Digitaliseringsministeriet
Att.: Lucas Bay Nielsen (LBN@digmin.dk) og
Johannes Ejerskov Pedersen (JEP@digmin.dk)

Dato: 11. december 2025

Sags ID: SAG-2025-04903
Dok. ID: 3641952

E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk


## KL's høringssvar – Generel Digital Omnibus

Digitaliseringsministeriet har den 20. november 2025 sendt EU-Kommissionens forslag til en general digital omnibus i høring. Forslaget indgår i Kommissionens samlede digitale lovgivningspakke og indeholder en række initiativer til at modernisere EU's digitale regelsæt. Ministeriet har oplyst, at det koordinerer regeringens høringssvar.

Ud over de generelle eventuelle bemærkninger til forslaget er KL blevet bedt om at udarbejde et kort resumé af de væsentligste anbefalinger, som kan indgå i regeringens grund- og nærhedsnotat til Folketinget.

KL vil indledningsvis bemærke, at nærværende høringssvar udgør KL's foreløbige bemærkninger. På trods af at høringsfristen er blevet forlænget med én uge, har den samlede tidsramme været forholdsvis kort. KL kan derfor få behov for at vende tilbage med yderligere bemærkninger til specialudvalget og vil eventuelt sende supplerende bemærkninger til Kommissionen i begyndelsen af det nye år.

### Resumé

KL støtter en forenkling og harmonisering af de digitale regelsæt og ser positivt på, at databeskyttelsesforordningen moderniseres. Forslaget fokuserer især på at styrke private virksomheders muligheder for at udvikle og anvende AI. Det er imidlertid centralt for kommunerne, at moderniseringen også tydeligt omfatter offentlige myndigheder, som i stigende grad har behov for at bruge AI i deres opgaveløsning, herunder til beslutningsstøtte.

KL anbefaler en tydeligere afgrænsning af "personoplysninger" og "pseudonymiserede data" samt større fleksibilitet ved utilsigtet behandling af særlige kategorier af oplysninger i AI-løsninger. KL støtter også muligheden for at afvise indsigtsanmodninger, der udgør chikane eller misbrug, og foreslår, at oplysningspligten – særligt i forbindelse med AI – gentænkes og gøres mere praktisk anvendelig. Derudover peger KL på behovet for en certificeringsordning for leverandører.

Endelig ser KL positivt på forslaget om et fælles "EU-single-entry-point", så kommuner kan indberette sikkerhedsbrud ét sted – også når bruddet omfatter flere regelsæt.

Dato: 11. december 2025

Sags ID: SAG-2025-04903
Dok. ID: 3641952

E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk


**Generelle bemærkninger**

Forslaget til den digitale omnibus indeholder en række ændringer af bl.a. databeskyttelsesforordning (EU) 2016/679 med det formål at skabe større forenkling samt at harmonisere det digitale regelsæt i EU.

KL støtter forenkling og harmonisering af de forskellige digitale regelsæt, og at der arbejdes for mere tydelige og anvendelige databeskyttelsesretlige regler, som kan lette de administrative byrder, der i dag er forbundet med overholdelsen af databeskyttelsesforordningen.

Forslaget lægger vægt på, at udvikling af AI-systemer og AI-modeller er central for innovation og økonomisk vækst. Det fremhæves derfor også, at behandling af personoplysninger i forbindelse med udvikling af AI i visse tilfælde vil kunne baseres på "legitim interesse" efter artikel 6, stk. 1, litra f, i databeskyttelsesforordningen. Med andre ord åbnes der for et mere fleksibelt behandlingsgrundlag, som kan understøtte private aktørers udvikling og brug af AI-løsninger. Det bemærkes imidlertid, at anvendelsen af artikel 6, stk. 1, litra f, som det altovervejende udgangspunkt ikke omfatter offentlige myndigheder.

Det er efter KL's opfattelse vigtigt, at offentlige myndigheder har tilsvarende klare og smidige muligheder for at udvikle og bruge AI-modeller og AI-systemer, særligt i lyset af at sådanne teknologier i stigende grad forventes at indgå i kommunernes opgaveløsning. I dag vil udvikling og brug af AI i offentligt regi ske med hjemmel i artikel 6, stk. 1, litra e, forudsat at der foreligger et supplerende nationalt retsgrundlag efter artikel 6, stk. 3. Det indebærer, at der skal etableres særskilte hjemler i dansk ret – et arbejde der allerede pågår – men som er forbundet med betydelig kompleksitet og derfor forsinker udvikling og ibrugtagning af nye teknologier.

Hvis Kommissionens forslag gav en udtrykkelig hjemmel i databeskyttelsesforordningen, der – i lighed med litra f for private – også understøttede offentlige myndigheders udvikling og anvendelse af AI til bl.a. beslutningsstøtte, ville medlemsstaterne i højere grad kunne sikre en ensartet og effektiv praksis uden behov for omfattende nationale særhjemler. Alternativt bør forslaget som minimum tydeliggøre, at offentlige myndigheder kan foretage tilsvarende behandlinger med hjemmel i artikel 6, stk. 1, litra e, når betingelserne i artikel 6, stk. 3, er opfyldt, så det står klart, at forslaget ikke utilsigtet stiller offentlige myndigheder ringere end private aktører.

Endvidere oplever kommunerne fortsat, at databeskyttelsesforordningen medfører betydelige administrative byrder og at efterlevelsen af reglerne er ressourcekrævende. Den udfordring bør anerkendes, og den offentlige sektor, herunder kommunerne, bør tænkes langt tydeligere ind i det videre arbejde med forenklingen af databeskyttelsesforordningen.

Det er positivt, at Kommissionen med NIS2-ændringsforslag vil forenkle og harmonisere indberetningen af sikkerhedshændelser på tværs af EU-reguleringer ved at etablere ét fælles "single-entry-point", da dette kan reducere den administrative byrde for kommunerne.

Dato: 11. december 2025

Sags ID: SAG-2025-04903
Dok. ID: 3641952

E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk


For at forslaget om ”single-entry-point” kan blive en reel forbedring for kommunerne, skal der sikres høj datasikkerhed, klarhed om indberetningskriterierne og garanti for, at kommuner kan indberette på dansk uden risiko for utilsigtet offentlighed.

**Ændringer til databeskyttelsesforordningen (EU) 2016/679 (GDPR) – bemærkninger til artikel 3**

**Bemærkninger til artikel 3, afsnit 1, artikel 4 - Definitioner**

KL forstår forslaget til ændring af artikel 4 sådan, at oplysninger kun vil være personoplysninger for en given aktør, hvis denne faktisk kan identificere personen med midler, der med rimelighed kan anvendes.

KL bemærker, at det bør præciseres, hvornår oplysninger ikke længere anses som personoplysninger. Gælder ændringen også i tilfælde, hvor kun en anden aktør – fx staten eller en leverandør – har mulighed for identifikation? Hvordan skal formuleringen ”midler, der med rimelighed kan anvendes” (“by means reasonably likely to be used”) forstås i praksis?

En klar afgrænsning vil styrke kommunernes mulighed for at arbejde hensigtsmæssigt med pseudonymiserede eller aggregerede datasæt, når kommunen ikke selv kan identificere personen. Det vil efter KL’s opfattelse fremme en mere praktisk anvendelse af reglerne uden at svække beskyttelsen af borgernes data.

**Bemærkninger til artikel 3, afsnit 3, artikel 9 – Særlige kategorier af personoplysninger**

KL ser positivt på, at forslaget giver kommunerne mere fleksibilitet, når de udvikler og bruger AI-systemer. I praksis kan der i store datamængder utilsigtet indgå særlige kategorier af personoplysninger – for eksempel helbredsoplysninger eller oplysninger om religion eller politisk overbevisning.

Forslaget lægger op til, at når f.eks. kommunerne har sikret, at utilsigtede særlige kategorier af personoplysninger ikke kan komme frem i AI-systemets output, vil kommunerne ikke automatisk være forpligtet til at fjerne sådanne oplysninger, hvis det i realiteten kræver, at hele AI-systemet eller AI-modellen skal bygges om eller gentrænes fra bunden.

Dette forslag om øget fleksibilitet er vigtig, fordi kommunerne skal kunne udvikle sikre og ansvarlige AI-løsninger, hvor også de særlige kategorier af data, der er nødvendige for at teste og kvalitetssikre systemerne, kan indgå. Hvis kravet om at fjerne selv meget små, utilsigtede mængder af særlige kategorier af personoplysninger i AI-systemet eller i AI-modellen er så omfattende, at systemet skal laves helt om, risikerer det at gøre udviklingen af AI både dyrere og mindre realistisk for kommunerne.

Det er samtidig vigtigt, at fleksibiliteten ikke kun gælder under selve udviklingen, men også når AI-systemet sættes i drift og bruges i praksis til administration og sagsbehandling mv. AI-systemer kan ændre sig over

Dato: 11. december 2025

Sags ID: SAG-2025-04903
Dok. ID: 3641952

E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk


tid, og kommunerne skal løbende kunne håndtere utilsigtede datafund uden at skulle starte forfra.

Endelig anbefaler KL, at forslaget ledsages af klare retningslinjer for, hvornår det anses for en "uforholdsmæssig stor indsats" at fjerne utilsigtede særlige kategorier af personoplysninger fra et AI-system. Sådanne retningslinjer vil sikre en ensartet praksis og gøre det tydeligere for kommunerne, hvornår de kan anvende alternative beskyttelsesforanstaltninger i stedet for at bygge eller træne AI-systemet helt om.

**Bemærkninger til artikel 3, afsnit 4. Artikel 12 i GDPR – Gennemsigtighed og indsigtsanmodninger**

KL støtter forslaget om at ændre artikel 12 i databeskyttelsesforordningen, så kommuner kan afvise anmodninger om indsigt, der er åbenbart grundløse, overdrevne eller udtryk for chikane og misbrug.

I praksis vil det kunne betyde, at kommunerne ikke skal bruge store mængder tid og ressourcer på henvendelser, der ikke reelt handler om beskyttelse af borgernes data, men som primært har til formål at belaste systemet. Det er vigtigt, at meget brede eller upræcise anmodninger kan vurderes som overdrevne, da de ofte kræver uforholdsmæssigt store ressourcer at behandle.

**Bemærkninger til artikel 3, afsnit 5. Artikel 13 i GDPR – Oplysningspligten**

KL har forstået forslaget sådan, at der i artikel 13 vil blive tilføjet et nyt stk. 5, der giver mulighed for at fravige oplysningspligten, når oplysninger anvendes til forskning, og det er umuligt eller uforholdsmæssigt ressourcekrævende at informere de registrerede direkte.

KL foreslår, at den foreslåede undtagelse fra oplysningspligten ikke kun begrænses til forskningsformål, men også tydeligt kommer til at omfatte udvikling og forbedring af AI-systemer og AI-modeller. Kommunerne har et stigende behov for at bruge data fra eksisterende sager for at kunne udvikle sikre, retvisende og ansvarlige AI-løsninger. Her er individuel underretning af alle berørte borgere ofte uforholdsmæssigt byrdefuldt.

KL foreslår derfor, at forslaget suppleres med en mulighed for, at offentlige myndigheder – herunder kommuner – kan opfylde oplysningspligten gennem central og generel information, eksempelvis via et offentligt opslag på kommunens hjemmeside, som orienterer om, at borgeres oplysninger kan indgå i udvikling og forbedring af AI-løsninger. En sådan model vil både understøtte kravet om gennemsigtighed og samtidig gøre det mere praktisk muligt at udvikle AI.

KL skal desuden fremhæve, at det i en kommunal kontekst – og hvor offentlige myndigheder i øvrigt træffer afgørelser – må anses for påregneligt for borgerne, at oplysninger fra deres sager kan blive brugt i nye, men relaterede sammenhænge. Det gælder f.eks. når kommunen gennemgår tidligere afgørelser for at sikre kvalitet, ensartet praksis og ligebehandling. At oplysninger fra en ældre sag kan blive anvendt til at forbedre

Dato: 11. december 2025

Sags ID: SAG-2025-04903
Dok. ID: 3641952

E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk


kommunens arbejdsgange eller kvalitetssikre afgørelser, ligger inden for det, borgere med rimelighed kan forvente af en offentlig myndigheds databehandling.

KL har tidligere i 2020 i forbindelse med Justitsministeriets høring vedrørende evaluering af anvendelsen af GDPR og databeskyttelsesloven peget på, at kommunerne generelt oplever betydelige udfordringer med at navigere i oplysningspligten efter artikel 13 og 14 – herunder vurderingen af, hvornår der er tale om et nyt formål, hvor snævert formål skal defineres, og hvor detaljeret oplysningerne skal gives. I praksis indebærer dette en risiko for enten for brede formålsvurderinger, som svækker gennemsigtigheden, eller for snævre vurderinger, som medfører gentagne og unødigt omfattende beskeder til borgerne. Samlet set efterlyses det, at oplysningspligten gentænkes, så den kan opfyldes på mere praktisk anvendelige måder.

**Bemærkninger til artikel 3, afsnit 8. Artikel 33 i GDPR – Anmeldelse af databrud**

KL ser positivt på, at forslaget lægger op til at gøre reglerne i artikel 33 og 34 om brud på persondatasikkerheden mere ensartede, at der kommer en skabelon for databrud, og at fristen for at anmelde et brud bliver forlænget fra 72 til 96 timer.

Det er meget vigtigt, at forslaget sikrer, at man kun skal anmelde et brud ét sted og inden for samme tidsfrist – også selvom bruddet samtidig er omfattet af andre regler, og det er derfor i god tråd med forslaget i NIS2-direktivet om en samlet indberetningsportal ”single-entry-point”.

KL skal bemærke, at i Danmark er det muligt at indberette til flere myndigheder ét sted på Virk.dk. Hvis der kun er én samlet anmeldelsespligt, mindskes det administrative arbejde, og myndighederne kan bruge tiden på at håndtere selve bruddet i stedet for at indsende flere parallelle anmeldelser. Derfor er det afgørende, at de endelige regler tager højde for, hvordan de spiller sammen med andre nationale og EU-regler om anmeldelser.

**Bemærkninger til artikel 3, afsnit 9. Artikel 35 - Konsekvensanalyse**

KL bemærker, at forslaget indebærer etableringen af en fælles EU-liste over behandlingsaktiviteter, der kræver en konsekvensanalyse, samt et krav om, at tilsynsmyndighederne i medlemslandene offentliggør en liste over aktiviteter, der ikke kræver en sådan analyse.

KL opfordrer til klarhed og præcisering af kriterierne for, hvornår en behandlingsaktivitet skal underlægges en konsekvensanalyse, herunder hvilke forhold der skal tillægges vægt, og om den fælles EU-liste vil være udtømmende. I kombination med en fælles skabelon — der bør sikre høj databeskyttelse og samtidig begrænse unødigt administrativt arbejde — samt en tydelig metode for udarbejdelse af konsekvensanalyser, vil initiativet muligvis kunne medvirke til at gøre det lettere i praksis at håndtere konsekvensanalyser i kommunerne.

Dato: 11. december 2025

Sags ID: SAG-2025-04903
Dok. ID: 3641952

E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk


**Bemærkninger til artikel 3, afsnit 10. Artikel 41a – Pseudonymisering**

I forbindelse med anvendelse af data til udvikling og test af AI-systemer åbner forslaget op for en begrænset mulighed for, at pseudonymiserede oplysninger – når de opfylder klart definerede kriterier og reelt ikke kan føre til re-identifikation – kan behandles som ikke-personoplysninger for bestemte formål og aktører. Da der efter forslaget er tale om helt afgrænsede tilfælde, der skal fastsættes af Kommissionen, vil KL opfordre regeringen til at søge klarhed om, hvorvidt forslaget vil finde anvendelse for kommunerne.

**Bemærkninger til artikel 3, afsnit 15. Artikel 88c – behandling af personoplysninger til udvikling og drift af AI-systemer**

KL forslår, at det tydeliggøres, at intentionen med artikel 88c også omfatter offentlige myndigheders behandlingen af personoplysninger i forbindelse med udvikling og drift af AI-systemer, og at retten til at træne AI-modeller med persondata gøres mere klar og ubetinget.

For det er imidlertid uklart, om forslaget også omfatter offentlige myndigheder, da behandlingsgrundlaget i artikel 6, stk. 1, litra f, om legitime interesser – som nævnt ovenfor – som den altovervejende hovedregel ikke gælder for offentlige myndigheder. For at undgå denne usikkerhed bør det derfor tydeliggøres, at forslaget også omfatter den offentlige sektor, herunder kommunerne. En sådan afklaring vil have stor betydning for kommunernes muligheder for at anvende AI, herunder til beslutningsstøtte, på et klart og tydeligt retsgrundlag.

**Yderligere bemærkninger til databeskyttelsesforordningen**

**Rollefordeling og dataansvar**

Kommunerne oplever fortsat betydelig usikkerhed om rollefordelingen mellem dataansvarlig, databehandler og fælles dataansvar i en lang række samarbejds- og leverandørsituationer. Selvom vi allerede i 2020 pegede på disse udfordringer, er kompleksiteten fortsat uændret i 2025.

De nuværende definitioner i GDPR af “dataansvarlig”, “databehandler” og “fælles dataansvarlige” er svære at anvende i praksis, særligt når kommunerne indgår i samarbejder med private leverandører, andre myndigheder eller aktører, der løser opgaver med både eget og kommunens formål. Det betyder, at der ofte bruges mange ressourcer på at afklare rollefordelingen.

Derfor er der fortsat behov for en forenkling af reglerne. Hvis uklarhederne består, bør det overvejes, om definitionerne i databeskyttelsesforordningen om dataansvarlige, databehandlere og fælles dataansvar skal præciseres, så rollefordelingen bliver lettere at anvende i praksis og bedre afspejler de samarbejdsformer, kommunerne indgår i.

Dato: 11. december 2025

Sags ID: SAG-2025-04903
Dok. ID: 3641952

E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk


**Certificerede leverandøraftaler**

For at rette op på den betydelige ubalance mellem store leverandører – herunder globale teknologivirksomheder – og dataansvarlige kommuner, bør der etableres en central, obligatorisk certificeringsordning for digitale løsninger og deres databehandlerkæder.

I dag står især mindre kommuner uden de tilstrækkelige juridiske og tekniske ressourcer til at forhandle ligeværdige aftaler med store databehandlere og til at kontrollere, om databehandlerkæden faktisk overholder databeskyttelsesforordningen i praksis. Det skaber en situation, hvor kommunerne kan risikere, at de ved at acceptere leverandørernes standardvilkår får en risiko for brud på GDPR-forpligtelserne.

En certificeringsordning – efter principper beslægtet med CE-mærkning eller MDR-godkendelse af medicinsk udstyr – vil sikre, at når en løsning én gang er godkendt, kan alle kommuner stole på, at både leverandøren og hele deres databehandlerkæde har dokumenteret overholdelse af GDPR, herunder at personoplysninger kun anvendes til de aftalte formål, og at data ikke utilsigtet overføres eller anvendes i strid med lovgivningen.

Med en sådan standardiseret ordning undgår kommunerne uforudsete ændringer i aftalegrundlaget, skjulte risici i databehandlerkæden eller vilkår, der viser sig at være uforenelige med databeskyttelsesforordningen. Det gør det muligt for kommunerne at indgå aftaler på et klart, trygt og forudsigeligt grundlag, der lever op til kravene, og det frigør ressourcer, så myndighederne kan fokusere på kernevelfærd og service til borgerne frem for at skulle gentage komplekse og ressourcekrævende juridiske vurderinger, som i dag udføres parallelt i hele EU. Der er således fortsat behov for, at staten eller EU tager ansvar for at finde løsninger, der ikke kan løses på kommunalt plan.

**Ændringer af NIS2-direktivet (EU) 2022/2555 - bemærkninger til artikel 5**

Udspillet til Omnibus på det digitale område indeholder forslag til at oprette en fælles og harmoniseret indgang til indberetning af cyberhændelser og lignende hændelser. Dette vil omfatte forpligtelser på bl.a. følgende EU-reguleringer: NIS2, GDPR, DORA og CRA.

I artikel 6 i den Generelle Digitale Omnibus fremlægger Kommissionen konkrete forslag til revision af Direktiv (EU) 2022/2555, dvs. NIS2-direktivet. Her fremgår, at forenklingen af hændelsesunderretning mv. etableres ved, at ENISA opretter et 'Single-entry-point' for relevante enheders hændelsesunderretninger.

Ambitionen er at samle underretningerne, således at administratoren og byrden for den enkelte enheder, der er underlagt underretningspligt, reduceres. Der er grundlæggende hensigtsmæssigt, at der er fokus på, at det skal være simpelt og gerne énstreget at foretage sikkerheds-relaterede hændelsesunderretninger.

Dato: 11. december 2025

Sags ID: SAG-2025-04903
Dok. ID: 3641952

E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk


For kommunerne vil et simpelt og effektivt underretnings-setup således som udgangspunkt være positivt. Samtidigt er hovedformålet med bl.a. NIS2-underretning at sikre enheder (og samfundet) imod spredning af cybertrusler samt negative og afledte konsekvenser via enheders forsyningskæder. Den kommunale sektor har derfor interesse i, at det sikres at den information og data, der overdrages til et centralt 'single-entry point' deles effektivt, sikkert og passende med nationale myndigheder, der har opgave i at træffe rette foranstaltninger tværgående, herunder at bidrage til at stoppe spredning via kommunikation og koordination samt egentlig bidrag til enheders hændelseshåndtering. Et centralt system bør således ikke være forsinkende led.

Der er særligt centralt at et 'single-entry point' iagttager størst mulig sikkerhed ift. håndtering af stærk kritiske oplysninger fra enheder (bl.a. danske kommuner) under angreb. De sårbarheder, der evt. blotlægges skal behandles varsomt, men samtidigt give afsæt for øget cybersikkerhed i bl.a. på tværs af den kommunale sektor. Indtrykket er, at enheder, der indberetter kritiske hændelser kan være underlagt krav om offentlighed ved aktindsigter. Dette kan dels være en sikkerhedsrisiko ift. at synliggøre evt. sårbarheder og iværksatte foranstaltninger, dels kan det i yderste instans betyde, at der samlet set indberettes færre hændelser. Der bør kunne garanteres, at indberetningen ikke i sig selv kan blive en sikkerhedstrussel for indberettende enheder.

Ift. kommunernes indberetninger – i henhold til de omfattede reguleringer – er det afgørende, at kommunerne kan indberette på dansk. Det forudsættes at være således, men løftes her som vigtigt opmærksomhedspunkt for at sikre datakvalitet og et tilstrækkeligt antal indberetninger.

Ved indberetninger til et 'Single-entry point' bør det sikres, at det er klart for indberettende enheder hvilke kriterier og formål, der er for de enkelte underretninger. Ift. NIS2 er det KL's indtryk, at der fortsat kan være tvivl hos enhederne om, hvilke og hvor mange hændelser, der skal indberettes. Dette hænger sammen med, at der fortsat opleves gråzoner i definitioner af kritikalitet af hændelser i NIS2-sammenhæng.

I ændringsforslaget til artikel 23a stk. 3, fremgår det, at de nationale CSIRTs og kompetente myndigheder inddrages i udvikling af specifikationerne til etablering af det "single-entry point". I den forbindelse bør det overvejes at inddrage enheder, der skal foretage indberetningerne – herunder kommunerne – for at sikre, at 'single-entry point' udvikles med brugerne for øje.

**Afsluttende bemærkninger**

Afslutningsvis bemærker KL, at den offentlige sektor – herunder kommunerne – bør indtænkes tydeligere i det igangværende europæiske arbejde med at skabe en mere fleksibel, risikobaseret og praktisk anvendelig GDPR-regulering. Ligesom virksomhederne har efterspurgt lempelser og klarere rammer, har kommunerne tilsvarende behov for en tidssvarende regulering, der gør det muligt at levere velfærd og løse lovbestemte opgaver og udvikle digitale løsninger på en effektiv og forsvarlig

måde. Samtidig er det vigtigt at sikre, at der ikke indføres nye bestemmelser, som skaber yderligere usikkerhed i kommunerne, når de skal vurdere risici og afgøre, om behandling af data lever op til de databeskyttelsesretlige regler.

KL vil også gerne understrege behovet for klare rammer for udvikling og brug af AI-systemer i den offentlige sektor. Uklare, overlappende og komplekse regelsæt skaber betydelig usikkerhed både i udviklingsarbejdet og i kommunernes daglige drift.

KL ser frem til dialog om, hvordan det digitale regelsæt i EU, herunder regler for data, AI og cybersikkerhed mv. kan moderniseres, så de europæiske regler spiller bedre sammen og understøtter innovation, digital udvikling og en effektiv offentlig sektor – samtidig med at borgernes rettigheder fortsat beskyttes.

KL deltager gerne i dialog og bidrager gerne til det videre arbejde.

Med venlig hilsen

Pia Færch
Kontorchef for Digitale projekter, Borgerservice & IT-arkitektur



E-mail: LOMJ@kl.dk
Direkte: 3370 3025

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk