

PRAKSISOVERSIGT · IT-RET

Praksisoversigt over AI-systemer og persondata

Datatilsynets praksis om retsgrundlag, automatiske afgørelser og transparens – og samspillet med AI-forordningen

Version 2 Opdateret 15. jul. 2026 23 afgørelser · 2020-2025

[Læs online](#)

INTRODUKTION

AI-systemer, der behandler personoplysninger, reguleres i dag af to regelsæt på én gang: databeskyttelsesforordningen, der er teknologineutral og har været gældende siden 2018, og AI-forordningen (EU) 2024/1689, der siden august 2024 er trådt trinvis i kraft. Datatilsynets praksis har på få år udviklet en klar keredoktrin: en offentlig myndighed kan som udgangspunkt *udvikle* og *gentræne* en AI-løsning med hjemmel i den lovgivning, der pålægger myndigheden opgaven, men *driften* af løsningen kræver et tilstrækkeligt klart supplerende nationalt retsgrundlag – og kravet til klarhed stiger med indgrebets intensitet. Den doktrin har udløst en hel bølge af danske hjemmelsbekendtgørelser i 2025-2026 og et generelt lovforslag om AI i den offentlige forvaltning, der var i høring i februar 2026. Oversigten samler Datatilsynets afgørelser og udtalelser, EU-Domstolens praksis om GDPR art. 22 og 15 samt Folketingets Ombudsmands praksis om automatiserede sagsskridt.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** Udvikling og gentræning af en AI-løsning kan efter Datatilsynets praksis ske på grundlag af den sektorlovgivning, der forpligter myndigheden til opgaven, mens DRIFTEN af løsningen kræver et selvstændigt og tilstrækkeligt klart nationalt retsgrundlag (j.nr. 2023-212-0015).
- 02** Kravet til retsgrundlagets klarhed er glidende: jo mere indgribende behandlingen af personoplysninger i AI-løsningen er for borgeren, desto klarere skal hjemlen være.
- 03** Udvikling af en AI-løsning anses databeskyttelsesretligt som et SELVSTÆNDIGT formål – forskelligt fra myndighedens daglige drift – og skal derfor hjemles og formålsafgrænses særskilt.
- 04** En trænet AI-model udgør som klart udgangspunkt ikke i sig selv personoplysninger; risikoen for genidentifikation ved målrettede angreb ændrer ikke dette (j.nr. 2023-212-0021).
- 05** GDPR art. 22 er ikke et generelt forbud, men en ret for den registrerede – den rammer kun afgørelser, der ALENE er baseret på automatisk behandling uden faktisk og reel menneskelig involvering, og som evaluerer personlige forhold.
- 06** Ren matematisk beregning uden evaluering af personlige forhold falder uden for art. 22; beslutningsstøtte, hvor en sagsbehandler reelt træffer afgørelsen, gør det også – men understøttelsen må ikke være proforma.

- 07** EU-Domstolen har i C-634/21 (SCHUFA) fastslået, at en automatisk fastsat scoringsværdi selv udgør en "afgørelse" efter art. 22, når tredjemand i afgørende grad lægger den til grund for sin beslutning.
- 08** Indsigtsretten i "logikken" bag en automatisk afgørelse, jf. art. 15, stk. 1, litra h, kræver en forståelig forklaring af den procedure og de principper, der konkret er anvendt – ikke udlevering af algoritmen – og forretningshemmeligheder skal i givet fald forelægges tilsynsmyndighed eller domstol til afvejning (C-203/22).
- 09** De danske AI-bekendtgørelser fra 2025-2026 tillader mønstergenkendelse og profilering til sagsUNDERSTØTTELSE, men forbyder udtrykkeligt afgørelser truffet alene på grundlag af automatisk behandling.
- 10** Bekendtgørelsen om kommunernes AI-brug i beskæftigelsesindsatsen pålægger en oplysningspligt, der går VIDERE end GDPR art. 13-14: det skal tydeligt fremgå for borgeren, når kunstig intelligens anvendes.
- 11** Ansigtsgenkendelse er behandling af biometriske data og forudsætter enten udtrykkeligt samtykke med reelle alternativer eller – for private – en konkret tilladelse fra Datatilsynet efter databeskyttelseslovens § 7, stk. 4; tilladelser gives snævert og formålsbestemt.
- 12** Datatilsynet er markedsovervågningsmyndighed for AI-forordningens forbud mod prædiktiv kriminalitetsprofilering og biometrisk kategorisering (art. 5, stk. 1, litra d og g), mens Digitaliseringsstyrelsen fører tilsyn med de øvrige forbud.
- 13** AI-forordningen berører ikke databeskyttelsesforordningen (art. 2, stk. 7) – compliance med den ene giver ikke lovlighed efter den anden.
- 14** Folketingets Ombudsmand kræver, at forvaltningsretlige krav – officialprincip, partshøring, begrundelse – tænkes ind fra START ved udvikling af automatiserede systemer; automatisering forudsætter, at sagsskridtet kan foretages efter objektive kriterier uden individuelt skøn.

To regelsæt, ét system: databeskyttelsesforordningen og

§ 1 AI-forordningen side om side

AI-systemer, der behandler personoplysninger, er underlagt **begge** regelsæt samtidig. Det er ikke et valg. [AI-forordningens artikel 2, stk. 7](#) fastslår udtrykkeligt, at forordningen ikke berører databeskyttelsesforordningen:

EU-retten om beskyttelse af personoplysninger, privatlivets fred og kommunikationshemmeligheden finder anvendelse på personoplysninger, som behandles i forbindelse med de rettigheder og forpligtelser, der er fastsat i denne forordning. Denne forordning berører ikke forordning (EU) 2016/679 [...]

Det betyder i praksis, at et AI-system godt kan være fuldt ud lovligt efter AI-forordningen (fx fordi det ikke er et højrisikosystem) og alligevel ulovligt, fordi der ikke er et gyldigt behandlingsgrundlag efter [GDPR artikel 6](#). Omvendt gør et gyldigt GDPR-hjemmelsgrundlag ikke en forbudt AI-praksis lovlig.

AI-forordningen trådte i kraft i august 2024 og finder anvendelse **trinvis**. Af forarbejderne til den danske gennemførelseslov fremgår tidsplanen:

Tidspunkt	Hvad finder anvendelse
2. februar 2025	Kapitel I (almindelige bestemmelser) og kapitel II (forbudte former for AI-praksis)
2. august 2025	Bl.a. kapitel III, afdeling 4, kapitel V (AI-modeller til almen brug), VII (forvaltning) og XII (sanktioner) samt art. 78
2. august 2026	Forordningen i øvrigt
2. august 2027	Artikel 6, stk. 1 (højrisiko-AI i produkter) og de tilsvarende forpligtelser

Danmark har suppleret forordningen ved [lov nr. 467 af 14. maj 2025 om supplerende bestemmelser til forordningen om kunstig intelligens](#), der efter [§ 12](#) trådte i kraft den 2. august 2025. Loven regulerer indtil videre kun tilsynet med de **forbudte** former for AI-praksis. Kompetencefordelingen efter [§ 2](#) er central for denne praksisoversigt:

- **Digitaliseringsstyrelsen** er bemyndigende myndighed, centralt kontaktpunkt og markedsovervågningsmyndighed for [artikel 5, stk. 1, litra a-c](#) og [litra e-f](#) (manipulerende teknikker, udnyttelse af sårbarheder, social scoring, ansigtsgenkendelsesdatabaser skabt ved ikke-måltrettet indsamling, følelsesgenkendelse på arbejdsplads og uddannelsesinstitution).
- **Datatilsynet** er markedsovervågningsmyndighed for [artikel 5, stk. 1, litra d](#) (prædiktiv kriminalitetsprofilering) og [litra g](#) (biometrisk kategorisering med henblik på at udlede race, politiske anskuelser, seksuel orientering m.v.) – dog kun for de dele, der ikke er omfattet af det danske retsforbehold.
- **Domstolsstyrelsen** fører tilsyn med domstolenes *administrative* brug af AI-systemer.

Af lovforarbejderne fremgår, at de kompetente myndigheder skal virke **funktionelt uafhængigt**:

De nationale kompetente myndigheders eventuelle overordnede myndigheder har således ikke instruktionsbeføjelse i de opgaver og sager, som behandles i medfør af den foreslåede lov, herunder i forbindelse med de nationale kompetente myndigheders udførelse af tilsyn og kontrol.

Efter [§ 3](#) kan myndighedernes afgørelser ikke indbringes for anden administrativ myndighed. Et efterfølgende lovforslag om en samlet dansk "AI-lov" ([L 111, fremsat 18. februar 2026](#)), der ville have ophævet 2025-loven og udbygget tilsynsbeføjelserne, **bortfaldt**. Retsstillingen er derfor fortsat lov nr. 467 af 14. maj 2025.

LOV

AI-forordningen § 2, stk. 7

AI-forordningen § 5, stk. 1

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 2

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 3

Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 12

§ 2 Hvornår foreligger der en "afgørelse alene baseret på automatisk behandling"? Afgrænsningen af GDPR art. 22

GDPR artikel 22, stk. 1 giver den registrerede ret til ikke at være genstand for en afgørelse, der **alene** er baseret på automatisk behandling, herunder profilering, og som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende. Bestemmelsen er ikke et generelt forbud. Betænkningsudvalget bag den danske databeskyttelseslov fastslog i [betænkning nr. 1565/2017, s. 371](#):

Det samme ses at være tilfældet med databeskyttelsesforordningen, idet bestemmelsen som anført stort set har samme ordlyd som direktivet, og da der heller ikke ses at fremgå et direkte forbud mod automatiske individuelle afgørelser. Forordningens artikel 22, vil derfor ligesom efter persondatalovens § 39 [...] skulle ses som en indsigelsesret for den registrerede.

Tre afgrænsninger er afgørende i praksis:

1) Der skal evalueres personlige forhold. Betænkningen fremhæver på [s. 373](#), at rene beregninger falder udenfor:

Der vil således ikke være tale om en afgørelse i artikel 22's forstand, såfremt den afgørelse, der træffes, sker ved en rent matematisk udregning ud fra de givne faktuelle forudsætninger, uden at der dermed sker en evaluering af personlige forhold vedrørende vedkommende.

Det er baggrunden for, at fx **automatisk hastighedsmåling og sektionskontrol** ikke er et art. 22-problem, men et almindeligt hjemmels- og proportionalitetsspørgsmål. I [2025-31-1798](#) vurderede Datatilsynet lovligheden af sektionskontrol på Storebæltsbroen efter [artikel 6, stk. 1, litra e](#) og dataminimeringsprincippet – ikke efter art. 22.

2) Afgørelsen skal have retsvirkning eller betydeligt påvirke. Betænkningen nævner som eksempler et forsikringsselskabs automatiske afslag på at tegne en police eller på at dække en skade, en banks automatiske afslag på lån, og et automatiseret frasorteringssystem i rekruttering. Generel markedsføring er derimod ikke omfattet.

3) "Alene" betyder uden reel menneskelig involvering. Den nyeste danske normering findes i [vejledningen til bekendtgørelsen om kommunernes AI-brug i beskæftigelsesindsatsen](#) (januar 2026):

Ved automatisk behandling forstås en afgørelse, der alene er baseret på automatisk behandling uden en vis grad af faktisk og reel menneskelig involvering.

Ordet **faktisk og reel** er kernen: et pro forma-klik af en sagsbehandler, der ikke reelt kan tilsidesætte modellens output, gør ikke afgørelsen "menneskelig".

EU-Domstolen har skubbet grænsen udad. I [C-634/21](#) (SCHUFA, 7. december 2023) fastslog Domstolen, at et kreditplysningsbureaus automatiske fastsættelse af en **scoringsværdi** i sig selv udgør en "afgørelse" i art. 22, stk. 1's forstand, når tredjemand – fx en bank – i afgørende grad lægger værdien til grund for sin beslutning om at indgå eller afvise en aftale. Det er en vigtig præcisering for AI-baserede scoring- og risikomodeller: **den, der leverer scoren, kan ikke gemme sig bag, at det formelt er kunden, der træffer beslutningen.** Samme dag afgjorde Domstolen [C-26/22](#), hvor grænserne for kreditplysningsbureauers lagring af oplysninger blev fastlagt, og hvor det blev slået fast, at tilsynsmyndighedens afgørelser er undergivet **fuld** domstolsprøvelse.

EU-Domstolen · Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	07.12.2023
Datatilsynet · Lovlighed af sektionskontrol og automatisk hastighedsmåling på Storebæltsbroen	09.10.2025

§ 3 Datatilsynets keredoktrin: udvikling kan hjemles i opgavelovgivningen – drift kræver et klart nationalt retsgrundlag

Den vigtigste enkeltafgørelse i dansk AI-databeskyttelsespraksis er Datatilsynets udtalelse af 17. november 2023 til Københavns Kommune, [j.nr. 2023-212-0015](#). Kommunen ville udvikle, idriftsætte og gentræne en AI-løsning, der som **beslutningsstøtte** for sagsbehandlere i sundheds- og omsorgsforvaltningen skulle identificere borgere med behov for vedligeholdende træning og rehabiliterende indsats. Datatilsynets vurdering:

Det er Datatilsynets vurdering, at udvikling, drift og gentræning af en AI-løsning, hvor der behandles personoplysninger og særlige kategorier af personoplysninger med henblik på at forudsige borgeres behov for og gavn af genoptræning for at undgå funktionsnedsættelse generelt kan ske på baggrund af databeskyttelsesforordningens artikel 6, stk. 1, litra e, samt artikel 9, stk. 2, litra g. Begge bestemmelser forudsætter dog et såkaldt supplerende nationalt retsgrundlag.

Og dernæst den afgørende sontring:

Behandling af personoplysninger til udvikling, herunder gentræning, af løsningen kan efter Datatilsynets vurdering ske under henvisning til de eksisterende bestemmelser i serviceloven, der forpligter kommunen til at træffe afgørelse om og levere vedligeholdende træning og rehabiliterende indsats.

Behandling af personoplysninger som led i driften af løsningen kan imidlertid ikke ske inden for rammerne af disse bestemmelser, da der ikke er tale om et tilstrækkeligt klart retsgrundlag i lyset af, hvor indgribende en behandlingsaktivitet der er tale om.

Doktrinen er dermed:

- **Udvikling og gentræning** ⇒ kan bæres af den sektorlov, der pålægger myndigheden opgaven ([art. 6, stk. 1, litra e](#) og [art. 9, stk. 2, litra g](#)).
- **Drift** ⇒ kræver et *særskilt* og *tilstrækkeligt klart* nationalt retsgrundlag.
- **Klarhedskravet er glidende**. Som Beskæftigelsesministeriet gengav doktrinen i bemærkningerne til [lovforslaget om Arbejdstilsynets AI-anvendelse \(L 143, 2024-25\)](#):

Kravet til klarheden af det nationale retsgrundlag afhænger således af, hvor indgribende behandlingen af personoplysninger, der finder sted i den pågældende løsning, vil være for borgeren; jo mere indgribende behandlingen er, desto mere klart skal det nationale retsgrundlag være for behandlingen af personoplysninger i driften af en kunstig intelligens-løsning.

Datatilsynet støtter kravet på EU-Domstolens dom af 24. februar 2022 i **sag C-175/20**, hvorefter lovgivningen bag behandlingen skal fastsætte "klare og præcise regler, der regulerer rækkevidden og anvendelsen af den omhandlede foranstaltning, og som opstiller mindstekrav, således at de personer, hvis personoplysninger er berørt, råder over tilstrækkelige garantier".

Samme spor ses i den tidligere udtalelse [j.nr. 2022-212-3676](#) om kommunernes brug af **AI-værktøjet Asta**, hvor Datatilsynet vurderede retsgrundlaget med inddragelse af både [art. 6, stk. 1](#), [art. 9, stk. 2](#) og [art. 22, stk. 2](#) samt

[databeskyttelseslovens § 7, stk. 4, § 11, stk. 1](#) og officialprincippet i [retssikkerhedslovens § 10](#). Kombinationen er sigende: spørgsmålet om automatiske afgørelser kan ikke behandles isoleret fra spørgsmålet om, hvorvidt sagen overhovedet er tilstrækkeligt oplyst.

Doktrinen blev anvendt igen i [j.nr. 2024-212-0371](#) om en AI-løsning til sagsbehandling af **SU-ansøgninger**, hvor Datatilsynet udtrykkeligt henviste tilbage til udtalelsen af 17. november 2023 og til tilsynets egen skabelon til konsekvensanalyse ved AI-løsninger, og hvor både [art. 6, stk. 1, litra e](#) og [art. 35, stk. 1](#) indgik i vurderingen.

LOV	Databeskyttelsesforordningen § 6, stk. 1	Databeskyttelsesforordningen § 9, stk. 2
	Databeskyttelsesforordningen § 22, stk. 2	Databeskyttelsesforordningen § 35, stk. 1
	Databeskyttelsesloven § 7, stk. 4	Databeskyttelsesloven § 11, stk. 1

PRAKSIS	Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger	12.06.2024
	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

§ 4 Hjemmelsbølgen 2025-2026: bekendtgørelserne som lovgivers svar på Datatilsynets praksis

Datatilsynets krav om et "tilstrækkeligt klart nationalt retsgrundlag" for **driften** af AI-løsninger satte myndighederne skakmat. Digitaliseringsministeriets AI-taskforce konstaterede i [juni 2025](#), at "mange myndigheder støder i dag på juridiske uklarheder", og at taskeforcen derfor ville "iværksætte en indsats for at etablere hjemler til brug af kunstig intelligens i den offentlige sektor".

Resultatet er en serie sektorspecifikke hjemmelsbekendtgørelser, der alle følger samme skabelon: bemyndigelse i sektorloven → bekendtgørelse med udtømmende opregning af datakategorier → sikkerhedskrav → forbud mod fuldautomatiske afgørelser.

Bekendtgørelse	Myndighed	Nøgleindhold
Bek. nr. 813 af 26. juni 2025	Uddannelses- og Forskningsstyrelsen	AI til at <i>understøtte</i> SU-sagsbehandling; formålet er at optimere sagsbehandlingsprocesser
Bek. nr. 868 af 28. juni 2025	Arbejdstilsynet	Samkøring og behandling i AI-løsninger til tilsyns- og vejledningsopgaver efter arbejdsmiljølovens § 72; udtømmende liste over 16 datakategorier – inkl. helbred, race, religion og strafbare forhold
Bek. nr. 100 af 20. januar 2026	Styrelsen for Arbejdsmarked og Rekruttering	Udvikling, idriftsættelse og træning af AI-modeller
Bek. nr. 101 af 20. januar 2026	Kommunerne (beskæftigelsesindsatsen)	Mønstergenkendelse og profilering tilladt til sagsunderstøttelse – men forbud mod fuldautomatiske afgørelser

Den kommunale beskæftigelsesbekendtgørelse er den mest gennemarbejdede. [§ 1](#) tillader udtrykkeligt mønstergenkendelse og profilering, genanvendelse af data til nye AI-behandlinger og træning af modeller – men slutter med en skarp begrænsning i stk. 6:

Kommunerne kan ikke efter bestemmelserne i denne bekendtgørelse træffe afgørelser, der alene er baseret på automatisk behandling, herunder profilering.

Vejledningen af 23. januar 2026 forklarer, at bestemmelsen "er en gengivelse af databeskyttelsesforordningens artikel 22, stk. 1", og at AI-behandlingen derfor "alene [skal være] sagsunderstøttende". Lovgiver har med andre ord *ikke* villet udnytte det nationale råderum i [art. 22, stk. 2, litra b](#) til at hjemle automatiske afgørelser på beskæftigelsesområdet. Samme linje ses i bemærkningerne til [beskæftigelsesreformen \(L 66, 2025-26\)](#):

Det er ikke hensigten, at bemyndigelsen skal kunne anvendes til at fastsætte regler om anvendelse af løsninger, der anvender kunstig intelligens til f.eks. profilering af borgerne med henblik på at træffe automatiske afgørelser.

Det står i modsætning til fx [L 75 om projekttilskud på Kulturministeriets område \(2025-26\)](#), hvor der *netop* skabes hjemmel til automatiseret sagsbehandling – og hvor lovgiver til gengæld udtrykkeligt indbygger art. 22, stk. 3-garantierne: mulighed for at anmode om genoptagelse ved menneskelig indgriben og ret til at fremkomme med sine synspunkter.

Den store brik mangler dog stadig. Digitaliseringsstyrelsen sendte den 12. februar 2026 et [lovforslag om en generel hjemmel til udvikling og anvendelse af AI-systemer og behandling af personoplysninger i den offentlige forvaltning](#) i høring med frist 2. marts 2026. Indtil det vedtages, må hver myndighed fortsat finde sin egen hjemmel – og Datatilsynets doktrin er den gældende målestok.

LOV

[Bekendtgørelse om Arbejdstilsynets anvendelse af kunstig intelligens § 3](#)[Bekendtgørelse om kommunernes behandling af personoplysninger med kunstig intelligens eller lignende digitale løsninger i beskæftigelsesindsatsen § 1](#)[Databeskyttelsesforordningen § 22, stk. 1, 2](#)

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

§ 5 Træningsdata og modeller: er en AI-model personoplysninger?

Spørgsmålet om træningsdata og modellers retlige status blev afklaret i Datatilsynets udtalelse [j.nr. 2023-212-0021](#) af 19. januar 2024. Sagen udsprang af et tværkommunalt samarbejde (med Sønderborg Kommune), der udviklede sprogmodeller til at identificere fortrolige oplysninger i sagsakter ved besvarelse af **aktindsigtsanmodninger**. Datasættet var dannet ved dataskrab fra danske kommuners hjemmesider.

Datatilsynet nåede frem til tre principielle vurderinger.

Modellen er som udgangspunkt ikke personoplysninger:

Datatilsynet lægger til grund, at en AI-model som et klart udgangspunkt ikke i sig selv udgør personoplysninger, men alene er resultatet af behandlingen af personoplysninger. Det svarer til, at en statistisk rapport ligeledes ikke vil anses som personoplysninger, hvis rapporten alene indeholder konklusioner og aggregerede data, der er resultaterne af den statistiske analyse.

Og videre om memorisering og angreb:

Risikoen for, at en ondsindet aktør genidentificerer borgere ved bevidst at gennemføre et angreb for at udlede data, der har indgået i træningsdata, indebærer efter Datatilsynets opfattelse således ikke, at modellen skal anses som personoplysninger i sig selv.

Udvikling er et selvstændigt formål:

Udviklingen af en AI-løsning skal efter Datatilsynets opfattelse anses som et formål i sig selv i konteksten af databeskyttelsesreglerne. Behandling af personoplysninger med henblik på at udvikle nye teknologiske løsninger tjener i sagens natur et andet formål end behandling af personoplysninger som led i myndighedens daglige drift.

Det er en central pointe for formålsbegrænsningen i [art. 5, stk. 1, litra b](#): man kan ikke uden videre genbruge driftsdata til modeludvikling – det kræver sin egen formåls- og hjemmelsvurdering.

Produktionsdata kan være nødvendige – og fravalg kan i sig selv være usikkert:

Jo tættere du (som virksomhed eller som myndighed) kommer på produktionsfasen, jo mere velbegrundet kan det være, at du anvender (flere) produktionsdata – herunder personoplysninger. Nogle gange vil det endda være et udtryk for manglende sikkerhed at sætte et system i produktion uden at have testet med produktionsdata – herunder personoplysninger – først.

Datatilsynet har i en parallel udtalelse om **etablering og deling af datasæt** (januar 2024, Alexandra Instituttet) taget stilling til lydoptagelser og fastslået, at en stemme kan gøre en person identificerbar, netop fordi "den nuværende teknologi, herunder stemmegenkendelsesværktøjer og kunstig intelligens, gør det muligt at gennemføre analyser og identificering". Datasættet kunne udgøre **biometriske data**, men var ikke omfattet af forbuddet i [art. 9, stk. 1](#), fordi behandlingen ikke skete med det formål entydigt at identificere en fysisk person. Det er den samme sontring, Datatilsynet anvendte i [j.nr. 2023-431-0018](#) (IDA Forsikring), hvor AI-analyse af transskriberede telefonsamtaler ikke faldt under art. 9, stk. 1, fordi systemet ikke anvendte stemmegenkendende teknologi og ikke havde til formål at identificere den, der ringede.

Den skarpe grænse går ved **ikke-måltrettet indsamling af ansigtsbilleder**. I [j.nr. 2023-211-0004](#) afviste Datatilsynet webskrabning til opbygning af en biometrisk ansigtsgenkendelsesdatabase. Den praksis er nu kodificeret som en **forbudt AI-praksis** i [AI-forordningens artikel 5, stk. 1, litra e](#).

For højrisiko-AI stiller [AI-forordningens artikel 10](#) selvstændige krav til datastyring: datasæt skal være relevante, tilstrækkeligt repræsentative og i videst muligt omfang fejlfrie, og udbyderen skal undersøge og afbøde bias. [Artikel 10, stk. 5](#) indeholder en snæver, betinget hjemmel til undtagelsesvis at behandle **særlige kategorier af personoplysninger** – netop for at kunne påvise og korrigere bias – men kun når det er strengt nødvendigt, ikke kan opnås med syntetiske eller anonymiserede data, og under skrappe sikkerheds-, adgangs- og sletningsbetingelser.

Endelig et forbehold om data af tvivlsom oprindelse: i [j.nr. 2024-32-0482](#) fastslog Datatilsynet (efter forelæggelse for Datarådet), at rimelighedsprincippet i [art. 5, stk. 1, litra a](#) kræver en konkret vurdering af, **hvordan og af hvem** oplysningerne er tilvejebragt, over for de modsatrettede interesser. Myndigheden måtte i den sag godt anvende ulovligt optagne lydfiler, fordi den ikke selv havde medvirket til den ulovlige aflytning, og fordi hensynet til barnets tarv vejede tungest. Overført på AI: **oprindelsen af træningsdata er en selvstændig rimelighedsparameter – ikke kun et hjemmelsspørgsmål**. (Ophavsretligt er billedet et andet: Østre Landsret ophævede ved kendelse af 11. maj 2026 i sag **BS-55572/2025-OLR** et midlertidigt forbud mod scraping af data fra boligportal.dk, bl.a. under inddragelse af ophavsretslovens regler om tekst- og datamining.)

LOV

AI-forordningen § 5, stk. 1

AI-forordningen § 10, stk. 5

Databeskyttelsesforordningen § 5, stk. 1

Databeskyttelsesforordningen § 9, stk. 1

PRAKSIS	Datatilsynet · Helsingør Kommunes behandling af ulovligt tilvejebragte lydoptagelser i en børnesag	13.09.2024
	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
	Datatilsynet · Retningslinjer for offentliggørelse af træningsdatasæt og AI-modeller	19.01.2024

§ 6 Biometrisk AI: ansigtsgenkendelse mellem samtykke og tilladelse

Ansigtsgenkendelse er den AI-anvendelse, hvor Datatilsynet har den tætteste og mest konkrete praksis – og hvor koblingen til AI-forordningen er stærkest, fordi Datatilsynet er markedsovervågningsmyndighed for [artikel 5, stk. 1, litra g](#).

Udgangspunktet er, at behandling af ansigtsbilleder med henblik på entydig identifikation er behandling af biometriske data, jf. [art. 4, nr. 14](#), og dermed forbudt efter [art. 9, stk. 1](#), medmindre en undtagelse finder anvendelse. To spor findes i praksis:

Spor 1 – udtrykkeligt samtykke ([art. 9, stk. 2, litra a](#)). I [j.nr. 2023-31-0028](#) om ansigtsgenkendelse som adgangskontrol i fitnesscentre stillede Datatilsynet skarpe krav til frivilligheden:

I en situation som den foreliggende er det Datatilsynets opfattelse, at kravet om, at et samtykke skal være informeret, indebærer, at den registrerede skal oplyses om de alternativer, der er til samtykke til ansigtsgenkendelse.

Datatilsynet fandt, at adgang via reception i bemandet tid **ikke** var et reelt alternativ (det ville begrænse den 24/7-adgang, medlemmet betalte for), mens døgnsupport og engangskoder var det. Da klageren konkret var blevet fejlinformeret af en medarbejder, var hendes samtykke ugyldigt, og der blev udtalt kritik. Samtykket skal desuden **granuleres** – adgangskontrol og statistik kræver hvert sit samtykke. Det samme granuleringskrav slog igennem i [j.nr. 2023-431-0018](#), hvor IDA Forsikring kun indhentedes ét samlet samtykke til både dokumentations- og kvalitetssikringsformål:

Datatilsynet kan konstatere, at der i forbindelse med, at en person ringer til IDA forsikring, alene indhentes ét samlet samtykke til både dokumentations- og kvalitetssikringsformål (uddannelse). Vedkommende, som ringer, får således ikke mulighed for at vælge kun at samtykke til et af formålene.

Spor 2 – tilladelse efter [databeskyttelseslovens § 7, stk. 4](#). Private dataansvarlige kan få Datatilsynets tilladelse til at behandle følsomme oplysninger af hensyn til væsentlige samfundsinteresser, jf. [art. 9, stk. 2, litra g](#). Bestemmelsen har efter forarbejderne "karakter af en opsamlingsbestemmelse" og "forudsættes at have et snævert anvendelsesområde". Datatilsynets praksis afspejler netop den snæverhed:

Sag	Formål	Udfald
2024-51-0012 (18. december 2024)	Ansigtsgenkendelse i Parken mod karantæneramte tilskuere	Tilladelse til fodboldkampe – men afslag for "øvrige arrangementer" (koncerter m.v.), da behandlingen dér ikke stod i rimeligt forhold til formålet
2024-51-0014 (16. juli 2025)	Superligaklubbers ansigtsgenkendelse mod karantæneramte	Tilladelse, med vilkår om bl.a. oplysningspligt og behandlingssikkerhed

Danske Shoppingcentre (8. december 2022)	Biometrisk behandling uden hjemmel	Politianmeldelse
--	------------------------------------	------------------

FCK-sagen er den mest instruktive: tilladelsen blev **formålsopdelt**. Behandlingen kunne rummes inden for "væsentlige samfundsinteresser" i den kontekst (fodboldkampe, sikkerhed, karantænelister), men ikke automatisk overføres til enhver anden begivenhed på samme stadion. Proportionalitetsvurderingen er **kontekstbunden, ikke stedbunden**.

I ansættelsesforhold gælder en tredje hjemmel. I [j.nr. 2019-31-1650](#) accepterede Datatilsynet (efter behandling i Datarådet, med dissens) fingeraftryksbaseret adgangskontrol på et slagteri med hjemmel i [databeskyttelseslovens § 12, stk. 1](#) sammenholdt med DA/LO-aftalen om kontrolforanstaltninger, fordi entydig identifikation var nødvendig for at opfylde fødevarer sikkerheds- og certificeringskrav, og fordi der kun blev lagret krypterede templates – ikke billeder.

LOV	AI-forordningen § 5, stk. 1	Databeskyttelsesforordningen § 9, stk. 1, 2
	Databeskyttelsesloven § 7, stk. 4	Databeskyttelsesloven § 12, stk. 1
PRAKSIS	Datatilsynet · Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere 16.07.2025 Datatilsynet · F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken 18.12.2024 Datatilsynet · Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre 03.07.2024 Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne 27.06.2024 Datatilsynet · Politianmeldelse af Danske Shoppingcentre for ulovlig behandling af biometriske oplysninger 08.12.2022 Datatilsynet · Virksomheds brug af fingeraftryk til adgangskontrol fundet lovlig på baggrund af samtykke 08.07.2020	

§ 7 Transparens: oplysningspligt, indsigt og retten til at forstå "logikken"

Transparens er det område, hvor GDPR og AI-forordningen overlapper mest – og hvor de danske bekendtgørelser går videre end begge.

GDPR-sporet. Efter [art. 13, stk. 2, litra f](#) og [art. 15, stk. 1, litra h](#) skal den dataansvarlige oplyse om forekomsten af automatiske afgørelser og give "som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede". Betænkning nr. 1565/2017 forudså allerede spændingen med forretningshemmeligheder, jf. [s. 384](#):

Eksempelvis må det antages, at retten til indsigt efter artikel 22 i selve logikken bag en virksomheds afslag på kredit vil kunne begrænses efter eksempelvis forordningens artikel 23, stk. 1, litra i, om beskyttelse af andres rettigheder og frihedsrettigheder af hensyn til virksomhedens forretningshemmeligheder.

EU-Domstolen har nu afgjort, hvordan den afvejning skal foretages. I [C-203/22](#) (Dun & Bradstreet Austria, 27. februar 2025) fastslog Domstolen, at "meningsfulde oplysninger om logikken" kræver en **kortfattet, gennemsigtig og forståelig** beskrivelse af den procedure og de principper, der **konkret** er anvendt, så den registrerede kan forstå, hvilke af vedkommendes personoplysninger der er indgået, og hvordan de er blevet brugt. Udlægning af selve algoritmen eller den fulde matematiske formel er hverken tilstrækkeligt (det er ikke forståeligt) eller påkrævet. Påberåber den dataansvarlige sig forretningshemmeligheder, kan vedkommende

ikke blot afvise indsigt: oplysningerne skal forelægges **tilsynsmyndigheden eller domstolen**, som herefter afvejer de modstående interesser. Sammenholdt med [C-634/21](#) betyder det, at scoringsleverandøren både er ansvarssubjekt for "afgørelsen" og forklaringspligtig for logikken.

Datatilsynets nationale praksis om oplysningspligt er streng, også når AI ikke er indblandet: se [j.nr. 2022-431-0204](#) (Tryk Forsikring, art. 13-14) og [j.nr. 2019-421-0028](#) (kritik af Udbetaling Danmarks håndtering af indsigtsretten). I [j.nr. 2023-431-0018](#) fandt Datatilsynet omvendt IDA Forsikrings information om AI-transskribering og -analyse tilstrækkelig – det indledende speak og persondatapolitikken opfyldte i det væsentlige art. 13.

Den danske skærpelse. [Bekendtgørelsen om kommunernes AI-brug i beskæftigelsesindsatsen § 2, stk. 4](#) kræver, at det "tydeligt fremgår for den, hvis personoplysninger behandles, når kunstig intelligens anvendes". [Vejledningen](#) er utvetydig om, at der er tale om en **selvstændig, skærpet pligt**:

Oplysningspligten efter bekendtgørelsens § 2, stk. 4, 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.

Vejledningen accepterer, at pligten kan opfyldes fleksibelt – fx ved henvisning til en privatlivspolitik eller ved en oplysning i sagsbehandlerens autosignatur.

AI-forordningens spor. [Artikel 26, stk. 11](#) pålægger idriftsættere af bilag III-højrisikosystemer, der træffer eller bistår med at træffe beslutninger om fysiske personer, at underrette de pågældende om, at de er genstand for systemet. Og [artikel 86](#) giver en **selvstændig ret til forklaring**:

Enhver berørt person, der er omfattet af en afgørelse truffet af idriftsætteren på grundlag af output fra et højrisiko-AI-system opført i bilag III [...] og som har retsvirkninger eller på tilsvarende måde i væsentlig grad påvirker den pågældende person [...] har ret til at få en klar og meningsfuld forklaring fra idriftsætteren om AI-systemets rolle i beslutningsprocessen og hovedelementerne i den trufne afgørelse.

Retten er subsidiær: den finder efter [art. 86, stk. 3](#) kun anvendelse, "for så vidt den [...] omhandlede ret ikke på anden vis er fastsat i EU-retten" – dvs. den udfylder hullerne, hvor GDPR art. 15 ikke rækker (typisk fordi afgørelsen *ikke* er fuldautomatisk og derfor falder uden for art. 22).

LOV	AI-forordningen § 26, stk. 11	AI-forordningen § 86, stk. 1, 3
	Databeskyttelsesforordningen § 13, stk. 2	Databeskyttelsesforordningen § 15, stk. 1
	Databeskyttelsesforordningen § 23, stk. 1	
PRAKSIS	EU-Domstolen · Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	27.02.2025
	EU-Domstolen · Automatisk kredit scoring som en individuel afgørelse efter GDPR	07.12.2023
	Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	27.06.2024
	Datatilsynet · Tryk Forsikrings overholdelse af oplysningspligten ved behandling af personoplysninger	02.01.2024
	Datatilsynet · Kritik af Udbetaling Danmarks håndtering af de registreredes ret til indsigt	26.02.2020

Konsekvensanalyse og risikostyring: DPIA, FRIA og det dobbelte spor

Brug af AI til behandling af personoplysninger vil ofte udløse pligt til **konsekvensanalyse** efter [GDPR artikel 35, stk. 1](#). Det er ikke en formalitet. [Vejledningen om digitaliseringsklar lovgivning](#) fremhæver eksplicit AI som en udløsende faktor:

Dette er navnligt tilfældet ved anvendelse af ny teknologi, fx brug af biometriske data, herunder iris-scanning, eller af kunstig intelligens, der skal behandle følsomme oplysninger, eksempelvis helbredsoplysninger.

Datatilsynets AULA-tilsyn viser, hvor hårdt tilsynet slår ned på mangelfulde konsekvensanalyser. I [j.nr. 2023-423-0005](#) udtalte Datatilsynet kritik af Københavns Kommune:

Det er imidlertid Datatilsynets vurdering, at Københavns Kommune ikke har gennemført en fyldestgørende konsekvensanalyse, jf. databeskyttelsesforordningens artikel 35, stk. 1, idet den fremsendte konsekvensanalyse ikke opfylder mindstekravene hertil i forordningens artikel 35, stk. 7, litra a-d.

Analysen manglede en vurdering af nødvendighed og proportionalitet, beskrivelsen af formål, retligt grundlag og datakategorier var utilstrækkelig, og der var ingen entydig sammenhæng mellem konsekvensanalysen og de bagvedliggende risikovurderingsskemaer. Af de seks kommuner i tilsynsrunden fik **samtlig**e kritik eller alvorlig kritik på konsekvensanalysedelen, og to fik påbud om at udarbejde en analyse inden for tre måneder.

Datatilsynet har efterfølgende udgivet en dedikeret **skabelon til konsekvensanalyse ved AI-løsninger**, som tilsynet selv henviste til i SU-sagen [j.nr. 2024-212-0371](#), og som supplerer tilsynets vejledninger "Brug af kunstig intelligens i den offentlige sektor" og "Offentlige myndigheders brug af kunstig intelligens – Inden I går i gang" (begge oktober 2023).

Hertil kommer AI-forordningens **konsekvensanalyse vedrørende grundlæggende rettigheder** (FRIA) i [artikel 27](#), som offentligretlige organer og private, der leverer offentlige tjenester, skal foretage før idriftsættelse af bilag III-højrisikosystemer. De to analyser er **komplementære, ikke alternative** – art. 27, stk. 4 fastslår, at FRIA'en "supplerer" en DPIA foretaget efter GDPR art. 35, og [art. 26, stk. 9](#) pålægger omvendt idriftsætteren at bruge udbyderens oplysninger efter art. 13 til at opfylde sin DPIA-forpligtelse.

En særligt vigtig klassifikationsregel: efter [AI-forordningens artikel 6, stk. 3](#) kan et bilag III-system undtagelsesvis falde ud af højrisikokategorien, hvis det kun udfører en snæver proceduremæssig eller forberedende opgave – **men**:

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

De danske bekendtgørelser tillader netop profilering til sagsunderstøttelse. Kommuner og styrelser, der udnytter den hjemmel på et bilag III-område, vil derfor som udgangspunkt være idriftsættere af et **højrisiko**-AI-system fra 2. august 2026 – med de dertil hørende pligter om menneskeligt tilsyn ([art. 26, stk. 2](#)), inputdatakvalitet, logopbevaring i mindst seks måneder og registrering i EU-databasen.

Størrelsesordenen er ikke trivial: Skatteforvaltningen oplyste i [april 2025](#), at den anvender 29 AI-modeller i kontrolarbejdet.

LOV

[AI-forordningen § 6, stk. 3](#)[AI-forordningen § 26, stk. 2, 9](#)[AI-forordningen § 27](#)[Databeskyttelsesforordningen § 35, stk. 1, 7](#)

PRAKSIS

Datatilsynet · Kritik af Udlændinge- og Integrationsministeriets behandling af personoplysninger i Visuminformationssystemet (VIS)	10.07.2024
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

§ 9 Den private sektor: profilering, scoring og samtykkets grænser

I den private sektor er behandlingsgrundlaget et andet – men fejlene er de samme.

Forkert behandlingsgrundlag ved profilering. I [j.nr. 2019-32-0709](#) udtalte Datatilsynet **alvorlig kritik** af en privat virksomhed for at have anvendt et forkert behandlingsgrundlag ved profilering, med inddragelse af [art. 5, stk. 1](#), [art. 6, stk. 1](#) og [art. 13](#). Pointen generaliserer: en virksomhed kan ikke først vælge teknologien og bagefter lede efter en hjemmel.

AI-analyse er ikke nødvendigvis et nyt formål. I [j.nr. 2023-431-0018](#) (IDA Forsikring) blev telefonsamtaler optaget, transskriberet af en talegenkender og analyseret af AI-modeller for temaer, opkaldsårsager og indikative kvalitetsscoringer. Datatilsynet fastslog:

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.

Selskabet kunne altså godt optage og AI-analysere samtalerne – men **samtykkeprocessen** holdt ikke, fordi der kun blev indhentet ét samlet samtykke til to formål. Datatilsynet pålagde selskabet fremadrettet at rette op, fx ved at kræve "to tryk" for at opnå den nødvendige granularitet, eller ved at basere optagelsen på et andet grundlag end samtykke.

Bemærk kontrasten til AI-udvikling i det offentlige: i [j.nr. 2023-212-0021](#) er *udvikling* af en model et selvstændigt formål, mens *analyse* som led i den løbende kvalitetssikring i IDA-sagen ikke var det. Sondringen er: **træner du en model, forfølger du et nyt formål; anvender du en model på data, du allerede lovligt behandler til et givet formål, gør du det typisk ikke.**

Samtykke og kontrakt som art. 22-undtagelser. Betænkning nr. 1565/2017 gennemgår på [s. 374-375](#) undtagelserne i [art. 22, stk. 2, litra a og c](#) og fremhæver, at nødvendighedskravet ved kontraktundtagelsen kan rumme ressourcemæssige hensyn – men **kun** hvis art. 22, stk. 3-garantierne er på plads. Betænkningen fastslår på [s. 380](#), at et samtykke efter litra c ikke er nok i sig selv: den dataansvarlige har samtidig ansvaret for at gennemføre passende foranstaltninger – **som minimum ret til menneskelig indgriben, til at fremkomme med synspunkter og til at bestride afgørelsen.**

Erstatning. Endelig har EU-Domstolen i [C-590/22](#) (20. juni 2024) præciseret rammerne for erstatningskrav efter [art. 82](#): en overtrædelse giver ikke i sig selv erstatning – der kræves skade og årsagssammenhæng – men skaden behøver ikke have en vis alvorsgrad, og erstatningen er rent **kompenserende**, ikke afskrækkende:

Den ret til erstatning, der er fastsat i databeskyttelsesforordningens artikel 82, stk. 1, har ikke en afskrækkende eller ligefrem straffende funktion. Erstatningsbeløbet kan således ikke fastsættes på et niveau, der overstiger fuld erstatning for denne skade.

For AI-leverandører betyder det, at den økonomiske risiko primært ligger i bøder og tilsynsindgreb – ikke i civile massekrav med pønalt præg.

LOV	Databeskyttelsesforordningen § 6, stk. 1	Databeskyttelsesforordningen § 22, stk. 2, 3
	Databeskyttelsesforordningen § 82, stk. 1	
PRAKSIS	EU-Domstolen · Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	20.06.2024
	Datatilsynet · IDA Forsikrings brug af AI til analyse af telefonsamtaler findes i overensstemmelse med databeskyttelsesreglerne	27.06.2024
	Datatilsynet · Retningslinjer for offentliggørelse af træningsdatasæt og AI-modeller	19.01.2024
	Datatilsynet · Alvorlig kritik af privat virksomhed for anvendelse af forkert behandlingsgrundlag ved profilering	03.11.2020

§ 10 Forvaltningsretten oven på databeskyttelsen: ombudsmandens praksis om automatiserede sagsskridt

Databeskyttelsesretten regulerer *behandlingen* af oplysninger. Forvaltningsretten regulerer *afgørelsen*. En offentlig AI-løsning skal bestå begge prøver – og Folketingets Ombudsmand har i en lang række sager slået fast, at de forvaltningsretlige krav ikke fraviges, fordi sagsbehandlingen digitaliseres.

Allerede i [FOB 2014-34](#) rejste ombudsmanden problemstillingen generelt over for Finansministeriet, og Digitaliseringsstyrelsen og Justitsministeriet erklærede sig enige:

Grundlæggende forvaltningsretlige regler og principper skal naturligvis iagttages af offentlige myndigheder. Dette gælder uanset, om forvaltningen varetages manuelt eller digitalt. Reglerne om blandt andet partshøring, begrundelse af afgørelser, klagevejledning, vejledningspligt, notatpligt, parterets ret til aktindsigt, offentlige myndigheders tavshedspligt mv. fraviges således ikke, når forvaltningen digitaliseres.

I [FOB 2023-3](#) formuleredes kravet skarpt: det er "et grundlæggende krav, at offentlige it-systemer kan understøtte en korrekt anvendelse af den relevante lovgivning" – både formelle regler (partshøring, begrundelse) og materielle regler (udøvelse af skøn i den enkelte sag). Ansvar ligger hos myndigheden, **uanset om systemet er leveret af en ekstern leverandør**.

Den mest direkte AI-relevante udtalelse er [FOB 2026-6](#) om Skatteforvaltningens automatiserede SMV-løsning (marts 2026), hvor ombudsmanden formulerer automatiseringens strukturelle risiko:

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.

Og om datakvalitet – direkte overførbart på AI-modellers inputdata:

Med automatiseringen vil systemet samtidig være direkte afhængigt af, at eksempelvis den underliggende sagsoplysning – systemets inddata – er tilstrækkelig og af den fornødne kvalitet.

Ombudsmanden fremhæver samme sted, at myndigheden må overveje, **om regelgrundlaget overhovedet understøtter den påtænkte automatisering**, idet "automatisering forudsætter bl.a., at de pågældende sagsskridt kan foretages uden udøvelse af et individuelt skøn og efter rent objektive kriterier". Det er den forvaltningsretlige pendant til Datatilsynets hjemmelskrav – og præcis den erkendelse, der ligger bag hjemmelsbølgen beskrevet ovenfor.

Hvad der sker, når automatiseringen fejler, viser [FOB 2025-13](#) om Vurderingsstyrelsens robotløsning, hvor samspillet mellem tilbagebetalingssystemet, administrationsgrundlaget og robotens automatiske sagsskridt "ikke fungerede efter hensigten". Og [FOB 2022-11](#) understreger, at ansvars- og rollefordelingen skal afklares, når flere systemer og myndigheder indgår i kæden frem mod en afgørelse – en pointe med stor vægt i AI-værdikæder med eksterne modelleverandører og databehandlere.

Underskriftskravet. Forvaltningsretten er dog ikke blind for automatisering: efter **forvaltningslovens § 32 b, stk. 2** gælder kravet om personlig underskrift ikke for dokumenter, hvor der anvendes automatisk sagsbehandling – dvs. "sagsbehandlingssystemer, der indebærer, at en sag helt eller delvist behandles og afgøres maskinelt på baggrund af faste og entydige kriterier, uden at en fysisk person sagsbehandler", jf. [vejledningen om digitaliseringsklar lovgivning](#).

Diskriminationsrisikoen. Automatiserede processer kan i sig selv være diskriminerende.

Ligebehandlingsnævnet fandt i [sag 21-9890](#), at en kommunes faste, it-understøttede praksis med automatisk at registrere **moderen** som "sagsperson" og betaler for institutionsplads – begrundet i, at børneydelsen typisk udbetales til mødre, og i systemets begrænsninger – udgjorde ulovlig forskelsbehandling på grund af køn. Afgørelsen illustrerer præcis den risiko, [AI-forordningens artikel 10, stk. 2, litra f](#) adresserer: bias, der "føre[r] til forskelsbehandling, som er forbudt i henhold til EU-retten".

Endelig har **Dataetisk Råd** i sit høringssvar til CBAM-lovforslaget ([L 17, 2024-25](#)) formuleret den principielle bekymring ved brede bemyndigelser til automatiseret sagsbehandling: at delegationen "reducerer den parlamentariske kontrol og offentlighedens indsigt", og at der mangler "klarhed om håndtering af klager og indsigt i afgørelsesgrundlaget". Rådet anbefalede klare rammer for åbenhed om algoritmerne og for prøvelse af automatisk trufne afgørelser.

LOV	AI-forordningen § 10, stk. 2	Databeskyttelsesforordningen § 22, stk. 1
PRAKSIS	Ligebehandlingsnævnet · Kommunal praksis med automatisk valg af moderen som betaler for institutionsplads var kønsdiskriminerende	
		12. 11. 2022

§ 11 Håndhævelse og sanktioner: bøder efter to spor

Sanktionerne løber i to parallelle spor, og de kan ramme samme adfærd.

Databeskyttelsessporet. Danmark har ikke administrative bøder efter [GDPR artikel 83](#); i stedet politianmelder Datatilsynet og indstiller til bøde, jf. [databeskyttelseslovens § 41](#). Datatilsynet har gjort netop det på det biometriske område – se [politianmeldelsen af Danske Shoppingcentre](#) (december 2022) for ulovlig behandling af biometriske oplysninger.

Anklagemyndighedens behandling er detaljeret reguleret i [Rigsadvokatmeddelelsen, afsnittet om Databeskyttelse – Straffesager](#). Retningslinjerne indebærer bl.a., at **Datatilsynet skal høres i alle sager, inden der træffes afgørelse om tiltaleespørgsmålet**, at tiltaleespørgsmålet og strafpåstanden skal forelægges

statsadvokaten, og at sagerne indtil videre **ikke må afgøres med bødeforelæg**, før sanktionsniveauet er tilstrækkeligt afklaret i retspraksis. Rigsadvokatmeddelelsen fastslår også, at bødeniveauet er markant hævet i forhold til persondataloven:

Reglerne i databeskyttelsesforordningen og databeskyttelsesloven lægger således op til en markant forøgelse af bødeniveauet i forhold til, hvad overtrædelser af persondataloven blev takseret til. Tidligere retspraksis kan derfor kun i meget begrænset omfang tillægges betydning ved afgørelse af sanktionsspørgsmålet efter de nuværende regler, mens såvel doms- som administrativ praksis fra andre EU-lande fremadrettet vil få øget betydning.

De momenter, der efter [art. 83, stk. 2](#) skal indgå i sanktionsvurderingen, gælder også ved bødeudmåling efter databeskyttelseslovens § 41, jf. lovens § 41, stk. 3.

AI-sporet. [AI-forordningens artikel 99, stk. 3](#) fastsætter for overtrædelse af de forbudte AI-praksisser i art. 5 administrative bøder på op til **35 mio. EUR eller 7 % af den samlede globale årlige omsætning** – det højeste beløb i hele EU's digitale regelværk. Danmark har valgt at sanktionere **strafferetligt**. Efter [AI-lovens § 10](#) straffes med bøde den, der bl.a. overtræder [artikel 5, stk. 1, litra a-g](#), afgiver urigtige oplysninger til myndighederne, hindrer kontrolbesøg eller undlader at efterkomme påbud eller midlertidige forbud. Der kan pålægges selskaber strafansvar efter straffelovens 5. kapitel, og **forældelsesfristen er 5 år**. Efter [§ 11](#) kan der fastsættes regler om bødeforelæg.

Af forarbejderne fremgår begrundelsen for valget:

Det er Digitaliseringsministeriets vurdering, 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.

Markedsovervågningsmyndighederne kan desuden kræve alle nødvendige oplysninger, få adgang til erhvervsmæssige lokaliteter **uden retskendelse**, udstede påbud, nedlægge midlertidige forbud mod et AI-system, der vurderes at kunne udgøre en risiko, og offentliggøre afgørelser i sager om forbudte former for AI-praksis.

Ikke-sanktionerede indgreb. I langt de fleste af Datatilsynets AI-sager er reaktionen dog en udtalelse, kritik eller alvorlig kritik – ikke bøde. Det gælder fx [j.nr. 2023-421-0015](#) (kritik af Udlændinge- og Integrationsministeriets behandling i Visuminformationssystemet efter art. 5, stk. 1, og art. 24, stk. 1) og AULA-sagerne. Praksis er med andre ord **vejledende og opdragende** snarere end pønål – indtil videre.

LOV

[AI-forordningen § 99, stk. 3](#)
[Databeskyttelsesforordningen § 83, stk. 2](#)
[Databeskyttelsesloven § 41](#)
[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 10](#)
[Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 11](#)

PRAKSIS

- Datatilsynet** · Kritik af Udlændinge- og Integrationsministeriets behandling af personoplysninger i Visuminformationssystemet (VIS) 10.07.2024
- Datatilsynet** · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA 23.05.2024
- Datatilsynet** · Politianmeldelse af Danske Shoppingcentre for ulovlig behandling af biometriske oplysninger 08.12.2022

§ 12 Sammenfatning: den danske AI-databeskyttelsesmodel i seks træk

Praksis tegner nu et forholdsvis klart billede, som kan sammenfattes i seks træk.

1. Hjemmelsdoktrinen er den styrende norm. Datatilsynets udtalelse i [j.nr. 2023-212-0015](#) – udvikling ja, drift kun med klart nationalt retsgrundlag, med et klarhedskrav der skærpes med indgrebets intensitet – er blevet den centrale målestok. Den er gengivet ordret i forarbejderne til flere lovforslag og har fremtvunget en hel serie af hjemmelsbekendtgørelser.

2. Danmark har (endnu) ikke udnyttet art. 22-råderummet på de store velfærdsområder. [Art. 22, stk. 2, litra b](#) tillader fuldautomatiske afgørelser med hjemmel i national ret og passende garantier. Men [bekendtgørelsen om kommunernes AI-brug i beskæftigelsesindsatsen § 1, stk. 6](#) forbyder dem udtrykkeligt. AI er sagsUNDERSTØTTENDE – mennesket træffer afgørelsen. Kun på afgrænsede, objektivt regulerede områder (fx tilskudsadministration) har lovgiver skabt hjemmel til egentlig automatiseret sagsbehandling.

3. "Reel menneskelig involvering" er det kritiske skøn. Fordi den danske model bygger på beslutningsstøtte, flytter det retlige tyngdepunkt sig til spørgsmålet om, hvornår sagsbehandlerens involvering er **faktisk og reel** – og ikke bare et gummistempel på modellens output. Her giver [C-634/21](#) et advarselssignal: hvis modellens score i praksis er determinerende, er der tale om en afgørelse i art. 22's forstand – uanset hvem der formelt trykker på knappen.

4. Transparens er skærpet, ikke lempet. [C-203/22](#) kræver en forståelig forklaring af den konkret anvendte logik, og forretningshemmeligheder giver ikke ret til tavshed, men til en afvejning ved tilsynsmyndighed eller domstol. Nationalt kræver AI-bekendtgørelserne, at det **tydeligt fremgår**, når AI anvendes – en pligt, der udtrykkeligt går videre end GDPR art. 13-14. Og fra 2. august 2026 supplerer [AI-forordningens artikel 86](#) med en ret til forklaring, netop hvor GDPR art. 22 ikke rækker.

5. Biometri er den skarpeste grænse. Ansigtsgenkendelse kræver enten et gyldigt, granuleret og reelt frivilligt samtykke ([j.nr. 2023-31-0028](#)) eller en snæver, formålsbestemt tilladelse efter [databeskyttelseslovens § 7, stk. 4](#) ([j.nr. 2024-51-0012](#) og [j.nr. 2024-51-0014](#)). Og ikke-måltrettet webskrabning til ansigtsgenkendelsesdatabaser er nu **forbudt** AI-praksis – Datatilsynet nåede dertil allerede i [j.nr. 2023-211-0004](#), før AI-forordningen fik virkning.

6. Forvaltningsretten er den anden halvdel af regnestykket. Ombudsmandens praksis – [FOB 2026-6](#), [FOB 2025-13](#), [FOB 2023-3](#) og [FOB 2014-34](#) – kræver, at officialprincip, partshøring, begrundelse og notatpligt tænkes ind fra systemudviklingens første fase, og at myndigheden erkender automatiseringens blinde vinkel over for atypiske sager. En AI-løsning kan være databeskyttelsesretligt upåklagelig og alligevel forvaltningsretligt uholdbar.

Det åbne spørgsmål er, om Danmark får den generelle hjemmel, som Digitaliseringsstyrelsen sendte i høring den [12. februar 2026](#) – og hvor langt den i givet fald går. Så længe den mangler, forbliver Datatilsynets doktrin fra november 2023 den afgørende adgangsbillet til AI i den offentlige forvaltning.

LOV

[AI-forordningen § 86](#)

Bekendtgørelse om kommunernes behandling af personoplysninger med kunstig intelligens eller lignende digitale løsninger i beskæftigelsesindsatsen § 1, stk. 6

[Databeskyttelsesforordningen § 22, stk. 2](#)
[Databeskyttelsesloven § 7, stk. 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 · Automatisk kredit scoring som en individuel afgørelse efter GDPR

07.12.2023

Datatilsynet · Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere	16.07.2025
Datatilsynet · F.C. København får tilladelse til brug af automatisk ansigtsgenkendelse ved indgange til Parken	18.12.2024
Datatilsynet · Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	03.07.2024
Datatilsynet · Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse	30.01.2024
Datatilsynet · Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	17.11.2023

REFERENCE

Lovgrundlag

10 paragraffer

AI-forordningen § 5	stk. 1	AI-forordningen § 26	stk. 11
AI-forordningen § 86	stk. 1	Databeskyttelsesforordningen § 6	stk. 1
Databeskyttelsesforordningen § 9	stk. 2	Databeskyttelsesforordningen § 15	stk. 1
Databeskyttelsesforordningen § 22	stk. 1-3	Databeskyttelsesforordningen § 35	stk. 1
Databeskyttelsesloven § 7	stk. 4	Lov om supplerende bestemmelser til forordningen om kunstig intelligens § 2	

MATERIALE

Citerede afgørelser

23 afgørelser

EU-DOMSTOLEN · EUROPÆISK DOMSTOL		4
27.02.2025	Indsigtsret i kreditvurderings-scoring: Krav til forklaring af logikken bag automatiske afgørelser og afvejning mod forretningshemmeligheder	C-203/22
20.06.2024	Erstatning for immateriel skade under GDPR: Retten til kompensation for frygt for datamisbrug og afvisning af alvorsgrad som betingelse	C-590/22
07.12.2023	Automatisk kredit scoring som en individuel afgørelse efter GDPR	C-634/21
07.12.2023	Grænser for kreditoplysningsbureauers datalagring og fuld domstolsprøvelse af tilsynsmyndigheders afgørelser	C-26/22
DATATILSYNET · NÆVN / KLAGEINSTANS		18
09.10.2025	Lovlighed af sektionskontrol og automatisk hastighedsmåling på Storebæltsbroen	2025-31-1798
16.07.2025	Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere	2024-51-0014
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
10.07.2024	Kritik af Udlændinge- og Integrationsministeriets behandling af personoplysninger i Visuminformationssystemet (VIS)	2023-421-0015

03.07.2024	Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	2023-31-0028
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
19.01.2024	Retningslinjer for offentliggørelse af træningsdatasæt og AI-modeller	2023-212-0021
02.01.2024	Tryk Forsikrings overholdelse af oplysningspligten ved behandling af personoplysninger	2022-431-0204
17.11.2023	Udtalelse om lovligt behandlingsgrundlag for AI-løsninger i den kommunale sundheds- og omsorgssektor	2023-212-0015
08.12.2022	Politianmeldelse af Danske Shoppingcentre for ulovlig behandling af biometriske oplysninger	
18.05.2022	Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	2022-212-3676
03.11.2020	Alvorlig kritik af privat virksomhed for anvendelse af forkert behandlingsgrundlag ved profilering	2019-32-0709
08.07.2020	Virksomheds brug af fingeraftryk til adgangskontrol fundet lovlig på baggrund af samtykke	2019-31-1650
26.02.2020	Kritik af Udbetaling Danmarks håndtering af de registreredes ret til indsigt	2019-421-0028
LIGEBEHANDLINGSNÆVNET · NÆVN / KLAGEINSTANS		1
12.11.2022	Kommunal praksis med automatisk valg af moderen som betaler for institutionsplads var kønsdiskriminerende	21-9890

FORARBEJDE Betænkninger

2 referencer

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 1)

nr. 1565 · 2017 · Justitsministeriet

Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning (Betænkning nr. 1565, Del I – bind 2)

nr. 1565 · 2017 · Justitsministeriet