

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over AI-forordningen – risikoklassificering, tilsyn og sanktioner

Fra forbudt AI-praksis til bødeudmåling – dansk tilsynsarkitektur og den praksis der findes indtil videre

Version 2 · Opdateret 3. sep. 2026 · 22 afgørelser · 2020-2025

[Læs online](#)

INTRODUKTION

AI-forordningen (forordning (EU) 2024/1689) indfører en risikobaseret regulering af kunstig intelligens med fire niveauer – forbudt praksis, højrisko, gennemsigtighedspligtig og fri anvendelse – og suppleres i Danmark af lov om supplerende bestemmelser til forordningen om kunstig intelligens (lov nr. 467 af 14. maj 2025), der udpeger Digitaliseringsstyrelsen, Datatilsynet og Domstolsstyrelsen som nationale kompetente myndigheder og strafbelægger overtrædelser med bøde. Egentlig forordningspraksis findes endnu ikke: der er hverken offentliggjorte afgørelser om forbudt AI-praksis eller domme om bødeudmåling efter gennemførelseslovens § 10. Til gengæld er der en betydelig og retningsgivende praksis fra Datatilsynet, EU-Domstolen, Folketingets Ombudsmand og Ligebehandlingsnævnet om de samme materielle spørgsmål – behandlingsgrundlag for AI-løsninger, biometri, forklaringspligt ved automatiserede afgørelser, menneskeligt tilsyn og algoritmisk profilering – som med stor sandsynlighed bliver den fortolkningsmæssige rygrad, når forordningen skal håndhæves.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** AI-forordningen finder anvendelse trinvist: forbudte AI-praksisser fra 2. februar 2025, sanktionskapitlet fra 2. august 2025, hovedparten fra 2. august 2026 og produktrelateret højrisko efter art. 6, stk. 1, først fra 2. august 2027 – forbudt AI-praksis kunne derfor først sanktioneres fra august 2025.
- 02** Danmark er som følge af retsforbeholdet ikke bundet af art. 5, stk. 1, litra h (realtids fjernidentifikation til retshåndhævelse), af stk. 2-6, af art. 26, stk. 10, og af litra d og g i det omfang de vedrører politisamarbejde og retligt samarbejde i straffesager.
- 03** Tilsynet er delt: Digitaliseringsstyrelsen dækker art. 5, stk. 1, litra a-c og e-f og er tillige bemyndigende myndighed og centralt kontaktpunkt; Datatilsynet dækker litra d og g uden for retsforbeholdet; Domstolsstyrelsen dækker domstolenes administrative AI-brug.
- 04** Bruger domstolene AI som led i deres judicielle funktion, træffes afgørelsen af vedkommende ret selv med kæreadgang til højere ret inden for en frist på 4 uger – ikke af en markedsovervågningsmyndighed.

- 05** De nationale kompetente myndigheders afgørelser kan ikke påklages administrativt, jf. gennemførelseslovens § 3; prøvelsen sker direkte ved domstolene efter grundlovens § 63, hvilket ifølge forarbejderne er nødvendigt for at sikre den uafhængighed forordningens art. 70, stk. 1, kræver.
- 06** Markedsovervågningsmyndighederne har adgang til erhvervsmæssige lokaliteter uden retskendelse, kan foretage tekniske undersøgelser af AI-systemet på stedet, lade sig bistå af uafhængige sagkyndige og kræve politiets bistand.
- 07** Overtrædelse af art. 5, stk. 1, litra a-g sanktioneres i dansk ret som strafferetlig bøde efter § 10 – ikke som administrativ bøde – men bødeudmålingen skal følge forordningens art. 99, stk. 3 og 5 (loft på 35 mio. EUR/7 % henholdsvis 7,5 mio. EUR/1 %) og hensynene i art. 99, stk. 7.
- 08** Forældelsesfristen er sat til 5 år i § 10, stk. 4 – en bevidst fravigelse af straffelovens § 93, stk. 11, om 2 år, begrundet i sagernes forventede størrelse og kompleksitet.
- 09** Offentlige myndigheder kan kun ifalde strafansvar efter straffelovens kap. 5, når de optræder som driftsherre på linje med private; lovovertrædelser begået som led i myndighedsudøvelse kan alene udløse personligt strafansvar.
- 10** Datatilsynet skelner skarpt mellem udvikling og drift af AI-løsninger: eksisterende opgavehjemler kan bære udviklings- og gentræningsfasen, men driften af en beslutningsstøttende AI-løsning kræver et klarere supplerende nationalt retsgrundlag.
- 11** Automatiseringsbias – at sagsbehandlere tillægger AI-outputtet større vægt end egen faglig vurdering – indgår som selvstændigt skærpende hensyn både i Datatilsynets vurdering af indgriben og i forordningens art. 14, stk. 4, litra b, om menneskeligt tilsyn.
- 12** EU-Domstolen kræver, at den dataansvarlige forklarer den konkret anvendte procedure og de anvendte principper bag en automatiseret afgørelse i kortfattet og letforståelig form; forretningshemmeligheder kan ikke generelt afskære indsigten, men skal afvejes konkret af tilsynsmyndigheden eller domstolen.
- 13** Ren stemmeanalyse uden stemmegenkendelse er ikke biometrisk behandling omfattet af forbuddet i GDPR art. 9, stk. 1, når formålet ikke er entydig identifikation – en sontring der er direkte relevant for afgrænsningen af følelsesgenkendelse og biometrisk kategorisering i AI-forordningens art. 5, stk. 1, litra f og g.
- 14** Dansk domspraksis om kunstig intelligens er indtil videre udelukkende strafferetlig og hviler på straffeloven – ikke på AI-forordningen; AI-genereret materiale bedømmes efter de almindelige gerningsindhold.

Den risikobaserede arkitektur og den trinvis anvendelse fra februar 2025 til august 2027

§ 1

AI-forordningen bygger på en risikopyramide: nogle former for AI-praksis er helt forbudt, en større gruppe klassificeres som højrisiko med krav til risikostyring, datakvalitet, dokumentation og menneskeligt tilsyn, en tredje gruppe er alene underlagt gennemsigtighedsforpligtelser, og resten er ureguleret. Forordningen trådte i kraft 2. august 2024, men anvendelsen er trinvis efter [artikel 113](#):

Bestemmelser	Anvendelse fra
Kapitel I (almindelige bestemmelser) og kapitel II (forbudte former for AI-praksis)	2. februar 2025
Kapitel III, afd. 4 (bemyndigende myndigheder og bemyndigede organer), kapitel V (AI-modeller til almen brug), VII (forvaltning), XII (sanktioner) samt art. 78 – dog ikke art. 101	2. august 2025
Forordningen i øvrigt	2. august 2026
Art. 6, stk. 1, om produktrelateret højrisiko og de tilsvarende forpligtelser	2. august 2027

Denne forskydning har en konkret retlig konsekvens, som lovgiver udtrykkeligt fremhævede i de almindelige bemærkninger til L 154: forbuddene galdt fra februar 2025, men kunne ikke sanktioneres, før sanktionskapitlet fandt anvendelse.

Kapitel XII om sanktioner finder imidlertid først anvendelse fra den 2. august 2025. Forbudte former for AI-praksis kan derfor først medføre sanktioner fra den 2. august 2025.

Den danske gennemførelseslov trådte følgelig i kraft netop den 2. august 2025, jf. [§ 12](#), og gælder ikke for Færøerne og Grønland, jf. [§ 13](#). Loven supplerer forordningen, hvis fulde tekst er optaget som bilag 1 til loven af rent praktiske hensyn – forordningen har direkte virkning i Danmark efter TEUF artikel 288, jf. [artikel 288 i TEUF](#).

Loven i sin nuværende skikkelse dækker altså kun det første trin. Digitaliseringsministeriet anførte allerede i forarbejderne, at der ville komme yderligere lovgivning: »Digitaliseringsministeriet vil hertil fremsætte forslag til yderligere supplerende lovgivning til de øvrige kapitler i forordningen om kunstig intelligens forud for, at disse dele af forordningen om kunstig intelligens skal finde anvendelse.« Det skete med [L 111 \(2025-26\)](#), fremsat 18. februar 2026, som skulle ophæve den gældende lov og etablere den fulde tilsyns- og sanktionsramme fra 2. august 2026. Lovforslaget bortfaldt ved samlingens afslutning.

LOV

AI-forordningen § 113

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 12

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 13

De otte forbudte former for AI-praksis i artikel 5 – og de dele

§ 2 Danmark ikke er bundet af

[Artikel 5, stk. 1](#) opregner otte former for AI-praksis, der er forbudt i EU:

- **litra a** – subliminale teknikker ud over den menneskelige bevidsthed eller bevidst manipulerende/vildledende teknikker, der i væsentlig grad fordrejer adfærden og forvolder betydelig skade
-

litra b – udnyttelse af sårbarheder på grundlag af alder, handicap eller en særlig social eller økonomisk situation

- **litra c** – social scoring, hvor evaluering eller klassificering over tid fører til skadelig eller ugunstig behandling
- **litra d** – prædiktiv politiarbejde-profilering, dvs. risikovurdering af, om en fysisk person vil begå en strafbar handling, når vurderingen *alene* er baseret på profilering eller vurdering af personlighedstræk
- **litra e** – opbygning eller udvidelse af ansigtsgenkendelsesdatabaser gennem ikkemåltrettet skrabning af ansigtsbilleder fra internettet eller kameraovervågning
- **litra f** – følelsesgenkendelse på arbejdspladser og uddannelsesinstitutioner, medmindre anvendelsen sker af medicinske eller sikkerhedsmæssige årsager
- **litra g** – biometrisk kategorisering med henblik på at udlede race, politiske anskuelser, fagforeningsmedlemskab, religiøs eller filosofisk overbevisning, seksuelle forhold eller seksuel orientering
- **litra h** – realtids biometrisk fjernidentifikation på offentlige steder med henblik på retshåndhævelse

Forbuddene er ikke absolutte i deres afgrænsning. Litra d finder ikke anvendelse på AI-systemer, der understøtter den menneskelige vurdering af en persons involvering i kriminel aktivitet, når vurderingen allerede hviler på objektive og verificerbare kendsgerninger direkte knyttet til den kriminelle aktivitet. Og litra g omfatter ikke mærkning eller filtrering af lovligt indhentede biometriske datasæt.

Retsforbeholdets rækkevidde. Forordningen er vedtaget med hjemmel i både artikel 114 og artikel 16 i TEUF, og de dele, der hviler på artikel 16 og vedrører behandling af personoplysninger under TEUF tredje del, afsnit V, kapitel 4 eller 5, er efter artikel 2a i protokol nr. 22 ikke bindende for Danmark. De almindelige bemærkninger til L 154 opregner præcist, hvad det omfatter:

Det følger af præambelbetragtning nr. 41 i forordningen om kunstig intelligens, at i medfør af artikel 2 og 2a i protokol nr. 22 om Danmarks stilling, er de regler, der er fastsat i artikel 5, stk. 1, litra g, i forordningen om kunstig intelligens, i det omfang den finder anvendelse på brugen af systemer til biometrisk kategorisering til aktiviteter inden for politisamarbejde og retligt samarbejde i straffesager, artikel 5, stk. 1, litra d, i det omfang den finder anvendelse på brugen af AI-systemer, der er omfattet af nævnte bestemmelse, artikel 5, stk. 1, litra h, og stk. 2-6, og artikel 26, stk. 10, ikke bindende for og finder ikke anvendelse i Danmark.

Det har en direkte og ofte overset konsekvens for straffebestemmelsen: [gennemførelseslovens § 10, stk. 1, nr. 1](#) strafbelægger kun art. 5, stk. 1, **litra a-g** – ikke litra h. Og Datatilsynets tilsynskompetence for litra d og g gælder efter forarbejderne udtrykkeligt kun »i det omfang disse ikke er omfattet af det danske retsforbehold«. Realtids fjernidentifikation til retshåndhævelse og den tilhørende ordning med forudgående judiciel tilladelse i art. 5, stk. 3, samt konsekvensanalysekravet i art. 5, stk. 2, sidste led, er dermed uden for den danske gennemførelse.

Digitaliseringsstyrelsen offentliggjorde i oktober 2025 en [vejledningsspakke om forbudt brug af AI](#) som opfølgning på forordningen – den er indtil videre det primære danske fortolkningsbidrag til artikel 5, idet der endnu ikke foreligger offentliggjorte afgørelser efter [§ 7](#), som netop giver markedsovervågningsmyndighederne hjemmel til at offentliggøre deres afgørelser i sager om forbudt AI-praksis.

LOV

[AI-forordningen § 5, stk. 1](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 7](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10, stk. 1](#)

Klassificering af højrisiko-systemer efter artikel 6 – to spor og en betinget undtagelse

Artikel 6 opererer med to selvstændige klassificeringsspor.

Produktsporet (stk. 1). Et AI-system er højrisiko, hvis det både (a) er tilsigtet anvendt som sikkerhedskomponent i – eller selv er – et produkt omfattet af EU-harmoniseringslovgivningen i bilag I, og (b) det pågældende produkt skal underkastes tredjeparts-overensstemmelsesvurdering efter samme lovgivning. Netop dette spor er det, der først finder anvendelse fra 2. august 2027.

Bilag III-sporet (stk. 2). De anvendelsesområder, bilag III opregner – herunder biometri, kritisk infrastruktur, uddannelse, beskæftigelse og personaleadministration, adgang til væsentlige offentlige og private ydelser, retshåndhævelse, migration og retspleje – er højrisiko i sig selv. Fagbevægelsens Hovedorganisation fremhævede i sit høringssvar til [L 111](#), at dette betyder, at »anvendelse af AI-systemer til personaleadministration og ledelse af medarbejdere betragtes som højrisiko-anvendelse«.

Undtagelsen i stk. 3 – og dens modundtagelse. Et bilag III-system er alligevel ikke højrisiko, hvis det ikke udgør en væsentlig risiko for sundhed, sikkerhed eller grundlæggende rettigheder, herunder ved ikke i væsentlig grad at påvirke resultatet af beslutningstagning. Det forudsætter, at systemet enten udfører en snæver proceduremæssig opgave, forbedrer resultatet af en tidligere afsluttet menneskelig aktivitet, påviser beslutningsmønstre uden at erstatte en menneskelig vurdering, eller udfører en forberedende opgave. Men undtagelsen har en hård grænse:

Uanset første afsnit betragtes et AI-system, der er omhandlet i bilag III, altid som højrisiko, hvis AI-systemet udfører profilering af fysiske personer.

Udbyderen skal dokumentere sin vurdering, inden systemet bringes i omsætning, og er uanset undtagelsen underlagt registreringsforpligtelsen i art. 49, stk. 2, jf. art. 6, stk. 4. Netop denne dokumentationsbyrde blev fremhævet som et praktisk problem i høringen over [L 111](#), hvor F&P pegede på de »de facto-krav, som ikke fremgår af forordningen« – hvad der kræves af en virksomhed for at *vis*, at den ikke falder under højrisiko.

Profileringsklausulen har konkret betydning for offentlige beslutningsstøtteværktøjer. Ligebehandlingsnævnet behandlede i [20-25601](#) Styrelsen for Arbejdsmarked og Rekrutterings profilafklaringsværktøj, der ved maskinlæring kobler et frivilligt spørgeskema med registerdata om alder, herkomst og ledighedshistorik for at forudsige risikoen for langtidsledighed. Nævnet frifandt styrelsen, fordi »herkomst« efter EU-Domstolens praksis i [C-668/15 Jyske Finans](#) ikke kan sidestilles med etnisk oprindelse. Afgørelsen angik alene forskelsbehandlingsloven – men værktøjet er et lærebogseksempel på et system, der efter AI-forordningen både ligger i bilag III (beskæftigelse) og udfører profilering af fysiske personer, og som derfor **altid** vil være højrisiko uanset stk. 3-undtagelsen.

Datatilsynets udtalelse i [2022-212-3676](#) om kommunernes AI-værktøj »Asta«, der skulle identificere nyledige dagpengemodtagere med forhøjet risiko for et langvarigt kontaktførelse, illustrerer den samme systemtype set fra databeskyttelsesretten.

LOV	AI-forordningen § 6, stk. 1-4	
PRAKSIS	Datatilsynet · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	18.05.2022
	Ligebehandlingsnævnet · Klage over anvendelse af herkomstkriterier i digitalt værktøj til profilafklaring af ledige	12.05.2022

Den danske tilsynsarkitektur – tre kompetente myndigheder og et fjerde spor for domstolene

§ 2 udmønter forordningens artikel 70, stk. 1, der kræver mindst én bemyndigende myndighed og mindst én markedsovervågningsmyndighed pr. medlemsstat. Danmark har valgt en delt model:

Myndighed	Rolle	Retligt grundlag
Digitaliseringsstyrelsen	Bemyndigende myndighed (art. 28, stk. 1), centralt kontaktpunkt (art. 70, stk. 2, 3. pkt.) og markedsovervågning af art. 5, stk. 1, litra a-c og e-f	§ 2, stk. 2
Datatilsynet	Markedsovervågning af art. 5, stk. 1, litra d og g – kun uden for retsforbeholdet	§ 2, stk. 3
Domstolsstyrelsen	Markedsovervågning af domstolenes AI-anvendelse, når domstolene <i>ikke</i> handler i deres egenskab af domstol	§ 2, stk. 4
Vedkommende ret selv	AI-anvendelse som led i domstolenes judicielle funktion; kære til højere ret, frist 4 uger	§ 2, stk. 5

Denne opdeling er ikke tilfældig. Forarbejderne til § 2 præciserer, at Domstolsstyrelsens »tilsyn alene omfatter domstolenes administrative forhold og ikke deres judicielle funktioner«, og at afgørelser om AI-anvendelse i den judicielle funktion træffes af retten selv med kære adgang – for særlige domstole uden almindelig ankeadgang til den landsret, i hvis kreds retten er beliggende. Domstolsstyrelsen har i august 2026 afholdt [en konference for retspræsidenter og dommere om etik og retssikkerhed ved AI i retterne](#).

Funktionel uafhængighed. Artikel 70, stk. 1, 2. pkt., kræver, at myndighederne udøver deres beføjelser »uafhængigt, upartisk og uden bias«. Forarbejderne omsætter det til et konkret instruktionsforbud:

De bemyndigende myndigheder og markedsovervågningsmyndigheder skal varetage deres opgaver og beføjelser uafhængigt af den pågældende ressortminister og skal være uafhængige af udefrakommende indblanding fra offentlige og private enheder. Dette indebærer også, at de bemyndigende myndigheder og markedsovervågningsmyndigheder ikke vil kunne modtage eller søge instrukser fra andre, herunder vedkommende ressortministre, uanset at de i øvrigt er organisatorisk underlagt det pågældende ressortministerium.

Uafhængigheden er dog ikke total isolation: forarbejderne åbner udtrykkeligt for, at en kompetent myndighed kan rådføre sig eller udveksle synspunkter med retshåndhævende myndigheder, krisestyringsmyndigheder eller andre markedsovervågnings- og datatilsynsmyndigheder og indhente teknisk bistand, når der er behov for særegen fagspecifik ekspertise.

Delingen af tilsynet blev kritiseret bredt under høringen over den kommende AI-lov, jf. [høringen af 16. september 2025](#). KL anbefalede at samle tilsynet hos Digitaliseringsstyrelsen for at sikre ensartet praksis, IT-Branchen advarede mod et fragmenteret tilsyn, F&P ønskede Finanstilsynet som sektormyndighed på forsikringsområdet, og Green Power Denmark ønskede Energistyrelsen. Institut for Menneskerettigheder fandt derimod, at sektoropdelingen giver mening, men understregede, at det i praksis bliver afgørende at sikre reel respekt for uafhængighedskravet – »især for de myndigheder, der ikke i forvejen er funktionelt uafhængige i

deres øvrige arbejde». Digitaliseringsstyrelsen fastholdt myndighedsstrukturen med henvisning til EU-retlige minimumskrav.

LOV

AI-forordningen § 70, stk. 1, 2

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 2, stk. 1-5

§ 5 Markedsovervågningsbeføjelserne – oplysningskrav, kontrolbesøg uden retskendelse, påbud og midlertidigt forbud

Efter [artikel 74, stk. 1](#) finder markedsovervågningsforordningen (EU) 2019/1020 anvendelse på AI-systemer. Den er i dansk ret suppleret ved lov om produkter og markedsovervågning, men den lov gælder efter sin § 2 netop **ikke** produkter omfattet af AI-forordningen. Gennemførelseslovens §§ 4-9 udfylder derfor huller. Digitaliseringsministeriet begrundede beføjelsernes omfang med, at markedsovervågningsmyndighedernes kompetence bør svare til det, de under alle omstændigheder skal besidde fra 2. august 2026 i medfør af henvisningen til markedsovervågningsforordningen.

Oplysningskrav (§ 5). Myndighederne kan af fysiske og juridiske personer omfattet af forordningens art. 2, stk. 1, litra a-f afkræve »alle oplysninger, som er nødvendige for myndighedernes tilsynsvirksomhed, herunder til fastlæggelse af, om et forhold hører under myndighedernes kompetence«. Forarbejderne til § 10 afgrænser bestemmelsen udtrykkeligt mod selvinkriminering: »Den foreslåede bestemmelse afgrænses af det almindelige forbud mod at udsætte andre for selvinkriminering, som det blandt andet kan udledes af Den Europæiske Menneskerettighedskonventions artikel 6 og § 10 i retssikkerhedsloven.«

Kontrolbesøg (§ 6). Myndighederne har »til enhver tid mod behørig legitimation og uden retskendelse adgang til alle erhvervsmæssige lokaliteter«, kan foretage tekniske undersøgelser af AI-systemet på stedet, kan lade sig bistå af uafhængige sagkyndige, og politiet yder om nødvendigt bistand. Digitaliseringsministeriet begrundede fraværet af retskendelseskrav både med effektivitetshensyn og med, at »muligheden for kontrolbesøg uden retskendelse vil have en afskrækkende effekt i forhold til udbredelsen af forbudte AI-systemer«. Netop dette punkt var det mest omstridte i høringen: DI, Dansk Erhverv og Danske Regioner kritiserede alle den vidtgående adgang uden retskendelse, men myndigheden fastholdt beføjelsen som nødvendig.

Påbud og midlertidigt forbud (§ 8). Myndighederne kan udstede påbud om overholdelse af art. 5, stk. 1, litra a-g, og kan udstede et midlertidigt forbud mod levering, markedsføring, udstilling eller anden tilgængeliggørelse af et AI-system, »hvis AI-systemet vurderes at kunne udgøre en risiko«. Forbuddets varighed kan ikke strække sig ud over, hvad der er nødvendigt for at træffe kontrolforanstaltninger til brug for undersøgelser eller vurderinger af systemets sikkerhed. Forarbejderne indsnævrer anvendelsesområdet betydeligt:

Bestemmelsen vil alene kunne anvendes i de tilfælde, hvor der er en formodning for, at et AI-system udgør en fare, og hvor det vurderes uforsvarligt ud fra et forsigtighedsprincip, at AI-systemet fortsat er i anvendelse, imens markedsovervågningsmyndigheden foretager de nødvendige undersøgelser af systemet med henblik på at træffe afgørelse.

Offentliggørelse (§ 7). Afgørelser i sager om forbudt AI-praksis kan offentliggøres for at oplyse offentligheden. Forarbejderne forbeholder dog fortrolige oplysninger om tekniske indretninger, fremgangsmåder og drifts- eller forretningsforhold af væsentlig økonomisk betydning, ligesom offentliggørelse er underlagt forordningens art. 78 om fortrolighed.

Bemyndigende myndighed (§ 9). Digitaliseringsstyrelsen kan efter forhandling med ministeren fastsætte regler om vurdering, udpegelse og notifikation af overensstemmelsesvurderingsorganer samt om suspension eller tilbagetrækning af udpegning efter art. 36, stk. 4, og kan delegere selve vurderingen til andre offentlige myndigheder eller private institutioner. Forarbejderne nævner som eksempel et krav om DANAK-akkreditering for organer, der ønsker notifikation.

LOV

[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 5](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 6, stk. 1-4](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 7](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 8, stk. 1, 2](#)[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 9, stk. 1, 2](#)

Afskåret administrativ rekurs efter § 3 – retssikkerhedsprisen for uafhængighed

§ 6

§ 3 bestemmer kort og kategorisk, at de nationale kompetente myndigheders afgørelser efter forordningen, loven og regler udstedt i medfør heraf »ikke kan indbringes for anden administrativ myndighed«. Forarbejderne knytter bestemmelsen direkte til uafhængighedskravet:

Bestemmelsen udelukker, at de nationale kompetente myndigheders afgørelser er undergivet administrativ rekurs. Sådanne afgørelser kan indbringes direkte for domstolene efter grundlovens § 63. [...] Digitaliseringsministeriet vurderer, at det er nødvendigt for at sikre markedsovervågningsmyndighedernes uafhængighed, at en afgørelse truffet af markedsovervågningsmyndigheden ikke kan omgøres eller ændres af myndighedens sædvanlige overordnede.

Konstruktionen betyder, at der ikke findes noget klagenævn på AI-området, og at en operatør, der rammes af et påbud eller et midlertidigt forbud efter § 8, må gå direkte til domstolene. Det var et hovedkritikpunkt i høringen: DI efterlyste udtrykkeligt et uafhængigt klagenævn, F&P kritiserede den manglende administrative klageadgang sammen med bødemodellen, og Danske Regioner advarede om, at kombinationen af administrative bødeforlæg og manglende klageadgang »kan føre til forskelsbehandling mellem operatører og skabe præcedens uden domstolsprøvelse«. Digitaliseringsstyrelsen fastholdt strukturen og afviste et klagenævn.

Som praktisk retssikkerhedsmodvægt gælder alene forordningens art. 99, stk. 10, hvorefter udøvelsen af sanktionsbeføjelserne skal være underlagt »fornødne procedurmæssige sikkerhedsforanstaltninger i overensstemmelse med EU-retten og national ret, herunder effektive retsmidler og retfærdig procedure«, samt de almindelige forvaltningsretlige krav. Sidstnævnte er ikke ubetydelige: en tilsvarende afskæring af klageadgang findes på fødevareområdet, og Miljø- og Fødevareklagenævnet har i [23/11051](#) fastslået, at et administrativt bødeforlæg overhovedet ikke er en afgørelse i forvaltningsretlig forstand, men et tilbud om at afslutte en sag om en lovovertrædelse uden inddragelse af politi og domstole. Den sondring bliver relevant, hvis bemyndigelsen i § 11 til administrative bødeforelæg engang udmøntes.

LOV

AI-forordningen § 99, stk. 10

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 3

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 11

Sanktionssporet – strafferetlig bøde efter § 10, forordningens § 7 bødelofter og den 5-årige forældelse

Forordningens [artikel 99, stk. 9](#) overlader det til medlemsstaterne, om administrative bøder pålægges af domstole eller af andre organer. Danmark har valgt domstolssporet. Digitaliseringsministeriet konkluderede i de almindelige bemærkninger, at »sanktioner for overtrædelser af forordningens bestemmelser efter dansk ret fastsættes som en strafferetlig sanktion i henhold til artikel 99, stk. 9, 1. pkt., jf. artikel 99, stk. 3 og 5«. Formelt er der altså tale om **straf**, ikke om en administrativ bøde.

[§ 10, stk. 1](#) strafbelægger fem forhold: overtrædelse af art. 5, stk. 1, litra a-g (nr. 1); afgivelse af ukorrekte, ufuldstændige eller vildledende oplysninger efter art. 99, stk. 5 (nr. 2); undladelse af at efterkomme oplysningskrav efter § 5 eller hindring af adgang efter § 6, stk. 1 (nr. 3); hindring af tekniske undersøgelser efter § 6, stk. 2 (nr. 4); og undladelse af at efterkomme påbud eller midlertidige forbud efter § 8 (nr. 5). Forarbejderne giver konkrete eksempler på nr. 3 og 4: nægtelse af at udlevere adgangskoder, kryptering af alle oplysninger så myndigheden skal omgå krypteringen, og fysisk blokering af adgangen til lokaliteter.

Bødelofterne. Selv om bøden er strafferetlig, skal udmålingen holde sig inden for forordningens rammer:

Overtrædelsestype	Loft (fast beløb)	Loft (omsætning)	Hjemmel
Forbudt AI-praksis, art. 5	35 mio. EUR	7 % af global årsomsætning	art. 99, stk. 3
Operatør- og gennemsigtighedspligter (art. 16, 22, 23, 24, 26, 31, 33, 34, 50)	15 mio. EUR	3 %	art. 99, stk. 4
Ukorrekte/vildledende oplysninger	7,5 mio. EUR	1 %	art. 99, stk. 5

Det højeste af de to beløb gælder – men for SMV'er og iværksættervirksomheder gælder efter art. 99, stk. 6, omvendt det **laveste**. Forarbejderne til § 10 gengiver dette udtrykkeligt og fastslår, at »ved udmåling af bødestraf skal de fastsatte beløbsgrænser i henhold til artikel 99, stk. 3 og 5, i forordningen om kunstig intelligens overholdes«.

Udmålingskriterierne. Forarbejderne henviser til [artikel 99, stk. 7](#), der opregner ti hensyn: overtrædelsens art, grovhed og varighed samt konsekvenser; om andre markedsovervågningsmyndigheder allerede har bødet den samme operatør for samme overtrædelse; om andre myndigheder har bødet for overtrædelser af anden EU-ret eller national ret som følge af samme aktivitet; operatørens størrelse, omsætning og markedsandel; skærpende eller formildende faktorer såsom opnåede økonomiske fordele eller undgåede tab; graden af samarbejde; graden af ansvar under hensyn til de gennemførte tekniske og organisatoriske foranstaltninger; hvordan myndigheden fik kendskab til overtrædelsen, herunder om operatøren selv underrettede; om overtrædelsen var forsætlig eller uagtsom; og tiltag for at afbøde skaden. Straffelovens § 51, stk. 3, og kapitel 10 om straffens fastsættelse finder i øvrigt anvendelse.

Juridiske personer og offentlige myndigheder. § 10, stk. 3 hjemler strafansvar for juridiske personer efter straffelovens 5. kapitel. Forarbejderne trækker en vigtig grænse for offentlige myndigheder med henvisning til straffelovens § 27, stk. 2:

Statslige myndigheder og kommuner kan ifølge straffelovens § 27, stk. 2, alene straffes i anledning af overtrædelser, der begås ved udøvelse af virksomhed, der svarer til eller kan sidestilles med virksomhed udøvet af private. [...] Reglerne i straffelovens kapitel 5 omfatter derimod ikke lovovertrædelser, der begås som led i myndighedsudøvelse. I sådanne tilfælde kan der alene blive tale om personligt strafansvar for de ansvarlige enkeltpersoner.

Forældelse. § 10, stk. 4 fastsætter en forældelsesfrist på 5 år. Det er en bevidst fravigelse: efter straffelovens § 93, stk. 11 ville fristen have været 2 år, når der ikke er hjemlet højere straf end fængsel i 1 år. Fravigelsen begrundes i, »at de omfattede straffesager kan antage en vis størrelse og kompleksitet«.

Subsidiaritetsklausulen. Bøden idømmes kun, »medmindre højere straf er forskyldt efter anden lovgivning«. Forarbejderne nævner det konkrete sammenstød med straffelovens §§ 162 og 163 om urigtige oplysninger til offentlige myndigheder: forholdet henføres da under den bestemmelse, der giver højest straf.

Den foreslåede bødemodel i det bortfaldne L 111. Det bortfaldne L 111 indeholdt en egentlig bødemodel med tre statiske grundbeløb – 700.000 EUR ved forbudt AI-praksis, 150.000 EUR ved overtrædelse af krav til højrisiko-systemer, gennemsigtighed og bemyndigede organer, og 37.500 EUR ved processuelle overtrædelser – samt tre dynamiske grundbeløb på henholdsvis 0,14 %, 0,03 % og 0,005 % af den globale årlige omsætning, som anvendes hvis de er højere. DI påpegede i høringssvaret, at fastsættelsen af bødeniveauet er overladt til medlemsstaterne, hvilket »kan give anledning til fragmentering i sanktionspraksis på tværs af EU«, og anbefalede koordinering med EU-praksis. Modellen er ikke gældende ret, da lovforslaget bortfaldt, men den er den hidtil klareste indikation af, hvilket niveau danske myndigheder forventer at lægge sig på.

LOV

AI-forordningen § 99, stk. 3-9

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10, stk. 1-4

Straffeloven § 27, stk. 2

Straffeloven § 93, stk. 11

§ 8 Datatilsynets AI-praksis – den afgørende sontring mellem udvikling og drift

Den vigtigste danske afgørelse om AI-løsninger i den offentlige sektor er Datatilsynets udtalelse i 2023-212-0015 af 17. november 2023 om et kommunalt beslutningsstøtteværktøj, der ved algoritmisk forudsigelse skulle identificere borgere med behov for vedligeholdende træning og rehabilitering. Tilsynet delte behandlingen i to faser og nåede modsatte resultater:

Fase	Supplerende retsgrundlag	Konklusion
Udvikling og gentræning	Serviceoven § 86 og § 112	Tilstrækkeligt
Drift (beslutningsstøtte i konkrete sager)	Samme bestemmelser	Ikke tilstrækkeligt klart

Begrundelsen er den centrale:

Kravene til klarheden af det retsgrundlag, som skal danne baggrund for jeres behandling af personoplysninger ved drift af en AI-løsning, afhænger af, hvor indgribende behandlingen er for borgerne. [...] Konsekvenserne for borgerne

er dermed ofte større, når AI-løsningen er i drift, og der stilles derfor højere krav til klarheden af det retsgrundlag, der danner baggrund for at anvende løsningen i drift.

Tilsynet opregnede de faktorer, der gjorde driften indgribende: løsningen producerer forudsigelser om enkeltpersoner, som myndigheden handler ud fra; der er risiko for, at medarbejdere tillægger AI'ens vurdering større vægt end deres egen faglige vurdering (**automatiseringsbias**); der behandles store mængder følsomme data; målgruppen er sårbare borgere; og AI kan finde sammenhænge ud over, hvad en menneskelig sagsbehandler kan, hvilket gør behandlingen grundlæggende forskellig fra traditionel sagsbehandling. Konklusionen var, at servicelovens opgavepålæg hverken regulerer rækkevidden af behandlingen eller muligheden for at anvende AI på den pågældende måde.

Denne dobbelthed går igen i [2024-212-0371](#) om Uddannelses- og Forskningsstyrelsens AI-løsning til screening af SU-handicaptillægsansøgninger, hvor løsningen skulle trænes på ca. 3.000 historiske sager og alene fungere som støtte uden at træffe endelige afgørelser, og i [2022-212-3676](#) om AI-værktøjet Asta, hvor tilsynet stillede krav til lovgivningsmæssig præcision ved profilering og behandling af følsomme data.

Konsekvensanalysen som fælles omdrejningspunkt. [AI-forordningens artikel 27](#) pålægger idriftsættere, der er offentligtretlige organer eller private enheder, som leverer offentlige tjenester, at foretage en konsekvensanalyse vedrørende grundlæggende rettigheder inden idriftsættelse af bilag III-højrisikosystemer. Analysen skal beskrive processerne, anvendelsesperioden, de berørte persongrupper, de specifikke risici for skade, gennemførelsen af menneskeligt tilsyn samt de foranstaltninger, herunder intern ledelse og klagemekanismer, der skal træffes, hvis risiciene opstår. Resultatet skal meddeles markedsovervågningsmyndigheden. Efter art. 27, stk. 4, **supplerer** analysen den databeskyttelsesretlige konsekvensanalyse efter GDPR art. 35 – den erstatter den ikke.

Datatilsynets praksis om GDPR-konsekvensanalyser er derfor direkte relevant. I [2023-423-0005](#) udtalte tilsynet alvorlig kritik af Københavns Kommunes konsekvensanalyse for AULA, og i [2023-423-0009](#) fik Hillerød Kommune både alvorlig kritik og påbud for manglende risikovurderinger og konsekvensanalyse. Mønsteret – at analyser udarbejdes for sent, for overfladisk eller slet ikke – er et af de mest sandsynlige første håndhævelsespunkter under artikel 27.

LOV	AI-forordningen § 27, stk. 1-5	Serviceloven § 86	Serviceloven § 112
PRAKSIS	Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger 12.06.2024 Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA 23.05.2024 Datatilsynet · Alvorlig kritik og påbud til Hillerød Kommune for utilstrækkelig behandlingssikkerhed og manglende risikovurderinger 22.12.2023 Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor 17.11.2023 Datatilsynet · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta 18.05.2022		

Biometri, følelsesgenkendelse og ansigtsgenkendelse – hvor grænserne allerede er blevet trukket

§ 9

Tre af artikel 5's forbud – litra e (ikkemåletrettet skrabning til ansigtsgenkendelsesdatabaser), litra f (følelsesgenkendelse på arbejdsplads og uddannelsesinstitution) og litra g (biometrisk kategorisering) – ligger tæt op ad områder, hvor Datatilsynet allerede har afsagt afgørelser under GDPR.

Følelses- og stemmeanalyse. I [2023-431-0018](#) af 27. juni 2024 undersøgte Datatilsynet af egen drift IDA Forsikrings AI-baserede transskribering og analyse af optagne telefonsamtaler, hvor systemet uddrager temaer, kvalitetsscoringer efter en samtalestandard og »root cause«-analyser. Tilsynet fandt for det første, at AI-analysen ikke er et selvstændigt behandlingsformål:

Det er i den forbindelse Datatilsynets opfattelse, at analysen af de optagne telefonsamtaler til brug for kvalitetssikring ikke skal anses for et selvstændigt formål. IDA Forsikring kan således basere analysen på samme grundlag som selve optagelsen af samtalen.

For det andet – og mere principielt for AI-forordningen – fandt tilsynet, at analysen ikke er omfattet af forbuddet mod behandling af særlige kategorier i GDPR art. 9, stk. 1: selv om stemme kan udgøre biometriske data efter art. 4, nr. 14, er formålet ikke entydigt at identificere hverken den, der ringer, eller medarbejderne, og systemet benytter ikke stemmegenkendende teknologi. Det er en mindre indgribende behandlingsform. Systemet analyserer kun ren tekst og tager ikke højde for tonefald, køn eller dialekter – hvilket tilsynet noterede primært kan føre til »falske positive« i kvalitetsscoringerne. Sagen faldt dog på samtykkets granularitet: der blev kun indhentet ét samlet samtykke til både dokumentations- og kvalitetssikringsformål, hvilket ikke var frivilligt og dermed ugyldigt.

Afgrænsningen har direkte betydning for art. 5, stk. 1, litra f og g: et system, der udleder *følelser* hos medarbejdere, ville falde under litra f, mens et system, der alene scorer sprogbrug i transskriberet tekst, ligger uden for. FH pegede i høringen over [L 111](#) netop på digital »stemmegenkendelse«, der indebærer en vurdering af en medarbejders humør og følelser, som eksempel på forbudt praksis på arbejdspladsen.

Ansigtsgenkendelse. I [2024-51-0012](#) af 18. december 2024 gav Datarådet F.C. København tilladelse efter [databeskyttelseslovens § 7, stk. 4](#) til automatisk ansigtsgenkendelse ved indgangene til Parken – men kun i forbindelse med fodboldkampe og under strenge vilkår, mens ansøgningen for koncerter og øvrige arrangementer blev afvist. Systemet sammenligner kameraoptagelser med fotos fra klubbens og politiets karantænelister. Afgørelsen viser en klar formålsbunden proportionalitetsprøvelse: den samme teknologi kan være lovlig til ét formål og ulovlig til et andet.

Skrabning af biometriske data. I [2023-211-0004](#) af 30. januar 2024 vurderede Datatilsynet etableringen og delingen af taledatasættet CoRal til udvikling af dansk taleteknologi. Tilsynet fastslog, at stemmeoptagelser er personoplysninger, men at art. 9-forbuddet ikke fandt anvendelse, fordi formålet ikke var entydig identifikation. Sagen illustrerer, at afgrænsningen af litra e i AI-forordningen – der forbyder oprettelse eller udvidelse af ansigtsgenkendelsesdatabaser gennem **ikkemåletrettet** indsamling – beror på både indsamlingsmetoden og formålet.

EU-Domstolens biometri-linje. Domstolen har i en række sager fastlagt strenge krav til myndigheders behandling af biometriske og genetiske data, som vil udgøre den ydre ramme for enhver dansk anvendelse af biometrisk AI:

- I [C-118/22](#) fastslog Store Afdeling, at ubegrænset opbevaring af politiregistrerede biometriske og genetiske data indtil den registreredes død uden periodisk nødvendighedsvurdering eller sletningsret er i strid med direktiv 2016/680 og chartret.

- I [C-80/23](#) fastslog Domstolen, at det er den kompetente myndighed selv – ikke domstolen – der skal efterprøve og godtgøre, at indsamlingen er »strengt nødvendig« efter art. 10 i direktiv 2016/680; en systematisk indsamling for alle sigtede uden konkret nødvendighedsvurdering er uforenelig med direktivet.
- Linjen er videreført i [C-57/23](#).
- I [C-548/21](#) fastslog Store Afdeling, at politiets adgang til data på en beslaglagt mobiltelefon kræver forudgående kontrol ved en domstol eller et uafhængigt forvaltningsorgan samt underretning af den registrerede.
- Og i [C-61/22](#) kendte Domstolen forordningen om biometriske identitetskort ugyldig på grund af forkert retsgrundlag, men opretholdt dens virkninger midlertidigt.

Disse afgørelser angår direktiv 2016/680 og ikke AI-forordningen, men de definerer det nødvendigheds- og proportionalitetsniveau, som biometriske AI-systemer under alle omstændigheder skal opfylde – også de områder, hvor det danske retsforbehold friholder Danmark fra selve forordningens forbud.

LOV	AI-forordningen § 5, stk. 1	Databeskyttelsesloven § 7, stk. 4	
PRAKSIS	EU-Domstolen · Beskyttelse af personoplysninger: Politiets indsamling og opbevaring af biometriske og genetiske data fra mistænkte		20.11.2025
	EU-Domstolen · Politimæssig registrering af følsomme oplysninger: Domstolens krav om »streng nødvendighed« og de kompetente myndigheders ansvar		28.11.2024
	EU-Domstolen · Politimyndigheders adgang til mobiltelefoner: Krav om retslig kontrol og proportionalitet ved databehandling i straffesager		04.10.2024
	EU-Domstolen · Ugyldighed af forordning om biometriske identitetskort pga. forkert retsgrundlag (C-61/22)		21.03.2024
	EU-Domstolen · Opbevaring af biometriske og genetiske politidata indtil den registreredes død er i strid med EU-retten		30.01.2024
	Datatilsynet · F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken		18.12.2024
	Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne		27.06.2024
	Datatilsynet · Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse		30.01.2024

§ 10 Gennemsigtighed og forklaringspligt – EU-Domstolens praksis om automatiserede afgørelser

[AI-forordningens artikel 50](#) pålægger gennemsigtighedsforpligtelser i fire lag: brugere skal oplyses om, at de interagerer med et AI-system (stk. 1); syntetisk genereret lyd-, billed-, video- eller tekstindhold skal mærkes maskinlæsbart (stk. 2); idriftsættere af følelsesgenkendelses- og biometriske kategoriseringssystemer skal underrette de berørte (stk. 3); og deepfakes samt AI-genereret tekst om spørgsmål af offentlig interesse skal mærkes (stk. 4). Oplysningerne skal gives klart og synligt senest ved første interaktion eller eksponering, jf. stk. 5. Overtrædelse af artikel 50 er efter art. 99, stk. 4, litra g, sanktioneret med op til 15 mio. EUR/3 %.

Den materielt beslægtede forklaringspligt ved automatiserede afgørelser er allerede udviklet af EU-Domstolen under GDPR. I [C-634/21](#) (SCHUFA) fastslog Domstolen, at et kreditoplysningsbureaus automatiske beregning af en kreditscore i sig selv udgør en automatisk individuel afgørelse efter GDPR art. 22, stk. 1, når scoren er afgørende for, om en tredjepart indgår aftaleforholdet – en snæver fortolkning ville skabe et hul i beskyttelsen, fordi den registrerede da ville miste indsichtsretten i logikken efter art. 15, stk. 1, litra h.

I [C-203/22](#) (Dun & Bradstreet) af 27. februar 2025 præciserede Domstolen indholdet af forklaringspligten. Den registrerede har ikke krav på formlen eller en trin-for-trin-beskrivelse, men på en egentlig forklaring:

De »meningsfulde oplysninger om logikken« ... skal således beskrive den procedure og de principper, der konkret er anvendt, på en sådan måde, at den registrerede kan forstå, hvilke af vedkommendes personoplysninger der blev anvendt på hvilken måde, da den pågældende automatiske afgørelse blev truffet, idet kompleksiteten af de operationer, der skal udføres i forbindelse med en automatisk afgørelse, ikke kan fritage den dataansvarlige for forklaringspligten.

Domstolen tilføjede, at det for en profilering som den omtvistede kan være tilstrækkeligt at oplyse, i hvilket omfang en ændring i de indgåede data ville have givet et andet resultat – en modkontrafaktisk forklaringsmodel, der er direkte anvendelig på AI-systemer.

Om forholdet til forretningshemmeligheder fastslog Domstolen, at den dataansvarlige ikke selv må afgøre spørgsmålet:

I dette tilfælde skal de nævnte oplysninger også videregives til den kompetente tilsynsmyndighed eller den kompetente ret, som skal afveje de omhandlede rettigheder og interesser med henblik på at fastlægge omfanget af den registreredes ret til indsigt i personoplysninger vedrørende den pågældende.

En national regel, der generelt afskærer indsichtsretten, når videregivelse truer en forretningshemmelighed, er derfor uforenelig med forordningen. Det er en vigtig parallel til AI-forordningens art. 78 om fortrolighed og til [§ 7](#) om offentliggørelse af afgørelser, hvor forarbejderne netop forbeholder oplysninger om tekniske indretninger og forretningsforhold: forbeholdet må efter [C-203/22](#) antages at forudsætte en konkret afvejning, ikke en generel afskæring.

Datatilsynets ældre praksis peger i samme retning. I [2019-41-0031](#) behandlede tilsynet netop spørgsmålet om automatisk prisberegning og GDPR art. 22 i forbindelse med indsichtsretten.

Et beslægtet aktindsigtsspørgsmål er behandlet af Folketingets Ombudsmand i [FOB 2022-23](#), hvor en journalist havde bedt om aktindsigt i modeldokumentationen for Udbetaling Danmarks Machine Learning-modeller, der bruges til at prioritere sager til manuel kontrol af barselsdagpenge, børnetilskud og pension. Ombudsmanden kunne ikke tilsidesætte myndighedens vurdering af, at det af væsentlige hensyn til gennemførelsen af offentlig kontrol var nødvendigt at undtage oplysninger fra modeldokumentationen efter offentlighedslovens § 33, nr. 2. Modellerne blev ikke i sig selv brugt til at vurdere ydelsesretten – en sontring der svarer nøje til AI-forordningens skel mellem beslutningsstøtte og automatiseret afgørelse.

LOV

[AI-forordningen § 50, stk. 1-5](#)
[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 7](#)

PRAKSIS

EU-Domstolen · Indsichtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder

27.02.2025

EU-Domstolen · Automatisk kreditscoring som en individuel afgørelse efter GDPR

07.12.2023

Menneskeligt tilsyn efter artikel 14 og de forvaltningsretlige krav – § 11 ombudsmandens praksis

[Artikel 14](#) kræver, at højrisiko-AI-systemer udformes, så fysiske personer effektivt kan overvåge dem i brugsperioden. Tilsynsforanstaltningerne skal stå i rimeligt forhold til risiciene, graden af autonomi og anvendelseskonteksten, og systemet skal leveres, så tilsynspersonen kan:

- forstå systemets kapacitet og begrænsninger og overvåge driften, herunder opdage uregelmæssigheder, funktionsforstyrrelser og uventet ydeevne
- være opmærksom på tendensen til at forlade sig på outputtet i overdreven grad – **automatiseringsbias** – navnlig ved systemer, der giver oplysninger eller anbefalinger til afgørelser truffet af mennesker
- fortolke outputtet korrekt
- beslutte ikke at anvende systemet eller se bort fra, tilsidesætte eller omgøre outputtet
- gribe ind eller afbryde systemet i en sikker tilstand ved en »stopknap«

For biometriske identifikationssystemer efter bilag III, punkt 1, litra a, gælder et skærpet krav i stk. 5: idriftsætteren må ikke handle på en identifikation, medmindre den er verificeret og bekræftet særskilt af mindst to fysiske personer med den nødvendige kompetence, uddannelse og myndighed – dog med undtagelse for retshåndhævelse, migrationsstyring, grænsekontrol og asylforvaltning, hvor kravet skønnes uforholdsmæssigt.

[Artikel 26](#) supplerer med idriftsætterforpligtelser: tilsynet skal overdrages til personer med den nødvendige kompetence og myndighed (stk. 2); inputdata skal være relevante og repræsentative i det omfang idriftsætteren kontrollerer dem (stk. 4); driften skal overvåges, og anvendelsen stilles i bero ved risiko (stk. 5); logfiler skal opbevares i mindst seks måneder (stk. 6); arbejdstagerrepræsentanter og berørte arbejdstagere skal informeres, inden systemet tages i brug på arbejdspladsen (stk. 7); og fysiske personer, der er genstand for et bilag III-system, som træffer eller bistår med at træffe beslutninger om dem, skal underrettes (stk. 11). Hertil kommer den generelle pligt i [artikel 4](#) til at sikre et tilstrækkeligt niveau af AI-færdigheder hos personalet.

Ombudsmandens parallelle krav. Folketingets Ombudsmand har uafhængigt af AI-forordningen udviklet en fast praksis om forvaltningsretlige krav til automatiserede systemer, som i vidt omfang dækker det samme terræn. I [FOB 2026-6](#) om Skatteforvaltningens automatiserede SMV-løsning sammenfattede ombudsmanden de generelle krav:

Det er et grundlæggende krav, at offentlige it-systemer kan understøtte en korrekt anvendelse af den relevante lovgivning – herunder forvaltningsretlige regler og principper. Dette kan bedst sikres ved en tidlig identifikation og systemindarbejdelse af de pågældende regelsæt.

Ombudsmanden fremhævede tillige den strukturelle risiko ved automatisering:

Automatiserede afgørelsessystemer forudsætter dermed også, at myndighederne på forhånd kan afgrænse, hvilket faktum der måtte være relevant i fremtidige sager, idet den faktiske del af beslutningsgrundlaget ikke længere bliver genstand for myndighedens konkrete vurdering. Automatiserede systemer indebærer derfor en risiko for, at myndighederne ikke fanger tilfælde med atypiske fakta eller tilfælde, hvor retsgrundlaget forpligter til at tage hensyn til forhold, der enten normalt ikke opstår eller normalt ikke er relevante.

Den juridiske ekspertise skal være til rådighed i alle væsentlige faser, systemet skal testes i den sammenhæng, hvor det skal anvendes, og myndigheden skal efter implementeringen følge op på, om systemet som forudsat understøtter en korrekt retsanvendelse. Ombudsmanden henviser i den forbindelse til [FOB 2025-13](#) om Vurderingsstyrelsens automatiske robotløsning, der førte til fejl, og til den ældre grundslag [FOB 2014-24](#) om SKATs EFI-system.

Den samme linje findes i [vejledningen om digitaliseringsklar lovgivning](#), der fastslår, at »brug af automatisk sagsbehandling ændrer ikke ved, at de forvaltningsretlige regler om f.eks. begrundelse, vejledning, partshøring, mv. skal overholdes«, og at en automatisk genereret begrundelse skal leve op til de almindelige krav i [forvaltningslovens § 24](#). En forudsætning for hel eller delvis automatisering er, at afgørelsen kan træffes efter rent objektive kriterier uden udøvelse af et individuelt skøn.

AI-forordningens artikel 14 og forvaltningsrettens krav peger dermed samme vej: menneskeligt tilsyn skal være reelt og ikke blot formelt, og systemet skal designes, så tilsynspersonen faktisk kan gennemskue og omgøre outputtet. Om afgrænsningen mellem beslutningsstøtte og bunden regel anvendelse kan der krydshenvises til [skoen-under-regel-pligtmaessigt-skoen](#).

LOV

AI-forordningen § 4

AI-forordningen § 14, stk. 1-5

AI-forordningen § 26, stk. 1-12

Forvaltningsloven § 24

Sektorbekendtgørelser – hvordan Danmark har lukket

§ 12 hjemmelshullet efter Datatilsynets praksis

Datatilsynets konklusion i [2023-212-0015](#) om, at generelle opgavehjemler ikke er tilstrækkeligt klare til at bære **driften** af en beslutningsstøttende AI-løsning, har haft direkte lovgivningsmæssig virkning. Der er siden 2025 udstedt en række sektorspecifikke bekendtgørelser, der etablerer det supplerende nationale retsgrundlag:

Bekendtgørelse	Område	Ikrafttræden
Bekendtgørelse om Arbejdstilsynets anvendelse af kunstig intelligens	Tilsyns- og vejledningsopgaver efter arbejdsmiljølovens § 72	1. juli 2025
Bekendtgørelse om Uddannelses- og Forskningsstyrelsens anvendelse af kunstig intelligens ...	Sagsbehandling efter SU-loven	2025
Bekendtgørelse om STAR's behandling af personoplysninger med kunstig intelligens ...	Styrelsens opgavevaretagelse, herunder jobmatch på Jobnet	1. februar 2026
Bekendtgørelse om kommunernes behandling af personoplysninger med kunstig intelligens ... i beskæftigelsesindsatsen	Kommunal beskæftigelsesindsats	1. februar 2026

De to sidste hviler på bemyndigelserne i § 52 a i lov om organisering og understøttelse af beskæftigelsesindsatsen, indsat ved lov nr. 1750 af 29. december 2025, jf. [startvejledningen](#). Formålet er ifølge vejledningen udtrykkeligt »at skabe et tilstrækkeligt klart nationalt retsgrundlag for STAR og kommunernes behandling af personoplysninger i kunstig intelligens-løsninger« – altså præcis den klarhed, Datatilsynet havde efterlyst.

Bekendtgørelserne indeholder tre gennemgående retlige greb, der ligger tæt op ad AI-forordningens systematik:

- **Forbud mod fuldautomatiske afgørelser.** Kommunerne kan efter bekendtgørelsens § 1, stk. 6, ikke træffe afgørelser, der alene er baseret på automatisk behandling, herunder profilering. [Vejledningen](#) præciserer, at bestemmelsen gengiver GDPR art. 22, stk. 1, og at AI-behandlingen »alene [skal være] sagsunderstøttende«.
- **Særsomt oplysningspligt om AI-anvendelse.** Efter § 2, stk. 4, skal kommunerne sikre, at det tydeligt fremgår for den registrerede, når kunstig intelligens anvendes. Vejledningen fastslår, at denne pligt »går således videre end den almindelige oplysningspligt efter databeskyttelsesforordningen, da den indeholder et eksplicit krav om at oplyse om anvendelsen af kunstig intelligens, hvilket ikke altid vil være et krav efter oplysningspligten i artikel 13 og artikel 14«. Det er reelt en national foregribelse af AI-forordningens art. 26, stk. 11, og art. 50.
- **Offentliggørelseskrav.** Både SU- og STAR-bekendtgørelserne pålægger styrelserne at offentliggøre, i hvilke tilfælde de anvender kunstig intelligens til at understøtte sagsbehandlingen.

Begrebsmæssigt henviser vejledningen til beskæftigelsesbekendtgørelsen direkte til forordningen: »For så vidt angår definitionen af kunstig intelligens, herunder hvordan bestemte typer af kunstig intelligens må og ikke må benyttes, henvises til AI-forordningen.« Begrebet »lignende digitale løsninger« er indsat for at fange teknologier, der minder om AI uden at opfylde forordningens definition.

Digitaliseringsstyrelsen sendte i februar 2026 [et lovforslag om generel hjemmel til udvikling og anvendelse af AI-systemer i den offentlige forvaltning](#) i høring – en tværgående afløsning for den nuværende sektorvise tilgang. Udkastet definerer »beslutningsstøtte« som situationer, hvor et AI-system anvendes som et fagligt understøttende redskab for en sagsbehandler, uden at systemet selv træffer afgørelser, og anerkender åbent, at grænsedragningen »ikke [er] fastlagt klart i retspraksis«, og at »fremtidig retspraksis vil bidrage til at præcisere, hvilken grad af menneskelig involvering« der kræves.

LOV

[AI-forordningen § 26, stk. 11](#)[AI-forordningen § 50, stk. 1](#)

PRAKSIS

Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor 17.11.2023

Dansk domspraksis om kunstig intelligens er endnu strafferetlig, ikke forordningsretlig

Der findes endnu ingen offentliggjorte danske domme om AI-forordningen eller gennemførelseslovens § 10. Den domspraksis, der faktisk foreligger om kunstig intelligens, er strafferetlig og hviler udelukkende på straffeloven – men den er værd at kende, fordi den viser, hvordan danske domstole hidtil har håndteret AI-genereret materiale.

I [SS-3195/2024-RAN](#) af 8. januar 2025 behandlede Retten i Randers fremstilling, besiddelse og udbredelse af 36.209 AI-genererede, fotorealistiske børnepornografiske billeder. Tiltalte hævdede, at materialet var lovligt, og at formålet var at afholde pædofile fra at søge ægte overgrebsmateriale. Retten fandt billederne omfattet af [straffelovens § 235](#) og idømte fængsel i 1 år og 3 måneder, heraf 3 måneder ubetinget, idet der blev lagt væsentlig vægt på, at det ikke kunne bevises, at de anvendte AI-modeller var trænet på ægte børnepornografi.

Vestre Landsret stadfæstede skyldkendelsen, men skærpede straffen til ubetinget fængsel i 1 år og 6 måneder under dissens 5-1, jf. [S-0141-25](#) af 12. juni 2025. Procesbevillingsnævnet behandlede sagen under j.nr.

25/17215 og tog stilling til, om den principielle problemstilling om strafudmåling for rent fiktivt, AI-genereret materiale kunne indbringes for Højesteret, jf. [U 2025.3571 V](#).

Sagskomplekset illustrerer et generelt mønster: dansk ret har hidtil håndteret AI ved at anvende eksisterende gerningsindhold på nye teknologiske frembringelser, ikke ved at regulere teknologien som sådan. AI-forordningen vender denne logik om ved at regulere systemet, dets udbyder og dets idriftsætter forud for skaden. De to spor kan mødes: en deepfake, der ikke er mærket efter [artikel 50, stk. 4](#), kan efter omstændighederne både udløse bøde efter forordningsspor og straf efter straffelovens bestemmelser om freds- og ærekrænkelser – hvorved subsidiaritetsklausulen i [§ 10, stk. 1](#) (»medmindre højere straf er forskyldt efter anden lovgivning«) bliver aktuel.

LOV

AI-forordningen § 50, stk. 4

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10, stk. 1

Straffeloven § 235, stk. 1, 2

PRAKSIS	Landsretten · Ubetinget fængsel for fremstilling, besiddelse og udbredelse af over 36.000 AI-genererede billeder af børnepornografisk karakter	12.06.2025
	Byretten · Dom for fremstilling og udbredelse af AI-genereret børnepornografi	08.01.2025
	Procesbevillingsnævnet · 3.-instansbevilling: Strafudmåling for besiddelse og udbredelse af ca. 36.000 AI-genererede børnepornografiske billeder (U 2025.3571 V)	21.11.2025

§ 14 Sammenfatning – hvad der er afklaret, og hvad der endnu udestår

Afklaret retstilstand. Danmark har med [lov nr. 467 af 14. maj 2025](#), vedtaget enstemmigt med 109 stemmer ved [L 154](#), etableret den institutionelle og strafferetlige ramme for forordningens første fase. Tilsynet er delt mellem Digitaliseringsstyrelsen, Datatilsynet og Domstolsstyrelsen med en fjerde ordning for domstolenes judicielle AI-brug. Markedsovervågningsbeføjelserne er vidtgående – oplysningskrav, kontrolbesøg uden retskendelse, tekniske undersøgelser på stedet, sagkyndig bistand, politibistand, påbud, midlertidigt forbud og offentliggørelse. Overtrædelser straffes med bøde, juridiske personer kan ifalde ansvar efter straffelovens kapitel 5, og forældelsesfristen er 5 år. Der er ingen administrativ rekurs.

Uafklaret. Fire ting står åbne:

- Bødeniveauet.** Der findes ingen dansk retspraksis om bødeudmåling efter § 10. Den foreslåede bødemodel i det bortfaldne [L 111](#) – statiske grundbeløb på 700.000/150.000/37.500 EUR og dynamiske på 0,14/0,03/0,005 % af global omsætning – er den eneste konkrete indikation, men den er ikke gældende ret.
- Anden fase af gennemførelsen.** Forordningen fandt anvendelse i sit fulde omfang fra 2. august 2026, men det lovforslag, der skulle etablere den fulde nationale tilsyns- og sanktionsramme for højrisiko-systemer, gennemsigtighed og GPAI, bortfaldt. Indtil ny lovgivning vedtages, dækker den gældende lov alene tilsyn med forbudt AI-praksis efter art. 5, stk. 1, litra a-g.
- Grænsen mellem beslutningsstøtte og automatiseret afgørelse.** Digitaliseringsstyrelsen erkender selv i [høringsudkastet af februar 2026](#), at kravet til den menneskelige involverings omfang ikke er fastlagt i retspraksis.
- Samspillet med GDPR.** Datatilsynet er både markedsovervågningsmyndighed for art. 5, stk. 1, litra d og g, og databeskyttelsestilsyn. En og samme AI-anvendelse kan derfor rammes ad to spor, og art. 99, stk. 7,

litra b og c, pålægger netop at tage hensyn til, om andre myndigheder allerede har sanktioneret den samme operatør for samme aktivitet – et ne bis in idem-hensyn, der endnu ikke er prøvet i dansk praksis.

Hvad praksis indtil videre siger. Den retningsgivende praksis findes uden for forordningen selv, men på dens materielle kerneområder: Datatilsynets sondring mellem udvikling og drift i [2023-212-0015](#), afgrænsningen af biometri i [2023-431-0018](#) og [2024-51-0012](#), EU-Domstolens forklaringspligt i [C-203/22](#) og [C-634/21](#), nødvendighedskravet ved biometriske politidata i [C-118/22](#) og [C-80/23](#), Ombudsmandens krav til automatiserede systemer i [FOB 2026-6](#), og Ligebehandlingsnævnets prøvelse af algoritmisk profilering i [20-25601](#). Beslægtede spørgsmål om Datatilsynets bødeindstillinger behandles under [datatilsynsboder-gdpr-overtraedelser](#), AI-systemers persondatabehandling under [ai-systemer-gdpr](#), og AI i ansættelsesforhold under [databeskyttelse-medarbejder](#).

LOV

[AI-forordningen § 99, stk. 7](#)

[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10, stk. 1-4](#)

PRAKSIS	EU-Domstolen · Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	27.02.2025
	EU-Domstolen · Politimæssig registrering af følsomme oplysninger: Domstolens krav om »streng nødvendighed« og de kompetente myndigheders ansvar	28.11.2024
	EU-Domstolen · Opbevaring af biometriske og genetiske politidata indtil den registreredes død er i strid med EU-retten	30.01.2024
	EU-Domstolen · Automatisk kreditscoring som en individuel afgørelse efter GDPR	07.12.2023
	Datatilsynet · F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken	18.12.2024
	Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	27.06.2024
	Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	17.11.2023
	Ligebehandlingsnævnet · Klage over anvendelse af herkomstkriterier i digitalt værktøj til profilafklaring af ledige	12.05.2022

REFERENCE **Lovgrundlag**

8 paragraffer

AI-forordningen § 5	stk. 1	AI-forordningen § 6	stk. 2, 3
AI-forordningen § 99	stk. 3-7	Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 2	stk. 1-5
Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 3		Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 6	stk. 1
Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 8	stk. 1, 2	Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10	stk. 1-4

MATERIALE **Citerede afgørelser**

22 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL

7

20.11.2025	Beskyttelse af personoplysninger: Politiets indsamling og opbevaring af biometriske og genetiske data fra mistænkte	C-57/23
27.02.2025	Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	C-203/22
28.11.2024	Politimæssig registrering af følsomme oplysninger: Domstolens krav om »streng nødvendighed« og de kompetente myndigheders ansvar	C-80/23
04.10.2024	Politimyndigheders adgang til mobiltelefoner: Krav om retslig kontrol og proportionalitet ved databehandling i straffesager	C-548/21
21.03.2024	Ugyldighed af forordning om biometriske identitetskort pga. forkert retsgrundlag (C-61/22)	C-61/22
30.01.2024	Opbevaring af biometriske og genetiske politidata indtil den registreredes død er i strid med EU-retten	C-118/22
07.12.2023	Automatisk kredit scoring som en individuel afgørelse efter GDPR	C-634/21

LANDSRETTEEN · ANKEINSTANS

1

12.06.2025	Ubetinget fængsel for fremstilling, besiddelse og udbredelse af over 36.000 AI-genererede billeder af børnepornografisk karakter	S-0141-25
------------	--	-----------

BYRETTEEN · FØRSTE INSTANS

1

08.01.2025	Dom for fremstilling og udbredelse af AI-genereret børnepornografi	6888-8272
------------	--	-----------

DATATILSYNET · NÆVN / KLAGEINSTANS

11

09.10.2025	Lovlighed af sektionskontrol og automatisk hastighedsmåling på Storebæltsbroen	2025-31-1798
18.12.2024	F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken	2024-51-0012
13.09.2024	Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag	2024-32-0482
27.06.2024	IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	2023-431-0018
12.06.2024	Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger	2024-212-0371
23.05.2024	Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA	2023-423-0005
30.01.2024	Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse	2023-211-0004
22.12.2023	Alvorlig kritik og påbud til Hillerød Kommune for utilstrækkelig behandlingssikkerhed og manglende risikovurderinger	2023-423-0009
17.11.2023	Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	2023-212-0015
18.05.2022	Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	2022-212-3676

26.02.2020	Tilsyn med Rejsekort & Rejseplan A/S og overholdelse af retten til indsig	2019-41-0031
------------	---	--------------

LIGEBEHANDLINGSNÆVNET · NÆVN / KLAGEINSTANS	1
---	---

12.05.2022	Klage over anvendelse af herkomstkriterier i digitalt værktøj til profilafklaring af ledige	20-25601
------------	---	----------

PROCESBEVILLINGSNÆVNET · NÆVN / KLAGEINSTANS	1
--	---

21.11.2025	3.-instansbevilling: Strafudmåling for besiddelse og udbredelse af ca. 36.000 AI-genererede børnepornografiske billeder (U 2025.3571 V)	U 2025.3571 V
------------	---	---------------
