VEJLEDNING ADFÆRDSKODEKSER OG CERTIFICERINGSORDNINGER

**Adfærdskodekser**

Hvad er adfærdskodekser?

Et adfærdskodeks er et sæt af retningslinjer, som sikrer, at virksomheder, der tilslutter sig kodekset overholder databeskyttelsesforordningens krav.

Kodekserne indeholder retningslinjer for, hvordan man i specifikke tilfælde skal håndtere behandlingen af personoplysninger for at overholde kravene i databeskyttelsesforordningen.

De virksomheder eller organisationer, der tilslutter sig et bestemt kodeks, kan ydermere bruge dette til at dokumentere/påvise, at der leves op til forpligtigelserne efter forordningen. Dog skal man være opmærksom på, at en tilslutning og en overholdelse af et godkendt adfærdskodeks ikke i sig selv er et bevis på overholdelse af forordningen. Ligeså kan adfærdskodekset ikke fritage den dataansvarlige ansvaret for, at forordningens krav overholdes.

Man er aldrig forpligtiget til at tilslutte sig et adfærdskodeks, og man kan sagtens overholde forordningens krav uden en sådan tilslutning.

Hvem kan lave adfærdskodekserne?

Efter databeskyttelsesforordningen er det bestemt, at sammenslutninger eller andre organer, der repræsenterer kategorier af dataansvarlige eller databehandlere, kan udarbejde adfærdskodekser. Dette kan f.eks. være brancheorganisationer eller andre foreninger.

Hvad kan adfærdskodekser bruges til?

Ifølge databeskyttelsesforordningen, kan adfærdskodekser tænkes at specificere anvendelse af en række af forordningens regler. I forordningen nævnes følgende eksempler:

* Rimelig og gennemsigtig behandling
* De legitime interesser, som forfølges af den dataansvarlige i specifikke sammenhænge
* Indsamlingen af personoplysninger
* Pseudonymiseringen af personoplysninger
* Informationen, der gives til offentligheden og til registrerede
* Udøvelsen af registreredes rettigheder
* Informationen, der gives til børn, og beskyttelsen af børn og den måde, hvorpå samtykket fra indehavere af forældremyndighed over børn skal indhentes
* Foranstaltningerne og procedurerne omhandlet i artikel 24 og 25 og foranstaltningerne til at sikre behandlingssikkerhed som omhandlet i artikel 32
* Anmeldelse af brud på persondatasikkerheden til tilsynsmyndighederne og underretningen af de registrerede om sådanne brud på persondatasikkerheden
* Overførslen af personoplysninger til tredjelande eller internationale organisationer, eller
* Udenretslige procedurer og andre procedurer for bilæggelse af tvister mellem dataansvarlige og registrerede vedrørende behandling, uden at det berører registreredes rettigheder i henhold til artikel 77 og 79.

Herudover kan et tilsluttet adfærdskodeks bruges som et element til at kunne påvise, at den dataansvarlige lever op til sine forpligtigelser.

Ligeledes kan kodekset bruges til at påvise, at den databehandler, som den dataansvarlige bruger, stiller de fornødne garantier i forhold til gennemførelse af tekniske og organisatoriske foranstaltninger.

Kodekset kan i den forbindelse også bruges til at påvise, at den dataansvarlige og databehandleren overholder kravene til behandlingssikkerhed.

Tilslutning af et adfærdskodeks skal også inddrages i en konkret konsekvensanalyse.

Hvis man som dataansvarlig har brug for at overføre personoplysninger til et tredjeland, skal man have et såkaldt overførelsesgrundlag for at gøre dette. Det er i forordningen bestemt, at et sådan overførelsesgrundlag godt kan sikres igennem et godkendt adfærdskodeks. Det er en betingelse for dette, at der foreligger et bindende tilsagn, som kan håndhæves fra den dataansvarlige eller databehandleren i tredjelandet om at anvende de fornødne garantier.

Til sidst, kan det tages i betragtning, om man har tilsluttet sig et godkendt adfærdskodeks i forbindelse med vurderingen af, om den dataansvarlige skal pålægges en administrativ bøde.

Indholdsmæssige minimumskrav til et adfærdskodeks

Adfærdskodekser skal, for at blive godkendt af Datatilsynet, indbefatte nogle indholdsmæssige minimumskrav.

Disse krav kan ændre sig over tid, men indtil videre fremfører Datatilsynet følgende garantier, som kodekset skal indeholde for at blive godkendt:

* Kodekset skal klart angive, hvilke typer af organisationer eller sektorer, som kodekset sigter efter at finde anvendelse på
* Kodekset skal rettes mod konkrete og veldefinerede behandlinger
* Der bør ved udarbejdelsen af kodekset ske høring af relevante interessenter
* Kodekset skal rettes mod konkrete behandlingssituationer
* Kodekset skal indeholde konkrete retningslinjer, som skal kunne hjælpe de tilsluttede virksomheder eller organisationer til at overholde databeskyttelsesforordningen
* Kodekset skal indeholde mekanismer, således at et kontrolorgan kan foretage kontrol af, om de tilsluttede rent faktisk overholder reglerne i kodekset
* Der skal altid være en instans, der løbende sørger for, at kodekset bliver opdateret og tilpasset

**Certificeringsordninger**

Hvad er en certificeringsordning?

En certificeringsordning i databeskyttelsesforordningens forstand er en ordning, hvor en tredjepart – kaldet certificeringsorganet - indestår for, at en virksomhed eller en organisation lever op til nogle foruddefinerede kriterier og/eller krav.

En certificering kan vedrøre f.eks. indsamling, sletning, registrering osv. af personoplysninger, men kan derimod ikke vedrøre f.eks. et it-system hvor behandlingen foregår.

Ligesom et adfærdskodeks, kan certificeringsordningen bruges til at sikre, at behandlingsaktiviteterne overholder forordningens krav, samt til at påvise at vedkommende virksomhed eller organisation faktisk overholder forordningens krav.

Hvis en virksomhed eller en organisation opnår en given certificering, så får pågældende et bevis, der viser, at den pågældende certificering er opnået, samt at behandlingsaktiviteten bør udføres på den specifikke måde, som er foreskrevet i certificeringsordningen.

Hvem kan lave en certificeringsordning?

Forordningen indeholder ikke nogle retningslinjer for, hvem der kan tage initiativ til at udarbejde en certificeringsordning.

Ifølge Datatilsynet, vil det i praksis ofte være en virksomhed, som kan se et forretningspotentiale i at lade sig selv blive et certificeringsorgan.

Hvad kan en certificeringsordning bruges til?

Ligeledes fremgår det heller ikke af forordningen, hvilke behandlinger en certificering skal specificere anvendelsen af.

Der må dog ifølge Datatilsynet være tale om nogle af de samme behandlinger, som fremgår af forordningen vedrørende adfærdskodekser.

Der er også, ligesom ved adfærdskodekser, steder i forordningen, hvor det kan tillægges betydning, om den pågældende virksomhed eller organisation har fået en certificering.

En certificering vil derved kunne bruges som et element til at påvise, at den dataansvarlige lever op til sine forpligtigelser efter forordningen.

Derudover vil certificeringen kunne bruges som et element til påvise overholdelsen af kravene om databeskyttelsen gennem design og standardindstillinger.

Certificeringen kan bruges til at påvise, at databehandleren stiller de fornødne garantier. Det samme gælder påvisning af databehandlerens overholdelse af kravene til behandlingssikkerhed.

Hvis man som dataansvarlig har brug for at overføre personoplysninger til et tredjeland, skal man have et såkaldt overførelsesgrundlag for at gøre dette. Det er i forordningen bestemt, at et sådan overførelsesgrundlag godt kan sikres igennem en godkendt certificeringsordning. Det er en betingelse for dette, at der foreligger et bindende tilsagn, som kan håndhæves fra den dataansvarlige eller databehandleren i tredjelandet om at anvende de fornødne garantier.

Til sidst, kan det tages i betragtning, om man har tilsluttet sig en godkendt certificeringsordning i forbindelse med vurderingen af, om den dataansvarlige skal pålægges en administrativ bøde og eventuelt størrelsen heraf.

Hvordan kan man blive certificeret?

Det fremgår af forordningen, at en certificering kan foretages af et certificeringsorgan eller af Datatilsynet. Certificeringen foretages på baggrund af kriterier, der er godkendt af Datatilsynet.

Datatilsynet vil offentliggøre oversigter over de godkendte certificeringsordninger. Hvis man ønsker at blive certificeret af en relevant certificeringsordning, skal man anmode certificeringsorganet om blive certificeret.

Det er certificeringsorganet, der vurderer om en den pågældende virksomhed eller organisation lever op til kravene og kriterierne for at blive certificeret af den pågældende certificeringsordning.

Certificeringsorganet skal herefter meddele Datatilsynet en begrundelse for udstedelsen af certifikatet. Datatilsynet kan eventuelt udstede et påbud om at en specifik certificering ikke udstedes. Hvis ikke dette er tilfældet, så udsteder certificeringsorganet certifikatet til virksomheden/organisationen. Herefter kan virksomheden eller organisationen benytte sig af sit certifikat.

De certifikater, der udstedes vil ofte offentliggøres af certificeringsorganet, således at registrerede kan se om en given virksomhed eller organisation er certificeret.

Datatilsynet kan føre tilsyn med, om kravene til certificering overholdes. De kan i den forbindelse tilbagetrække et certifikat. Certificeringsorganet vil også løbende gennemføre en revision i overensstemmelse med bestemmelserne i selve certificeringsordningen.

Hvordan bliver man certificeringsorgan?

Førend man kan udstede en certificeringsordning, skal man godkendes som certificeringsorgan.

I Danmark kan man godkendes som certificeringsorgan af enten Datatilsynet eller det danske akkrediteringsorgan (DANAK) – i praksis vil det dog være DANAK.

Der stilles høje krav til hvornår en virksomhed eller organisation kan godkendes som certificeringsorgan.