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.

Justitsministeriet har udarbejdet to delrapporter som resultat af den nationale evaluering af databeskyttelsesreglerne:

- Delrapport som blev oversendt til Folketingets Europaudvalg den 29. januar 2021: https://www.ft.dk/samling/20201/almdel/EUU/bilag/269/2327380.pdf (i det følgende kaldet "**Første delrapport**")

- Delrapport II som blev oversendt til Folketingets Europaudvalg den 1. juli 2021: https://www.ft.dk/samling/20201/almdel/EUU/bilag/685/2425672.pdf (i det følgende kaldet "**Delrapport II**")

Datatilsynet har udarbejdet særskilt bidrag til delrapport II: https://www.ft.dk/samling/20201/almdel/EUU/bilag/685/2425671.pdf (i det følgende kaldet "**Datatilsynets bidrag til delrapport II**")

	Konkret beskrivelse af problemstillingen	**Hvilken databeskyttelsesretlig regel knytter problemstillingen sig til?** (Alle henvisninger er til databeskyttelsesforordningen medmindre andet er anført).	**Har I overvejet, hvordan man kan løse problemet? (Fx via ændring af reglerne, mere vejledning, nye centrale, organisatoriske tiltag etc.)**	**STATUS pr. 11. februar 2022**
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).	Datatilsynet tager stilling til fortolkningen af nødvendighedskravet s. 30 i Datatilsynets bidrag til delrapport II. Datatilsynet fastslår, at nødvendighedskravet skal forstås som et krav om saglighed, relevans og proportionalitet (”ikke unødigt indgribende”). Datatilsynet fastslår, at krav om samtykke efter sektorlovgivningen ikke fører til, at behandlingsgrundlaget efter GDPR da også er samtykke. Behandlingsgrundlaget er fortsat myndighedsudøvelse. JM tilkendegiver i øvrigt på s. 33 i Delrapport II, at samspillet mellem GDPR og faglovgivning og udveksling/videregivelse af oplysninger vil blive taget op i et tværministerielt samarbejde i igangværende år (d.v.s. 2021).

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.	Spørgsmålet behandles ikke i Justitsministeriet eller Datatilsynets rapportering. Datatilsynet har dog i sin praksis taget stilling til et delspørgsmål i forbindelse med sociale medier i 3 tilfælde – se link: Nye afgørelser: Behandling af personoplysninger i rent private sammenhænge (datatilsynet.dk) Desuden synes Datatilsynet at forudsætte, at fx morgenbrødslister skal anses for rent personlige eller familiemæssige aktiviteter. Men der ses ikke at være givet nogen juridisk begrundelse for standpunktet. Se note 1 i link om udtalelse til Herning Kommune: Vedrørende Herning Kommunes spørgsmål om arbejdspladsens krisebreve og pårørendes telefonnumre (datatilsynet.dk)
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.	Datatilsynet skriver på s. 7 i deres bidrag til delrapport II, at de vil tage initiativ til, at det vejledende materiale om dataansvarlige og databehandlere, som pt. er tilgængelig på Datatilsynets hjemmeside, løbende opdateres og udbygges med praksisnære eksempler. Datatilsynet har udarbejdet et tillæg med primært kommunale eksempler til deres oprindelige vejledning om dataansvarlige og databehandlere: https://www.datatilsynet.dk/Media/637800004810345413/Vejledende%20tekst%20om%20rollefordelingen_2022.pdf
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	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	JM skriver på s. 33 i Delrapport II, at de er indstillet på sammen med relevante ressortministerier at se nærmere på mulighederne og behovet for regulering af fastlæggelsen af rollefordelingen mellem dataansvarlig og databehandler mellem offentlige myndigheder.

	definitionen, "... der behandler personoplysninger på den dataansvarliges vegne", jf. art. 4, nr. 8, i mange tilfælde ikke afspejler det reelle setup. 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).		kommuner fremfor en databehandlerkonstruktion. Alle databehandleraftaler 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 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,	Problemstillingen er adresseret i Datatilsynets bidrag til delrapport II s. 35-36, hvor det påpeges, at der i vidt omfang er tale om videreførelse af gældende ret, men udover tilsagnet om at offentliggøre flere afgørelser og opdatere vejledningen om registreredes rettigheder, er der ikke givet fortolkningsbidrag til spørgsmålet om smalle hhv brede formålsangivelser. Der er fortolkningsbidrag til, hvornår oplysningspligt kan undlades ift fx bipersoner og tavshedspligter, men altså ikke til spørgsmålet om, HVORNÅR en ny oplysningspligt aktiveres.

			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. 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 kan finde sted på grundlag af ikke-uforenelighedstesten i art. 6, stk. 4. Justitsministeriet har udarbejdet en vejledning om udveksling (og dermed videreanvendelse) af oplysninger i SSP-samarbejdet. Løsningsforslag: - 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.	Sondringen mellem overdragelse og videregivelse og viderebehandling. Hvornår er der tale om hhv overdragelse, videregivelse og viderebehandling i forskellige situationer. *Hermed menes:* - *overdragelse = til databehandler* - *videregivelse = til tredjemand (selvstændig dataansvarlig)*	Art. 5, stk. 1, litra b og art. 6 stk. 2-3	Der er behov for øget opmærksomhed på samspillet mellem databeskyttelsesreglerne og forvaltningretten mv., fx formålsbegrænsningsprincippet sammen med officialsprincippet, herunder betydning af, hvis der er tale om en ansøgningssag (FVL § 29).	Spørgsmålet er ikke afklaret i Justitsministeriets eller Datatilsynets afrapporteringer. JM tilkendegiver dog på s. 33 i Delrapport II, at samspillet mellem GDPR og faglovgivning og udveksling/videregivelse af oplysninger vil blive taget op i et tværministerielt samarbejde i igangværende år (d.v.s. 2021).

	- *viderebehandling = til nyt formål inden for den dataansvarliges organisation.* Eksempler: - 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.*			
7.	Eksempler på formål (abstraktionsniveau) ift. fortegnelser efterlyses, og er formålsafgrænsningen den samme i fortegnelsen som ifm. oplysningspligten? *	art. 5, stk. 1, litra b og art. 30		Datatilsynet giver på s. 28 i Datatilsynets bidrag til delrapport II eksempler på formål ift. fortegnelseskravet. Eksemplerne er imidlertid ikke nye men fremgår allerede af Datatilsynets fortegnelsesvejledning fra august 2020.

				Ift. spørgsmålet om, hvorvidt formålsafgrænsningen er den samme i fortegnelserne som ifm. oplysningspligten skriver Datatilsynet på s. 27 i Datatilsynets bidrag til delrapport II : "*Det er endvidere Datatilsynets opfattelse, at formålsafgrænsningen, som dataansvarlige kan foretage i forbindelse med oplysningspligten, også gælder ved kravet om fortegnelse.*"
8.	Dataminimeringsprincippet stiller krav om, at behandling af personoplysninger kun må ske i det omfang, 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.	Art. 5, stk. 1, litra c	Grundlæggende den samme problematik som nr. 1 om sundhedslovgivning m.v.	Dataminimeringsprincippet og nødvendighedskravet omtales mere generelt s. 29-30 i Datatilsynets bidrag til delrapport II. Datatilsynet fastslår, at nødvendighedskravet skal forstås som et krav om saglighed, relevans og proportionalitet (”ikke unødigt indgribende”).
9.	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? 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.	Art. 5, stk. 2	Kommunerne efterlyser konkretisering og uddybning af påvisningskravet via mere vejledning.	Datatilsynet skriver i Datatilsynets bidrag til delrapport II s. 28-29, at der ikke er nogen formkrav til dokumentation og, at det væsentlige er, at: "*Datatilsynet bliver betrygget i, at principperne overholdes, og at den dataansvarlige kan demonstrere, hvordan dette sker. Datatilsynet vurderer altid sagens oplysninger samlet, og alle bidrag omkring den dataansvarliges forretningsvaretagelse kan benyttes til dokumentation. Særligt relevant er de overvejelser, der indeholder en vurdering eller afvejning af risikoen for den registreredes rettigheder,som den dataansvarlige har foretaget.* *Datatilsynet udviser en betydelig accept af en mere summarisk beskrivelse af de nødvendige*

	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?			*overvejelser, når det gælder behandlinger, der som følge af deres natur og oplysningernes karakter alene udgør en begrænset risiko for de registreredes rettigheder. Her vil kravet efter omstændighederne også kunne dokumenteres i mere generelle brancheanbefalinger eller den blotte konstatering af forholdene omkring behandlingen. Dette gælder også, hvis forholdet er reguleret ved lov. Konkrete dele af databeskyttelsesforordningen kan give støtte til påvisningen, f.eks. kravene til fortegnelse, konsekvensanalyse og databehandleraftaler."* Ift. spørgsmålet om dokumentationskrav ift. allerede eksisterende behandlingsaktiviteter skriver Datatilsynet ligeledes s. 27: "*Kravet om at føre en fortegnelse er ikke helt nyt. Persondatalovens kapitel 12-14 indeholdt således regler om anmeldelse af behandling af personoplysninger til Datatilsynet mv. Ud over denne generelle anmeldelsespligt var den dataansvarlige forpligtet til at stille de i lovens § 43, stk. 2, nr. 1, 2 og 4-6, nævnte oplysninger om alle de behandlinger af personoplysninger, som vedkommende udførte, til rådighed for enhver, som anmodede herom, jf. persondatalovens § 54, stk. 2. Dette betød, at den dataansvarlige på anmodning havde pligt til at udarbejde og inden for rimelig tid udlevere en oversigt over alle behandlinger, denne foretog, herunder behandlingsaktiviteter som ikke var anmeldelsespligtige."*
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	Problemstillingen er inddraget under bemærkningerne til pkt. 1 (samspil mellem GDPR og faglovgivning inkl. generelle forvaltningsretlige regler). 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.	Datatilsynet omtaler problemstillingen på s. 30-31 i Datatilsynets bidrag til delrapport II og skriver bl.a., at billeder af skolebørn, der deles internt med forældrene, godt kan være myndighedsudøvelse. Datatilsynet udtaler, at offentliggørelse af billeder på nettet må anses for mere indgribende. Datatilsynet har efterfølgende udgivet en vejledning om brug af billeder i daginstitutioner: Ny tjekliste til vuggestuer og børnehaver ved brug af billeder og video (datatilsynet.dk)

11.	Tvivl om behandlingsgrundlag og hjemmel ved samarbejde med civilsamfundet (herunder foreninger, lokalråd og landdistriktsråd) og understøttelse af samskabelse er blevet besværliggjort, fx: ○ 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. ○ Må vi eksempelvis offentliggøre fx foreninger, vandværksformænd og lodsejere på hjemmesiden? *	Art. 6		Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.
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		Datatilsynet omtaler problemstillingen på s. 30 ff. i Datatilsynets bidrag til delrapport II: *"Det kan heller ikke afvises, at det i andre tilfælde må anses for en del af myndighedens opgaver, at myndigheden informerer offentligheden omkring myndighedens aktiviteter på et givent område – f.eks. skoleområdet. I det omfang dette er tilfældet, vil man også kunne anvende billeder i den sammenhæng, uden at der indhentes samtykke. I disse situationer er det imidlertid vigtigt at være opmærksom på, at offentliggørelse på internettet sædvanligvis må anses for at være mere indgribende end en deling af billeder internt på et (forældre)intranet. Man bør derfor i sådanne tilfælde bruge sund fornuft og ikke vælge billeder, hvor specifikke personer har en fremtrædende rolle – f.eks. portrætfotoer. Derimod er der typisk ikke noget til hinder for*

				at anvende fotos, hvor enkeltpersoner ikke er i særligt fokus, f.eks. et harmløst foto af en gruppe legende børn eller et luftfoto af en hel skole. Hvis man er i tvivl om, hvorvidt nogen med rimelighed kan føle sig udstillet, vil det naturlige være, at man spørger vedkommende, *hvilket ikke nødvendigvis betyder, at der skal indhentes et egentligt samtykke*." Datatilsynet har desuden udgivet guide om brug af billeder og video i daginstitutioner, der kan være retningsgivende også i andre situationer: Ny tjekliste til vuggestuer og børnehaver ved brug af billeder og video (datatilsynet.dk)
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)	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 myndighedsuøvelse/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. 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.	Se række 2.
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	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.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.

			Flere konstaterer, at Datatilsynet har svaret, men at behandlingshjemlen ikke er angivet. 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. 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 databeskyttelsesretligt samtykke. Det bidrager endvidere til tvivl, når det i vejledningen om samtykke hedder: ”*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*.” 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.	
15.	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.	Art. 6, stk. 1, litra e	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. 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	Problemstillingen vedr. nødvendighedskravet er adresseret af Datatilsynet på s. 30 i Datatilsynets bidrag til delrapport II. Se række 1.

			forbindelse fortolkningen af nødvendighedskravet.	
16.	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. 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?	Art. 6, stk. 1, litra e	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. Grundlæggende er problemstillingen den samme, som der er redegjort for i punkt. 1.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer. Men Datatilsynet har taget stilling til spørgsmålet i en afgørelse: Kommuners offentliggørelse af oplysninger mv. i offentligt tilgængelige webarkiver (datatilsynet.dk)
17.	Må der ske offentliggørelse af høringssvar fra borgere, som indeholder personoplysninger, i forbindelse med en politisk behandling.*	Art. 6	Ifølge Datatilsynets svar på KLs benspænd har vi fået oplyst: *Så længe der er tale om almindelige oplysninger som navn og adresse, må kommunerne – ligesom f.eks. Folketinget – offentliggøre høringssvarene.* 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 personoplysninger. Der holder det ikke helt at sige ”Når Folketinget må det, så må vi også”.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer. Datatilsynet har dog offentliggjort udtalelse om webarkiver (se række 16) og udtalelse om offentligørelse af høringssvar (screening fra fx cpr-numre): Klage over offentliggørelse af personnummer på kommunal hjemmeside (datatilsynet.dk)
18.	GDPR er svær at forstå: • Det er svært at forstå hvor langt et givent behandlingsgrundlag mv. egentligt strækker og, hvor grænsen så går.	Art. 6, stk. 1, litra e		Datatilsynet uddyber art. 6, stk. 1, litra e, i Datatilsynets bidrag til delrapport II s. 30 ff.: *”Det vil således ligge inden for rammerne af databeskyttelsesforordningens artikel 6, stk. 1, litra e, hvis myndigheden kan pege på et*

	○ Hvordan det defineres som en del af det at drive kommune og, hvornår det bliver "nice-to-have". *			*lovgrundlag som årsagen til behandlingen, og hvis behandlingen ikke – ud fra en generel betragtning – er unødigt indgribende for den registrerede, f.eks. fordi behandlingen udelukkende er en praktisk måde for myndigheden at opfylde formålet på, som ikke tager hensyn til den registrerede."*
19.	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. Idet Datatilsynets vejledning kræver, at kommunerne skal foretage en vurdering af, om billederne indeholder følsomme oplysninger, der kræver indhentning af samtykke 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 faktisk forvaltningsvirksomhed end ved at indhente samtykke. At administrere samtykker – indhentning, specificering, tilbagetrækning mv. er administrativt tunge processer. 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.	Art. 6, stk. 1, litra e og art. 9		Problemstillingen vedr. følsomme oplysninger ifm. billeder er ikke italesat på en for kommunerne relevant måde i Justitsministeriets eller Datatilsynets delrapporteringer (kun vedr. fagforeninger, s. 54 i Datatilsynets delrapport II).
20.	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	Art. 6, stk. 4	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.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer. Datatilsynet kommenterer heller ikke spørgsmålet om brede/hhv. smalle formål og hvordan, dataansvarlige i praksis kan iagttage art. 6, stk. 4, om uforenelighedstesten.

	behandlingsformål er udfoldet i artikel 6, stk. 4, litra a-e, er bestemmelsen stadig tung og svær at administrere efter. Det samme er kravet i artikel 6, stk. 4, om, at der skal ske en vurderingen 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".			
21.	Der er generelle usikkerheder om (gen)anvendelse af data inden for enhedsforvaltningen, når der ikke er tale om ansøgningssager (med det deraf følgende samtykkekrav). Litteraturen lægger til grund, at data indsamlet i én forvaltning kan genanvendes i en anden forvaltning, når blot formålene er ikkeuforenelige, men det giver alligevel anledning til jævnlig tvivl om, hvordan ikke-uforeneligheden skal fortolkes ved genanvendelse af data på tværs af de enkelte fagforvaltninger inden for enhedsforvaltningen. Særligt, når det kommer til art. 9-oplysninger. 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?*	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.	Problemstillingen om udveksling af oplysninger på tværs af forvaltninger, der administrerer forskellige faglovgivninger er ikke ikke behandlet i hverken Justitsministeriets eller Datatilsynets delrapporteringer, men problemstillingen vil naturligt indgå som en del af det tværministerielle arbejde om samspillet mellem GDPR og faglovgivningen.
22.	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	Art. 6 og art. 9 (Art. 6, stk. 4, og art. 5, stk. 1, litra b/ DBL § 5, stk. 3, og § 23/DBL § 10)		Justitsministeriet skriver på s. 22 i Delrapport II, at "*Efter databeskyttelseslovens § 23 er der inden for rammerne af forordningens artikel 23 fastsat en undtagelse fra reglerne om fornyet oplysningspligt*

	brug for ledelsesinfo efter de nye regler om databeskyttelse som efter den tidligere gældende persondatalov. Både fsva. almindelige og følsomme oplysninger, herunder sondring mellem ikke-anonyme, anonyme og psydonymiserede personoplysninger. Hvordan forholder de nye regler sig til: - 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) I hvilke tilfælde er der oplysningspligt overfor borgeren vedrørende samkøringen? Er der fx oplysningspligt, hvis samkøringen sker i kontroløjemed, jf. § 23, sidste pkt.? 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. 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?			*i situationer, hvor offentlige myndigheder viderebehandler personoplysninger på baggrund af regler fastsat i henhold til lovens § 5, stk. 3, til et andet formål end det, hvortil de er indsamlet, dog ikke når formålet er sammenstilling eller samkøring af personoplysninger i kontroløjemed. Ifølge forarbejderne til databeskyttelsesloven er bestemmelsen fastsat inden for rammerne af forordningens artikel 23 af hensyn til, at fornyet oplysningspligt kan opleves som administrativt byrdefuldt, og at det synes tvivlsomt, om en fornyet oplysningspligt i den omhandlede situation reelt vil skabe større retssikkerhed for den registrerede. Der henvises til Folketingstidende 2017-18, tillæg A, L 68 som fremsat, side 145 f. og Folketingstidende 2017-18, tillæg B, betænkning over L 68 (omtryk), side 8 ff.*" Justitsministeriet og Datatilsynet forholder sig i deres delrapporteringer ikke til spørgsmål om samkøring.

	Vedr. oplysningspligt Man kan enten oplyse om samkøring i opstarten af en sag (i oplysningspligtsskabelon) eller man kan opfylde sin oplysningspligt om samkøringen umiddelbart forud for 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 behandlingshjemlen 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.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer, men problemstillingen vil naturligt indgå som en del af det tværministerielle arbejde om samspillet mellem GDPR og faglovgivningen.
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)		Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer, men problemstillingen vil naturligt indgå som en del af det tværministerielle arbejde om samspillet mellem GDPR og faglovgivningen.
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.	Art. 6 og art. 9 (Art 6, stk. 4)		Datatilsynet behandler særlovgivningens samspil ift. art. 6 på s. 29 ff. i Datatilsynets bidrag til delrapport II: *"I andre og langt de fleste tilfælde vil særlovgivningen imidlertid ikke indeholde specifikke krav til behandlingen af personoplysninger eller i øvrigt foreskrive specifikt, om og hvilke personoplysninger der skal behandles. Behandling af personoplysninger vil imidlertid*

	skolelederens særlige beføjelser. Eller er skoleområdet altid en intern videregivelse?*			*typisk være en forudsætning for, at myndigheden kan løse de opgaver, som lovgivningen foreskriver. Dette kunne f.eks. være en myndigheds vurdering af en borgers ret til sociale ydelser efter den sociale lovgivning eller lovgivning om myndighedens opgaver på børne- og skoleområdet.”* Dette svarer dog ikke på det rejste spørgsmål, men problemstillingen vil naturligt indgå som en del af det tværministerielle arbejde om samspillet mellem GDPR og faglovgivningen.
26.	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. Hvis man som børnehave 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.	Art. 7, stk. 3, 2. pkt.	Hos kommunerne giver det primært anledning til tvivl, hvilket behandlingsgrundlag der er det rigtige – altså grundlæggende samme problemstilling som pkt. 1.	Se række 10.
27.	Muligheden for at kunne leve op til kravet om, at samtykke skal afgives "frit" er uklar i regi af den offentlige	Art. 7, stk. 4	Høringssvarene afspejler, at dét, der særligt volder problemer er samspillet mellem samtykker i forvaltningsloven,	Datatilsyneti adresserer spørgsmålet om sondringen mellem GDPR-samtykke og forvaltningsretligt

	sektor, idet borgerens samtykke oftest vil medføre en form for service, hjælp etc.		retssikkerhedsloven og sundhedsloven og andre faglovgivninger over for samtykke i GDPR. Altså samme problematik som er skitseret i pkt. 1.	samtykke i Datatilsynets bidrag til delrapport II s. 30, men delrapporten klarlægger ikke problemet med samspillet mellem samtykker i div. faglovgivninger over for samtykke i GDPR generelt. Problemstillingen vil naturligt indgå som en del af det tværministerielle arbejde om samspillet mellem GDPR og faglovgivningen.
28.	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.	Art. 9	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. 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). 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).	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapportering. Men spørgsmålet er afklaret i Datatilsynets praksis: Hvidovre Kommunes behandling af oplysninger om børn (datatilsynet.dk)
29.	Hvornår kan artikel 9, stk. 2, litra g, "samfundsinteresser" anvendes?*	Art. 9, stk. 2, litra g	Vejledning ønskes.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer. Spørgsmålet kan ikke besvares udtømmende, men se række 28 om faktisk forvaltningsvirksomhed.

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.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.
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 personerne, 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	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.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer. Der er dog i Datatilsynets bidrag til delrapport II, s. 54, gjort bemærkninger om brug af billeder ifm. fagforeningsaktiviteter.

	møde op på en given adresse mhp. en given behandling.			
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 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"?*	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. 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. 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. 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 –	Spørgsmålet om oplysningspligt ift bipersoner er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer. Datatilsynet omtaler dog kort "bipersoner" på s. 36-37 i Datatilsynets bidrag til delrapport II. Omtalen bidrager ikke til noget nyt. Herudover nævner Justitsministeriet på s. 29-30 i Delrapport II, at *"Oplysningspligten vil eksempelvis kunne opfyldes ved, at en forud udfyldt skabelon fra den nævnte vejledning udleveres samtidig med modtagelsen af oplysningerne, f.eks. som en del af et autosvar på en e-mail. Som det endvidere fremgår af vejledningen, skal oplysningspligten som udgangspunkt kun iagttages én gang over for den registrerede, medmindre den dataansvarlige på et senere tidspunkt vil behandle oplysningerne til andre formål."* Det fremgår af Datatilsynets bidrag til delrapport II, s. 37, *at "Datatilsynet vil løbende offentliggøre afgørelser, som kan belyse omfanget af oplysningspligten, ligesom tilsynet arbejder på en opdatering af vejledningen om de registreredes rettigheder."*

			uforholdsmæssigt stor indsats. Denne del af vejledningen kan med fordel udbygges med konkrete eksempler med udgangspunkt i den kommunale virkelighed. Se i øvrigt pkt. 5 vedr. art. 5, stk. 1, litra b.	
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".	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.
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		Justitsministeriets bemærkninger i delrapport II s. 28-30 må forstås sådan, at der ikke er planer om lempelse af reglerne. Dataansvarlige kan fx ikke lægge til grund, at den registrerede på forhånd kender de oplysninger, som oplysningspligten angår.
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 dække os ind under art. 14, stk. 5 litra b, men det virker uklart?*	Art. 14		Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.
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 egenacces i offentlighedslovens § 8. Kommunerne oplever, at kravet om vejledning om det mest gunstige retsgrundlag for borgeren, vil være vanskeligt at gennemføre for	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.

			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.	
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 sondring 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 egenacces i offentlighedsloven skal revideres, så den enten bringes i overensstemmelse med databeskyttelsesforordningens art. 15 eller helt tydeligt adskiller sig.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.
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		Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.
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 Datatilsynets bidrag til delrapport II, s. 26-27, skriver Datatilsynet: "*Databeskyttelsesforordningen stiller overordnet ingen formkrav til, hvordan dokumentation skal foretages. Dette giver netop råderum til, at den dataansvarlige selv kan vælge en metode. Det væsentlige er, at Datatilsynet bliver betrygget i, at principperne overholdes, og at den dataansvarlige kan demonstrere, hvordan dette sker.*

				Datatilsynet vurderer altid sagens oplysninger samlet, og alle bidrag omkring den dataansvarliges forretningsvaretagelse kan benyttes til dokumentation. Særligt relevant er de overvejelser, der indeholder en vurdering eller afvejning af risikoen for den registreredes rettigheder, som den dataansvarlige har foretaget. Datatilsynet udviser en betydelig accept af en mere summarisk beskrivelse af de nødvendige overvejelser, når det gælder behandlinger, der som følge af deres natur og oplysningernes karakter alene udgør en begrænset risiko for de registreredes rettigheder. Her vil kravet efter omstændighederne også kunne dokumenteres i mere generelle brancheanbefalinger eller den blotte konstatering af forholdene omkring behandlingen. Dette gælder også, hvis forholdet er reguleret ved lov. *Konkrete dele af databeskyttelsesforordningen kan give støtte til påvisningen, f.eks. kravene til fortegnelse, konsekvensanalyse og databehandleraftaler."*
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 Datatilsynets bidrag til delrapport II, s. 7, skriver Datatilsynet: *"De indkomne høringssvar viser, at det i praksis ikke altid er lige let at afklare rollefordelingen, og at der er behov for yderligere – praksisnær – vejledning på området. Datatilsynet vil derfor tage initiativ til, at det vejledende materiale om dataansvarlige og databehandlere, som pt. er tilgængelig på Datatilsynets hjemmeside, løbende opdateres og udbygges med praksisnære eksempler."* samt *" Datatilsynet har også i regi af Det Europæiske Databeskyttelsesråd (EDPB) bidraget til udarbejdelsen af en fælleseuropæisk vejledning om databeskyttelsesforordningens begreber dataansvarlige og databehandlere (vejledning 07/2020). Vejledningen har været sendt i offentlig høring og forventes snart vedtaget med de ændringer, som de indkomne høringssvar måtte give anledning til. Når den endelige vejledning foreligger, vil Datatilsynets nationale vejledning blive opdateret i overensstemmelse hermed."* Retningslinjerne/vejledningen er vedtaget 7. juli 2021: https://edpb.europa.eu/system/files/2021-

				07/eppb_guidelines_202007_controllerprocessor_final_en.pdf
41.	Det er umuligt for kommunerne at få indgået et retvisende aftalegrundlag med Facebook (databehandleraftale eller aftale om fælles dataansvar) – og de øvrige store tech-giganter. Facebook har udarbejdet egne databehandleraftalevilkår, 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 Datatilsynets bidrag til delrapport II, s. 9, skriver Datatilsynet: *" Der er ... efter Datatilsynets opfattelse ikke noget til hinder for, at det er databehandleren, som tager initiativ til udarbejdelsen af databehandleraftalen, eller i øvrigt fastlægger indholdet heraf. Dette vil særligt være relevant, hvor den ydelse, som databehandleren leverer, kan karakteriseres som en standardydelse, hvor det ikke vil være muligt individuelt at "forhandle" spørgsmålet om f.eks. tekniske og organisatoriske foranstaltninger. Den dataansvarlige må i disse tilfælde vurdere, om den tilbudte aftale, de beskrevne foranstaltninger og forholdene, behandlingerne sker under, indebærer, at forordningen overholdes, jf. forordningens artikel 28, stk. 1. Det samme gælder i forhold til den ordning, som skal fastlægges i henhold til forordningens artikel 26."*
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 databehandleraftaler mellem den enkelte kommune og staten. Databehandleraftaler, som vil være enslydende for alle kommuner. Kommunerne vil derfor skulle bruge tid på hver især at gennemlæse og forholde sig til databehandleraftalerne, 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 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 databehandler-konstruktion. Alle databehandleraftaler mellem kommunerne og staten foreslås i stedet reguleret af bekendtgørelser, "andet retligt dokument", jf. artikel 28, stk. 3.	Justitsministeriet skriver på s. 33 i Delrapport II, at "*I forhold til efterspørgslen på en mere "central" regulering af fastlæggelsen af rollefordelingen mellem dataansvarlig og databehandler mellem offentlige myndigheder, er Justitsministeriet indstillet på sammen med relevante ressortministerier at se nærmere på mulighederne og behovet for regulering heraf inden for rammerne af databeskyttelsesforordningen."* I Datatilsynets bidrag til delrapport II, s. 7, skriver Datatilsynet: *"De indkomne høringssvar viser, at det i praksis ikke altid er lige let at afklare rollefordelingen, og at der er behov for yderligere – praksisnær – vejledning på området. Datatilsynet vil derfor tage initiativ til, at det vejledende materiale om dataansvarlige og databehandlere, som pt. er tilgængelig på Datatilsynets hjemmeside, løbende opdateres og udbygges med praksisnære eksempler."*
43.	Indgåelse af databehandleraftaler. Vi finder det ofte uklart hvornår der skal indgås en databehandleraftale (der ikke handler om IT-leverandører) fx. med	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.	I Datatilsynets bidrag til delrapport II, s. 7, skriver Datatilsynet: *"De indkomne høringssvar viser, at det i praksis ikke altid er lige let at afklare rollefordelingen, og at der er behov for yderligere – praksisnær – vejledning på*

	samarbejdspartnere, beskæftigelsestilbud, tilkøb af udredninger.*			*området. Datatilsynet vil derfor tage initiativ til, at det vejledende materiale om dataansvarlige og databehandlere, som pt. er tilgængelig på Datatilsynets hjemmeside, løbende opdateres og udbygges med praksisnære eksempler."* Datatilsynet har november 2021 offentliggjort et tillæg til deres oprindelige vejledning om dataansvarlige og databehandlere med nye eksempler: https://www.datatilsynet.dk/Media/637800004810345413/Vejledende%20tekst%20om%20rollefordelingen_2022.pdf
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?	I Datatilsynets bidrag til delrapport II, s. 22, skriver Datatilsynet: "*Dataansvarlige inden for samme område, brancher og lovgivningsområde vil typisk have mange identiske behandlinger og betydeligt sammenfald i opgavetilgangen til løsningen heraf. Det er Datatilsynets opfattelse, at der i disse tilfælde er en stor synergi i at benytte fælles tilgang til at finde et passende niveau af sikkerhed. Det kunne være med fælles udarbejdede vurderinger af behandlinger foretaget med samme software på samme måde i flere kommuner. I den yderste konsekvens ville det antageligt svare til adfærdskodekser, jf. artikel 40, idet et adfærdskodeks netop er tænkt rettet imod specifikke behandlingssektorer, brancher, mv., med sammenlignelige behandlinger af personoplysninger, ensartede behov, ens organisationer, osv."* og *"Datatilsynet opfordrer i øvrigt til, at organisationer, der udfører samme typer af behandlinger under sammenlignelige forhold, kan hjælpe hinanden ved at dele risikovurderinger. Man skal blot være opmærksom på, at ansvaret ikke derved deles eller overføres, og den enkelte dataansvarlige/databehandler skal stadig sikre sig, at risikovurdering også passer til egne behandlinger af personoplysninger".*
45.	Indgåelse af databehandleraftale vil ofte ske efter forudgående udbudsproces, hvor forhåndsvurderingen af databehandleren, jf. art. 28, stk. 1, giver praktiske og ressourcemæssige	Art. 28, stk. 1		Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.

	udfordringer i relation til afviklingen af udbudsprocessen.*			
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 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?	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 Datatilsynets bidrag til delrapport II, s. 8, skriver Datatilsynet: "*De indkomne høringssvar viser ..., at der, som det er tilfældet i forhold til afklaringen af rollefordelingen, er behov for yderligere vejledning på området, herunder ved inddragelsen af praksisnære eksempler, tjeklister mv. Datatilsynet forventer derfor i 2. kvartal 2021 at opdatere og supplere tilsynets vejledende materiale om tilsyn med databehandlere og underdatabehandlere.*" Datatilsynet har i oktober 2021 udgivet en ny vejledning om tilsyn med databehandlere, der beskriver, hvad og hvordan der skal føres tilsyn: https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf
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.	Se række 46. Datatilsynets nye vejledning tager dog ikke eksplicit stilling til 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.	Se række 46 og 47. Af Datatilsynets nye vejledning s. 12 fremgår det eksplicit, at der skal føres tilsyn med: *"At databehandleren pålægger eventuelle underdatabehandlere samme forpligtelser som i databehandleraftalen mellem dig og databehandleren, herunder at databehandleren fører tilsyn med eventuelle underdatabehandlere."*
49.	Kontrol af, hvorvidt databehandlere har kontrolleret	Art. 28 og 32		Se række 48.

	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.*			
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.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer eller i Datatilsynets nye vejledning om tilsyn med databehandlere: https://www.datatilsynet.dk/Media/637710957381234368/Datatilsynet_Vejledning%20om%20tilsyn%20med%20databehandlere_oktober-2021.pdf
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.	Se række 46.
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.	Se række 46.
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?	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.	Se række 39.

	Og i fald kommunerne selv har gennemført fysisk tilsyn, hvordan skal de så dokumentere dette?			
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 revisionsskabelon til brug i kommunerne, tiltænkt aftaler med mindre leverandører, gratis systemer eller leverandører med få almindelige personoplysninger - i form af fx spørgeskema.	I Datatilsynets bidrag til delrapport II, s. 8, skriver Datatilsynet: *"Endvidere lancerede Datatilsynet og FSR - danske revisorer sammen i februar 2019 en revisorerklæring, som skal hjælpe dataansvarlige med at påse, at deres databehandlere lever op til kravene i GDPR. I november 2020 blev erklæringen fulgt op af en ny udgave med en begrænset grad af sikkerhed, når der f.eks. er mindre kompleksitet i behandlingen af personoplysninger. Formålet med den nye erklæring var at bidrage til at sikre, at brugen af revisorerklæringer står mål med behovet i den konkrete situation. Det er ikke nødvendigt at benytte revisorerklæringer for at efterleve databeskyttelsesforordningen, men kan være en god måde at sikre, at de relevante områder bliver belyst, og at man får foretaget en uvildig kontrol af sikkerhedsniveauet. Begge revisorerklæringer er tilgængelige på FSR – danske revisorers og Datatilsynets hjemmesider."*
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 Datatilsynets bidrag til delrapport II, kapitel 7, skriver Datatilsynet om fortegnelseskravet, men spørgsmålet om de lovregulerede behandlinger adresseres ikke direkte.
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	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	I Datatilsynets bidrag til delrapport II, s. 27, skriver Datatilsynet: *"For så vidt angår bemærkningerne om Datatilsynets reviderede vejledning om fortegnelseskravet fra august 2020 bemærkes indledningsvis, at opdateringen skete på baggrund af en række erfaringer, som Datatilsynet – som led i sin tilsynsopgave – havde gjort sig efter den 25. maj 2018, hvor databeskyttelsesforordningen*

	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.		ikke at overholde databeskyttelsesforordningens art. 30, i fald Datatilsynets opdaterede vejledning ikke følges fsva. de nye indholdsmæssige krav fra Datatilsynet til fortegnelserne.	*begyndte at finde anvendelse. Opdateringen af vejledningen bestod primært i en tydeliggørelse af, at fortegnelsen over behandlingsaktiviteter – efter Datatilsynets vurdering, når man ser på formålene med fortegnelseskravet – skal indeholde en tydelig angivelse af, hvilke kategorier af personoplysninger der behandles om de enkelte kategorier af registrerede. Hvis der bliver eller vil blive videregivet personoplysninger i forbindelse med en behandlingsaktivitet, skal fortegnelsen også indeholde information om, hvilke kategorier af personoplysninger der bliver eller vil blive videregivet til den pågældende modtager. I tilknytning hertil skal det også fremgå, hvilke kategorier af registrerede de pågædende oplysninger vedrører. Datatilsynet kan ikke afvise, at der vil være dataansvarlige, der vil skulle foretage visse ændringer i deres fortegnelser efter artikel 30 som følge af tilsynets ændringer fra august 2020. Datatilsynet forventer imidlertid ikke, at dataansvarlige – som følge af ændringerne – genåbner deres fortegnelse. Datatilsynet forventer, at eventuelle tilpasninger eller justeringer af fortegnelsen sker løbende, når dokumenterne alligevel skal justeres eller ajourføres."*
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.	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.	Datatilsynet adresserer spørgsmålet i Datatilsynets bidrag til delrapport II, s. 19-22. Her nævnes en lang række værktøjer til risikovurderinger. Desuden skriver Datatilsynet s. 21: *"Hvornår et sådant "passende sikkerhedsniveau" er etableret vil bero på en konkret vurdering. Som vejledende pejlemærke kan nævnes, at et passende sikkerhedsniveau vil afhænge af, hvilke og hvor store risici der er for sikkerhedsbrud og dermed for, at fysiske personers rettigheder og frihedsrettigheder krænkes."* og

	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 nok, når der ikke står nogen steder, hvad der er tilstrækkeligt.			*"Det er tilsynets opfattelse, at der gennem sammenhængen med artikel 25 og tanken om, at når der laves forretningsudvikling, allerede i designet af behandlingerne af persondata bliver indlejret de fornødne garantier for, at databeskyttelsesforordningen overholdes, ligger en betydelig fokus på redskaber, der netop realiserer det "passende", også set i forhold til det teknologiske niveau og implementeringsomkostninger."* og *"De mange aspekter, som kan påvirke risikoniveauet, betyder også, at der ikke kan defineres et sæt "passende foranstaltninger" alene ud fra information om, hvilken type personoplysninger der behandles."* og *"Dataansvarlige inden for samme område, brancher og lovgivningsområde vil typisk have mange identiske behandlinger og betydeligt sammenfald i opgavetilgangen til løsningen heraf. Det er Datatilsynets opfattelse, at der i disse tilfælde er en stor synergi i at benytte fælles tilgang til at finde et passende niveau af sikkerhed. Det kunne være med fælles udarbejdede vurderinger af behandlinger foretaget med samme software på samme måde i flere kommuner. I den yderste konsekvens ville det antageligt svare til adfærdskodekser, jf. artikel 40, idet et adfærdskodeks netop er tænkt rettet imod specifikke behandlingssektorer, brancher, mv., med sammenlignelige behandlinger af personoplysninger, ensartede behov, ens organisationer, osv. Adfærdskodekser kan udarbejdes af sammenslutninger og andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, jf. artikel 40, stk. 2. Dette kunne f.eks. være en interesseorganisation, et fagforbund, KL eller Danske Regioner. Det er dog væsentligt at minde om, at både adfærdskodeks og certificeringer i en eller anden udstrækning begrænser autonomien*

				i opgaveløsningen. Datatilsynet arbejder på at gøre tilsynets vejledninger mere konkrete, f.eks. ved at lave vejledning om specifikke emner. Dette kunne være forhold om kryptering, sletning, sikkerhed ved flytbare medier, brug af produktionsdata til test og andre emner inden for sikkerhed. Datatilsynet vil have fokus på, at vejledninger så vidt muligt kommer til at indeholde lister over de trusler, som er vigtige at have for øje og undersøge, og forslag til foranstaltninger. Begge dele kan hjælpe ved gennemførsel af risikovurderinger og iværksættelse af passende foranstaltninger. Datatilsynet opfordrer i øvrigt til, at organisationer, der udfører samme typer af behandlinger under sammenlignelige forhold, kan hjælpe hinanden ved at dele risikovurderinger. Man skal blot være opmærksom på, at ansvaret ikke derved deles eller overføres, og den enkelte dataansvarlige/databehandler skal stadig sikre sig, at risikovurdering også passer til egne behandlinger af personoplysninger."
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 af rammerne for autorisationer med eksempler fra det kommunale område.	Se række 57.
59.	Databeskyttelsesforordningens retlige rammer for medarbejderadgang til personoplysninger i it-løsninger kontra princippet/ønsket om helhedsorienteret sagsbehandling (forvaltningslovens § 29 og	Art. 32		Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer. JM tilkendegiver dog på s. 33 i Delrapport II, at samspillet mellem GDPR og faglovgivning og udveksling/videregivelse af

	muligheden for udveksling af oplysninger inden for enhedsforvaltningen). Brugerautorisationer ctr videregivelse.*			oplysninger vil blive taget op i et tværministerielt samarbejde i igangværende år (d.v.s. 2021).
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.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.
61.	Sletning i backup af IT systemer og dokumentation for dette er meget kompliceret.*	Art. 32 og art. 5, stk. 2		Sletningsudfordringer er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer. Vedrørende dokumentation se række 9.
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.	Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 25, om brugen af SMS følgende: *"Datatilsynets generelle retningslinjer for brugen af e-mail og SMS er ikke ufravigelige, men udtryk for det, der normalt må anses for passende sikkerhed ved behandling af følsomme og fortrolige oplysninger."*
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,	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	Justitsministeriet skriver på s. 30-31 i Delrapport II, at *"Mulighederne for at begrænse databeskyttelsesforordningens regler er behandlet ovenfor under afsnit 3 og 5.1. Som det fremgår under afsnit 3.2 og 3.3, er medlemsstaterne ikke efterladt mulighed for at fastsætte begrænsninger i forhold til forordningens artikel 33. På den baggrund vil der efter*

	som ikke giver megen læring og sikkerhed, jf. princippet om risikotilgang i forordningen. 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.		klart, hvornår der ikke behøver at blive foretaget anmeldelse som følge af en vurdering af det samlede aktuelle risikobillede.	*Justitsministeriets vurdering ikke kunne fastsættes en anden minimumsgrænse eller frist for, hvornår der skal ske anmeldelse til Datatilsynet om brud på persondatasikkerheden, end den, der allerede følger af artikel 33. Det bemærkes, at Datatilsynet og Justitsministeriet i januar 2018 har udgivet en vejledning om håndtering af brud på persondatasikkerheden, hvor der fremgår nærmere information om, hvornår der skal ske anmeldelse til Datatilsynet. Det bemærkes, at der i flere høringssvar til erfaringsindsamlingen efterspørges mere vejledning om forståelsen af pligten til at anmelde brud på persondatasikkerheden. Som det bl.a. fremgår af Datatilsynets bidrag til erfaringsindsamlingen, vil tilsynet se på en mulig revision af vejledningen om håndtering af brud på persondatasikkerheden med henblik på at supplere med flere konkrete eksempler (afsnit 5 i bilag 1)."* Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 13, at: *"EDPB har den 14. januar i år vedtaget en ny vejledning, som følger op på de erfaringer, de europæiske tilsynsmyndigheder har gjort på området. I vejledningen, der har været sendt i offentlig høring, og som forventes endelig vedtaget i løbet af i år, gennemgår EDPB 18 konkrete eksempler på brud på persondatasikkerheden og redegør for, hvilke handlinger den dataansvarlige bør tage i forlængelse heraf. Kan den dataansvarlige "nøjes" med at skrive bruddet på den liste over alle sikkerhedshændelser, som den dataansvarlige skal føre efter databeskyttelsesforordningens artikel 33, stk. 5, eller skal der ske anmeldelse til tilsynsmyndigheden, ligesom vejledningen også forholder sig spørgsmålet om underretning af de registrerede i hver af de 18*

				konkrete eksempler på brud på persondatasikkerhed." Link til retningslinjerne: *https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf* Datatilsynet skriver videre: *"Datatilsynet har alligevel forståelse for, at afvejningen af, hvorvidt der skal ske anmeldelse til tilsynet, til tider kan være vanskelig. Datatilsynet vil derfor se på en revision af tilsynets vejledning om håndtering af brud på persondatasikkerheden med henblik på at supplere med flere konkrete eksempler."* På side 15 skriver Datatilsynet: *"Efter Datatilsynets opfattelse vil det ikke være foreneligt med reglerne i databeskyttelsesforordningens artikel 33 at indføre en bagatelgrænse, hvor mindre sikkerhedsbrud undtages fra anmeldelsespligten. Datatilsynet er derudover af den opfattelse, at intern dokumentation og anmeldelse til tilsynet – uanset bruddets karakter – varetager en række saglige hensyn i den dataansvarliges arbejde med at styrke informationssikkerheden."*
64.	Anmeldelse til Datatilsynet, hvor der sker løbende indberetning. Her skal oplysninger udfyldes igen, selvom de tidligere er indberettet. Det er unødig resursetid.*	Art. 33		Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 14, at *"For så vidt angår bemærkningen om, at det synes uproportionelt, at dokumentationspligten i forbindelse med databrud følger samme procedure uanset bruddets omfang og de forbundne risici for de registrerede, skal Datatilsynet for en god ordens skyld bemærke, at kravet om dokumentation varierer i forhold til bruddets karakter. Datatilsynet er opmærksom på, at ressourceforbruget ved håndtering af intern dokumentation og anmeldelse til tilsynet er ressourcekrævende. Datatilsynet er derfor ved at*

				undersøge løsninger, som vil lette ressourceforbruget ved anmeldelser af brud. Datatilsynet vil som nævnt ovenfor endvidere se på en revision af vejledningen om håndtering af brud på persondatasikkerheden med henblik på at supplere med flere konkrete eksempler, og tilsynet vil i den forbindelse også præcisere dokumentationskravet."
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.	Justitsministeriet skriver på s. 3 i Delrapport II, at "*I databeskyttelsesforordningens artikel 23 er der under nærmere betingelser mulighed for at begrænse rækkevidden af forpligtelserne og rettighederne i forordningens artikel 12-22 og 34 samt tilsvarende regler i artikel 5. Det er Justitsministeriets vurdering, at råderummet i artikel 23 f.eks. kan anvendes til at fastsætte, at den dataansvarlige efter en konkret vurdering kan gøre visse undtagelser fra disse regler af hensyn til en eller flere af de interesser, der er oplistet i artikel 23, stk. 1, litra a-j. Denne mulighed er for så vidt angår artikel 13-14 (om oplysningspligt) og artikel 15 (om indsigtsret) samt artikel 34 (om underretningspligt ved sikkerhedsbrud) allerede udnyttet i databeskyttelseslovens § 22, stk. 1 og 2."* Ligeledes behandler Justitsministeriet spørgsmålet på s. 10-12, hvor ministeriet på s. 11 skriver: *"Fastsættelse af begrænsninger i disse rettigheder og forpligtelser efter artikel 23, stk. 1, skal som anført ske ved lovgivningsmæssig foranstaltning."*
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.	Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 13, at: *"EDPB har den 14. januar i år vedtaget en ny vejledning, som følger op på de erfaringer, de europæiske tilsynsmyndigheder har gjort på området. I vejledningen, der har været sendt i offentlig høring, og*

				som forventes endelig vedtaget i løbet af i år, gennemgår EDPB 18 konkrete eksempler på brud på persondatasikkerheden og redegør for, hvilke handlinger den dataansvarlige bør tage i forlængelse heraf. Kan den dataansvarlige "nøjes" med at skrive bruddet på den liste over alle sikkerhedshændelser, som den dataansvarlige skal føre efter databeskyttelsesforordningens artikel 33, stk. 5, eller skal der ske anmeldelse til tilsynsmyndigheden, ligesom vejledningen også forholder sig spørgsmålet om underretning af de registrerede i hver af de 18 konkrete eksempler på brud på persondatasikkerhed." Link til retningslinjerne: *https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202101_databreachnotificationexamples_v1_en.pdf*
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~~ 10, 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.	Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 13, at *"Datatilsynet gør endvidere opmærksom på forordningens artikel 35, stk. 10, om muligheden for at udarbejde konsekvensanalyser i forbindelse med lovforslag. Det er dog væsentligt at notere, at dette kræver, at de krav, der er til en konsekvensanalyse, alle er iagttaget under det lovforberedende arbejde. Datatilsynet skal også erindre om, at en sådan fælles konsekvensanalyse skal holdes opdateret i forhold til uforudsete trusler, ændringer i it-miljøer, organisatorisk implementering og ændringer i det generelle trusselsbillede."*
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.	Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 20, at " *Endvidere kan nævnes ISO/IEC DIS 29134 "Information technology – Security techniques – Privacy impact assesment – Guidelines", som er en international standard udarbejdet af den internationale standardiseringsorganisation,*

				International Organization for Standardization, ISO. Standarden er en vejledning i, hvorledes en konsekvensanalyse (Privacy Impact Assesment proces) kan udføres. Standarden beskriver processen i en række trin, hvoraf et trin f.eks. vedrører identifikation af risici, mens et senere trin f.eks. vedrører beslutning om foranstaltninger. Standarden sætter bl.a. fokus på, at behandlingssikkerhed bliver iagttaget og indarbejdet i f.eks. design og implementeringen af IT-løsninger. Datatilsynet har også bidraget til Det Europæiske Databeskyttelsesråds (EDPB) vejledning af oktober 2017 (wp 248rev.01) om "konsekvensanalyser vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko"", ligesom tilsynet i samarbejde med Justitsministeriet har udarbejdet en national vejledning om konsekvensanalyser, der er offentliggjort i marts 2018. I januar 2019 offentliggjorde Datatilsynet i overensstemmelse med databeskyttelsesforordningen endvidere en endelig liste over situationer, hvor dataansvarlige altid skal udarbejde konsekvensanalyser, efter at listen i udkastform havde været forelagt EDPB til udtalelse."

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.	Justitsministeriet skriver på s. 33-34 i Delrapport II, at "*Der er opstået udfordringer i forhold til tredjelandsoverførsler som følge af Schrems II-afgørelsen. Ministeriet følger udviklingen tæt og kan oplyse, at der kort tid efter domsafsigelsen i EU-regi blev iværksat konkrete arbejdsstrømme for at finde løsninger på de udfordringer, som afgørelsen har affødt. F.eks. har EU-Kommissionen og relevante amerikanske myndigheder meddelt, at man kort tid efter domsafsigelsen indgik i dialog for at vende mulighederne for en afløser for den overførselsmekanisme (Privacy Shield), som EU-Domstolen erklærede ugyldig. Senest har EU-kommissær for retlige anliggender Didier Reynders og USA's handelsminister Gina Raimondo den 25. marts 2021 offentliggjort en fælles pressemeddelelse, hvoraf det fremgår, at EU og USA vil intensivere forhandlingerne om at finde en ny løsning. Som det bl.a. fremgår af Datatilsynets bidrag til erfaringsindsamlingen (afsnit 4 i bilag 1), er Datatilsynet i gang med at opdatere sin vejledning om tredjelandsoverførsler. Vejledningen vil ifølge Datatilsynet indeholde en række praktiske eksempler, herunder om anvendelse af cloud-baserede løsninger. Vejledningen forventes offentliggjort i juli 2021."* Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 11, at "*Schrems II-afgørelsen giver anledning til en række overvejelser i forhold til den fremtidige overførsel af personoplysninger til lande uden for EØS, såkaldte tredjelande, og Datatilsynet er enig i behovet for praktisk vejledning i den henseende. På den baggrund har Datatilsynet – i regi af Det Europæiske Databeskyttelsesråd (EDPB) – udarbejdet anbefalinger om, (1) hvilke kriterier man som dataeksportør skal lægge vægt på*

				ved vurderingen af beskyttelsesniveauet i et tredjeland, og (2) hvilke supplerende foranstaltninger man som dataeksportør kan iværksætte, hvis beskyttelsesniveauet i et tredjeland vurderes utilstrækkeligt. Anbefalingerne indeholder en række eksempler vedrørende praktisk forekommende overførselssituationer, herunder anvendelse af cloud-baserede løsninger. Begge disse anbefalinger har til formål at give praktisk vejledning til dataeksportører i lyset af Schrems II-afgørelsen. Datatilsynet er endvidere i gang med at opdatere Datatilsynets egen nationale vejledning om overførsel til tredjelande efter Schrems II-afgørelsen. Datatilsynet har som led i arbejdet hermed afholdt et møde med relevante aktører med henblik på, at den opdaterede vejledning kan adressere de udfordringer, man som dataeksportør oplever i praksis. Vejledningen vil også komme til at indeholde en række praktiske eksempler, herunder om anvendelse af cloud-baserede løsninger, ligesom den vil adressere spørgsmålet om overførsel til Grønland. Vejledningen forventes offentliggjort i juli 2021. Datatilsynet vil i øvrigt løbende overveje, om der er behov for yderligere vejledning på området. I forhold til opfordringen om, at der nationalt eller i EU-regi foretages en generel vurdering af forholdene i relevante tredjelande, kan Datatilsynet oplyse, at man som dataeksportør er ansvarlig for at sikre sig, at man overholder reglerne i databeskyttelsesforordningen, når man overfører personoplysninger til et tredjeland. Det er derfor dataeksportøren, som selv skal sikre sig, at beskyttelsesniveauet i tredjelandet er tilstrækkeligt, hvilket også er bekræftet af EU-Domstolen i Schrems II-afgørelsen. Ved vurderingen af beskyttelsesniveauet i tredjelandet vil det være naturligt for

				dataeksportøren at involvere dataimportøren, men også f.eks. brancheorganisationer vil kunne spille en vigtig rolle i den forbindelse. Datatilsynet er opmærksom på, at det kan være en vanskelig vurdering at foretage i praksis, og det er også bagrunden for, at EDPB har udarbejdet anbefalinger herom. Det bemærkes i øvrigt, at ifølge databeskyttelsesforordningens artikel 45 er det EU-Kommissionen, der kan fastslå, at et tredjeland, et område i et tredjeland, en sektor i et tredjeland eller en internationale organisation beliggende i et tredjeland er sikkert, og dermed har et beskyttelsesniveau, som i det væsentlige svarer til det beskyttelsesniveau, der gælder i EU." Link til Datatilsynets opdaterede vejledning om tredjelandsoverførsler: https://www.datatilsynet.dk/Media/637626336767031457/Datatilsynet_Overf%C3%B8rsel_til_tredjelande_V3_1.0_juli2021.pdf
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 det modsatte er tilfældet. Er det så leverandørens ansvar, eller påhviler ansvaret fortsat os som dataansvarlige?*	Art. 32		Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 9-10, vedrørende brugen af underdatabehandlere, at *"Der kan dog aldrig foretages behandlinger, hverken med hensyn til type, formål og midler, der ikke til fulde er omfattet af – og tilgodeser – de databeskyttelsesretlige forpligtelser, der er fastsat i kontrakten mv. mellem den oprindelige databehandler og den dataansvarlige. Dette gælder, uanset hvor mange underdatabehandlere der benyttes. Hvis de behandlinger, hvortil der bruges en underdatabehandler, alene tilsiger anvendelse af en del af de samlede forhold, der udgør databeskyttelsesforpligtelsen i den oprindelige kontrakt mv., kan dette afspejles i aftalen med denne. Databeskyttelsesforordningens artikel 28, stk. 4, har til formål at*

				sikre, at der ikke ved kæder af databehandlere sker en udvanding af de oprindelige krav, den dataansvarlige har indføjet i kontrakten mv., over for den oprindelige databehandler, ligesom bestemmelsen holder den oprindelige databehandler ansvarlig for eventuel manglede overholdelse i de efterfølgende led i forholdet til den dataansvarlige. Det er væsentligt at erindre, at det er den dataansvarlige, der ultimativt står til ansvar for overholdelsen af forordningen i forhold til varetagelsen af de registreredes rettigheder, uanset om der benyttes ingen, en eller flere databehandlere."
71.	Datatilsynet tilbyder ikke mulighed for bindende forhåndssvar.*	Art 57		Justitsministeriet adresserer spørgsmålet i Delrapport II, hvor ministeriet sammenfattende på s. 2 skriver, at *"Sammenfattende er det Justitsministeriets vurdering, at det ikke vil være foreneligt med databeskyttelsesforordningen at indføre en generel ordning, hvor Datatilsynet skal meddele en bindende udtalelse om lovligheden af en påtænkt aktivitet, der indebærer en behandling af personoplysninger."* Dette er nærmere uddybet i afrapporteringens afsnit 4. Det er ifølge Justitsministeriet ikke mulighed for, at Datatilsynet kommer til at kunne give bindende forhåndssvar, da det vil påvirke tilsynets uafhængige opgavevaretagelse. Selv en formalisering af Datatilsynets mulighed for vejledning er Justitsministeriet skeptisk over for, at man kan lave. Justitsministeriet skriver på s. 8: *"(…) finder Justitsministeriet samlet set, at det er tvivlsomt, om der inden for databeskyttelsesforordningens rammer kan indføres national regulering, som formaliserer Datatilsynets konkrete vejledning, herunder muligheden for at fremkomme med ikke bindende forhåndstilkendegivelser.*

				Justitsministeriet bemærker i den forbindelse, at en endelig afklaring af spørgsmålet om, hvorvidt en sådan ordning kan indføres inden for forordningens rammer, henhører under EU-Domstolen.".
72.	Er presseaktiviteter i kommunen at sidestille med "behandling i journalistisk øjemed"? *	Art. 85		Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 58, generelt om journalistisk arbejde: *"... at medier generelt er undtaget fra de databeskyttelsesretlige regler. Hvis en behandling af personoplysninger er omfattet af lov om massemediers informationsdatabaser, er behandlingen således undtaget fra databeskyttelsesloven og databeskyttelsesforordningen, jf. databeskyttelseslovens § 3, stk. 4. I databeskyttelseslovens § 3, stk. 5-7, begrænses anvendelsen af databeskyttelsesreglerne også i forbindelse med, hvad der generelt kan karakteriseres som behandling, der sker i relation til "nyhedsformidling/journalistisk virksomhed".*
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		Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.

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 offentliges brug af data til myndighedsudøvelse, herunder ledelsesinformation, samt statistik.	Spørgsmålet er ikke adresseret i Justitsministeriets eller Datatilsynets delrapporteringer.
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.	Datatilsynet skriver i Datatilsynets bidrag til delrapport II, s. 6, at "*Datatilsynet har i de senere år brugt og bruger fortsat betydelige ressourcer på at rådgive og vejlede om de nye databeskyttelsesregler. Alligevel har de aktører, som har en interesse i Datatilsynets arbejde, oplevet, at tilsynets vejledning ikke har været tilstrækkelig konkret eller tilstrækkelig anvendelig i praksis. Datatilsynet har derfor foretaget en række organisatoriske tiltag for at styrke tilsynets vejledningsindsats yderligere, idet fokus på mere konkret og anvendelig vejledning nu er en del af tilsynets strategiske grundlag, hvilket gerne skulle bidrage til at sikre, at tilsynets vejledning også opleves sådan i praksis. Et af disse initiativer er, at Datatilsynet har oprettet en ny enhed – Vejledning og Informationssikkerhed – som bl.a. skal have et særligt fokus på at give mere konkret vejledning til virksomheder, myndigheder og borgere, herunder ved udarbejdelse af vejledninger, skabeloner, tjeklister mv. I forlængelse heraf har Datatilsynet nedsat to forskellige kontaktudvalg, som har til formål at skabe et tættere samspil mellem*

				tilsynet og centrale interessenter i såvel den private som den offentlige sektor, for at tilsynet kan være tæt på de problemer, som virksomheder og myndighederne står med, således at tilsynet bedre kan hjælpe dem til at overholde reglerne, hvilket i sidste ende også er til gavn for alle de borgere, hvis oplysninger det hele drejer sig om. Datatilsynet arbejder endvidere på at få offentliggjort så mange afgørelser som muligt på tilsynets hjemmeside. Afgørelserne vil blive offentliggjort med et lille resume, hvor tilsynet dels "oversætter" afgørelsen for offentligheden og dels angiver, hvad den dataansvarlige burde have gjort eller har gjort godt. Datatilsynet er således også opmærksom på at få fremhævet de dataansvarlige, som gør det godt og har udviklet nogle gode løsninger mv. Herudover arbejder Datatilsynet målrettet på at stille de samme budskaber til rådighed i flere forskellige formater, f.eks. vejledninger, korte tekster, små animerede videoer og podcasts, ligesom tilsynet i disse år har stor opmærksomhed på, hvordan tilsynet formulerer sig, og hvor øvelsen som på så mange andre områder består i at finde den rette balance, så formidlingen ikke kun er korrekt, men også til at forstå. Dette har bl.a. betydet, at Datatilsynet har valgt at ansætte flere kommunikationsmedarbejdere."
76.	Behov for afklaring eller forenkling af GDPR-reglerne • Behov for flere generelle redskaber, fx hvilke regler en kontor medarbejder generelt skal overholde for at være inden for GDPR (dagligdagsting).*	GDPR generelt		Se række 75.