Bech·Bruun

Sagsnr. 068387-0006 tmr/leas/akhu
Dok.nr. 21557588.1

DPO Audit

Køge Kommune

Den dataansvarlige
Køge Kommune
Torvet 1
4600 Køge
CVR-nr.: 29 18 93 74

Emne
DPO Audit

Dato
September 2019

Databeskyttelsesrådgiver (DPO)
Bech-Bruun Advokatpartnerselskab
CVR-nr.: 38 53 80 71
Langelinie Allé 35
2100 København Ø

Bech·Bruun

Indholdsfortegnelse

1. Indledning 3
1.1 De udvalgte emner 3
1.2 Grundlaget for DPO Audit 3
1.3 Metodik for DPO Audit rapporten 4
2. Sammenfatning af observationer og anbefalinger 4
3. Uddybning af observationer og anbefalinger 5

Bilag

Bilag 1: Spørgeskema om fortegnelser
Bilag 2: Spørgeskema om håndtering af databehandlere
Bilag 3: Spørgeskema om brud på persondatasikkerheden
Bilag 4: Gennemgang af databehandleraftaler

1. Indledning

Som led i aftalen om levering af DPO-service til Køge Kommune har Bech-Bruun som databeskyttelsesrådgiver (”DPO”), gennemført den årlige auditering (”DPO Audit”) af Køge Kommune.

Formålet med DPO Audit er at kontrollere Køge Kommunes overholdelse af databeskyttelsesforordningen, databeskyttelsesloven og dertil hørende praksis (”databeskyttelsesreglerne”).[1]

DPO Audit er tilrettelagt efter databeskyttelsesforordningens krav til det kontrolarbejde, der skal udføres af Bech-Bruun i rollen som DPO for Køge Kommune. DPO Audit er således gennemført ud fra den risikobaserede tilgang, som databeskyttelsesforordningen foreskriver. Det indebærer, at DPO Audit alene omfatter kontrol af udvalgte behandlingsaktiviteter hos Køge Kommune i relation til de udvalgte forretningsområder.

Resultat af den gennemførte DPO Audit danner grundlag for rapportering til Køge Kommunes øverste ledelse.

1.1 De udvalgte emner

For Køge Kommune er der som genstand for DPO Audit i 2019 valgt følgende emner:

1. **Fortegnelser**.
   Køge Kommunes håndtering af forpligtelsen til at føre fortegnelser over sine behandlinger af personoplysninger (databeskyttelsesforordningen artikel 30).
2. **Databehandlere**.
   Køge Kommunes håndtering af forpligtelsen til at indgå databehandleraftaler, indholdet af databehandleraftalerne samt Køge Kommunes kontrol med de anvendte databehandlere (databeskyttelsesforordningens artikel 28).
3. **Sikkerhedsbrud**.
   Køge Kommunes håndtering af brud på persondatasikkerheden samt evt. opfølgende skridt og awareness-aktiviteter (databeskyttelsesforordningens artikel 32, 33 og 34).

Inden for hvert af disse emner er der udtaget områder til nærmere stikprøvevis kontrol. Det fremgår af spørgeskemaerne, der vedlægges som bilag 1 - 3, hvilke områder der er udtaget til nærmere stikprøvevis kontrol.

1.2 Grundlaget for DPO Audit

Gennemgangen på hvert af de ovennævnte områder er sket på grundlag af:

- Køge Kommunes besvarelse af et spørgeskema udarbejdet af DPO samt materiale, som Køge Kommune skulle fremsende til DPO. De tre spørgeskemaer, som er udsendt og besvaret af Køge Kommune, er vedlagt som bilag 1 - 3 til denne rapport.
- Udvalgte stikprøver af, om databeskyttelsesreglerne er overholdt.
- Vurdering af, hvorvidt der forefindes skriftlige politiker, procedurer, retningslinjer og informationsmaterialer.

[1] Jf. databeskyttelsesforordningens artikel 39, stk. 2.

1.3 Metodik for DPO Audit rapporten

På baggrund af vores kontrol af de udvalgte områder, jf. afsnit 1.1. ovenfor, har vi udarbejdet en oversigt over vores væsentligste observationer samt anbefalinger til tiltag, som Køge Kommune bør igangsætte med henblik på fremadrettet at højne compliance-niveauet.

Vores sammenfatning fremgår af afsnit 2 nedenfor, og en mere detaljeret oversigt fremgår af afsnit 3 nedenfor. Oversigten indeholder en angivelse af relevant område, beskrivelse af observationerne, vores anbefaling samt en angivelse af compliance-niveau markeret med rød, gul og grøn.

Vi har modtaget kopi af de databehandleraftaler, som kommunen har indgået på udvalgte områder. Vi har udvalgt tre aftaler til en stikprøvevis gennemgang, hvor vi ser på fire spørgsmål og markerer med rød, gul eller grøn, hvorvidt aftalen efter vores vurdering håndterer spørgsmålet. Resultatet kan ses i bilag 4.

Det skal for god ordens skyld bemærkes, at der ikke er foretaget en fuldstændig gennemgang af Køge Kommunes efterlevelse af databeskyttelsesreglerne, herunder de modtagne databehandleraftaler mv.

1.3.1 Beskrivelsen af compliance-niveau

Compliance-niveau	Betydning
	Compliance-niveau er i strid med lovgivning eller retningslinjer fra Datatilsynet og/eller andre relevante myndigheder. Manglende overholdelse kan medføre bøde.
	Compliance-niveau er i strid med anbefalinger fra Datatilsynet og/eller andre relevante myndigheder. Manglende overholdelse kan medføre kritik/advarsel. Risikoen for bøder er ikke høj, men kan ikke udelukkes.
	Compliance-niveau overholder lovgivning samt retningslinjer og anbefalinger udstedt af Datatilsynet og/eller andre relevante myndigheder, men det kan i nogle tilfælde med fordel forbedres af hensyn til kommunens retsstilling.

2. Sammenfatning af observationer og anbefalinger

Resultatet af den gennemførte DPO Audit viser, at Køge Kommune har gennemført en række tiltag og foretaget en række handlinger, som medvirker til kommunens efterlevelse af databeskyttelsesreglerne i relation til de udvalgte emner.

Den gennemførte DPO Audit har imidlertid også vist, at det nuværende compliance-niveau ikke er fuldt ud tilstrækkeligt til at sikre og dokumentere Køge Kommunes overholdelse af databeskyttelsesreglerne.

I afsnit 3 gennemgås Køge Kommunes compliance på i alt 39 punkter. Kommunen har fået 28 grønne, 7 gule og 4 røde vurderinger.

Henset til ovenstående er det vores anbefaling, at Køge Kommune bør:

1) Udforme og iværksætte en plan for gennemgang og opdatering af kommunens fortegnelser.
2) Sikre at manglende databehandleraftaler bliver indgået, og at databehandlere, som herefter kommer til, ligeledes bliver håndteret i overensstemmelse med databeskyttelsesreglerne.
3) Iværksætte tilsyn med de databehandlere, som kommunen anvender. Opgaven kan tilrettelægges ud fra en risikobaseret tilgang.
4) Overveje om der skal ske opdatering af de databehandleraftaler, som har fået røde eller gule markeringer ved vores gennemgang (bilag 4). Under alle omstændigheder bør kommunen håndtere disse spørgsmål bedre i fremtidige aftaler.
5) Regelmæssigt gennemgå – og efter behov opdatere – kommunens procedurer, retningslinjer, standardaftaler og standardbreve, så der tages højde for udviklingen i bl.a. kravene fra Datatilsynet.

Den mere detaljerede oversigt fremgår som nævnt under afsnit 3 nedenfor.

3. Uddybning af observationer og anbefalinger

Fortegnelser			
Underemne	**Observation**	**Anbefaling**	**Niveau**
Procedurer.	Ja. Informationssikkerhedshåndbogens kapitel 8 Styring af aktiver, udstikker retningslinje for førelse af fortegnelser.	For at sikre, at kommunens fortegnelser vedvarende føres i overensstemmelse med databeskyttelsesreglerne, anbefaler vi, at kommunen har retningslinjer for førelse af fortegnelser.	
Placering af ansvar.	Ja. Styregruppeformand Informationssikkerhed. Direktør Lene Østergaard Lunde, Kultur- & Økonomiforvaltningen. IT- & Digitaliseringschef Ivan Harreskov, Kultur- & Økonomiforvaltningen.		
Brug af KL's standarder.	Ja. Kommunen anvender KL's standardfortegnelse og konsekvensanalyseværktøj.	Køge Kommune bør være opmærksom på, at KL har opdateret standardfortegnelserne senest i maj 2019, så de nu foreligger i version 1.2. Køge Kommune bør endvidere være opmærksom på, at Datatilsynet har bebudet, at de vil opdatere deres vejledning vedrørende fortegnelseskravet i forlængelse af de tilsyn, som blev foretaget i efteråret 2018.	
Lagring i specifik løsning.	Ja. Alle oplysninger arkiveres i Køge Kommunes ESDH-system eDoc, i et beskyttet område, der kun kan tilgås af medlemmerne af		

	Informationssikkerhedsstyregruppen og Informationssikkerhedskoordinator.		
Fortegnelser som dataansvarlig.	Kommunen har udformet et samlet forretningsoverblik, hvori bl.a. indgår 16 fortegnelser baseret på standard-fortegnelserne fra KL. Kommunen er færdig med at udforme fortegnelser som dataansvarlig. Der er vedlagt de fortegnelser, baseret på KL's standard, som DPO har anmodet om at se.		
Fortegnelser som databehandler.	Nej. Køge Kommune har ikke udformet fortegnelser for aktiviteter som databehandler. Køge Kommune har én aftale som databehandler og er i gang med at undersøge om sekretariatsbetjening for de selvejende institutioner kræver en databehandleraftale.	Kravet om fortegnelser som databehandler, hvis kommunen har aktiviteter som en sådan, findes i databeskyttelsesforordningens artikel 30, stk. 2. Køge Kommune bør skaffe sig overblik over, om der mangler fortegnelser, og udforme disse.	
Stikprøver vedrørende specifikke fortegnelser.	KL's standardfortegnelser er brugt med minimal udfyldelse. Felter for delt dataansvar og for tredjelandsoverførsler fremstår uden individuelt indhold.	Køge Kommune bør udfylde alle felter. Hvis et felt ikke er aktuelt, kan der fx skrives "ikke aktuelt" eller "der sker ikke tredjelandsoverførsel".	
Databehandlere			
Underemne	**Observation**	**Anbefaling**	**Niveau**
Procedurer.	Ja. Køge Kommune har vedlagt fem dokumenter: 1. Skabelon til databehandleraftale 2. Vejledning til databehandleraftale 3.Vejledning og anbefaling (DIGIT) 4. Køge Kommunes skabelon for organisationers Databehandleraftale med kommunen. 5. IT-Sikkerhedstjekliste.	Kommunens procedurer og retningslinjer bør regelmæssigt gennemgås og efter behov opdateres, så der tages højde for udviklingen i bl.a. kravene fra Datatilsynet.	
Placering af ansvar.	Ja. Ansvaret for håndtering af databehandlere, herunder at der er databehandleraftaler og der foretages tilsyn med databehandlere, ligger hos de enkelte forvaltninger.		
Lagring i specifik løsning.	Ja. Databehandleraftaler skal lagres i Køge Kommunes ESDH-system eDoc. Køge Kommune arbejder på at alle aftaler skal registreres i KITOS. Det vil blive et fokus-punkt i Q3-Q4.		

Databehandler-aftaler.	90 databehandleraftaler. Der udstår databehandleraftaler på følgende områder: 1) Børn & Unge Forvaltningen: Systemer der benyttes i digital undervisning i folkeskolen, da der anmodes om nye systemer og samarbejdspartner. 2) Der mangler 3 aftaler i BUF og 17 på skoleområdet. 3) Teknik & Miljø Forvaltningen: Mangler at lukke 13 aftaler og forventer at være færdig ultimo maj. I alt 34 databehandleraftaler mangler at blive indgået. Disse forventer Køge Kommune forventer er indgået ultimo Q2-2019 Skoleafdelingen har yderligere 25 leverandører, som de ikke mener der skal indgås aftale med. De ligger til juridisk vurdering.	Kravet om databehandleraftaler findes i databeskyttelsesforordningens artikel 28, stk. 3. Køge Kommune bør sikre sig, at de manglende databehandleraftaler bliver indgået. Køge Kommune bør afklare, om der skal være databehandleraftaler på de uafklarede områder i skoleafdelingen, hvis dette ikke allerede er sket, og i givet fald sørge for at aftalerne bliver indgået. Vi anbefaler generelt, at kommunen regelmæssigt gennemgår og eventuelt opdaterer sin standard-databehandleraftale o.l., så der tages højde for udviklingen i bl.a. kravene fra Datatilsynet. Datatilsynet har i forbindelse med tilsyn hos en kommune[2] bemærket, at det under alle omstændigheder klart bør fremgå, om der behandles oplysninger af følsom eller fortrolig karakter, idet dette vil have en betydning for eksempelvis fastlæggelsen af sikkerhedsforanstaltninger og den dataansvarliges løbende tilsyn med behandlingen hos databehandleren.	
Fælles dataansvar.	Nej. Kommunen har ikke fælles dataansvar.	Køge Kommune bør være opmærksom på, at der er fælles dataansvar for flere centrale løsninger på undervisningsområdet. Her er databehandleraftale imidlertid ikke nødvendig, da Styrelsen for IT og Læring har reguleret forholdene i cirkulæreskrivelser.	
Procedurer for tilsyn med databehandlere.	Nej. Køge Kommune forventer at have en procedure klar i juni måned, hvor vi samtidig starter rykkerprocedure op på de aftaler, som vi ikke har modtaget revisionserklæring på.	Køge Kommune bør have retningslinjer eller procedurer, der sikrer, at der føres tilsyn med databehandlere. Efter ikrafttræden af GDPR skal Køge Kommune leve op til ansvarlighedsprincippet. Derfor bør	

[2] Datatilsynets udtalelse af 5. august 2019 til Viborg Kommune, j.nr. 2018-423-0022.

		Køge Kommune overveje, om der for de enkelte databehandlere er behov for at føre tilsyn med andet end sikkerhed, herunder de generelle principper for behandling af personoplysninger, og om der foreligger gyldigt overførselsgrundlag for eventuelle overførsler af personoplysninger til tredjelande.	
Tilsyn med databehandlere i 2018.	Ja. Køge Kommune har ført tilsyn med 2 databehandlere i 2018. Tilsynet er udført ved modtagelse af revisorerklæringer. Resultatet er vurderet som tilfredsstillende.	Også under den tidligere persondatalov var der krav om tilsyn med databehandlere. Dette fulgte direkte af loven. Under GDPR følger kravet af forordningens princip om ansvarlighed. På den baggrund må det lægges til grund, at der burde være udført flere tilsyn i 2018.	
Tilsyn med databehandlere i 2019.	Nej. Køge Kommune modtog først sent revisorerklæring fra KMD og er i gang med at behandle erklæringerne. Der vil blive rettet spørgsmål til revisionsbemærkninger i ISAE 3000 (efter 25 maj 2018). Der er modtaget enkelte revisionserklæringer løbende. Efterhånden som kommunen modtager revisionserklæringerne, vil disse blive læst og godkendt. Hvis de ikke indgår, er der rykkerprocedure i juni. Databehandlere med aftale uden revisionserklæring vil modtage en mail, hvor de skal bekræfte at de overholder præmissen for aftalen. Primo maj måned kontaktes alle ledere/medarbejdere i Køge Kommune, der er ansvarlige for indgåelse af databehandleraftaler for at deltage i en detaljeret gennemgang af de enkelte aftaler. Vores interne audit har afdækket et behov for en samlet registrering af alle databehandleraftaler. Der er behov for at skærpe og udvide proceduren for indgåelse af- og kontrol af databehandleraftaler.	Kravet om tilsyn med databehandlere følger af forordningens princip om ansvarlighed. Køge Kommune bør derfor bør foretage tilsyn med de databehandlere, som kommunen anvender. Opgaven kan tilrettelægges ud fra en risikobaseret tilgang. Hvis Køge Kommune iværksætter arbejdet i 2019 vil det være muligt for kommunen at komme helt eller delvist i compliance. Den skitserede fremgangsmåde, hvor der sendes en mail til databehandlere uden revisionserklæring, hvor de skal bekræfte, at de overholder præmissen for aftalen, vil efter vores vurdering ikke i sig selv være tilstrækkelig. Der bør stilles mere specifikke spørgsmål. Vi anbefaler, at der foretages en vurdering af, hvordan tilsynet skal gribes an i forhold til de enkelte databehandlere.	

Dokumentation for udført tilsyn med databehandler (stikprøve vedrørende databehandlere, der begynder med bogstavet K).	Køge Kommune har fremsendt dokumentation i form af en mail fra april 2018 med noter vedrørende kommunens gennemgang af KMD revisionserklæringerne fra PwC vedr. 2017, hvor kommunen havde kommentarer til en ISAE 3000 rapport og besluttede at følge op på svar og spørge ind til et område. Herudover har vi modtaget en notits med en række spørgsmål, som Køge Kommune i april 2019 har stillet i forhold til revisionsrapporterne ISAE 3000 og 3403 vedr. 2018 udarbejdet af PwC.	Vi lægger til grund, at Køge Kommune også anvender mindst en yderligere databehandler begyndende med bogstavet K (KOMBIT). Kommunen burde derfor være i besiddelse af dokumentation for udført kontrol. Vi anbefaler, at Køge Kommune, som det også sker, ud over det materiale, fx revisorerklæringer, der modtages, også dokumenterer kommunens egen vurdering af det modtagne og kommunens eventuelle opfølgende skridt. Vi anbefaler, at kommunen sammenholder de modtagne revisorerklæringer med de indgåede databehandleraftaler. Vi anbefaler endvidere, at kommunen – hvor dette er relevant – er særlig opmærksomhed på databehandlerens håndtering af eventuelle underdatabehandlere og tredjelandsoverførsler.	

Sikkerhedsbrud			
Underemne	**Observation**	**Anbefaling**	**Niveau**
Procedurer.	Ja. ”Procedure for håndtering af informationssikkerhedshændelser og brud” er fremsendt til DPO.		
Placering af ansvar.	Ja. Ansvaret er placeret jf. dokument ”Om sikkerhedsbrud”. Ansvaret for anmeldelse af databrud håndteres decentralt i de enkelte forvaltninger. Afdelingschefen fra den enkelte forvaltning er altid indover anmeldelse og underretning. i-sikkerhedskoordinator sikrer at alle brud dokumenteres.		
Lagring i specifik løsning.	Informationssikkerhed har et lukket område i kommunens ESDH-system eDoc, hvor alle sikkerhedshændelser og brud registreres. Her samles dokumentation om den enkelte sag. Samtidig registreres hændelser og brud i Excel fil med alle relevante		

	oplysninger jf. datatilsynets vejledning omkring dokumentationspligt. Samtidig registrerer Hændelser/brud registreres anonymiseret i ISMS med fokus på hvilket system, der er involveret i hændelsen/bruddet.		
Udpegelse af kontaktpunkter for kommunens medarbejdere.	Ja. Den enkelte medarbejder kontakter nærmeste leder. Hvis denne ikke er til rådighed, så kan afdelingschefen for forvaltningen kontaktes. Informationssikkerhedskoordinator kan også kontaktes.		
Udpegelse af kontaktpunkter for kommunens databehandlere.	Ja. - Dpo.koege@bechbruun.com - raadhus@koege.dk - Informationssikkerhed@koege.dk		
Awareness-aktiviteter omfattende, hvad der udgør sikkerhedsbrud, og hvordan de skal håndteres?	Ja: I 2018 gennemgik alle medarbejdere i Køge Kommune en quiz omkring informationssikkerhed. Alle nye medarbejdere skal også gennemføre Quiz.		
Hvornår fandt aktiviteterne sted?	2018		
Hvor stor en del af kommunens medarbejdere er nået med aktiviteterne (sæt kryds)?	75-100 %		
Undervisning eller træning af medarbejdere omfattende informationer om, hvad der udgør sikkerhedsbrud, og hvordan de skal håndteres.	Ja. Informationssikkerhedskoordinator deltager på personale/team møder, hvor emnet ofte er sikkerhedshændelser/brud. Der tages udgangspunkt i pjecen ”Informationssikkerhed”, og efterfølgende relateres sikkerhedsarbejdet til den enkelte afdelings udfordringer.		
Hvornår fandt undervisning	Den finder sted løbende. Der planlægges undervisning af alle		

og/eller træning sted?	medarbejdere i Q3-2019, hvor emnet er sikkerhedshændelser og brud.		
Hvor stor en del af kommunens medarbejdere er nået (sæt kryds)?	0-25 %	Køge Kommune bør øge aktivitetsniveauet mht. undervisning, herunder ved den omtalte undervisning, der er planlagt i Q3-2019.	
Modtaget informationsmateriale.	DPO har modtaget - pjecer om Informationssikkerhed, hvori indgår afsnit om håndtering af sikkerhedsbrud, - teksten "Om sikkerhedsbrud", som bl.a. beskriver, hvem der gør hvad i forhold til sikkerhedsbrud og -hændelser - tekst "Værktøjskasse" med vejledning og links.	Køge Kommune bør regelmæssigt gennemgå de anvendte kampagne- og træningsmaterialer og foretage eventuelle nødvendige optageringer i lyset af den viden, som pt. findes om sikkerhedsbrud.	
Anmeldelse af brud til Datatilsynet. Er det kommunens vurdering, at den har anmeldt alle brud, som skal anmeldes efter artikel 33, stk. 1?	Antal: 13. Ja, det er Køge Kommunes vurdering. Hvis der har været tvivlsspørgsmål, så er DPO kontaktet for gode råd.	Udgangspunktet er, at brud på persondatasikkerheden skal anmeldes til Datatilsynet. Kun når det er usandsynligt, at bruddet indebærer risiko for personer rettigheder eller frihedsrettigheder, kan anmeldelse undlades. På baggrund af Datatilsynets praksis anbefaler vi, at der foretages anmeldelse i tilfælde, hvor fortrolige oplysninger er fremsendt usikkert via internettet (uden kryptering).	
Stikprøver af anmeldelser	Tre anmeldelser er fremsendt til DPO. Den sidste af de ønskede anmeldelser var Køge Kommune ikke i besiddelse af. Køge Kommune har kontaktet Datatilsynet for at få en kopi af anmeldelsen, men uden held. Datatilsynet svarer ikke på kommunens henvendelser.	Køge Kommune bør sikre sig, at kommunen er i besiddelse af kopier af de anmeldelser, der er sendt til Datatilsynet.	
72-timers fristen. Hvor lang tid er der gået fra det tidspunkt, hvor man i kommunen blev bekendt med bruddet?	Under 72 timer.	Når sikkerhedsbrud skal anmeldes til Datatilsynet, skal det ske uden unødig forsinkelse og om muligt senest 72 timer efter, at den dataansvarlige er blevet bekendt med bruddet. Foretages anmeldelsen ikke inden for 72 timer, skal den ledsages af en begrundelse for forsinkelsen.	

Intern registrering af sikkerhedsbrud.	Antal: 30.		
Kommunens oversigt over alle brud. Er det kommunens vurdering, at den har registeret alle brud, som skal dokumenteres efter artikel 33, stk. 5?	Excel ark er modtaget. Ja, det er Køge Kommunes vurdering. Hvis der har været tvivlsspørgsmål, så er DPO kontaktet for gode råd.	Køge Kommunes registrering af sikkerhedsbrud er detaljeret. Vi anbefaler, at oversigten indeholder alle de informationer, som kan ses i eksemplet på side 28 i Datatilsynets vejledning[3]. Vi anbefaler, at Køge Kommune mere konsekvent registrerer, om der er sendt underretning til de berørte personer, og begrundelser for ikke at underrette de registrerede, og at der herudover i de enkelte sager gemmes den fulde kommunikation og beslutningsgrundlag.	
Den samlede dokumentation vedrørende de tre sidste sikkerhedsbrud, som kommunen har registreret i 2018.	Den modtagne dokumentation indeholder typisk interne mails, mail med DPO, anmeldelse til Datatilsynet, evt. afgørelse fra Datatilsynet.		
Underretning af berørte personer. Er det kommunens vurdering, at den har underrettet i alle de tilfælde, hvor det skulle ske efter artikel 34?	Køge Kommune har underrettet de registrerede i forbindelse med tre sikkerhedsbrud. Det er Køge Kommunes vurdering, at der er underrettet i alle tilfælde, hvor dette skulle ske. Hvis der har været tvivlsspørgsmål, så er DPO kontaktet for gode råd.	Antallet er ret lavt, sammenlignet med andre kommuner, men det kan evt. skyldes, at de brud, som Køge Kommune har haft, ikke har været så alvorlige som de andre kommuners. Vi anbefaler, at Køge Kommune til stadighed har fokus på forpligtelsen til at underrette berørte personer. Vi opfordrer endvidere kommunen til fortsat at søge rådgivning hos DPO, hvis der er tvivl om, hvorvidt der skal ske underretning i de enkelte tilfælde.	

[3] https://www.datatilsynet.dk/media/6558/haandtering-af-brud-paa-persondatasikkerheden.pdf

Stikprøve vedr. underretning.	Vi har modtaget kopi af en underretning, som Køge Kommune har givet i 2018. Brevet indeholder oplysninger om fejlen, men ikke udtrykkelige oplysninger om, hvem der kan kontaktes for yderligere oplysninger, sandsynlige konsekvenser af bruddet, eller beskrivelse af foranstaltninger, som kommunen har truffet eller planlægger at træffe for at afhjælpe sikkerhedsbruddet eller begrænse skaden. Brevet fremstår som dateret med datoen for modtagelsen (åbningen) hos DPO (6. august 2019). Det fremgår ikke, hvem den eller de specifikke modtagere af brevet er.	Køge Kommune bør sikre sig, at underretninger til de berørte personer lever op til de krav, som databeskyttelsesforordningen stiller til indholdet af underretningen. Når der er pligt til underretning, skal underretningen til berørte personer som minimum indeholde: 1) Navn og kontaktoplysninger til et kontaktpunkt i Køge Kommune, der kan uddybe, hvad der er sket og gjort, eller DPO 2) En beskrivelse af de sandsynlige konsekvenser af bruddet 3) En beskrivelse af de foranstaltninger, som kommunen har truffet eller planlægger at træffe for at afhjælpe sikkerhedsbruddet eller begrænse skaden. Hvis underretning gives mundtligt, herunder telefonisk, anbefaler vi, at Køge Kommune sikrer sig, at den mundtlige information lever op til ovennævnte krav, og at det dokumenteres, fx ved et referat eller telefonnotat, at der er givet information om de nævnte forhold. information følges op med skriftlig information, der lever op til minimumskravene. Vi går ud fra, at dateringen i august 2019 skyldes den tekniske indretning af den anvendte brevskabelon. Vi anbefaler, at dokumentationen af underretninger sker på en sådan en måde, så brevdato og modtagere dokumenteres.	
Brug af undtagelserne i artikel 34, stk. 3, litra a (fx at data var krypteret), litra b (efterfølgende foranstaltninger) eller litra c	Nej. Køge Kommune har ikke anvendt disse undtagelser.	I de fleste tilfælde, hvor der ikke sker underretning, vil begrundelsen netop være, at bruddet vurderes sandsynligvis ikke at indebære en høj risiko fysiske personers rettigheder eller frihedsrettigheder. Som nævnt ovenfor anbefaler vi, at Køge Kommune fremover	

(uforholds-mæssig ind-sats)?		registrerer i sin oversigt over sik-kerhedsbrud, med hvilken begrun-delse det er besluttet ikke at fore-tage underretning.	
Opfølgning på sikkerheds-brud. Har sik-kerhedsbrud givet kommu-nen anledning til at iværk-sætte yderli-gere tekniske eller organisa-toriske sikker-hedsforanstalt-ninger, eller at foretage forny-ede risikovur-deringer vedrø-rende risici i forhold til de registrerede personer, og i hvor mange til-fælde?	Ja. Antal tilfælde: 13. Alle sikkerhedsbrud har givet anled-ning til opfølgning på interne procedu-rer, information til medarbejderne, præcisering af interne procedurer etc.	Kommunen bør i alle tilfælde, hvor der er sket sikkerhedsbrud, tage initiativer til at afhjælpe det skete. Vi går ud fra, at de 13 tilfælde, der omtales her, er egentlige ændrin-ger til tekniske og organisatoriske foranstaltninger. Vi noterer os det oplyste om, at alle sikkerhedsbrud har givet an-ledning til opfølgning på interne procedurer, information til medar-bejderne, præcisering af interne procedurer etc.	
Eksempler på opfølgning.	2018-022059 Helbredsoplysninger eksponeret til beboere i Agerbæk-huse. Dette sikkerhedsbrud resulte-rede i skærpede interne processer. 2018-024551 Fejlagtig login på medi-cinmodulet FMK. Der er truffet de nødvendige ledelsesmæssige beslut-ninger på baggrund af hændelsen, både i forhold til medarbejderne og i forhold til at få præciseret instruksen omkring FMK. 2019-000895 Henvendelse fra tidli-gere medarbejder omkring modta-gelse af fortrolig mail i mailboks. Der er indskærpet, at brug af almindelig mail til korrespondance mellem bor-ger og kommune ikke er korrekt selvom borgeren ønsker det.		

Bech·Bruun

---o0o---

København, september 2019

Thomas Munk Rasmussen
Partner

Lena Andersen Salin
Senioradvokat

Bilag 1: Spørgeskema om fortegnelser

Spørgeskema om fortegnelser

Spørgeskema udfyldt på vegne af

Kommunens navn

af

Navn	Telefonnummer
E-mail	Dato

Fortegnelser

	Spørgsmål	Besvarelse	
	1. Procedurer til sikring af kommunens efterlevelse af databeskyttelsesforordningens artikel 30		
Art. 30	Har kommunen udformet en skriftlig procedure, retningslinje eller lignende for førelsen af fortegnelser?	**Ja:** Vedlæg venligst kopi af retningslinjer og lignende.	**Nej:** Beskriv venligst hvordan kommunen i stedet sikrer, at artikel 30 efterleves:
Art. 30	Har kommunen placeret ansvaret for fortegnelserne?	**Ja:** Beskriv hvordan ansvaret for fortegnelserne er placeret, fx ved angivelse af stillingsbetegnelser på de personer, der har ansvaret:	**Nej:** Beskriv venligst hvordan kommunen i så fald sikrer, at artikel 30 efterleves:
Art. 30	Anvender kommunen skabeloner, herunder KL's standardfortegnelser?	**Ja:** Beskriv:	**Nej:** Beskriv venligst hvordan det sikres, at indholdet af kommunens fortegnelser lever op til artikel 30:

Art. 30	Har kommunen fastlagt, at fortegnelserne skal lagres i en specifik løsning, arkiv-mappe eller lignende?	**Ja:** Beskriv hvordan fortegnelserne lagres:	**Nej:** Beskriv hvordan fortegnelserne lagres:
	2. Fortegnelser for kommunen som dataansvarlig		
Art. 30 (1)	Hvor mange fortegnelser for aktiviteter som dataansvarlig har kommunen udformet?	**Antal:** Vedlæg venligst en oversigt over alle fortegnelser for kommunen som dataansvarlig. Vedlæg venligst fortegnelser vedr.: • Behandlingsaktiviteter angående beskæftigelse. • Behandlingsaktiviteter angående løn- og personaleadministration. • Behandlingsaktiviteter angående omsorg og sundhed. • Behandlingsaktiviteter angående social service. • Behandlingsaktiviteter angående kontante ydelser.	
Art. 30 (1)	Er kommunen færdig med at udforme fortegnelser for sine aktiviteter som dataansvarlig?	**Ja:**	**Nej:** Hvilke områder udestår: Hvor mange fortegnelser mangler: Hvad er tidshorisonten for udformning af de sidste fortegnelser?
	3. Fortegnelser for kommunen som databehandler		

Art. 30 (2)	Har kommunen udformet fortegnelser for aktiviteter som databehandler og hvor mange?	**Ja** **Antal:** Vedlæg venligst en oversigt over alle fortegnelser for kommunen som databehandler. Vedlæg venligst fortegnelser vedr.: • Databehandlinger, der fortages på vegne af kommunale fællesskaber (§ 60-selskaber), såfremt kommunen er databehandler for sådanne. • Databehandlinger, der fortages på vegne af selvejende institutioner, såfremt kommunen er databehandler for sådanne.	**Nej:** Begrund:
Art. 30 (2)	Er kommunen færdig med at udforme fortegnelser for sine aktiviteter som databehandler?	**Ja:**	**Nej:** Hvilke områder udestår: Hvor mange fortegnelser mangler: Hvad er tidshorisonten for udformning af de sidste fortegnelser?

Bech·Bruun

Bilag 2: Spørgeskema om håndtering af databehandlere

Spørgeskema om håndtering af databehandlere

Spørgeskema udfyldt på vegne af

Kommunens navn

af

Navn	Telefonnummer
E-mail	Dato

Håndtering af databehandlere

Spørgeskemaet bedes besvaret for 2018 og første kvartal af 2019

	Spørgsmål	Besvarelse	
	1. Procedurer til sikring af kommunens efterlevelse af databeskyttelsesforordningens artikel 28		
Art. 28	Har kommunen udformet en skriftlig procedure, retningslinje eller lignende for håndtering af databehandlere	**Ja:** Vedlæg venligst kopi af retningslinjer og lignende.	**Nej:** Beskriv venligst hvordan kommunen i stedet sikrer, at artikel 28 efterleves:
Art. 28	Har kommunen placeret ansvaret for håndtering af databehandlere, herunder at der er databehandleraftaler og foretages tilsyn med databehandlerne?	**Ja:** Beskriv hvordan ansvaret er placeret, fx ved angivelse af stillingsbetegnelser på de personer, der har ansvaret:	**Nej:** Beskriv venligst hvordan kommunen i så fald sikrer, at artikel 28 efterleves:
Art. 28	Har kommunen fastlagt, at databehandleraftaler skal lagres i en specifik løsning, arkiv-mappe eller lignende?	**Ja:** Beskriv hvordan databehandleraftalerne lagres:	**Nej:** Beskriv hvordan databehandleraftalerne lagres:

	2. Databehandleraftaler		
Art. 28(3)	Hvor mange databehandleraftaler har kommunen indgået pr. 31. marts 2019?	**Antal:** Vedlæg venligst en oversigt over alle databehandlere, som kommunen har indgået aftale med. Vedlæg venligst alle databehandler-aftalerne vedr.: • Behandlingsaktiviteter angående dagtilbud og uddannelse. • Behandlingsaktiviteter angående kultur, idræt og folkeoplysning. • Behandlingsaktiviteter angående kommunens styrelse og administrative systemer.	
Art. 28(3)	Er kommunen færdig med at indgå databehandleraftaler?	**Ja:**	**Nej:** Hvilke områder udestår: Hvor mange databehandleraftaler mangler (evt. anslået tal): Hvad er tidshorisonten for indgåelse af de sidste databehandleraftaler?
	3. Fælles dataansvar		

Art. 26	Har kommunen fælles dataansvar med andre myndigheder eller virksomheder mv.?	**Ja:** Med hvor mange: Angiv venligst, hvilke organisationer kommunen har fælles dataansvar med: Foreligger der i de nævnte tilfælde aftaler om fælles dataansvar eller et andet retligt dokument, der fastlægger, hvilket ansvar og forpligtelser parterne har?	**Nej:**
	4. Tilsyn med databehandlere (efter Datatilsynets praksis en del af kravet om ansvarlighed)		
Art. 5(2) og 24	Har kommunen en procedure eller plan for, hvordan kommunen fører tilsyn med sine databehandlere?	**Ja:** Beskriv:	**Nej:**

Art. 5(2) og 24	Har kommunen foretaget tilsyn med databehandlere **i 2018**, og med hvor mange? Besvar venligst også spørgsmål om hvordan og udfaldet.	**Ja:** Med hvor mange: Angiv venligst hvordan disse tilsyn er gennemført som antal ud for følgende kategorier: ○ Besøg: ○ Spørgeskema: ○ Revisionserklæring: ○ Andet: Angiv venligst hvordan udfaldet af de udførte tilsyn har været som antal ud for følgende kategorier: ○ Tilfredsstillende: ○ Behov for yderligere tilsyn: ○ Yderligere tilsyn fravalgt ud fra en risikovurdering: ○ Andet:	**Nej:** Begrund:
Art. 5(2) og 24	Har kommunen foretaget tilsyn med databehandlere i første kvartal af **2019**, og med hvor mange? Besvar venligst også spørgsmål om hvordan og udfaldet.	**Ja:** Med hvor mange: Angiv venligst hvordan disse tilsyn er gennemført som antal ud for følgende kategorier: ○ Besøg: ○ Spørgeskema: ○ Revisionserklæring: ○ Andet: Angiv venligst hvordan udfaldet af de udførte tilsyn har været som antal ud for følgende kategorier ○ Tilfredsstillende: ○ Behov for yderligere tilsyn: ○ Yderligere tilsyn fravalgt ud fra en risikovurdering: ○ Andet:	**Nej:** Begrund:

Art. 5(2) og 24	Dokumentation for den udførte kontrol	Vedlæg venligst kommunens dokumentation for den udførte kontrol med alle databehandlere, der begynder med bogstavet K.	
Art. 5(2) og 24	Har kommunen planer om at føre yderligere tilsyn med databehandlere i 2019?	**Ja:** Beskriv:	**Nej:** Begrund:

Bilag 3: Spørgeskema om brud på persondatasikkerheden

Spørgeskema om brud på persondatasikkerheden

Spørgeskema udfyldt på vegne af

Kommunens navn

af

Navn	Telefonnummer
E-mail	Dato

Håndtering af brud på persondatasikkerheden

Spørgeskemaet bedes besvaret for perioden **fra 25. maj 2018 til og med 31. marts 2019**

	Spørgsmål	Besvarelse	
	1. Procedurer til sikring af kommunens efterlevelse af databeskyttelsesforordningens artikel 33 og 34		
Art. 33 og 34	Har kommunen udformet skriftlige procedurer, retningslinjer eller lignende for håndtering af brud på persondatasikkerheden?	**Ja:** Vedlæg venligst kopi af retningslinjer og procedurer samt eventuelle skemaer, som anvendes i kommunen i forbindelse med håndtering af brud på persondatasikkerheden.	**Nej:** Beskriv venligst hvordan kommunen i stedet sikrer, at artikel 33 og 34 efterleves:
Art. 33 og 34	Har kommunen placeret ansvaret for håndtering af brud på persondatasikkerheden, herunder at alle brud dokumenteres, og at der sker anmeldelse til Datatilsynet og underretning til de berørte, når dette er påkrævet?	**Ja:** Beskriv hvordan ansvaret er placeret, fx ved angivelse af stillingsbetegnelser på de personer, der har ansvaret:	**Nej:** Beskriv venligst hvordan kommunen i så fald sikrer, at artikel 33 og 34 efterleves:

Art. 33 og 34	Har kommunen fastlagt, at brud på persondatasikkerheden skal registreres i en specifik løsning, arkiv-mappe eller lignende?	**Ja:** Beskriv hvordan brud på persondatasikkerheden registreres:	**Nej:** Beskriv hvordan brud på persondatasikkerheden registreres:
	2. Udpegelse af kontaktpunkter		
Art. 33 og 34	Har kommunen udpeget et (eller flere) kontaktpunkt(er), hvor medarbejderne kan henvende sig i tilfælde af sikkerhedsbrud?	**Ja:** Beskriv:	**Nej:** Uddyb:
Art. 33 og 34	Har kommen udpeget et (eller flere) kontaktpunkt(er), hvor kommunens databehandlere kan henvende sig i tilfælde af sikkerhedsbrud, der omfatter personoplysninger, som kommunen er dataansvarlig for?	**Ja:** Beskriv:	**Nej:** Uddyb:
	3. Awareness-aktiviteter og uddannelse/træning		

Art. 33 og 34	Har kommunen gennemført awareness-aktiviteter over for medarbejdere omfattende informationer om, hvad der udgør sikkerhedsbrud, og hvordan de skal håndteres?	**Ja:** Beskriv: Vedlæg venligst eksempler på materiale udformet i forbindelse med awareness-aktiviteterne. Hvornår fandt aktiviteterne sted? Hvor stor en del af kommunens medarbejdere er nået med aktiviteterne (sæt kryds)? 0-25 % 25-50 % 50-75 % 75-100 %	**Nej:** Uddyb:
Art. 33 og 34	Har kommunen gennemført undervisning eller træning af medarbejdere omfattende informationer om, hvad der udgør sikkerhedsbrud, og hvordan de skal håndteres?	**Ja:** Beskriv: Vedlæg venligst eksempler på materiale udformet i forbindelse med undervisning eller træning. Hvornår fandt undervisning og/eller træning sted? Hvor stor en del af kommunens medarbejdere er nået (sæt kryds)? 0-25 % 25-50 % 50-75 % 75-100 %	**Nej:** Uddyb:
	4. Anmeldelse til Datatilsynet og intern registrering		

Art. 33, stk. 1	Har kommunen anmeldt brud på persondatasikkerheden til Datatilsynet, og hvor mange?	**Ja:** **Antal:** Vedlæg venligst kopi af anmeldelsen vedrørende de **første to sikkerhedsbrud**, som kommunen har anmeldt til Datatilsynet i 2018, samt de **første to sikkerhedsbrud**, som kommunen har anmeldt til Datatilsynet i 2019 (eller henvisning til DPO-platformen, hvis kommunen har lagt anmeldelserne på platformen).	**Nej:** Uddyb:
Art. 33, stk. 1	Er det kommunens vurdering, at den har anmeldt alle brud, som skal anmeldes efter artikel 33, stk. 1?	**Ja:**	**Nej:** Uddyb:
Art. 33, stk. 1	Når kommunen i den omhandlede periode (fra 25. maj 2018 til og med 31. marts 2019) har anmeldt brud til Datatilsynet, hvor lang tid er der da gået fra det tidspunkt, hvor man i kommunen blev bekendt med bruddet?	**Angiv antal ud for de forskellige tidsintervaller:** Under 72 timer Mellem 72 timer og en uge En uge til 14 dage Over 14 dage	

Art. 33, stk. 5	Har kommunen registreret brud på persondatasikkerheden i den omhandlede periode, og hvor mange?	**Ja:** **Antal:** Vedlæg venligst en oversigt over alle de brud på persondatasikkerheden, som kommunen har registreret i perioden fra 25. maj 2018 til og med 31. marts 2019. Vedlæg venligst den samlede dokumentation vedrørende **de tre sidste** sikkerhedsbrud, som kommunen har registreret i 2018.	**Nej:** Uddyb:
Art. 33, stk. 5	Er det kommunens vurdering, at den har registeret alle brud, som skal dokumenteres efter artikel 33, stk. 5?	**Ja:**	**Nej:** Uddyb:
	5. Underretning af berørte personer (artikel 34)		

Art. 34	Har kommunen haft sikkerhedsbrud, der gav anledning til at underrette berørte personer i medfør af artikel 34, og hvor mange?	**Ja:** Hvor mange sikkerhedsbrud gav anledning til underretning: Vedlæg venligst dokumentation for underretningen af de berørte personer i **de sidste tre sikkerhedsbrud**, hvor kommunen har underrettet efter artikel 34 i 2018.	**Nej:** Begrund:
Art. 34	Er det kommunens vurdering, at den har underrettet i alle de tilfælde, hvor det skulle ske efter artikel 34?	**Ja:**	**Nej:** Uddyb:
Art. 34	Har kommunen i forbindelse med sikkerhedsbrud benyttet undtagelserne i artikel 34, stk. 3, litra a (fx at data var krypteret), litra b (efterfølgende foranstaltninger) eller litra c (uforholdsmæssig indsats)?	**Ja:** **Angiv venligst antal pr. undtagelse:** Litra a) Litra b) Litra c)	**Nej:**

	6. Opfølgning på sikkerhedsbrud med tekniske eller organisatoriske foranstaltninger (artikel 32)		
Art. 32	Har sikkerhedsbrud givet kommunen anledning til at iværksætte yderligere tekniske eller organisatoriske sikkerhedsforanstaltninger, eller at foretage fornyede risikovurderinger vedrørende risici i forhold til de registrerede personer, og i hvor mange tilfælde?	**Ja:** **Antal tilfælde:** Beskriv venligst **tre konkrete tilfælde**, hvor et sikkerhedsbrud er fulgt op med tekniske eller organisatoriske foranstaltninger, herunder fx ændrede procedurer, interne restriktioner eller nye løsninger.	**Nej:** Uddyb: Hvis der ikke altid er fulgt op med nye foranstaltninger mv., bedes kommunen, med afsæt i **et konkret tilfælde** (hvis der har været et tilfælde), venligst beskrive, hvorfor dette ikke er sket.

Bilag 4: Gennemgang af databehandleraftaler

Vi har udvalgt tre af de databehandleraftaler, som vi har modtaget fra Køge Kommune, til stikprøvevis gennemgang.

For hver af disse aftaler har vi valgt at se på fire spørgsmål, hvor vi har markeret med rød, gul eller grøn, i hvorvidt aftalen efter vores vurdering håndterer spørgsmålet.

Det skal understreges, at der ikke er foretaget en fuldstændig gennemgang af aftalerne, og at vi ikke har set eventuel ledsagende mailkorrespondance, som eventuelt supplerer aftalerne.

Vores vurdering er primært foretaget i forhold til den gældende vejledning og standardaftale fra Datatilsynet. Vores anbefalinger vedrørende databehandleraftaler kan ses i rapportens afsnit 2 og 3.

1. Køge Ungdomsskole og Feliks (administrationssystem)

Procedure for godkendelse af underdatabehandlere	
Spørgsmål	**Niveau**
Er der beskrevet en procedure for godkendelse af underdatabehandlere?	●
Beskrivelse af oplysningerne, der behandles	
Spørgsmål	**Niveau**
Er typer af personoplysninger beskrevet?	●
Behandlingssikkerhed	
Spørgsmål	**Niveau**
Indeholder kontrakten krav til behandlingssikkerheden (uden blot at henvise til den gamle sikkerhedsbekendtgørelse)?	●
Underskrift og datering	
Spørgsmål	**Niveau**
Er kontrakten underskrevet af begge parter og dateret?	●

2. Kultur- og Økonomiforvaltningen (Køge Kommune) og Computopic

Procedure for godkendelse af underdatabehandlere	
Spørgsmål	**Niveau**
Er der beskrevet en procedure for godkendelse af underdatabehandlere?	●

Beskrivelse af oplysningerne, der behandles	
Spørgsmål	**Niveau**
Er typer af personoplysninger beskrevet?	
Behandlingssikkerhed	
Spørgsmål	**Niveau**
Indeholder kontrakten krav til behandlingssikkerheden (uden blot at henvise til den gamle sikkerhedsbekendtgørelse)?	
Underskrift og datering	
Spørgsmål	**Niveau**
Er kontrakten underskrevet af begge parter og dateret?	

3. Køge Bibliotek (Køge Kommune) og Publizon A/S

Procedure for godkendelse af underdatabehandlere	
Spørgsmål	**Niveau**
Er der beskrevet en procedure for godkendelse af underdatabehandlere?	
Beskrivelse af oplysningerne, der behandles	
Spørgsmål	**Niveau**
Er typer af personoplysninger beskrevet?	
Behandlingssikkerhed	
Spørgsmål	**Niveau**
Indeholder kontrakten krav til behandlingssikkerheden (uden blot at henvise til den gamle sikkerhedsbekendtgørelse)?	
Underskrift og datering	
Spørgsmål	**Niveau**
Er kontrakten underskrevet af begge parter og dateret?