Dansk persondataret

Bent Ole Gram Mortensen (red.)

Dansk persondataret

Ex Tuto
PUBLISHING
www.extuto.com

Bent Ole Gram Mortensen (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Markvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Starup, Jøren Ullits & Frederik Waage
Dansk persondataret
Første udgave, første oplag

Denne bog er udgivet i januar 2020 af Ex Tuto Publishing A/S. Grafisk tilrettelæggelse og sats af mere.info A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis František Štorm i 2000 og Robert Slimbach i 1996. Jan Trzaskowski har stået for forlagsredaktion og Tove Møgelvang-Hansen har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m^2 af Narayana Press, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af Buchbinderei S.R. Büge GmbH i Celle. Bogen er fagfællebedømt.

Ex Tuto A/S er medlem af Forening for Boghaandværk, og vi støtter bæredygtig skovforvaltning ved at anvende FSC-certificeret papir.

Printed in Denmark 2020
ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S
Toldbodgade 55, 1.
DK-1253 København K
www.extuto.com

MIX
Papir fra ansvarlige kilder
FSC® C010651
www.fsc.org

Udgivet med støtte fra
dreyersfond

FairPublishing

Kapiteloversigt

Kapitel 11

Databeskyttelsesrådgiveren

Lisa Hjerrild

11.1. Indledning

Databeskyttelsesrådgiveren (DPO – *Data Protection Officer*) er en nyskabt aktør og rolle, som blev etableret i kraft af og med databeskyttelsesforordningen. Med virkning fra 25. maj 2018 er offentlige myndigheder, offentlige organer og visse virksomheder forpligtet til at have en uafhængig databeskyttelsesrådgiver med ekspertise i databeskyttelsesret og -praksis til at hjælpe den dataansvarlige eller databehandleren med at overvåge myndigheden eller virksomhedens interne overholdelse af forordningen.

Den danske terminologi er rettelig *databeskyttelsesrådgiveren*, men den engelske forkortelse DPO er blevet udbredt også i Danmark. Forkortelsen DPO bliver også anvendt i det følgende som fuldstændigt synonym med databeskyttelsesrådgiver.

Baggrunden for, at man valgte at indføre DPO-rollen, skal ses i sammenhæng med databeskyttelsesforordningens fokus på ansvarlighed, se herom i kapitel 9, afsnit 9.2. Forordningens fokus på beskyttelse af de registrerede, underbygges af den status, DPO har fået i forordningen, og i praksis, hvor der i tiden op til forordningens ikrafttræden var betydeligt fokus på uddannelse og certificering af DPO'er.[1] Der er tale

1. Se GDPR præambelbetragtning nr. 97.

om en nyskabt rolle og derfor også en rolle, som skal finde sit ståsted i de enkelte organisationer, der er forpligtet til at have en DPO og få fodfæste i forhold til, hvilken rolle og funktioner DPO'en har internt i organisationen såvel som udadtil.

Forordningens artikel 37-39 indeholder de formelle og materielle bestemmelser om DPO'ens rolle, ansvar og pligter. Databeskyttelseslovens § 24 supplerer med en bestemmelse om tavshedspligt for DPO'ere i den private sektor. Reguleringen af DPO'ere er derudover suppleret af retningslinjer og vejledninger som hjælp til at forstå reglerne om DPO'ere. Artikel 29-Gruppen for Databeskyttelse har udarbejdet Retningslinjer for Databeskyttelsesrådgivere (WP 243).[2] Den danske tilsynsmyndighed, Datatilsynet, har udgivet Vejledning om Databeskyttelsesrådgivere.[3] Datatilsynets formål med vejledningen er at redegøre for kravene i forordningen til at udpege en databeskyttelsesrådgiver, dennes opgaver, kvalifikationer, stilling og inddragelse, og kan således bruges som et værktøj for virksomheder, der er i tvivl om reglerne for DPO'ere.[4]

11.2. DPO'ens funktion og formål

Dataansvarlige og databehandlere skal altid være opmærksomme på efterlevelse af databeskyttelsesforordningens krav og have overblik over, hvilke personoplysninger der behandles, hvordan de behandles, og hvordan de sikre, at forordningens krav efterleves. Formålet med at etablere en ordning med DPO'er er at sikre, at organisationer, hvis kerneaktiviteter består i behandlingsaktiviteter, som kræver regelmæssig og systematisk overvågning af registrerede i stort omfang, eller hvis den dataansvarliges eller databehandlerens kerneaktiviteter består af behandling i stort omfang af særlige kategorier af oplysninger og oplysninger vedrørende straffedomme og lovovertrædelser, bliver bistået af en person med ekspertise i databeskyttelsesret og -praksis til at overvåge den interne overholdelse af forordningen.[5]

2. Artikel 29-Gruppens WP 243.
3. Datatilsynet 2017a.
4. Ibid., s. 2.
5. Artikel 37 og præambelbetragtning 97.

11.3. Hvem er forpligtet til at have en DPO (artikel 37)

Databeskyttelsesforordningens artikel 37 fastlægger, hvilke dataansvarlige og databehandlere der er forpligtet til at udpege en DPO. De forpligtede til at udpege en DPO kan opdeles i offentlige myndigheder eller private. Det vil blive behandlet separat i det følgende.

11.3.1. DPO hos offentlige myndigheder og offentlige organer

Offentlige myndigheder og offentlige organer skal i alle tilfælde uanset, om de er dataansvarlige eller databehandlere, udpege en DPO.[6] Offentlige myndigheder kan behandle personoplysninger som led i deres almindelige funktionsområde, eller hvis den offentlige myndighed som dataansvarlig vælger at outsource sin databehandling til en privat, som ellers ikke ville være forpligtet til at udpege en DPO. Dette kan eksempelvis være tilfældet, hvor en offentlig myndighed som dataansvarlig vælger at overlade selve den praktiske behandling af personoplysninger til en privat aktør. I disse tilfælde vil den offentlige myndighed som dataansvarlig stadig være forpligtet til at udpege en DPO.

Det er dog i nogle tilfælde ikke altid entydigt at fastlægge, hvilke virksomheder eller aktører der skal henregnes til at være offentlige myndigheder eller offentlige organer. Det følger af Datatilsynets Vejledning om Databeskyttelsesrådgivere, at de omfattede myndigheder er de myndigheder, der efter forvaltningslovens § 1, stk. 1-2, anses for at være offentlige myndigheder eller organer. Dette inkluderer alle dele af den offentlige forvaltning samt al virksomhed, der udøves af selvejende institutioner, foreninger, fonde m.v., der er oprettet ved lov eller i henhold til lov, og selvejende institutioner, foreninger, fonde m.v., der er oprettet på privatretligt grundlag, og som udøver offentlig virksomhed af mere omfattende karakter og er undergivet intensiv offentlig regulering, intensivt offentligt tilsyn og intensiv offentlig kontrol.[7] Særligt for selvejende institutioner, der er oprettet på privatretligt grundlag, vil det være afgørende, om de udøver offentlig virksomhed af mere omfat-

6. Jf. artikel 37, stk. 1, litra a.
7. Forvaltningslovens § 1, stk. 1 og 2.

tende karakter og er undergivet intensiv offentlig regulering, tilsyn og kontrol, eksempelvis universiteter eller selvejende institutioner.

Domstole og andre domstolslignende organer er undtaget fra kravet om at udpege en DPO og er således ikke forpligtet til at udpege en DPO, når de handler i egenskab af domstole.[8]

11.3.2. DPO i den private sektor

I langt de fleste tilfælde skal dataansvarlige og databehandlere i den private sektor ikke udpege en DPO. En dataansvarlig eller en databehandler skal altid udpege en databeskyttelsesrådgiver, når den dataansvarliges eller databehandlerens kerneaktiviteter består af behandlingsaktiviteter, der i medfør af deres karakter, omfang og/eller formål kræver regelmæssig og systematisk overvågning af registrerede i stort omfang,[9] eller hvis den dataansvarliges eller databehandlerens kerneaktiviteter består af behandling i stort omfang af særlige kategorier af oplysninger (artikel 9), og personoplysninger vedrørende straffedomme og lovovertrædelser (artikel 10).[10]

Forordningen opstiller tre betingelser for, hvornår private er forpligtet til at udpege en DPO. Betingelserne omhandler, hvilke typer af personoplysninger organisationen har, hvordan og i hvilket omfang de behandles. Alle tre betingelser skal være opfyldt og er derfor kumulative betingelser.

Den første betingelse er, at behandling af personoplysninger skal være organisationens kerneaktivitet.[11] Det skal altså være organisationens primære opgave og ikke en biaktivitet som f.eks. kunderegister i en butik eller HR-oplysninger, som anses for at være almindelig behandling af personoplysninger, som de fleste virksomheder er i berøring med. Af eksempler på organisationer, der behandler personoplysninger som deres kerneaktivitet, nævner Datatilsynets vejledning bl.a. cloud-løsninger, hosting af hjemmesider og data, forsikringsselskaber og søgemaskiner.[12]

8. Jf. artikel 37, stk. 1, litra a, sidste led.
9. Jf. artikel 37, stk. 1, litra b.
10. Jf. artikel 37, stk. 1, litra c.
11. Betingelsen gælder både for aktiviteter omfattet af artikel 37, stk. 1 litra b og c.
12. Datatilsynet 2017a, s. 8.

Den anden betingelse er, at behandling af personoplysninger skal foregå i et stort omfang.[13] Termen "i et stort omfang" kan være flertydigt. Artikel 29-Gruppen har udtalt, at der ved vurdering af, om der er tale om behandling af personoplysninger, i et stort omfang navnlig kan lægges vægt på følgende fire kriterier: (1) højt antal af registrerede, som behandles – enten som specifikt tal eller som en procentdel af befolkningen, (2) stor mængde af data og/eller omfanget af forskellige datatyper, som behandles, (3) databehandlingsaktivitetens varighed er lang eller permanent og (4) databehandlingsaktivitetens geografiske udstrækning dækker et stort område.[14] Af eksempler på virksomheder, der behandler personoplysninger i et stort omfang, er større privathospitaler, større forsikringsselskaber, søgemaskiners behandling af personoplysninger og tele- og internetudbydere.[15]

Hvis behandling af personoplysninger er organisationens kerneaktivitet, og det foregår i et stort omfang, er tredje og sidste betingelse for, at organisationen er forpligtet til at udpege en DPO, at behandling af personoplysningerne består af regelmæssig og systematisk overvågning af personer *eller* vedrører følsomme personoplysninger eller oplysninger om strafbare forhold. For så vidt angår betingelsen for regelmæssig og systematisk overvågning af personer, omfatter det eksempelvis sporing (tracking) på internettet eller profilering, f.eks. i forbindelse med vurdering af forsikringspræmier, kreditvurdering eller lokationstracking. De omhandlede følsomme oplysninger følger af forordningens artikel 9 og strafbare forhold (straffedomme og lovovertrædelser) af forordningens artikel 10. Typeeksemplerne på virksomheder, der opfylder alle tre betingelser, er eksempelvis større privathospitaler, større forsikringsselskaber, tele- og internetudbydere eller reklamebureauer, der tilbyder marketingsundersøgelser.

11.3.3. Fælles DPO

For koncerner er der mulighed for at udpege en fælles DPO.[16] Det er dog en forudsætning, at alle dele af koncernen har let adgang til

13. Kriteriet gælder både for aktiviteter omfattet af artikel 37, stk. 1, litra b og c.
14. Se Artikel 29-Gruppen WP 243 rev.01, s. 8.
15. Se Datatilsynet 2017a, s. 9.
16. Jf. artikel 37, stk. 2.

DPO'en, og at denne opfylder uafhængighedskravet for alle virksomhederne. Både offentlige myndigheder og private virksomheder kan inden for deres koncern have en fælles DPO. Hvis to eller flere organisationer ikke er koncernforbundne, men ønsker at dele en DPO, vil de være nødsaget til at ansætte DPO'en i hver enkelt virksomhed, eventuelt på en deltidskontrakt.

11.3.4. Frivillig udpegelse af DPO

Databeskyttelsesforordningen udelukker ikke, at andre virksomheder end de forpligtede frivilligt kan udpege en DPO. Virksomheden skal da være opmærksom på, at der gælder de samme krav til DPO'en som i de tilfælde, hvor virksomheden ville være forpligtet til at udpege en DPO.[17] Anvendes et andet navn for opgaven, f.eks. "complience-officer", stilles der ikke tilsvarende krav om, at DPO'en skal efterleve forordningens krav til DPO'er.

11.4. DPO'ens stilling (krav til DPO'en) (artikel 38)

De omfattede virksomheder, som omtalt ovenfor i afsnit 11.3, skal efter artikel 38 bistås af en rådgiver (DPO) med ekspertise i databeskyttelsesret og -praksis.[18] DPO'en skal være uafhængig og på baggrund af sin ekspertise kunne udøve uvildig rådgivning til organisationen såvel som overvåge, at forordningens regler bliver efterlevet.[19] Relationen mellem rådgiveren og den dataansvarlige/databehandleren må indgyde til fortrolighed, men også en respekt for DPO'ens ekspertise til at understøtte en effektiv databeskyttelse i virksomheden.[20]

11.4.1. DPO'en skal udpeges

Med forordningens terminologi skal DPO'en "udpeges" af den dataansvarlige eller databehandleren.[21] Udtrykket understreger DPO'ens vigtige position i virksomheden; hos den dataansvarlige/databehandleren. Det er ikke blot en vilkårlig medarbejder placeret et vilkårligt sted

17. Se herom i Datatilsynet 2017a, s. 12.
18. Jf. artikel 37, stk. 1 og 5.
19. Artikel 39, stk. 1.
20. GDPR præambelbetragtning nr. 97.
21. Jf. artikel 37, stk. 1.

i organisationen, men en person, som er udpeget til at udføre en række lovbestemte opgaver i organisationen. DPO'en rapporterer direkte til det øverste ledelsesniveau hos den dataansvarlige eller databehandleren og skal have en direkte adgang til at rådgive og underrette om databeskyttelsesmæssige udfordringer i organisationen.[22] DPO'ens opgaver vil blive gennemgået nedenfor under afsnit 11.5.

Ved udpegning af en DPO skal der særligt lægges vægt på DPO'ens faglige kvalifikationer og ekspertise for at besidde hvervet. Det er afgørende, at vedkommende har en nødvendig faglig indsigt i forordningen. Forordningen stiller eksplicit krav om, at DPO'en skal besidde en særlig ekspertise inden for databeskyttelsesret og -praksis.[23] Ekspertisen skal ses i forhold til de behandlingsaktiviteter, der foretages, og det beskyttelsesniveau, de behandlede personoplysninger kræver. Endvidere skal graden af DPO'ens ekspertise vurderes ud fra evnen til at udføre de opgaver, som følger af artikel 39, og som organisationen kræver. Der stilles ikke krav om, at DPO'en skal have en særlig uddannelsesmæssig baggrund, f.eks. som it-specialist, revisor, jurist eller være særlig certificeret. For nogle organisationer vil det være nødvendigt, at DPO'en har en særligt høj ekspertise på grund af de kategorier og typer af personoplysninger, der behandles, mens det for andre organisationer vil være tilstrækkeligt, at en intern medarbejder udpeges, evt. efter at have deltaget i relevante kurser om emnet.[24]

11.4.2. Placering i virksomheden

Der er som nævnt ovenfor ingen krav til, hvor i en organisation DPO'en er placeret, eller hvem denne har som overordnet. Men at DPO'en skal have direkte adgang til ledelsen, må betyde, at DPO'en ikke blot kan have en mindre rolle i myndigheden eller virksomheden. DPO'en kan enten være ansat som konsulent eller indgå i et medarbejderforhold med virksomheden.[25] Det er den dataansvarlige og databehandlerens ansvar at sikre, at DPO'en ikke modtager instrukser vedrørende udførelsen af sine opgaver i medfør af databeskyttelsesforord-

22. Jf. artikel 38, stk. 3, sidste punktum.
23. Jf. artikel 37, stk. 5.
24. Datatilsynet 2017a, s. 20 f.
25. Jf. artikel 37, stk. 6.

ningen.[26] Der er tale om en særlig ansættelsesretlig beskyttelse, idet man i sædvanlige ansættelsesforhold er underlagt arbejdsgiverens instrukser. Af samme grund er det eksplicit fastsat i forordningen, at DPO'en ikke kan afskediges eller straffes af den dataansvarlige eller databehandleren for at udføre sine opgaver, som følger af forordningen.[27] Det betyder omvendt også, at beskyttelsen ikke er en immunitet. Det er derfor ikke usandsynligt, at DPO'en kan afskediges for mangelfuld opfyldelse af sine opgaver efter forordningen eller andre opgaver, som ikke er relateret til arbejdet som DPO.

Det er ikke altid, opgaverne som DPO modsvarer en fuldtidsstilling i en virksomhed, og der er ej heller noget i vejen for, at DPO'en kan udføre andre opgaver og have andre pligter i virksomheden. Det er op til den dataansvarlige eller databehandleren at sikre, at sådanne opgaver og pligter ikke medfører en interessekonflikt mellem rollen som DPO (at være uvildig rådgiver) og virksomhedens øvrige interesser.[28] Der kan eksempelvis opstå interessekonflikter, hvis DPO'en ligeledes var øverste it-ansvarlige eller HR-ansvarlige. Det afgørende er ifølge Datatilsynet, at medarbejderen ikke har det øverste ansvar.[29] Således kan ledende it-medarbejdere, complience-officers eller it-sikkerhedskoordinatorer godt udøve rollen som DPO, men ikke deres chef. Er der meget få ansatte i en virksomhed, som er forpligtet til at have en DPO, kan det være nødvendigt at anvende en ekstern konsulent som DPO eller udpege en fælles DPO sammen med andre virksomheder.[30]

11.4.3. Forholdet til den dataansvarlige og databehandleren

Den dataansvarlige og databehandleren skal sikre, at DPO'en inddrages tilstrækkeligt og rettidigt i alle spørgsmål vedrørende beskyttelse af personoplysninger.[31] Det kræver, at virksomheden giver DPO'en

26. Jf. artikel 38, stk. 3.
27. Jf. artikel 38, stk. 3, 2. punktum.
28. Jf. artikel 38, stk. 6.
29. Datatilsynet 2017a, s. 21.
30. Se artikel 37, stk. 3 og 4.
31. Jf. artikel 38, stk. 1.

mulighed og adgang til at få indsigt i virksomhedens ansvar og forpligtelser, som følger af databeskyttelsesforordningen.

Den dataansvarlige og databehandleren skal støtte DPO'en i forbindelse med udførelsen af de opgaver, som følger af artikel 39. Det indebærer blandt andet, at den dataansvarlige og databehandleren skal give DPO'en nødvendige ressourcer til at udføre disse opgaver.[32] Det medfører også, at de skal medvirke til at opretholde databeskyttelsesrådgiverens ekspertise, samt adgang til personoplysninger og behandlingsaktiviteter.

11.4.4. DPO'ens forhold til Datatilsynet

I medfør af DPO'ens opgaver, som følger af artikel 39, må det antages, at DPO'en har en særlig rolle i forhold til Datatilsynet. DPO'en skal fungere som kontaktleddet mellem Datatilsynet og virksomheden, og DPO'en må derfor være opdateret på nyeste lovgivning, afgørelser, vejledninger, praksis mv. Ved indsamling af personoplysninger er den dataansvarlige forpligtet til at oplyse den registrerede om DPO'ens kontaktoplysninger.[33]

11.4.5. Tavshedspligt

En DPO vil naturligt komme i berøring med en stor mængde personoplysninger i den enkelte organisation – både almindelige og følsomme personoplysninger. For DPO'er hos offentlige myndigheder er de underlagt den almindelige tavshedspligt i medfør af forvaltningslovens § 27. For DPO'er i den private sektor, som er udpeget efter artikel 37, stk. 1, litra b og c, følger tavshedspligten af databeskyttelseslovens § 24, hvorefter DPO'en ikke uberettiget må videregive eller udnytte oplysninger, som de under udøvelsen af deres hverv som DPO er blevet bekendt med.

11.5. DPO'ens opgaver (artikel 39)

Databeskyttelsesforordningens artikel 39 fastlægger DPO'ens obligatoriske opgaver, dvs. de opgaver, DPO'en som minimum skal udføre for

32. Jf. artikel 38, stk. 2.

33. Se artikel 13 og 14 om oplysningskrav ved indsamling af personoplysninger.

at opfylde forordningens krav. DPO'en kan udføre en række andre opgaver i organisationen, men disse andre opgaver må ikke give anledning til, at der kan opstå interessekonflikter, eller at DPO'en ikke kan varetage sine opgaver som DPO.[34]

DPO'ens opgave består først og fremmest i at underrette og rådgive den dataansvarlige eller databehandleren og de ansatte, der behandler personoplysninger, om deres forpligtelser i henhold til databeskyttelsesforordningen og anden EU-ret eller national ret i de enkelte medlemsstater om databeskyttelse.[35] Opgaven skal ses i sammenhæng med den tilsvarende forpligtelse for den dataansvarlige eller databehandleren til at sikre, at DPO'en rettidigt inddrages i alle spørgsmål vedrørende beskyttelse af personoplysninger.[36]

Derudover består en væsentlig opgave for DPO'en i at overvåge den dataansvarliges overholdelse af databeskyttelsesforordningen og andre regler om databeskyttelse og af den dataansvarliges eller databehandlerens politikker om beskyttelse af personoplysninger, herunder fordeling af ansvar, oplysningskampagner og uddannelse af det personale, der medvirker ved behandlingsaktiviteter, og de tilhørende revisioner.[37] Heri ligger også, at DPO'en skal være synlig i organisationen og agere tydeligt i forholdet til de øvrige ansatte.

Yderligere skal DPO'en rådgive den dataansvarlige eller databehandleren, når de anmodes herom i forhold til udarbejdelse af konsekvensanalysen vedrørende databeskyttelse og overvåge dens opfyldelse.[38] Se mere om konsekvensanalysen i kapitel 12.

Endvidere er DPO'en forpligtet til at samarbejde med tilsynsmyndigheden.[39] DPO'en skal fungere som tilsynsmyndighedens kontaktpunkt i spørgsmål vedrørende behandling personoplysninger i organisationen, f.eks. ved den forudgående høring i forbindelse med konsekvensanalyser.[40] Når det er relevant og hensigtsmæssigt, skal DPO'en

34. Jf. artikel 38, stk. 6.
35. Jf. artikel 39, stk. 1, litra a.
36. Jf. artikel 38, stk. 1.
37. Jf. artikel 39, stk. 1, litra b.
38. Jf. artikel 39, stk. 1, litra c.
39. Jf. artikel 39, stk. 1, litra d.
40. Jf. artikel 39, stk. 1, litra e.

høre tilsynsmyndigheden om eventuelle spørgsmål, som vil være relevante at få afdækket, for at DPO'en kan udføre sine opgaver som uafhængig rådgiver for organisationen.

11.6. Hvis ingen DPO – Adfærdskodeks (artikel 40)

Såfremt en virksomhed ikke har en DPO, kan de i deres arbejde med at sikre databeskyttelse have gavn af at anvende adfærdskodeks og certificeringsordninger. Der er ikke krav om, at der skal anvendes adfærdskodeks, men en kodeks kan udgøre et værktøj for den enkelte organisation. Med forordningen har Kommissionen ansporet en bedre databeskyttelse for de registrerede og opfordret til at fremme certificeringsmekanismer og databeskyttelsesmærkninger og -mærker, så registrerede hurtigt kan vurdere databeskyttelsesniveauet i forbindelse med relevante produkter og tjenester.[41]

En adfærdskodeks efter forordningen er et sæt retningslinjer, som skal bidrage til at sikre, at de virksomheder, der har tilsluttet sig kodeksen, anvender reglerne i databeskyttelsesforordningen korrekt.[42] Kodeksens retningslinjer skal bidrage til at sikre en korrekt anvendelse af forordningens regler ved at angive, hvordan man i specifikke typetilfælde skal håndtere behandlingen af personoplysninger. Det kan f.eks. være ved at fastlægge nogle procedurer, som skal følges for en specifik type behandling af personoplysninger. Det gælder især små og mellemstore virksomheder. Brancheforeninger har stort indblik i den enkelte branche eller kategori af virksomheder, som de repræsenterer, og kan med fordel udarbejde adfærdskodeks om databeskyttelse med henblik på at fremme en effektiv anvendelse af forordningens bestemmelser under hensyntagen til de specifikke typer af behandling, der foretages i visse sektorer, og de særlige behov hos mikrovirksomheder og små og mellemstore virksomheder.[43] Sådanne adfærdskodekser bør navnlig kunne justere dataansvarliges og databehandleres forpligtelser, og derved kan der tages hensyn til den risiko, som sandsynligvis vil følge af behandlingen for fysiske personers rettigheder og frihedsrettigheder. Ved udarbejdelsen af en adfærdskodeks bør brancheforeninger og

41. GDPR præambelbetragtning nr. 100.
42. Datatilsynet 2018c, s. 4.
43. Artikel 40, stk. 1 og præambelbetragtning nr. 98.

andre sammenslutninger, der repræsenterer kategorier af dataansvarlige eller databehandlere, høre relevante interessenter, herunder også de registrerede, hvis det er muligt, og tage hensyn til bemærkninger og synspunkter, der er fremsat som svar på sådanne høringer.[44] Endvidere skal en adfærdskodeks i medfør af forordningen (artikel 40) godkendes af den nationale tilsynsmyndighed, i Datatilsynet i Danmark.[45]

En adfærdskodeks kan indeholde bestemmelser om rimelig og gennemsigtig behandling, de legitime interesser, som forfølges af den dataansvarlige i specifikke sammenhænge, indsamlingen af personoplysninger, pseudonymiseringen af personoplysninger, den information, der gives til offentligheden og til registrerede, udøvelsen af registreredes rettigheder, den information, der gives til børn, og beskyttelsen af børn og den måde, hvorpå samtykket fra indehavere af forældremyndighed over børn skal indhentes, og hvordan brud på persondatasikkerheden skal anmeldes til tilsynsmyndighederne og håndteringen af underretningen af de registrerede om sådanne brud på persondatasikkerheden. Overholdelsen af en adfærdskodeks kan på den måde være medvirkende til at påvise, at den dataansvarlige eller databehandleren overholder forordningen, men det kan formentlig ikke være et egentligt bevis på overholdelse af forordningens regler.

44. GDPR præambelbetragtning nr. 99.
45. Jf. artikel 40, stk. 5.