stk. 4 og art. 5, stk. 1, litra b	Ja, drøftet på tværs af forvaltningerne og med DPO'en, men uden at nå til en fælles forståelse.	Ja. DPO'en anser det ikke som en uklart.

	<p>data på tværs af de enkelte fagforvaltninger inden for enhedsforvaltningen. Særligt, når det kommer til art. 9-oplysninger.</p> <p>Der er også tvivl om behovet for selvstændig behandlingshjemmel, hvis én forvaltning, der har hjemmel i faglovgivning til at iværksætte en aktivitet for en borger, bestiller udførelsen af opgaven i en anden forvaltning; Skal den anden forvaltning så have en selvstændig behandlingshjemmel til de personoplysninger, der måtte registreres ifm. udførelsen af opgaven, eller er behandlingshjemmelen den samme som den bestillende forvaltnings?*</p>			
22.	<p>I forbindelse med kommunernes behov for at sikre sammenhængende borgerforløb er det uklart, om der er de samme muligheder for samkøring af oplysninger i kontroløjemed og til brug for ledelsesinfo efter de nye regler om databeskyttelse som efter den tidligere gældende persondatalov.</p> <p>Både fsva. almindelige og følsomme oplysninger, herunder sondring mellem ikke-anonyme, anonyme og psydonymiserede personoplysninger.</p> <p>Hvordan forholder de nye regler sig til:</p> <ul style="list-style-type: none"> - Samkøring af almindelige personoplysninger (og sondringen mellem ikke-anonyme, anonyme og psydonymiserede personoplysninger) - Samkøring af følsomme data (og sondringen mellem ikke-anonyme, anonyme og psydonymiserede personoplysninger) <p>I hvilke tilfælde er der oplysningspligt overfor borgeren vedrørende samkøringen? Er der fx oplysningspligt, hvis samkøringen sker i kontroløjemed, jf. § 23, sidste pkt.?</p> <p>Bestemmelsen om statistik i databeskyttelseslovens § 10, hvorefter følsomme data må behandles, hvis det er til videnskabelige og statistiske formål af væsentlig samfundsmæssig betydning mv. finder ikke anvendelse, hvis samkøringen alene er til brug for ledelsesinfo, jf. lovbemærkningerne, side 175, 2. spalte. Det er uklart, om der ved samkøring i kontroløjemed og til brug for ledelsesinformation skal findes hjemmel i §§ 6-10.</p> <p>Hvis der er tale om samkøring af fuldstændigt anonyme oplysninger, finder databeskyttelsesreglerne ikke anvendelse. Hvordan forholder det sig, hvis der er tale om psydonymiserede oplysninger?</p> <p><i>Vedr. oplysningspligt</i> Man kan enten oplyse om samkøring i opstarten af en sag (i oplysningspligtsskabelon) eller man kan opfylde sin oplysningspligt om samkøringen umiddelbart forud for</p>	<p>Art. 6 og art. 9 (Art. 6, stk. 4, og art. 5, stk. 1, litra b/ DBL § 5, stk. 3, og § 23/DBL § 10)</p>		<p>Ingen bemærkninger</p>

	samkøringen (behandlingen), jf. art 14, stk. 4. Vil oplysningspligten i en kontrolsituation kunne vente til, man fx har foretaget screening således, at kun de personer, der bliver "udtrukket" til nærmere gennemgang får oplysning? Ellers er det et stort antal mennesker, der skal oplyses.*			
23.	Der er tvivl om, hvorvidt behandlingshjælpen i artikel 6 (og for så vidt også artikel 9) også dækker videregivelse til aktører uden for kommunen, som fx private vognmænd. Reglerne for videregivelse både internt i kommunen og til eksterne parter volder ofte besvær. Både forvaltningslovens § 29 og det forvaltningsretlige begreb "enhedsforvaltningen" er med til at skabe uklarhed omkring de retlige rammer for videregivelse.	Art. 6 og art. 9	Der er grundlæggende tale om samme udfordringer, som er anført i forbindelse med pkt. 1 – altså afgrænsning af behandlingsgrundlaget myndighedsudøvelse/samfundsinteresse i art. 6, stk. 1, litra e, og samspillet mellem GDPR og de generelle forvaltningsretlige regler om tavshedspligt og udveksling af oplysninger samt faglovgivning. Flere har i høringssvarene bemærket, at det ofte er svært at sondre mellem overdragelse, videregivelser og viderebehandling.	De fleste, der angiver, at denne problematik er væsentlig, angiver tillige, at problematikken jævnligt drøftes med DPO'en og, at det er et vanskeligt område. Der henvises til bemærkningen under pkt. 1.
24.	Videregivelse af personoplysninger i forbindelse med enhedsforvaltning i kommunerne og andre institutioner og kommuner har givet usikkerhed blandt medarbejderne og dermed øget ressourceforbrug, f.eks. i forbindelse med overgange fra børnehave til skole og skoleskift.*	Art. 6 og art. 9 (Art. 6, stk. 4)		Ingen bemærkninger
25.	Der er uklarhed om reglerne for videregivelse, hvis der ikke er klar hjemmel i særlovgivningen. Må en kommune altid videregive oplysninger, hvis kommunen vurderer, at videregivelsen sker til et saglig og fagligt formål? Der tænkes især på kommunikation mellem skoleområdet internt og mellem skoleområdet og det specialiserede børneområde i de situationer, hvor emnet ikke hører under enhedsforvaltningen pga. skolelederens særlige beføjelser. Eller er skoleområdet altid en intern videregivelse?*	Art. 6 og art. 9 (Art 6, stk. 4)		Ingen bemærkninger

26.	<p>Det er let at komme i tvivl om, hvorvidt samtykke, der trækkes tilbage, betyder, at de behandlinger, der bagudrettet er foretaget på baggrund af samtykket, også skal "trækkes tilbage". Særligt fordi borgeren, på trods af "samtykke-tilbagetrækningsreglen" i artikel 7, stk. 3, 2. pkt., har ret til at få slettet sine oplysninger (bagudrettet) i medfør af artikel 17, stk. 1, litra b, hvis det eneste hjemmelsgrundlag for behandlingen af oplysningerne har været vedkommendes samtykke. Bestemmelsen gælder dog ikke, hvis behandlingen af oplysningerne er nødvendig for at "udføre en opgave ... som henhører under offentlig myndighedsudøvelse", jf. artikel 17, stk. 3, litra b.</p> <p>Hvis man som børnehaver er i tvivl om, hvorvidt brugen af billeder er sket som led i myndighedsudøvelse og hjemlet i artikel 6, stk. 1, litra e, eller er sket uden at henhøre under myndighedsudøvelsen og derfor er alene er hjemlet via samtykke, jf. artikel 6, stk. 1, litra a, kan man hurtigt komme i tvivl om, hvorvidt tilbagetrækning af forældresamtykker til brug af billeder betyder, at billederne skal slettes.</p>	Art. 7, stk. 3, 2. pkt.	<p>Hos kommunerne giver det primært anledning til tvivl, hvilket behandlingsgrundlag der er det rigtige – altså grundlæggende samme problemstilling som pkt. 1.</p>	<p>Flere kommuner angiver at have involveret DPO'en, men der er ikke, bortset fra enkeltstående besvarelser, uddybende bemærkninger om involveringen.</p>
27.	<p>Muligheden for at kunne leve op til kravet om, at samtykke skal afgives "frit" er uklar i regi af den offentlige sektor, idet borgerens samtykke oftest vil medføre en form for service, hjælp etc.</p>	Art. 7, stk. 4	<p>Høringssvarene afspejler, at dét, der særligt volder problemer er samspillet mellem samtykker i forvaltningsloven, retssikkerhedsloven og sundhedsloven og andre faglovgivninger over for samtykke i GDPR.</p> <p>Altså samme problematik som er skitseret i pkt. 1.</p>	<p>DPO'en er involveret i nogle kommuner. Enkelte kommuner angiver, at DPO'en har udarbejdet skriftlig eller mundtlig vejledning.</p>
28.	<p>Det er uklart, hvad hjemlen er til behandling af følsomme oplysninger ifm. faktisk forvaltningsvirksomhed, fx angivelse af fødevareallergi i forhold til fremstilling af mad på et plejehjem. Om det fx kan siges at være nødvendigt af hensyn til "væsentlige samfundsinteresser", jf. artikel 9, stk. 2, litra g, eller nødvendigt "for at et retskrav kan fastlægges, gøres gældende eller forsvares", jf. artikel 9, stk. 2, litra f. Alternativt, om kommunerne skal indhente samtykke til listen, jf. artikel 9, stk. 2, litra a.</p>	Art. 9	<p>Flere kommune har – ikke kun til denne problemstilling – nævnt, at det kan være tvivlsomt, hvilken hjemmel i art. 9, stk. 2, der er den korrekte mht. faktisk forvaltningsvirksomhed.</p> <p>Betænkning 1565 er ganske uklar og nævner, at art. 9, stk. 2, litra f, om retskrav i et vist omfang formentlig kan udgøre hjemmel til at behandle oplysninger som led i faktisk forvaltningsvirksomhed, når det sker i tilknytning til at fastslå et retskrav. Fx viser høringssvarene, at der er tvivl om den databeskyttelsesretlige hjemmel til at behandle følsomme oplysninger, fx inden for ældreplejen, i forbindelse med faktisk forvaltningsvirksomhed, bl.a. på grund af de meget vage formuleringer herom i betænkningen om databeskyttelsesforordningen (Bind 1, s. 215).</p> <p>Det må ret klart kunne slås fast i vejledning, hvilken bestemmelse i art. 9, der er relevant. Behandlingsgrundlaget er art. 6, stk. 1, litra e, og afløftning af forbuddet i art. 9 stk. 1, kan efter KL's opfattelse ske mere generelt efter art. 9, stk. 2, litra g, (hvis der skal være parallelitet mellem henvisning til behandling i samfundets interesse i art. 6, stk. 1, litra, e og tilsvarende behandling i af hensyn til væsentlige samfundsinteresser efter art. 9, stk. 2, litra g).</p>	<p>Generelt er der ikke gjort bemærkninger om involvering af DPO. Ganske få har angivet at have drøftet problematikken med DPO'en.</p>

29.	Hvornår kan artikel 9, stk. 2, litra g, "samfundsinteresser" anvendes?*	Art. 9, stk. 2, litra g	Vejledning ønskes.	Ingen bemærkninger
30.	Det er uklart, hvad der er hjemlen til at tage kopi af skoleelevers pas i forbindelse med skolerejser, såfremt passene indeholder biometriske data. Det er ikke umiddelbart klart, om kommunerne kan anvende bestemmelsen i artikel 9, stk. 2, litra f, som hjemmel for behandlingen. Med andre ord om behandlingen/fotokopieringen er nødvendig for "at retskrav kan fastlægges, gøres gældende eller forsvares". Alternativt skal hjemlen findes i samfundsinteresse, jf. litra g, eller skolerne skal til at indhente forældrenes samtykke til kopi af passet?	Art. 9	Høringssvarene viser, at kommunerne er i tvivl om, hvorvidt hjemlen i art. 9, skal findes i stk 2, litra a, om samtykke, litra f om retskrav eller litra g om væsentlig samfundsinteresse. Flere kommuner henviser til, at Datatilsynet har svaret på spørgsmålet ifm. benspændskataloget. Men det bemærkes også, at Datatilsynets svar ikke er begrundet.	Generelt er der ikke gjort bemærkninger om involvering af DPO. Ganske få har angivet at have drøftet problematikken med DPO'en.
31.	Det er en udfordring at finde ud af om, der behandles følsomme oplysninger, der er omfattet af de skærpede hjemmelskrav i artikel 9, når man fx på en aktivitetsoversigt i et botilbud anfører oplysninger om, at en person deltager i en given aktivitet som fx fysioterapi/genoptræning eller ledsaget indkøb. Oplysninger på en aktivitetstavle kan være helbredsoplysninger og dermed karakteriseres som følsomme personoplysninger, når oplysningerne kan afsløre information om en persons fysiske eller mentale helbred. Ifølge Datatilsynets vejledning ift. brugen af SMS'er kan helbredsoplysninger fx udledes af oplysninger om, at en person skal møde op på en given (hospitals)adresse. På samme måde kan billeder af personer (fx børn i en institution) være følsomme oplysninger om personer, når billederne kan afsløre information om fx en persons helbred eller religion. Det kræver ligeledes en nærmere juridisk vurdering at finde ud, om der behandles følsomme eller fortrolige oplysninger, når man skriver i en SMS til borgeren, at borgeren fx skal møde op på en given adresse mhp. en given behandling.	Art. 9	Det synes at give anledning til tvivl i hvilke situationer på overfladen almindelige oplysninger skal ses som følsomme oplysninger. Med hensyn til billeder har Datatilsynet sagt, at foto af et barn i en kørestol ikke nødvendigvis er en følsom oplysning. Derimod er kan en adresse være en følsom oplysning, hvis der er tale om adressen på fx et psykiatrisk hospital. Der efterspørges vejledning om, hvad der skal være styrende for vurderingen.	En stor andel af de kommuner, der har angivet at problematikken er væsentlig har også involveret DPO'en. Det er dog ikke uddybende bemærkninger om involveringen.
32.	Det er uklart, 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? Oplysningspligt ift. bipersoner – hvornår og hvordan? Eksempel: I forbindelse med start i daginstitution, skole, SFO eller klub eller ved en borgers indflytning på bosted, plejehjem m.v. er det uklart, hvor præcis kommunens angivelse af formålet med behandlingen af borgerens personoplysninger skal være. Er det fx nok, at kommunen ved et barns skolestart henviser til folkeskolelovens formålsbestemmelse, som siger, at "folkeskolen skal i samarbejde med forældrene give eleverne kundskaber og færdigheder, der: forbereder dem til videre uddannelse og	Art. 13 og 14	Kommunerne er fuldstændig opmærksomme på formålet med de registreredes rettigheder, men er i flere situationer bekymrede for, at reglerne desværre ikke altid skaber den ønskede åbenhed og gennemsigtighed om behandlingen af personoplysninger og mange gange desværre opleves af borgerne som unødvendig og ligegyldig spamming fra kommunerne. Generelt oplever kommunerne de største udfordringer med oplysningspligten i forhold til de øvrige regler om registreredes rettigheder. Datatilsynets vejledning om registreredes rettigheder kan derfor med fordel udbygges med flere eksempler indenfor oplysningspligten og gerne flere med kommunal relevans.	Ja, de fleste kommuner har involveret deres DPO i spørgsmålet. Dette har desværre ikke ført til en reel løsning af problemstillingen.

	<i>giver dem lyst til at lære mere, gør dem fortrolige med dansk kultur og historie, giver dem forståelse for andre lande og kulturer, bidrager til deres forståelse for menneskets samspil med naturen og fremmer den enkelte elevs alsidige udvikling”?</i>		<p>Konkret oplever kommunerne, 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.</p> <p>Kommunerne oplever også, at det kan være vanskeligt at afklare, hvor specifikt formålene skal angives i oplysningspligten. Er det for generelt, er der principielt risiko for, at oplysningspligten ikke opfyldes, og er det ”for præcist”, er der risiko for, at oplysningspligten skal gentages for jævnligt overfor borgeren (belastning af forvaltningens effektivitet). Tvivlen opstår fx i ansøgningssager, hvor det er uklart for kommunerne, hvornår det er tilstrækkeligt at henvise til særlovgivning, fx serviceloven, og, hvornår der skal ske henvisning til databeskyttelsesforordningen og databeskyttelsesloven.</p> <p>Mange kommuner oplever endvidere, 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.</p> <p>Se i øvrigt pkt. 5 vedr. art. 5, stk. 1, litra b.</p>	
33.	Vi ser en udfordring i en del borgeres reaktion over at modtage oplysningssedler, som de har svært ved at forholde sig til oven i den øvrige kontakt, de har med kommunen. Det kommer meget ofte bag på borgerne, hvor nogen bliver mere forvirrede end godt er og tilmed forskrækkede.*	Art. 13 og 14, jf. artikel 12	En central oplysningskampagne, der går ud på at fortælle den danske befolkning, at det er et vilkår, at borgerne skal modtage en oplysningsseddel – og ikke ”kommunens skyld”.	Nej
34.	Oplysningspligten – det er vores vurdering, at det er tungt at håndtere administrativt, og at virkningen af oplysningspligten har den modsatte effekt end den ønskede. Alle borgere modtager nu så mange breve mv omkring oplysningspligt, at det bliver for meget. Borgerne læser formentligt ikke halvdelen af det, som sendes frem, dvs. borgerne er mindre oplyste.*	Art. 13 og 14		Ingen bemærkninger
35.	Oplysningspligten ved indsamling af personoplysninger ved en anden end den registrerede kan give store udfordringer og have voldsomme konsekvenser. Fx i tilfælde hvor der oplyses om eventuelt misbrug eller, kommunen er ved at undersøge en sag om en familie. Vi går ud fra, at vi kan	Art. 14		Ingen bemærkninger

	dække os ind under art. 14, stk. 5 litra b, men det virker uklart?*			
36.	Det er uklart, om der er adgang til indsigt i fx eksamensbesvarelser eller notater, som en ansat har forfattet ifm. sit arbejde. Det er endvidere uklart, hvilke krav forordningen stiller til omfanget af de undersøgelser, man skal foretage for at finde oplysninger om en person, som henvender sig med anmodning om indsigt.	Art. 15 (og art. 11)	I forhold til reglerne om indsigt efter databeskyttelsesreglerne sammenholdt med reglerne om aktindsigt efter offentlighedsloven og forvaltningsloven oplever kommunerne, at det kan være svært at afklare hvilket retsgrundlag, der stiller borgeren bedst, særligt i forhold til reglen om egenaces i offentlighedslovens § 8. Kommunerne oplever, at kravet om vejledning om det mest gunstige retsgrundlag for borgeren, vil være vanskeligt at gennemføre for medarbejdere, som ikke har den fornødne juridiske indsigt. Denne problemstilling kan med fordel indarbejdes i Datatilsynets vejledning om registreredes rettigheder under emnet indsigtsret med udgangspunkt i en række konkrete kommunale eksempler.	Generelt er der ikke gjort bemærkninger om involvering af DPO. Ganske få har angivet at have drøftet problematikken med DPO'en.
37.	Retten til indsigt suppleres af retten til aktindsigt efter bl.a. offentlighedsloven og forvaltningsloven. Som offentlig myndighed skal vi behandle en anmodning efter det retsgrundlag, der stiller borgeren bedst. Det kan være en vanskelig sontring for den enkelte sagsbehandler, særligt i den situation, hvor borgeren ikke er part i en sag, men hvor borgerens retsstilling skal afgøres efter databeskyttelsesforordningen art. 15 eller offentlighedsloven § 8. Hvilket lovgrundlag giver borgeren da ret til flest oplysninger? Er begrebet "personlige forhold" sammenfaldende med "personoplysninger vedr. den pågældende"? Eller giver "personlige forhold" ret til at få udleveret flere oplysninger? Særligt i forhold til personens samspil med andre personer.*	Art. 15	Forholdet kunne give anledning til overvejelser om reglen om egenaces i offentlighedsloven skal revideres, så den enten bringes i overensstemmelse med databeskyttelsesforordningens art. 15 eller helt tydeligt adskiller sig.	Ja, men uden resultat.
38.	Sletning af personoplysninger i backup. Er det eventuelt tilstrækkeligt at sikre, at eventuelle anfordrede rettelser og sletninger gentages efter genindlæsning fra backup?*	Art. 17		Ingen bemærkninger
39.	Det er uklart, om artikel 24 om den dataansvarliges ansvar pålægger kommunerne nye dokumentationsforpligtelser, jf. formuleringen "... gennemfører ... foranstaltninger ... for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning."	Art. 24	Påvisnings-/dokumentationskravene i medfør af art. 5, stk. 2, sammenholdt med art. 24 er et tema, som fylder en del hos kommunerne. Rækkevidden af dokumentationsforpligtelsen opleves som uklar. Kommunerne efterlyser konkretisering og uddybning af påvisningskravet via mere vejledning.	I en række kommuner har problemstillingen været drøftet med kommunens DPO.
40.	Det er uklart, hvornår der er tale om en fælles dataansvarlige-konstruktion. Hvornår vil man sige/ikke sige, at formålene med og hjælpemidler til behandling er fastlagt "i fællesskab"?	Art. 26	Kommunerne efterlyser mere vejledning med flere konkrete eksempler, som også ikke GDPR-kyndige kan bruge. Gerne løbende udbygning af Datatilsynets vejledning. Det foreslås også, at Datatilsynet træffer flere afgørelser på området for at lægge en mere tydelig linje.	I en række kommuner har problemstillingen været drøftet med kommunens DPO.

41.	Det er umuligt for kommunerne at få indgået et retvisende aftalegrundlag med Facebook (databehandlersaftale eller aftale om fælles dataansvar) – og de øvrige store tech-giganter. Facebook har udarbejdet egne databehandlersaftalevilkår, som ikke lever op til GDPR-kravene. Når den enkelte kommune anvender Facebook, bliver kommunen omfattet af disse vilkår og har ikke mulighed for at ændre disse.	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 kommuner 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.
42.	Det er en udfordring, at når kommunerne samarbejder med staten om løsningen af forskellige opgaver, fx borger.dk siden, vil der i mange tilfælde skulle indgås databehandlersaftaler mellem den enkelte kommune og staten. Databehandlersaftaler, som vil være enslydende for alle kommuner. Kommunerne vil derfor skulle bruge tid på hver især at gennemlæse og forholde sig til databehandlersaftalerne, desuagtet at det ikke har vist sig muligt for den enkelte kommune at kunne aftale individuelle aftalevilkår med staten.	Art. 28	Kommunerne har foreslået overvejet, om problemstillingen kan løses via særskilt lovhjemmel til, at der ikke skal indgås databehandlersaftaler, 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 databehandler-konstruktion. Alle databehandlersaftaler mellem kommunerne og staten foreslås i stedet reguleret af bekendtgørelser, "andet retligt dokument", jf. artikel 28, stk. 3.	I de fleste kommuner er DPO'en ikke inddraget i problemstillingen, idet kommunerne reelt ikke oplever at have anden handlemulighed end at indgå databehandlersaftalerne med staten.
43.	Indgåelse af databehandlersaftaler. Vi finder det ofte uklart hvornår der skal indgås en databehandlersaftale (der ikke handler om IT-leverandører) fx. med samarbejdspartnere, beskæftigelsestilbud, tilkøb af udredninger.*	Art. 28 og art. 4, nr. 7 og 8	Der bliver brugt mange ressourcer på området. Hovedårsagen er, at vi bliver usikre på, om persondata er ordentligt beskyttede, eller om vi indgår for mange aftaler. Det kunne hjælpe med klarere retningslinjer.	Ja – i konkrete tilfælde, hvor vi har brug for hjælp til afklaring.
44.	98 x det samme arbejde er ikke ligefrem befordrende. Kommunerne arbejder med de samme opgaver, samme leverandører og samme sikkerhedskrav til infrastrukturen.*	Art. 28 og 32	Er det muligt at finde løsninger, der kan effektivisere arbejdet?	Ja, forslag fra DPO.
45.	Indgåelse af databehandlersaftale vil ofte ske efter forudgående udbudsproces, hvor forhåndsvurderingen af databehandleren, jf. art. 28, stk. 1, giver praktiske og ressourcemæssige udfordringer i relation til afviklingen af udbudsprocessen.*	Art. 28, stk. 1		Ingen bemærkninger
46.	Det er uklart, hvad der reelt er genstanden for tilsynet med databehandlere. Hvad er minimumsforpligtelsen i forhold til tilsynsforpligtelsen? Vil det være tilstrækkeligt, at det påses, at de sikkerhedsforanstaltninger, som konkret er aftalt i databehandlersaftalen, er blevet gennemført? Eller vil det ligeledes skulle påses, at databehandleren overholder alle dele af databehandlersaftalen, jf. artikel 28, stk. 3, litra a-h?	Art. 28, stk. 3, litra h	Der ønskes opdatering og udbygning af Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere, gerne med tjeklister og/eller tilsynsskabeloner.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.

47.	Det er uklart, om det er et krav, at det via tilsynet med databehandlere ligeledes skal påses, at databehandleren 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?	Art. 28, stk. 3, litra h	Der ønskes opdatering og udbygning af Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere, gerne med tjeklister og/eller tilsynsskabeloner.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.
48.	Det er uklart, 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?	Art. 28, stk. 3, litra h	Der ønskes opdatering og udbygning af Datatilsynets vejledende tekst om tilsyn med databehandlere og underdatabehandlere, gerne med tjeklister og/eller tilsynsskabeloner.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.
49.	Kontrol af, hvorvidt databehandlere har kontrolleret underdatabehandlere, er et meget omfattende stykke arbejde. I og med at databehandlerne er ansvarlige for kontrol af deres underdatabehandlere, burde vi ikke skulle kontrollere dette. Det er i forvejen en kæmpe opgave, og den bliver helt urealistisk stor, hvis dette arbejde skal gøres for hver databehandler.*	Art. 28 og 32		Ingen bemærkninger
50.	Det er uklart, hvordan kommunerne i praksis kan føre fælles tilsyn med deres leverandører. Vil kommunerne fx kunne "dele" en tilsynsrapport fra et eksternt revisionsfirma, sådan at én kommunes tilsyn med en leverandør "genanvendes" af andre kommuner?	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.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.
51.	Der er uklart, i hvilket omfang tilsynsforpligtelsen kan opfyldes ved at føre fysiske "stikprøvetilsyn" – at kommunerne ud fra et tilfældighedsprincip udvælger et antal leverandører til tilsyn og/eller, at alene et givent antal af de samlede sikkerhedsforanstaltninger kontrolleres.	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.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.
52.	Der er uklart, hvornår kommunerne 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? Og hvordan gennemføres et fysisk tilsyn i fald, der er krav herom, bl.a. hos cloud-leverandører?	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.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.
53.	Det er uklart hvilke krav, der er til dokumentation af tilsyn med databehandlere og, hvoraf disse krav evt. følger? Vil en revisionsrapport udarbejdet af fx et revisionsfirma være tilstrækkeligt, eller skal det ligeledes dokumenteres, at man har forholdt sig til/gennemgået rapporten? Og i givet fald hvordan? Og i fald kommunerne selv har gennemført fysisk tilsyn, hvordan skal de så dokumentere dette?	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.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.

54.	Vi oplever ofte, at mindre leverandører og leverandører af gratis systemer har store udfordringer med at levere revisorerklæringer.*	Art. 28, stk. 3, litra h	Centralt udarbejdet revisionskabelon til brug i kommunerne, tiltænkt aftaler med mindre leverandører, gratis systemer eller leverandører med få almindelige personoplysninger - i form af fx spørgeskema.	Nej
55.	Kravet om at kommunerne skal udarbejde fortegnelser er udtryk for unødvendig meradministration, idet de databehandlinger kommunerne udfører, for langt hovedparten, er reguleret ved lov. Lovgivningen beskriver allerede i vidt omfang, hvem der er ansvarlig for en given opgave, hvad formålet med behandlingen er, hvilke oplysninger, der skal behandles, samt hvem oplysningerne eventuelt skal videregives til.	Art. 30	En lang række kommuner påpeger, at kravet om udarbejdelse af fortegnelser er en stor administrativ opgave. Ved næste evaluering af databeskyttelsesforordningen kan man med fordel se på, om de administrative resurser forbundet med løsningen af fortegnelsesopgaven står mål med, hvad de dataansvarlige får ud af at udarbejde fortegnelserne.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.
56.	Det er uklart, hvilke krav kommunerne skal leve op til ift. at føre fortegnelser. Særligt hvoraf det følger, at der for hver enkelt kategori af registrerede skal angives nøjagtigt hvilke oplysninger, der behandles om hver kategori. Samt hvoraf det følger, at den dataansvarlige skal udspecificere, hvilke artikel 9-oplysninger, der behandles. Ligeledes hvoraf det følger, at det skal det fremgå specifikt af fortegnelsen, hvilke kategorier af personoplysninger, der bliver eller vil blive videregivet til den pågældende modtager samt hvilke kategorier af registrerede, de pågældende oplysninger vedrører.	Art. 30	Datatilsynet har den 10. august offentliggjort en opdateret udgave af deres vejledning om fortegnelseskravet. Opdateringen betyder nye og omfattende krav til, hvad fortegnelserne skal indeholde. Krav, der ikke ses eksplicit at følge af databeskyttelsesforordningens art. 30, og som for kommunerne ses unødvendige i forhold til kommunerne, hvis behandlinger af allerede er nøje beskrevet i lovgivningen. Der ønskes en afklaring fra Justitministeriet af, i hvilket omfang kommunerne vil blive anset for ikke at overholde databeskyttelsesforordningens art. 30, i fald Datatilsynets opdaterede vejledning ikke følges fsva. de nye indholdsmæssige krav fra Datatilsynet til fortegnelserne.	I en række kommuner har DPO'en været inddraget i drøftelsen af spørgsmålet.
57.	Databeskyttelsesforordningens artikel 32 stiller krav om, at kommunerne skal sikre, at personoplysningerne er tilstrækkeligt beskyttet og ikke kommer til uvedkommendes kendskab, herunder ikke hænger tilgængeligt for uvedkommende. Det er imidlertid uklart, hvad der konkret skal til for at overholde artikel 32. Det fremgår ikke af bestemmelsen, herunder hvad der er "passende" sikkerhedsforanstaltninger, jf. artikel 32. 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, jf. udfordringerne beskrevet ift. art. 9. Der skal udarbejdes en risikovurdering, som skal tage hensyn til en lang række forhold, førend der kan foretages selv helt almindelige behandlinger af oplysninger. 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	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.

	nok, når der ikke står nogen steder, hvad der er tilstrækkeligt.			
58.	Det er uklart, hvad der konkret skal til for at overholde artikel 32, når vi skal definere rammerne for autorisationer af medarbejdere og adgangskontroller. I kommunerne gives der ofte en "bred adgang" til de store it-systemer (fx omsorgsløsning, jobcenterløsning) af hensyn til et helhedssyn i sagsbehandlingen og en afvejning af omfanget af administrationsopgaven og tilliden til medarbejderne.*	Art. 32	Der mangler en uddybende beskrivelse rammerne for autorisationer med eksempler fra det kommunale område.	
59.	Databeskyttelsesforordningens retlige rammer for medarbejderadgang til personoplysninger i it-løsninger kontra princippet/ønsket om helhedsorienteret sagsbehandling (forvaltningslovens § 29 og muligheden for udveksling af oplysninger inden for enhedsforvaltningen). Brugerautorisationer ctr videregivelse.*	Art. 32		Ingen bemærkninger
60.	Leverandører til risikostyringssystemer har deres egen sikkerhedsopsætning (risikovurdering), der afviger fra Datatilsynets anbefalinger.*	Art. 32	Øget kommunikation målrettet leverandører om bl.a. privacy by design and by default.	Ja, forslag fra DPO.
61.	Sletning i backup af IT systemer og dokumentation for dette er meget kompliceret.*	Art. 32 og art. 5, stk. 2		Ingen bemærkninger
62.	Det giver anledning til tvivl, hvornår kommunerne må sende SMS'er (eller almindelig mail) til borgerne, der indeholder følsomme og fortrolige oplysninger, da SMS'er ikke kan krypteres og dermed ikke er tilstrækkeligt beskyttet. Det er et problem, hvis hensynet til grupper af registreredes interesser i behandlingen ikke kan tillægges stor vægt i risikovurderingen ifm. fastlæggelse af sikkerhedsniveauet.	Art. ,32, stk. 2	Kommunerne må som hovedregel ikke sende følsomme og fortrolige oplysninger som SMS, da SMS'er ikke kan krypteres og dermed ikke er tilstrækkeligt beskyttet. Det følger af Datatilsynets vejledning på området, hvor tilsynet har foretaget en risikovurdering ift. brugen af SMS. Det betyder, at SMS kun undtagelsesvis og i konkrete tilfælde kan benyttes. Flere kommuner efterlyser mere vejledning med flere konkrete eksempler på disse undtagelsessituationer, hvor SMS (og mailkommunikation) er mulig, når der skal kommunikeres følsomme og fortrolige oplysninger. Kommunerne oplever, at i denne sag vinder paragrafferne over hensynet til de svage borgere. På sigt, i forbindelse med en eventuel revision af GDPR-reglerne, bør man derfor se på, om art. 32, stk. 2, bør ændres sådan, at den registreredes interesse i behandlingen indgår som en væsentlig del af risikoafvejningen.	Flere kommuner har drøftet udfordringen med deres DPO.
63.	Det er uklart, i hvilket omfang der reelt er sikkerhedsbrud, som ikke skal anmeldes, eftersom anmeldelse alene kan undlades, såfremt det er "usandsynligt, at bruddet ... indebærer en risiko for fysiske personers rettigheder...". Niveauet for indberetning er meget forskelligt i kommunerne. Der savnes en bagatelgrænse, så der ikke skal bruges tid på at indberette detaljer, som ikke giver megen læring og sikkerhed, jf. princippet om risikotilgang i forordningen.	Art. 33, stk. 1	At der fastlægges en højere bagatelgrænse, der er noget højere grad end i dag afspejler databeskyttelsesforordningens risikobaserede tilgang til arbejdet med datasikkerhed. Enten via revision af national vejledning eller på sigt revision af artikel 33, stk. 1. Evt. hvor stikprøvekontroller af hændelsesloggen erstatter anmeldelsesordningen. En udbygning af Datatilsynets vejledning med flere kommunale eksempler, der gør det mere klart, hvornår der ikke behøver at	Kommunerne anvender i et vist omfang DPO'erne til sparring ift. vurderingen af risici forbundet med et sikkerhedsbrud.

	Fx hvis man har en procedurebeskrivelse om, at man skal lukke computeren, og man har et "åbent for borgere"-rådhus, skal man så anmelde et brud, hvor man har glemt at lukke computeren i et kortere tidsrum – fx ved en tur til printeren.		blive foretaget anmeldelse som følge af en vurdering af det samlede aktuelle risikobillede.	
64.	Anmeldelse til Datatilsynet, hvor der sker løbende indberetning. Her skal oplysninger udfyldes igen, selvom de tidligere er indberettet. Det er unødigt resursetid.*	Art. 33		Ingen bemærkninger
65.	Det er uklart, hvornår underretning af den registrerede om sikkerhedsbrud kan undlades, fx i forhold til svage eller udsatte borgere, som i forvejen har vanskeligt ved at forstå breve fra kommunen.	Art. 34	Flere kommuner tilkendegiver, at det er en problemstilling, der drøftes, idet det opleves, at fx ældre borgere kan blive meget forvirrede og bekymrede over at modtage et underretningsbrev, som de ikke forstår indholdet af. De ved ikke hvad eks. identitetstyveri er. Der efterspørges vejledning til, hvordan problemstillingen kan håndteres inden for rammerne af reglerne.	Flere kommuner har drøftet udfordringen med deres DPO.
66.	Det kan være svært at vurdere, hvornår der foreligger en "høj risiko" for den registreredes frihedsrettigheder, og vedkommende dermed skal underrettes.*	Art. 34	Datatilsynets vejledning udbygges med yderligere eksempler.	Ingen bemærkninger
67.	Det er en uhensigtsmæssig anvendelse af de kommunale ressourcer, at kommunerne er forpligtede til at foretage risikovurderinger, herunder omfattende konsekvensvurderinger, af behandlinger af personoplysninger, som de ved lov er pålagt at udføre.	Art. 35	Kommunerne efterlyser, at konsekvensanalyserne, i det omfang der er krav om at disse skal udarbejdes, i større omfang udarbejdes centralt. KL opfordrer til at der ses på, om art. 35, stk. 2, hvorefter udarbejdelsen af konsekvensanalyser kan afløftes for den enkelte dataansvarlige ved, at analyserne udarbejdes i forbindelse med lovudarbejdelsen, bliver anvendt af ministerierne i tilstrækkeligt omfang.	Flere kommuner har drøftet udfordringen med deres DPO.
68.	Det er stadig uklart, hvornår der skal gennemføres konsekvensanalyser på det kommunale område, og der savnes vejledning og redskaber til at gennemføre analysen på en hensigtsmæssig måde.*	Art. 35	Vejledning på området revideres eller reglerne justeres, så de bliver lettere tilgængelige. Det udarbejdes koncepter for gennemførelsen af konsekvensanalyse, der er anvendelige i en kommunal kontekst.	Ingen bemærkninger
69.	Reglerne for overførsler af personoplysninger til tredjelande, fx via cloud-løsninger, er besværlige at arbejde med – særligt i lyset af Schrems II-dommen. At skulle indgå særskilte standardkontrakter med sine leverandører og herunder skulle vurdere, om lovgivningen i de enkelte tredjelande, som data placeres i, 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. Det er tungt og omstændigt at arbejde med.	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 erstatning for Privacy Shield-ordningen. Opdateret vejledning om reglerne for overførsler til tredjelande efterlyses.	Enkelte kommuner har inddraget DPO'en i spørgsmålet, men oplevelsen er generelt, at problemet ikke kan løses af den enkelte kommune alene.
70.	Med udgangspunkt i Schrems II, kan det generelt være svært at vurdere, hvor ansvaret for underdatabehandlere præcist ligger. Hvis en kommune fx. via en dialog med en leverandør konkluderer, at de ikke overfører personoplysninger til et 3. land, men at det så viser sig, at	Art. 32		Ingen bemærkninger

	det modsatte er tilfældet. Er det så leverandørens ansvar, eller påhviler ansvaret fortsat os som dataansvarlige?*			
71.	Datatilsynet tilbyder ikke mulighed for bindende forhåndssvar.*	Art 57		Ja, observation fra DPO.
72.	Er presseaktiviteter i kommunen at sidestille med "behandling i journalistisk øjemed"? *	Art. 85		Ingen bemærkninger
73.	Der bør indføres en forældelsesfrist for gamle byggesagsarkiver (og generelt alle arkiver), så informationer, der ligger fx 30 år bagud ikke er omfattet af reglerne (i lighed med åbenhed i gamle, lukkede krigsarkive). Offentlige myndigheder skal således ikke ende i sager om databrud for dokumenter, der ligger fx 50 år bagud. De gamle dokumenter er typiske blevet scannet ind i vores digitale byggesagsarkiv fra fx håndskrevne (og dermed vanskeligere at fange i en digital screeningsprocedure) dokumenter – eller blanketter, der er udfyldt i hånden.*	Art. 89		Ingen bemærkninger
74.	Det er uklart, hvilke af kommunens statistikberegninger, som er omfattet af begrebet "ledelsesinformation" og gerne må genanvendes som led i myndighedsudøvelsen, og hvilke som er omfattet af begrebet "statistiske undersøgelser" og ikke må genanvendes. Ligeledes er det uklart, om fx resultaterne fra et forskningsprojekt omkring alkohol i 9. klasse må bruges til at implementere nye alkoholpræventive initiativer i den pågældende klasse? Projektet kommer frem til, at der er 40 % af eleverne, der drikker for meget. Hvornår er gruppen af testede for lille?	Databeskyttelseslovens § 10, stk. 2	Der efterlyses mulighed for dialog om reglerne målrettet det offentlige brug af data til myndighedsudøvelse, herunder ledelsesinformation, samt statistik.	Nogen kommuner har drøftet udfordringen med deres DPO.
75.	Awareness for visse medarbejdergrupper. Kommunerne rummer mange forskelligartede medarbejdergrupper, der varetager mange forskelligartede opgaver. I arbejdet med awareness omkring persondatareglerne (og informationssikkerhed generelt) er det en udfordring at kommunikere meningsfuldt til visse medarbejdergrupper, der kan have svært ved at se relevansen af GDPR for deres kerneopgave. Eksempler herpå kunne være medarbejdere inden for rengøring, vej og park, teknisk service etc.*	Hele forordningen	Flere centrale eksempler/cases fra frontlinjemedarbejdere, der viser, at databeskyttelsesreglerne er relevante for alle dele af den kommunale opgaveløsning.	Nej
76.	Behov for afklaring eller forenkling af GDPR-reglerne <ul style="list-style-type: none"> Behov for flere generelle redskaber, fx hvilke regler en kontor medarbejder generelt skal overholde for at være inden for GDPR (dagligdagsting).* 	GDPR generelt		Ingen bemærkninger

