NOTAT

Databeskyttelsesforordningens dokumentationskrav - Kommunale anbefalinger

Dato: 5. juli 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Indledning

Med indførelsen af reglerne i databeskyttelsesforordningen, GDPR, understreges og skærpes kravene til den dataansvarliges ansvarlighed i forhold til behandlingen af personoplysninger, kravet om accountability. Dette kommer bl.a. til udtryk i forordningens artikel 5, stk. 2, og artikel 24, hvor der stilles nye krav om påvisning af overholdelse af reglerne.

Kommunerne har efterspurgt vejledning til, hvordan kommunerne lever op til disse påvisnings-/dokumentationskrav. Der foreligger pt. ikke officiel vejledning om emnet, og bestemmelserne giver ikke i sig selv megen hjælp til niveauet for dokumentation.

Fortolkning og udmøntning af de retlige standarder i artikel 5 og artikel 24 vil først kunne ske ved Datatilsynets stillingtagen i konkrete sager. Datatilsynet har oplyst, at der er i dag endnu ikke er tilstrækkelig praksis omkring dokumentationskravene til, at tilsynet kan vejlede generelt omkring kravene.

Selvom det ikke er muligt at udarbejde en facitliste til opfyldelse af dokumentationskravene, finder kommunerne ikke desto mindre behov for hjælp til, hvordan man som dataansvarlig forholder sig til kravene.

Anbefalingerne i dette notat er udarbejdet i regi af KL´s partnerskabsprojekt om informationssikkerhed. 43 kommuner har deltaget i partnerskabsprojektet, og anbefalingerne er udarbejdet af deltagerkommunerne. Formålet med anbefalingerne er at give kommunerne et fælles værktøj til, hvordan man som kommune kan forholde sig til de krav til påvisning og dokumentation, som følger af databeskyttelsesforordningen.

Anbefalingerne er udtryk for kommunernes bedste bud på, hvad der som minimum skal til for at leve op til påvisningskravene i artikel 5, stk. 2, og artikel 24. Den enkelte kommune kan vælge at tilvejebringe yderligere dokumentation. Det anbefales at tage kommunens databeskyttelsesrådgiver med på råd i forbindelse med arbejdet med dokumentation.

KL har forelagt Datatilsynet anbefalingerne til kommentering. Datatilsynets bemærkninger er indarbejdet i nærværende anbefalinger. I forhold til anbefalingernes afsnit 2 og 3, hvor kommunen skal udarbejde konkrete produkter og/eller databeskyttelsespolitikker har Datatilsynet understreget, at det naturligvis altid vil afhænge af produkternes konkrete indhold, hvorvidt kommunen som dataansvarlig har påvist, at behandlingen er i overensstemmelse med forordningen, jf. artikel 24, stk. 1.

NOTAT

Indhold

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

NOTAT

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Dokumentationskravene i databeskyttelsesforordningen

Artikel 5, stk. 2

Efter artikel 5, stk. 2, er den dataansvarlige forpligtet til at påvise overholdelse af forordningens grundlæggende principper i artikel 5, stk. 1, om lovlighed, rimelighed, gennemsigtighed, formålsbegrænsning, dataminimering, rigtighed, opbevaringsbegrænsning, integritet og fortrolighed.

Ordlyden af artikel 5 er følgende (egen fremhævning):

Artikel 5

Principper for behandling af personoplysninger

1. Personoplysninger skal:

a) behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«)

b) indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål; viderebehandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, skal ikke anses for at være uforenelig med de oprindelige formål (»formålsbegrænsning«)

c) være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles (»dataminimering«)

d) være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges (»rigtighed«)

e) opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de pågældende personoplysninger behandles; personoplysninger kan opbevares i længere tidsrum, hvis personoplysningerne alene behandles til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål i overensstemmelse med artikel 89, stk. 1, under forudsætning af, at der implementeres passende tekniske og organisatoriske foranstaltninger, som denne forordning kræver for at sikre den registreredes rettigheder og frihedsrettigheder (»opbevaringsbegrænsning«)

f) behandles på en måde, der sikrer tilstrækkelig sikkerhed for de pågældende personoplysninger, herunder beskyttelse mod uautoriseret eller ulovlig behandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (»integritet og fortrolighed«).

2. Den dataansvarlige er ansvarlig for og skal kunne **påvise**, at stk. 1 overholdes (»ansvarlighed«).

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Artikel 24

Efter artikel 24 er den dataansvarlige forpligtet til at gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at påvise, at behandling af personoplysninger er i overensstemmelse med forordningens regler.

Ordlyden af artikel 24 er følgende (egen fremhævning):

Artikel 24

Den dataansvarliges ansvar

1. Under hensyntagen til den pågældende behandlings karakter, omfang, sammenhæng og formål samt risiciene af varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder gennemfører den dataansvarlige passende tekniske og organisatoriske foranstaltninger for at sikre og for at være i stand til at **påvise**, at behandling er i overensstemmelse med denne forordning. Disse foranstaltninger skal om nødvendigt revideres og ajourføres.

2. Hvis det står i rimeligt forhold til behandlingsaktiviteter, skal de foranstaltninger, der er omhandlet i stk. 1, omfatte den dataansvarliges implementering af passende databeskyttelsespolitikker.

3. Overholdelse af godkendte adfærdskodekser som omhandlet i artikel 40 eller godkendte certificeringsmekanismer som omhandlet i artikel 42 kan bruges som et element til at påvise overholdelse af den dataansvarliges forpligtelser.

Bidrag til forståelse af reglerne

Artikel 5, stk. 2

I KL´s høringssvar til Justitsministeriets nationale evaluering af databeskyttelsesreglerne fra oktober 2020, bilag 1, s. 17-18, har KL påpeget følgende i forhold til artikel 5, stk. 2:

"Det er uklart, hvilke og hvor mange foranstaltninger den enkelte dataansvarlige kommune skal iagttage for at leve op til kravet om at kunne påvise ansvarlighed ift. overholdelsen af behandlingsprincipperne. Kommunerne bruger tid og resurser på at diskutere indholdet af kravet om accountability.

Hvilke dokumentationskrav fordrer bestemmelsen? Kommunernes opgavevaretagelse, herunder håndtering af persondata, er allerede i vidt omfang detaljeret reguleret ved lov. Dvs. håndteringen sker allerede "lovligt, rimeligt og på en gennemsigtig måde", til "legitime formål" og med korrekte og relevante data, der gemmes så længe, der er administrativt eller

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk
Side 5 af 15

arkivmæssigt formål, jf. art. 5, stk. 1, litra a-e. Det virker i udgangspunktet som unødvendigt bureaukrati for kommunerne at bruge tid på at skrive ned, at man gør det, man er pålagt i medfør af loven."

Hertil har Datatilsynet i deres bidrag til den nationale evaluering, s. 26, svaret følgende (egen fremhævning):

"Databeskyttelsesforordningen stiller overordnet ingen formkrav til, hvordan dokumentation skal foretages. Dette giver netop råderum til, at den dataansvarlige selv kan vælge en metode. Det væsentlige er, at Datatilsynet bliver betrygget i, at principperne overholdes, og at den dataansvarlige kan demonstrere, hvordan dette sker."
Datatilsynet vurderer altid sagens oplysninger samlet, og alle bidrag omkring den dataansvarliges forretningsvaretagelse kan benyttes til dokumentation. Særligt relevant er de overvejelser, der indeholder en vurdering eller afvejning af risikoen for den registreredes rettigheder, som den dataansvarlige har foretaget.

Datatilsynet udviser en betydelig accept af en mere summarisk beskrivelse af de nødvendige overvejelser, når det gælder behandlinger, der som følge af deres natur og oplysningernes karakter ***alene udgør en begrænset risiko for de registreredes rettigheder****. Her vil kravet efter omstændighederne også kunne dokumenteres i mere generelle brancheanbefalinger* ***eller den blotte konstatering af forholdene omkring behandlingen. Dette gælder også, hvis forholdet er reguleret ved lov.*** *Konkrete dele af databeskyttelsesforordningen kan give støtte til påvisningen, f.eks. kravene til fortegnelse, konsekvensanalyse og databehandleraftaler."*

Datatilsynet har i forhold til ovennævnte afsnit oplyst, at kommunerne ikke som en del af i risikovurderingen vil kunne lade deres resurseforbrug til dokumentationsudarbejdelse indgå som et paramenter.

Ligeledes har Datatilsynet oplyst, at når behandlinger specifikt er reguleret ved lov, fx lovregulering af slettefrister, vil lovgivningen i sig selv kunne være tilstrækkelig dokumentation.

Datatilsynet har truffet afgørelse i en konkret sag vedrørende Danske Bank[1], hvor tilsynet ikke fandt, at artikel 5, stk. 2, var opfyldt i forhold til ansvarlighed i forhold til dataminimeringsprincippet. Det skyldtes, at banken ikke kunne dokumentere, hvilke slettefrister der gjaldt for de enkelte behandlinger. Ifølge Datatilsynet vil det i nogen sager givetvis være rigeligt, at systemerne i praksis er sat op til sletning indenfor en rimelig frist, mens der i andre sager kan være krav om, at der skriftligt er taget stilling til en slettefrist, og hvordan dette i praksis sikres og evt. kontrolleres for at leve op til kravene i artikel 5, stk. 2. I de fleste sager vil en opførelse i fortegnelsen i sådan en situation være tilstrækkelig – afhængig af fortegnelsens detaljeringsgrad.

[1] Danske Bank indstilles til bøde (datatilsynet.dk)

NOTAT

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Artikel 24

I KL´s høringssvar til Justitsministeriets nationale evaluering af databeskyttelsesreglerne fra oktober 2020, bilag 2, s. 13, har KL påpeget følgende i forhold til artikel 24:

"Det er uklart, om artikel 24 om den dataansvarliges ansvar pålægger kommunerne nye dokumentationsforpligtelser, jf. formuleringen "... gennemfører ... foranstaltninger ... for at være i stand til at påvise, at behandling er i overensstemmelse med denne forordning."

Påvisnings-/dokumentationskravene i medfør af art. 5, stk. 2, sammenholdt med art. 24 er et tema, som fylder en del hos kommunerne. Rækkevidden af dokumentationsforpligtelsen opleves som uklar. Kommunerne efterlyser konkretisering og uddybning af påvisningskravet via mere vejledning."

Datatilsynet har i deres bidrag til den nationale evaluering, s. 17-19, skrevet følgende om artikel 24 (egne fremhævninger):

"Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24 stiller krav om, at den dataansvarlige kan påvise overholdelsen af forordningen. Det fremgår ikke direkte af forordningen, hvordan form eller indhold af denne dokumentation skal være.

Tankegangen om ansvarlighed i artikel 24 udmøntes også i andre bestemmelser i forordningen, såsom artikel 30 om fortegnelser over behandlingsaktiviteter og artikel 35 om konsekvensanalyse vedrørende databeskyttelse.

I forhold til de tidligere regler er der ikke noget nyt i, at der efter forordningens artikel 24 stilles krav om, at den dataansvarlige skal efterleve de databeskyttelsesretlige regler. Størstedelen af de krav, som stilles til den dataansvarlige efter bestemmelsen fandtes således allerede i tidligere lovgivning, om end mindre eksplicit. Se f.eks. Artikel 29-gruppens udtalelse nr. 173/2010 om princippet om ansvarlighed.

Ud over kravet om, at den dataansvarlige skal kunne påvise, at dennes behandling er i overensstemmelse med forordningen, pålægges den dataansvarlige således ikke krav, som ikke var gældende tidligere."

Og videre:

"Det er Datatilsynets opfattelse, at det direkte af måden, databeskyttelsesforordningen er opbygget på, er forudsat, at der – for en given behandlings udstrækning, fra vugge til grav – foretages en vurdering af risikoen for de registreredes rettigheder og frihedsrettigheder. Dels fremgår det af artikel 25, at dette skal ske i hele behandlingens livscyklus ("fra fastlæggelse af midlerne"), dels forudsætter artikel 35, at ingen behandling, hvor der er en høj risiko for den registreredes rettigheder og frihedsrettigheder, må påbegyndes, uden en konsekvensanalyse er blevet udført. En sådan analyse kan betragtes som en endnu grundigere risikovurdering, hvortil der er knyttet yderligere formkrav, der skal sikre, at den identificerede høje risiko nedbringes.

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Dette kan ses i sammenhæng med databeskyttelsesforordningens artikel 32, hvor fastsættelsen af de "passende tekniske og organisatoriske foranstaltninger" sker i en afvejning af risikoen for de registreredes rettigheder og frihedsrettigheder. Artikel 32, stk. 2, giver herudover en beskrivelse af, hvilke typer af scenarier der navnligt skal indgå i vurderingen.

***Samlet set skal den dataansvarlige derfor kunne dokumentere, at disse overvejelser er foretaget,** og kunne godtgøre dette også i tilfælde, hvor risikoen for den registrerede er mindre end høj.*

Det er Datatilsynets opfattelse, at dette mest hensigtsmæssigt foretages ved en struktureret tilgang, men der er intet krav herom. Uanset tilgang og form er det dog væsentligt, at Datatilsynet – hvis der kommer en klagesag eller ved tilsyn – kan modtage et samlet sæt af informationer fra den dataansvarlige, der betrygger tilsynet i, at vurderingerne er foretaget, og på de påkrævede tidspunkter i behandlingens levetid.

Datatilsynet er herudover af den overbevisning, at der kan være betragtelige forretnings- og udviklingsmæssige synergieffekter ved en sådan struktureret tilgang."

Og videre:

"Det blot at gøre gældende, at "der er gennemført en risikovurdering, og den viste lav risiko" uden nogen dokumentation til at understøtte en sådan påstand, er derfor ikke nødvendigvis nok til at betrygge Datatilsynet. Det er dog væsentligt at fastslå, at Datatilsynet i sin praksis normalt kun spørger til vurderingen i det omfang, der rent faktisk er opstået tvivl om databeskyttelsesreglernes overholdelse. Datatilsynet har herudover oplevet, at "vurderingen" af risiko først er foretaget, efter der er opstået en problematisk situation, som den dataansvarlige er havnet i (f.eks. gentagne sikkerhedsbrud). Dokumentationskravet skal derfor også sikre, at en dataansvarlig ikke blot kan påstå at have foretaget en risikovurdering (uden faktisk at have gjort det) eller påstå, at en databehandling var fundet forsvarlig grundet lav risiko uden dokumentation for, hvordan man har vurderet risikoen til at være lav.

Databeskyttelsesforordningen stiller i øvrigt ingen formkrav til risikovurderinger eller konsekvensanalyser ud over indholdskravet i databeskyttelsesforordningens artikel 35, stk. 7. Dette giver netop råderum til, at den dataansvarlige selv kan vælge en metode.

Datatilsynet vurderer altid sagens oplysninger samlet, og en vurdering eller afvejning af risikoen for den registreredes rettigheder, som den dataansvarlige har foretaget, vil altid indgå heri, selv om den ikke har titlen "Risikovurdering", og uanset hvilken metodik den følger. En titel på et dokument kan dog indikere noget om formålet/hensigten med dokumentet og kan derved være med til at henlede opmærksomheden på dets relevans.

Datatilsynet udviser en betydelig accept af en mere summarisk beskrivelse af de nødvendige overvejelser, når det gælder de små og mellemstore virksomheder samt for de behandlinger, der generisk (som følge af deres

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

natur og oplysningernes karakter) ***eller grundet stor ensartethed*** *alene udgør en begrænset risiko for de registreredes rettigheder."*

Ifølge Datatilsynet er sidste afsnit ikke møntet på kommunerne. Kommunernes behandling udgør ikke en begrænset risiko for de registreredes rettigheder, da kommunerne behandler mange oplysninger om mange personer, herunder følsomme oplysninger.

Anbefalinger til dokumentationsniveau

Læsevejledning

Nedenfor er samtlige databeskyttelsesforordningens 99 artikler gennemgået og kategoriseret i fire kategorier. Hvor artiklerne i de to første kategorier efter partnerskabets vurdering ikke medfører særskilte dokumentationsopgaver, medfører artiklerne i de sidste to kategorier krav om nedskreven dokumentation. Kategorierne er:

- Ingen krav til dokumentation
- Dokumentation via produktet i sig selv (fx fortegnelse eller databehandleraftale)
- Nedskrevne politikker og procedurer
- Dokumentation af foranstaltningers effektivitet

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

1. Ingen krav til dokumentation

I denne kategori oplistes de artikler, som partnerskabet vurderer ikke indebærer en særskilt dokumentationsforpligtelse for kommunerne. Herunder falder forordningens generelle bestemmelser, der ikke pålægger kommunerne særskilte forpligtelser. Ligeledes de bestemmelser, som kommunerne ikke anvender i praksis eller konkret ikke er omfattet af.

Art. 1-4	Omhandler forordningens genstand og formål, materielle anvendelsesområde og definitioner.
Art. 5	Efterlevelse af anbefalingerne i dette dokument udgør dokumentation for overholdelse af art. 5.
Art. 8	Omhandler informationssamfundstjenester.
Art. 11	Ikke en bestemmelse der anvendes i kommunerne.
Art. 17	Retten gælder ikke kommunale aktiviteter, jf. stk. 3.
Art. 20	Retten gælder ikke offentlig myndighedsudøvelse, jf. stk. 3.
Art. 23	Omhandler lovgivningsmæssige begrænsninger.
Art. 24	Efterlevelse af anbefalingerne i dette dokument udgør dokumentation for overholdelse af art. 24.
Art. 27	Omhandler repræsentanter der ikke er etableret i Unionen.
Art. 31	Omhandler samarbejde med tilsynsmyndigheden.
Art. 36	Kommunerne foretager ikke behandlinger uden at have begrænset risiciene ved behandlingen via foranstaltninger. Høring af Datatilsynet i denne situation vil derfor ikke blive aktuelt.
Art. 38-43	Omhandler databeskyttelsesrådgiverens stilling og opgaver, adfærdskodekser, kontrol af godkendte adfærdskodekser, certificering og certificeringsorganer.
Art. 44	Omhandler generelt princip for tredjelandsoverførsler.
Art. 47-49	Omhandler bindende virksomhedsregler, overførsel eller videregivelse uden hjemmel i EU-retten og undtagelser i særlige situationer. Bestemmelserne anvendes ikke af kommunerne.
Art. 50 + kap. VI (art. 51-59)	Omhandler internationalt samarbejde og uafhængige tilsynsmyndigheder.
Kap. VII (art. 60-76)	Omhandler samarbejde og sammenhæng.
Kap. VIII (art. 77-84)	Omhandler retsmidler, ansvar og sanktioner.
Kap. IX (art. 85-91)	Omhandler bestemmelser vedrørende specifikke behandlingssituationer.
Kap. X (art. 92-93	Omhandler delegerede retsakter og gennemførelsesforanstaltninger.

NOTAT

Kap. XI (art. 94-99)	Omhandler afsluttende bestemmelser.

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

2. Dokumentation via produktet i sig selv

I denne kategori oplistes de artikler, hvor partnerskabet vurderer, at der ikke er behov for udarbejdelse af særskilt dokumentation, udover de "produkter" der udarbejdes i medfør af bestemmelserne. Jævnfør Datatilsynets bidrag til den national evaluering af databeskyttelsesreglerne, s. 27: *"Konkrete dele af databeskyttelsesforordningen kan give støtte til påvisningen, f.eks. kravene til fortegnelse, konsekvensanalyse og databehandleraftaler."* De oplistede artikler fordrer for langt størsteparten en form for skriftlighed, som kan bruges som dokumentation. Dette gælder dog ikke hjemmelsbestemmelserne artikel 6, 9 og 10. Hjemmelsgrundlaget for kommunernes behandlinger af personoplysninger fremgår imidlertid af KL´s standardfortegnelser via henvisningen til de relevante KLE-numre (journaliseringsnøgle), hvor lovgrundlaget for behandlingerne er angivet.

En stor del af kommunernes dokumentationsforpligtelse indgår i denne kategori, og det er således vigtigt, at man i kommunen har et systematisk overblik over de produkter, der udarbejdes i medfør af de nedenfor nævnte artikler og opbevarer dem, så de er let tilgængelige ved et evt. tilsyn.

Art. 6	Angivelsen af hjemmelsgrundlaget for behandlingerne i fortegnelserne, jf. art. 30, udgør dokumentationen.
Art. 9	Angivelsen af hjemmelsgrundlaget for behandlingerne i fortegnelserne, jf. art. 30, udgør dokumentationen.
Art. 10	Angivelsen af hjemmelsgrundlaget for behandlingerne i fortegnelserne, jf. art. 30, udgør dokumentationen.
Art. 13	De oplysninger, man giver til den registrerede som led i opfyldelse af oplysningsforpligtelsen (fx selvbetjeningsløsninger, blanketter, mailtekst), udgør dokumentationen.
Art. 14	De oplysninger, man giver skriftligt til den registrerede som led i opfyldelse af oplysningsforpligtelsen, udgør dokumentationen.
Art. 26	Aftalerne om fælles dataansvar er dokumentationen.
Art. 28	Databehandleraftalerne og tilsynsrapporter for tilsyn med databehandlere er dokumentationen.
Art. 29	Databehandleraftalen eller en fortrolighedserklæring er dokumentationen.
Art. 30	Fortegnelserne er dokumentationen.
Art. 32	De nedskrevne risikovurderinger og de på den baggrund gennemførte foranstaltninger udgør dokumentationen.
Art. 33	Anmeldelsen af sikkerhedsbruddet, jf. stk. 1 og 3, samt dokumentationen af sikkerhedsbrud, jf. stk. 5, er dokumentationen.
Art. 34	Underretningen om sikkerhedsbruddet er dokumentationen.
Art. 35	Konsekvensanalysen er dokumentationen.
Art. 37	Udpegelsen af databeskyttelsesrådgiveren, som er sendt til Datatilsynet, jf. stk. 7, er dokumentationen.
Art. 45	Overførselsgrundlaget for tredjelandsoverførsler angivet i databehandleraftalerne er dokumentationen.
Art. 46	Overførselsgrundlaget for tredjelandsoverførsler angivet i databehandleraftalerne er dokumentationen.

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Kommunale eksempler

Reguleringen af brugen af databehandlere i art. 28 er et eksempel på, hvor dokumentationen udgøres af de "produkter", som bestemmelsen kræver. Det vurderes fx ikke påkrævet, at kommunerne udarbejder særskilt dokumentation for vurderingen af, hvorvidt databehandleren kan stille fornødne garantier for at ville gennemføre passende foranstaltninger, jf. stk. 1. Idet det fremgår af databehandleraftalen, at databehandleren forpligter sig hertil. Det samme gør sig gældende for det øvrige indhold af databehandleraftalen, herunder eventuelle krav om revisionsrapporter. At processen omkring indgåelsen af en databehandleraftale ikke dokumenteres som følge af databeskyttelsesforordningens dokumentationskrav betyder ikke, at dokumentation af forhandlingsprocessen ikke kan være relevant af fx forvaltningsretlige eller kontraktuelle årsager.

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

3. Nedskrevne politikker og procedurer

I denne kategori oplistes artikler, hvor partnerskabet vurderer, at der bør foreligge nedskrevne procedurer i kommunen for at opfylde dokumentationsforpligtelsen. Disse procedurer nedskrives som handlingsanvisende retningslinjer, der konkret beskriver, hvordan en medarbejder bør agere i forhold til et krav i forordningen. At procedurerne er nedskrevet og gjort synligt tilgængelige for kommunens medarbejdere medvirker dels til, at medarbejderne agerer ensartet og efter kommunens instruktioner dels, at kommunen kan påvise overholdelsen af bestemmelserne. Det vil i praksis være svært at dokumentere, at medarbejdere kender til en procedure, hvis den ikke er nedskrevet og tilgængelig. Medarbejdere kan eventuelt informeres om de nedskrevne procedurer via kommunens formelle dokumenter om informationssikkerhed, databeskyttelse og GDPR.

Partnerskabet vurderer, at en kommune bør have ét eller flere dokumenter af formel karakter, som medarbejderne introduceres til, fx i forbindelse med ansættelse eller kurser. De fleste kommuner har en informationssikkerhedspolitik og en del har en GDPR-håndbog, it-håndbog mv. hvor medarbejdere og ledere i kommunen kan få en forståelse af kommunens arbejde med informationssikkerhed og databeskyttelse, og hvilke forpligtelser de selv har i overholdelsen af GDPR.

Nedenstående nævnte artikler er et anbefalet minimum af procedurer, som kommunerne bør have. For den enkelte kommune kan det være relevant at udarbejde yderligere retningslinjer og procedurer. For eksempel hvis kommunen ønsker at udarbejde procedurebeskrivelser rettet mod kommunens enkelte fagområder og/eller særskilte funktioner.

Det er dog væsentligt at være opmærksom på, at ifølge artikel 24, stk. 2, skal kommunerne alene implementere databeskyttelsespolitikker, "Hvis det står i rimeligt forhold til behandlingsaktiviteter". Det betyder ifølge Datatilsynet, at kommunerne i situationer, hvor behandlingsaktiviteter er sjældent forekommende, fx ved få indsigtsanmodninger fra borgerne, ikke behøver at udarbejde nedskrevne politikker og/eller procedurebeskrivelser for de pågældende behandlingsaktiviteter. Her vil det ifølge Datatilsynet fx være tilstrækkeligt organisatorisk at have sikret, at der er én eller flere medarbejdere, der kender til procedurerne for den pågældende behandlingsaktivitet, "dem tager Bjarne sig af".

Art. 7	Dokumentation via nedskrevet procedure for, hvordan der indhentes samtykke og, hvordan samtykke trækkes tilbage.
Art. 12	Dokumentation via nedskrevet procedure for håndtering af de registreredes rettigheder, herunder krav til kommunikation.
Art. 15	Dokumentation via nedskrevet procedure for, hvordan man behandler en anmodning om indsigtsret.
Art. 16	Dokumentation via nedskrevet procedure for, hvordan man behandler en anmodning om berigtigelse.
Art. 18	Dokumentation via nedskrevet procedure for, hvordan man behandler en anmodning om begrænsning.

Art. 19	Dokumentation via nedskrevet procedure for, hvordan man underretter modtagere om berigtigelse, sletning eller begrænsning.
Art. 21	Dokumentation via nedskrevet procedure for, hvordan man behandler en anmodning om indsigelse mod behandling.
Art. 22	Dokumentation via nedskrevet procedure for, hvordan man behandler en anmodning om indsigelse mod automatiske, individuelle afgørelser og profilering.
Art. 25	Dokumentation via en nedskrevet procedure for sikring af databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i forbindelse med indkøb, udvikling og opsætning af nye systemer (bruger-/rettighedsstyring).
Art. 32	Dokumentation via nedskrevet procedure for, hvornår og hvordan der udarbejdes risikovurderinger af kommunens behandlingsaktiviteter samt gennemføres sikkerhedsforanstaltninger (tekniske som organisatoriske), på baggrund af risikovurderingerne.
Art. 33	Dokumentation via en nedskrevet procedure for håndtering af sikkerhedsbrud.
Art. 34	Dokumentation via en nedskrevet procedure for underretning om brud på persondatasikkerheden til den registrerede.

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk

Dato: 21. juni 2022

Sags ID: SAG-2021-06054
Dok. ID: 3206455

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

Weidekampsgade 10
Postboks 3370
2300 København S

www.kl.dk
Side 15 af 15

4. Dokumentation af foranstaltningers effektivitet

For at leve op til den dataansvarliges ansvar i medfør af artikel 24 skal kommunen, udover at gennemføre givne foranstaltninger, også sikre sig, at disse foranstaltninger er effektive. I denne kategori oplistes de artikler, hvor partnerskabet vurderer, at kommunen bør have en "opfølgningsplan" for at kunne dokumentere foranstaltningernes effektivitet.

Opfølgningen bør tilrettelægges ud fra en risikobaseret betragtning ift. konsekvensen af en foranstaltnings manglende effektivitet.

Art. 5 og 24	Kommunens medarbejdere skal indføres i reglerne i databeskyttelsesforordningen, herunder behandlingsprincipperne, og de udarbejdede procedurebeskrivelser via skriftlig information, undervisning etc. Kommunen bør have en skriftlig plan for uddannelse af medarbejderne, herunder for nye medarbejdere og løbende "genopfriskning" af medarbejdernes viden. Uddannelsesplanen er kommunens dokumentation.
Art. 28	Via tilsynsrapporterne for tilsyn med databehandlerne følges der op på, om de aftalte iværksatte tekniske og organisatoriske sikkerhedsforanstaltninger til stadighed er effektive. Skriftlig stillingtagen til tilsynsrapport, herunder beslutning om nødvendige justeringstiltag, er dokumentationen.
Art. 30	Kommunen udarbejder en plan for at følge op på, at fortegnelserne til stadighed er dækkende for kommunens behandlingsaktiviteter.
Art. 32	Der følges op på, om de iværksatte tekniske og organisatoriske sikkerhedsforanstaltninger i kommunen til stadighed er effektive. Denne opfølgning bør tilrettelægges efter en struktureret og risikobaseret tilgang, fx. via et "årshjul".
Art. 33, stk. 5	Kommunen udarbejder en plan for opfølgning på, hvorvidt kommunens tiltag til at undgå sikkerhedsbrud er effektive.