KL
MAJ 2018

DATABESKYTTELSE

IMPLEMENTERING AF DATABESKYTTELSES-FORORDNINGEN

ANBEFALINGER TIL DIREKTIONENS OPMÆRKSOMHEDSPUNKTER

NOTAT

Anbefalinger til direktionens opmærksomhedspunkter ift. implementering af databeskyttelsesforordningen

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Indhold

1. Etablér en implementeringsorganisation

Krav og anbefalinger:
Implementeringen af databeskyttelsesforordningen kræver, at flere forskellige kompetencer bringes i spil, fx pga. de nye krav om anmeldelse og dokumentation af sikkerhedsbrud. Derfor anbefales det, at kommunerne etablerer en decideret implementeringsorganisation, som kan trække på medarbejdere med viden om databeskyttelsesjura, datasikkerhed, it, digitalisering, fagområderne/arbejdsgange, HR samt ledelsen.

Det er ikke et decideret krav i forordningen, men vurderes at være en forudsætning for en vellykket implementering. Derfor anbefaler KL, at direktionerne sørger for, at der etableres en implementeringsorganisation.

Databeskyttelse og informationssikkerhed er et ledelsesansvar, ligesom økonomistyring, håndtering af arbejdsmiljø, serviceniveauet eller borgerbetjening. Den ledelsesforankring, der er nødvendig på databeskyttelsesområdet, skal konkret komme til udtryk ved, at den øverste ledelse fastlægger niveauet for sikkerhed i organisationen, idet sikkerhedsniveauet har økonomiske, ressourcemæssige og organisatoriske konsekvenser.

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

KL-bidrag og værktøjer:
KL har udviklet en drejebog med tilhørende ledelsespræsentation og skabeloner til brug for informationssikkerhedsaktiviteter i kommunerne. Drejebogen dækker ikke hele arbejdet med databeskyttelsesforordningen, men øvelsen med øget fokus på sikkerhed og arbejdet med risikobaseret håndtering af sikkerhedsudfordringer. I drejebogen beskrives behovet for samarbejde i hele organisationen:

http://www.kl.dk/ImageVaultFiles/id_84122/cf_202/Informationssikkerhedsaktiviteter.PDF

KL har i Digitaliseringsstyrelsen, i regi af den fællesoffentlige digitaliseringsstrategi, medvirket til udarbejdelsen af drejebogen: "En rejsefortælling om funktioner, roller og ledelse i forhold til informationssikkerhed". Drejebogen er gennemgået og revideret i samarbejde med en kommunal referencegruppe:

http://www.kl.dk/ImageVaultFiles/id_84171/cf_202/KL_Informationssikkerhed_en_rejsefort-lling_om_fun.PDF

2. Brug årlige sikkerhedsmålinger og analyser til at øge sikkerheden

Krav og anbefalinger:
Databeskyttelsesforordningen stiller yderligere krav til kommunernes datasikkerhed samtidig med, at kommunerne skal til at arbejde med, at valget af kommunens sikkerhedstiltag skal ske ud fra vurderinger af risici forbundet med de enkelte behandlinger af persondata, den såkaldte "risikobaserede" tilgang.

Samtidig med forordningens yderligere krav til datasikkerhed er sikkerhedsudfordringerne for kommunerne generelt stigende med bl.a. hackerangreb, ligesom de fleste kommuner har et efterslæb på arbejdet med informationssikkerhed. Derfor er det aftalt i økonomiaftaler med regeringen, at sikkerheden i kommuner (og hele den offentlige sektor) skal øges.

KL anbefaler, at direktionerne anvender de årlige fælleskommunale sikkerhedsmålinger og analyser af sikkerhedsarbejdet til at fokusere kommunens indsats for at øge sikkerheden.

KL-bidrag og værktøjer:
KL gennemfører måling og analyse af kommunernes arbejde med informationssikkerhed hvert år i perioden 2016-2020. Analysen viser den aktuelle status for kommunernes arbejde med sikkerhed. Kommunen kan se egen status op mod det samlede landsresultat for alle kommuner. Ligesom man kan foretage egne analyser i kølvandet på KL's analyse af status for sikkerhedsarbejdet.

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Analysen udgør grundlaget for de fælleskommunale indsatser, der skal medvirke til at øge informationssikkerheden i kommunerne og understøtte, at kommunerne kan implementere databeskyttelsesforordningen og overgå til at arbejde risikobaseret og dermed efter principperne i ISO 27.001-standarden, som det er aftalt i økonomiaftalen for 2017.

Måling og analyse foregår via et digitalt redskab (en portal), som kommunen kan anvende som en hjælp til kommunens eget arbejde med at følge og udvikle arbejdet med informationssikkerhed. Herunder særligt til at udpege områder, hvor der er behov for at styrke informationssikkerheden og bl.a. via ledelsesinformation fra portalen følge udviklingen i arbejdet. Kommunens adgang til portalen sker via kommunens kontaktperson i netværket af kommunale sikkerhedskoordinatorer for informationssikkerhed i KL´s Sikkerhedsprogram.

Kontakt kommunens kontaktperson til sikkerhedsprogrammet eller programleder Beth Tranberg, beth@kl.dk, for yderligere informationer om målingen og adgang til denne.

3. Udpeg en databeskyttelsesrådgiver

Krav og anbefalinger:
Det er et krav efter databeskyttelsesforordningen, at alle kommuner skal have udpeget en databeskyttelsesrådgiver til at understøtte, at kommunen overholder de databeskyttelsesretlige regler.

Direktionen skal sikre, at databeskyttelsesrådgiveren inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger. En sådan inddragelse bør ske på øverste ledelsesmæssige niveau (f.eks. ved deltagelse på direktions- og ledelsesmøder). Det anbefales, at direktionen implementerer procedurer, som sikrer dette.

Databeskyttelsesrådgiveren afrapporterer direkte til kommunalbestyrelsen om kommunens overholdelse af de databeskyttelsesretlige regler. Dette kan ske ved fx en årlig status, og når der opstår konkrete sager om fx sikkerhedsbrud, pressesager eller besøg fra Datatilsynet. Direktionen bør implementere procedurer, der understøtte databeskyttelsesrådgiverens afrapportering.

KL-bidrag og værktøjer:
På www.kl.dk om implementering af forordningen kan der læses mere om databeskyttelsesrådgiveren:

http://www.kl.dk/Okonomi-og-administration/Administration-og-digitalisering/Databeskyttelse-og-sikkerhed/Information-om-forordningen/Status---Databeskyttelsesradgiver/

Justitsministeriet, Datatilsynet, Digitaliseringsstyrelsen og Erhvervsstyrelsen har efter ønske fra KL udarbejdet en vejledning om

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

den nye databeskyttelsesrådgiverfunktion. KL har bidraget til vejledningens indhold:

https://www.datatilsynet.dk/media/6561/databeskyttelsesraadgivere.pdf

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne for databeskyttelsesrådgiveren:

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om databeskyttelsesrådgiveren er beskrevet på side 569-587 i betænkningen.

4. Informér medarbejderne om de databeskyttelsesregler, der gælder pr. 25. maj 2018

Krav og anbefalinger:
For at kommunens medarbejdere kan efterleve reglerne i databeskyttelsesforordningen, skal medarbejderne være informeret om reglerne – både de helt nye regler som indføres med forordningen og de regler i forordningen, som er en videreførelse af de gældende regler i persondataloven. Det gælder alle medarbejdere, som håndterer personoplysninger i større eller mindre omfang. At medarbejderne skal have den fornødne viden og kompetencer følger implicit af forordningens krav om, at databeskyttelsesrådgiveren er forpligtet til at overvåge kommunens uddannelse af personale.

KL anbefaler, at direktionerne drøfter med fagcheferne, hvordan det sikres, at alle relevante medarbejdere får og vedligeholder deres viden om databeskyttelse. Særligt er det vigtigt med fokus på de medarbejdere, som behandler personoplysninger, men hvor det ikke sker som led i decideret sagsbehandling, fx medarbejdere i institutioner og skoler.

KL-bidrag og værktøjer:
KL har i både 2016 og 2017 udbudt kurser om de nye databeskyttelsesregler i COK-regi. KL udbyder også kurser i 2018:

https://www.cok.dk/soeg?keys=databeskyttelse

Mellem kommunerne er der i KL´s Sikkerhedsprogram delt materialer og erfaringer med informationer til forskellige medarbejdergrupper om awareness ift. informationssikkerhed. Materialerne kan genbruges af andre kommuner.

KL´s Sikkerhedsprogram har oprettet og driver det fælleskommunale netværk med deltagelse af alle 98 kommuner. Netværkets medlemmer er udpeget at kommunaldirektørerne til at repræsentere kommunens

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

arbejde med at øge sikkerheden. Formålet med netværket er bl.a. at understøtte vidensdeling på tværs af kommunerne. Netværket har en digital platform til deling af viden og erfaringer med informationssikkerhed og deling af skabeloner, dokumenter, planer, undervisningsmateriale i form af film m.m.

Der udarbejdes awarenesskampagner og undervisningsmateriale om it-sikkerhed til medarbejdere sammen med stat og regioner i det fællesoffentlige digitaliseringssamarbejde. Materialerne forventes udsendt ultimo april 2018.

KL udarbejder også yderligere materiale sammen med de kommunale arbejdstagerorganisationer i regi af Fremfærd arbejdet. Dette forventes udgivet med løbende leverancer fra foråret 2018 og resten af året.

Der er udarbejdet en kampagne rettet mod borgere, som findes her:

https://digst.dk/sikkerhed/kampagner-og-analyser/informationsindsatser/vi-holder-hackerne-ude/ og i foråret kommer der ovennævnte kampagne rettet mod offentlige medarbejdere.

5. Indgå databehandleraftaler

Krav og anbefalinger:
Med databeskyttelsesforordningen følger nye skærpede krav til indholdet af de databehandleraftaler, kommunerne skal have med leverandører og øvrige eksterne samarbejdsparter, der behandler persondata på vegne af kommunen. Det betyder, at kommunerne skal have opdateret alle databehandleraftaler, herunder sikre, at der er indgået alle nødvendige databehandleraftaler.

KL anbefaler, at direktionerne sikrer, at kommunens implementeringsorganisation har en plan for opdatering af kommunens databehandleraftaler.

KL-bidrag og værktøjer:
Justitsministeriet og Datatilsynet har på KL´s foranledning udarbejdet en vejledning om, hvornår der skal indgås databehandleraftaler. KL har bidraget til vejledningens udarbejdelse:

https://www.datatilsynet.dk/media/6560/dataansvarlige-og-databehandlere.pdf

KL og KOMBIT har i april 2017 offentliggjort en skabelon for databehandleraftaler, som kommunerne kan anvende, når de skal indgå databehandleraftaler med deres leverandører. Skabelonen foreligger også i en engelsk udgave. Skabelonen anbefales af DI til deres medlemmer, og KOMBIT har senest aftalt med KMD, at de også følger skabelonen.

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Link til skabelonerne med tilhørende kommentarnotat/vejledning til udfyldelse af skabelonen:

http://www.kl.dk/Okonomi-og-administration/Administration-og-digitalisering/Databeskyttelse-og-sikkerhed/Information-om-forordningen/Databehandleraftale/

Datatilsynet har den 16. februar 2018 offentliggjort en skabelon til databehandleraftaler. KL har givet input til skabelonen, og KL vil i løbet af marts informere nærmere om brugen af Datatilsynets skabelon på det kommunale område.

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne for databehandleraftaler.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om kravene til databehandleraftalerne er beskrevet på side 429-441 i betænkningen.

6. Færdigudfyld fortegnelser, når de kommer fra KL i 1. kvartal 2018

Krav og anbefalinger:
Med databeskyttelsesforordningen følger et nyt krav om, at kommunerne skal udarbejde og opbevare fortegnelser over alle behandlinger af persondata. Da kommunerne efter lovgivningen er pålagt at udføre de samme opgaver/behandlinger af persondata anbefaler KL, at kommunerne anvender de standardfortegnelser, som KL har udarbejdet og udsender til alle kommuner ultimo marts 2018.

KL anbefaler, at direktionerne sikrer, at kommunens implementeringsorganisation har en plan for færdigudfyldelse af fortegnelser for kommunens behandlinger af personoplysninger, herunder at samtlige fagområder gennemgår fortegnelserne.

KL-bidrag og værktøjer:
Justitsministeriet og Datatilsynet har på KL´s foranledning udarbejdet en vejledning om kravene til indholdet af fortegnelserne. KL har bidraget til vejledningen:

https://www.datatilsynet.dk/media/6567/fortegnelse.pdf

KL har udarbejdet standardfortegnelser, hvor den enkelte kommune kan nøjes med at udfylde de elementer, der er kommunespecifikke. Standardfortegnelserne udsendes ultimo marts 2018. Link til information om arbejdet med standardfortegnelserne til kommunerne:

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk
Side 7 af 13

http://www.kl.dk/Okonomi-og-administration/Administration-og-digitalisering/Databeskyttelse-og-sikkerhed/Information-om-forordningen/Status---fortegnelseskravet/

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne for fortegnelseskravet.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om kravene til fortegnelserne er beskrevet på side 443-463 i betænkningen.

7. Tilret blanketter ift. nye oplysninger til borgerne

Krav og anbefalinger:
Databeskyttelsesforordningen stiller skærpede krav til de oplysninger, kommunen på bl.a. kommunens blanketter skal give borgerne om kommunens behandling af borgerens data. Det betyder, at kommunerne skal opdatere alle blanketter med de nye oplysninger.

KL tilretter samtlige blanketter i KL's blanketsamling, så det kan slå igennem til kommunens blanketter, men KL anbefaler, at direktionerne sikrer, at kommunens implementeringsorganisation har en plan for opdatering af kommunens egne blanketter og efterfølgende ibrugtagning af disse.

KL-bidrag og værktøjer:
KL tilretter samtlige blanketter i KL's blanketsamling inden 25. maj 2018, og kommunen skal derfor alene sørge for, at egne blanketter er opdaterede.

Justitsministeriet har på KL´s foranledning udarbejdet en vejledning om registreredes rettigheder, som også gennemgår kravene til kommunernes oplysningspligt (oplysningerne på blanketterne). Ministeriet har oplyst, at vejledningen vil foreligge primo marts.

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne om oplysningspligten.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om kravene til oplysningspligten på blanketter er beskrevet på side 279-296 i betænkningen.

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

8. Implementér de nødvendige processer og arbejdsgange, herunder proces for håndtering og dokumentation af sikkerhedsbrud

Krav og anbefalinger:
Med databeskyttelsesforordningen følger et nyt krav om, at kommunerne ved sikkerhedsbrud/kompromittering af borgernes data skal anmelde sikkerhedsbruddet til Datatilsynet inden 72 timer. Samtidig skal kommunerne udarbejde dokumentation af samtlige sikkerhedsbrud i kommunen – uanset om sikkerhedsbruddene har haft konsekvenser for borgerne.

KL anbefaler, at direktionerne sikrer, at kommunens implementeringsorganisation med udgangspunkt i KL´s skabelon og procesbeskrivelse implementerer en procedure for håndtering af sikkerhedsbrud – konstatering, håndtering, anmeldelse, dokumentation og orientering af de berørte borgere. Dels bør direktionerne snarest sikre, at kommunens nuværende beredskabsplan er opdateret og testet, da denne kommer til at være afsættet for implementeringen af de nye krav i databeskyttelsesforordningen.

Databeskyttelsesforordningen stiller ligeledes krav om, at borgerne har ret til at få udleveret de data, kommunen har om den pågældende borger i "et struktureret, almindeligt anvendt og maskinlæsbart format" (såkaldt "dataportabilitet"). Da det er uafklaret, i hvilket omfang dette krav gælder kommunerne, anbefaler KL, at kommunerne ikke pt. udarbejder processer og arbejdsgange for håndtering af borgernes eventuelle anmodning om dataportabilitet.

Databeskyttelsesforordningen stiller desuden skærpede krav til de oplysninger, kommunen skal give borgerne, hvis kommunerne – typisk i forbindelse med sagsoplysning – indhenter oplysninger om borgeren andre steder end hos borgeren selv, fx fra andre myndigheder. KL anbefaler, at direktionerne sikrer, at kommunens implementeringsorganisation får opdateret kommunens procedurer for opfyldelse af oplysningspligten i disse situationer.

KL-bidrag og værktøjer:

Sikkerhedsbrud
Justitsministeriet og Datatilsynet har på KL´s foranledning udarbejdet en vejledning om håndtering af brud på persondatasikkerheden. KL har bidraget til vejledningen, som forventes offentliggjort i februar.

Når vejledningen foreligger, vil KL's Sikkerhedsprogram i samarbejde med programmets kommunale referencegruppe udarbejde en generisk skabelon og procesbeskrivelse, som den enkelte kommune kan anvende til håndtering af anmeldelse af brud på persondatasikkerhed.

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk
Side 9 af 13

præciseret reglerne om anmeldelse af brud på persondatasikkerheden og underretning til borgerne om sikkerhedsbrud.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om anmeldelse af sikkerhedsbrud og underretning af borgerne er beskrevet på side 490-521 i betænkningen.

Dataportabilitet
I forhold til dataportabilitet udarbejder Justitsministeriet på KL´s foranledning en vejledning om registreredes rettigheder, som også gennemgår reglerne om borgerens ret til dataportabilitet. Ministeriet har oplyst, at vejledningen vil foreligge umiddelbart efter vedtagelsen af databeskyttelsesloven, forventeligt primo maj.

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne dataportabilitet.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om dataportabilitet er beskrevet på side 346-355 i betænkningen.

Oplysningspligten
Justitsministeriet har på KL´s foranledning udarbejdet en vejledning om registreredes rettigheder, som også gennemgår kravene til kommunernes oplysningspligt ved indhentning af oplysningerne om borgerne hos andre end borgerne selv. Ministeriet har oplyst, at vejledningen vil foreligge primo marts. Vejledningen vil give gode anvisninger på, hvad der skal oplyses til borgerne i de situationer, hvor kommunen indsamler personoplysninger om borgeren ved siden af indsamling via blanketter og selvbetjeningsløsninger.

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne om oplysningspligten.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om kravene til oplysningspligten, hvis oplysninger om borgerne er indsamlet hos andre end borgeren selv, er beskrevet på side 296-312 i betænkningen.

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk
Side 10 af 13

9. Sørg for at it-systemerne lever op til databeskyttelseskravene

Krav og anbefalinger:
De behandlinger af personoplysninger, som sker i kommunens it-systemer, skal overholde de såkaldte "databeskyttelsesprincipper" – bl.a. kravet om, at data ikke må ligge i systemerne i længere tid end nødvendigt. Og kravet om, at de kommunale medarbejdere ikke må behandle flere oplysninger om borgerne end højst nødvendigt. Dette er allerede i dag krav efter persondataloven, men bliver understreget med databeskyttelsesforordningens krav om "databeskyttelse gennem design og databeskyttelse gennem standardindstillinger", hvor der stilles krav om at databeskyttelse tænkes ind fra starten, når nye it-løsninger skal designes. It-løsninger skal understøtte både databeskyttelsesprincipperne, borgernes rettigheder efter forordningen, fx retten til indsigt i egne data, og databeskyttelsesforordningen generelt.

Det er fortsat er uafklaret, hvilken betydning kravet om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger – samt forordningens generelle krav om behandlingssikkerhed – får for kommunens eksisterende it-systemer, herunder om systemernes standardindstillinger skal ændres, hvis de kan. KL forventer ikke, at kommunerne skal til at stille krav til leverandørerne om at ændre eksisterende systemer i væsentligt omfang, men der kan eventuelt komme krav om, at gamle systemer med utilstrækkelig databeskyttelse skal suppleres af organisatoriske sikkerhedstiltag.

Indtil dette er endeligt afklaret, anbefaler KL, at direktionerne har fokus på, at kommunens *nye* it-systemer overholder databeskyttelseskravene. Dette kan ske ved at sikre, at kommunens implementeringsorganisation informerer alle medarbejdere og ledere med ansvar for at indkøbe it-systemer om de nye krav. KOMBIT tager hånd om dette ift. de nye fælleskommunale løsninger, som KOMBIT står for udviklingen af.

KL-bidrag og værktøjer:
Justitsministeriet og Digitaliseringsstyrelsen er på KL´s foranledning ved at udarbejde en vejledning om databeskyttelse gennem design og standardindstillinger. KL har bidraget til vejledningen, som forventes offentliggjort ultimo februar.

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger er beskrevet på side 410-423 i betænkningen.

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Digitaliseringsstyrelsen har udsendt et omfattende og komplekst kravkatalog med afsæt i forskellige sikkerhedsstandarder, som understøtter krav i databeskyttelsesforordningen. Kravkataloget er ikke en fast opskrift, men kan anvendes som inspiration i forbindelse med udbud og indgåelse af it-kontrakter med leverandører. KL og KOMBIT overvejer pt., om det er muligt at udarbejde brugbare eksempler fra kravkataloget til kommunerne.

10. Implementér de nye sikkerhedskrav

Krav og anbefalinger:
Når persondataloven ophæves den 25. maj 2018 som følge af databeskyttelsesforordningen, bortfalder sikkerhedsbekendtgørelsen[1] (og den tilhørende sikkerhedsvejledning[2]) . Det betyder, at kommunerne står uden håndfaste regler, som beskriver sikkerhedskravene til kommunens håndtering af personoplysninger. I stedet stiller databeskyttelsesforordningen krav om, at kommunerne selv skal vurdere, hvilke sikkerhedstiltag der vil være passende, bl.a. ud fra en vurdering af de konkrete risici forbundet med håndtering af persondata, fx i et konkret it-system.

KL anbefaler, at direktionerne sikrer, at kommunens implementeringsorganisation opdaterer kommunens interne sikkerhedsregler i overensstemmelse med de nye krav, herunder aktivt tager stilling til, om kommunen fremadrettet vil efterleve kravene i sikkerhedsbekendtgørelsen uanset, at de ikke længere vil være krav, men nu alene kan betragtes som forslag til sikkerhedsforanstaltninger.

KL-bidrag og værktøjer:
Justitsministeriet er på KL´s foranledning ved at udarbejde en vejledning om behandlingssikkerhed, som skulle offentliggøres i februar. KL har dog endnu ikke haft vejledningen i høring, så forventelig offentliggøres vejledningen først i marts.

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne behandlingssikkerhed.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om behandlingssikkerhed er beskrevet på side 469-490 i betænkningen.

[1] Bek. nr. 528 af 15. juni 2000
[2] Vejl. nr. 37 af 2. april 2001

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Justitsministeriet har i forslag til databeskyttelsesloven[3] beskrevet en såkaldt "værktøjskasse" – en opregning af forskellige sikkerhedstiltag som kommunen kan lade sig inspirere af, når kommunen skal fastlægge sit niveau for behandlingssikkerhed.

Link til lovforslaget:
http://www.ft.dk/ripdf/samling/20171/lovforslag/l68/20171_l68_som_fremsat.pdf

Værktøjskassen er beskrevet på side 132-133.

Center for Cybersikkerhed har udarbejdet en vejledning om, hvilke sikringstiltag en offentlig virksomhed bør overveje til at imødegå aktuelle trusler fra hacking. Det er aftalt i den fællesoffentlige digitaliseringsstrategi, at vejledningens "Top fire" sikkerhedstiltag implementeres. Sikkerhedstiltagene er indarbejdet i spørgerammen for KL's sikkerhedsundersøgelse og analyse. Her vil man således kunne følge kommunens arbejde med dette.

11. Udarbejd evt. konsekvensanalyser

Krav og anbefalinger:
Det er et krav efter databeskyttelsesforordningen, at kommunerne skal udarbejde såkaldte "konsekvensanalyser", når kommunerne foretager "højrisikobehandlinger" af personoplysninger. Konsekvensanalyser er analyser af, hvilke risici kommunens databehandlinger er forbundet med og hvilke sikkerhedsforanstaltninger, der kan imødegå disse risici.

Det er imidlertid uafklaret, i hvilket omfang kommunerne skal udarbejde konsekvensanalyser, herunder om der alene skal udarbejdes konsekvensanalyser for databehandlinger i nye it-systemer og ændringer af eksisterende systemer, eller om der også skal foretages konsekvensanalyser af eksisterende, uændrede it-systemer.

Datatilsynet vil udarbejde en liste over, hvornår der skal udarbejdes konsekvensanalyser. Men selv, hvis kommunale databehandlinger kommer på Datatilsynets liste, er det ikke sikkert, at den enkelte kommune skal udarbejde konsekvensanalyser. Dels kan kommunernes forpligtelse til at udarbejde analyserne blive afløftet ved, at konsekvensanalyserne udarbejdes for alle kommuner i forbindelse med udarbejdelse af lovforslag (hvor konsekvensanalysen indgår som en del af det lovforberedende arbejde). Dels kan flere, evt. alle, kommuner gå sammen om at udarbejde en konsekvensanalyse, fx i forbindelse med fælles indkøb og kravsspecifikation via KOMBIT.

KL anbefaler derfor pt. alene direktionerne at sikre, at kommunens implementeringsorganisation er opmærksom på kravet om konsekvensanalyser og sørger for, at kommunen forholder sig konkret til

[3] L68 fremsat 25. oktober 2017

Dato: 23. februar 2018

Sags ID: SAG-2016-04111
Dok. ID: 2482798

E-mail: LPJ@kl.dk
Direkte: 3370 3160

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

kravet i forhold til kommunens anskaffelse af nye it-systemer og ændringer af eksisterende systemer.

KL-bidrag og værktøjer:
Justitsministeriet og Datatilsynet er på KL´s foranledning ved at udarbejde en vejledning om konsekvensanalyser. KL har bidraget til vejledningen, som forventes offentliggjort ultimo februar.

KL har deltaget i Justitsministeriets udarbejdelse af betænkning 1565/2017 om databeskyttelsesforordningen, bl.a. med henblik på at få præciseret reglerne konsekvensanalyser.

Link til betænkningen:
http://justitsministeriet.dk/sites/default/files/media/Pressemeddelelser/pdf/2017/bet_1_1.pdf

Reglerne om konsekvensanalyser er beskrevet på side 522-537 i betænkningen.

Sikkerhedsprogrammets drejebog og værktøjskasse for informationssikkerhedsaktiviteter indeholder vejledning til identifikation af konsekvenser af databehandlinger. Drejebogen og værktøjskassen opdateres, såfremt der i den kommende vejledning fra Datatilsynet og Justitsministeriet er noget, der betinger det. Link til materialet:
http://www.kl.dk/Administration-og-digitalisering/Ny-drejebog-om-informationssikkerhedsaktiviteter-id227537/