

PRAKSISOVERSIGT · GDPR & COMPLIANCE-DOKUMENTER

Konsekvensanalyse (DPIA)

Databeskyttelseskonsekvensanalyse efter GDPR art. 35 – hvornår pligten udløses, mindstekravene til indholdet og forhåndshøring af Datatilsynet efter art. 36

Version 1 Opdateret 21. jul. 2026 14 afgørelser · 2020-2025

[Læs online](#)

INTRODUKTION

En **konsekvensanalyse vedrørende databeskyttelse** (DPIA – *Data Protection Impact Assessment*) er en struktureret, skriftlig forhandsanalyse af, hvad en planlagt behandling af personoplysninger gør ved menneskers rettigheder, og hvad man konkret gør for at nedbringe risikoen. Den er hverken en it-sikkerhedsrapport, en fortegnelse over behandlingsaktiviteter eller en privatlivspolitik: den er den proces, hvor man – inden systemet tændes – beskriver behandlingen, prøver nødvendigheden, sætter tal og ord på risikoen for de registrerede og beslutter, hvilke foranstaltninger der skal bygges ind.

Parterne er få og deres roller er skarpt fordelt. **Den dataansvarlige** ejer analysen, træffer beslutningerne og bærer ansvaret – pligten kan ikke outsources til leverandøren. **Databeskyttelsesrådgiveren (DPO)** skal rådføres og rådgive, men overtager ikke ansvaret. **Databehandleren/leverandøren** skal bistå med oplysninger og dokumentation. **Datatilsynet** er modtager, hvis restrisikoen fortsat er høj – så skal tilsynet høres, før behandlingen starter. Og **de registrerede** (eller deres repræsentanter, fx tillidsrepræsentanter) skal efter omstændighederne høres om den planlagte behandling.

Oversigten er ordnet efter dokumentets naturlige livscyklus: først hvornår pligten udløses (og hvornår den ikke gør), dernæst checklisten over det obligatoriske indhold med hjemmel punkt for punkt, så de typiske fejl med deres konsekvenser – og til sidst uddybende afsnit om tærskelvurderingen, rollefordelingen, metoden frem mod forhåndshøring, håndhævelsen i dansk praksis og samspillet med AI-forordningens konsekvensanalyse for grundlæggende rettigheder.

PRINCIPPER UDLEDT AF PRAKSIS

- 01** DPIA er en **betinget** pligt, der udløses af behandlingens risikoprofil – ikke af virksomhedens størrelse. En lille klinik med biometrisk adgangskontrol kan have pligten, mens en stor koncern med almindelig lønadministration ikke har den.
- 02** Tre behandlingstyper er altid omfattet (profilering med retsvirkning, følsomme oplysninger i stort omfang og systematisk overvågning af offentligt tilgængeligt område), jf. art. 35, stk. 3 – suppleret af Datatilsynets offentliggjorte liste efter art. 35, stk. 4.
- 03** Analysen skal være **færdig, før behandlingen påbegyndes**. Datatilsynet har både politianmeldt og nedlagt forbud, hvor en konsekvensanalyse først blev færdiggjort efter, at behandlingen var sat i gang.

- 04** Art. 35, stk. 7, opstiller fire ufravigelige mindstekrav – beskrivelse, nødvendigheds- og proportionalitetsvurdering, risikovurdering og afhjælpende foranstaltninger. En it-sikkerhedsrisikovurdering efter art. 32 er ikke i sig selv en konsekvensanalyse.
- 05** Databeskyttelsesrådgiveren **skal** rådføres, når der laves DPIA (art. 35, stk. 2), og rådgivningen indgår i DPO'ens lovbestemte opgaver efter art. 39, stk. 1, litra c – men ansvaret bliver hos den dataansvarlige.
- 06** Er restrisikoen fortsat høj efter de planlagte foranstaltninger, er behandlingen **spærret**, indtil Datatilsynet er hørt efter art. 36 – høringen er en retssikkerhedsgaranti, ikke en godkendelsesstempling.
- 07** Manglende eller mangelfuld DPIA er strafbelagt i Danmark efter [databeskyttelseslovens § 41, stk. 1, nr. 1](#) (bøde eller fængsel indtil 6 måneder), og ligger i GDPR's høje bødeleje på 10 mio. EUR eller 2 % af global omsætning.
- 08** Én analyse kan dække flere lignende behandlinger – Datatilsynet har fx opfordret kommunerne til at udarbejde en **fælles** konsekvensanalyse for AULA i stedet for 98 enkeltstående.

§ 1 Hvornår er dokumentet påkrævet?

Betinget lovpligt – risikoen udløser pligten. En DPIA skal foretages, når en type behandling "sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder", jf. [databeskyttelsesforordningens artikel 35, stk. 1](#). Pligten er altså hverken knyttet til virksomhedens størrelse, omsætning eller antal ansatte, men til behandlingens **karakter, omfang, sammenhæng og formål** – navnlig ved brug af nye teknologier. Analysen skal foreligge **forud for behandlingen**; en enkelt analyse kan dække flere lignende behandlingsaktiviteter med lignende høje risici.

Altid – de tre formodningstilfælde i stk. 3. DPIA er navnlig påkrævet ved (a) systematisk og omfattende vurdering af personlige forhold baseret på automatisk behandling, herunder profilering, som er grundlag for afgørelser med retsvirkning eller tilsvarende betydelig påvirkning, (b) behandling i stort omfang af særlige kategorier af oplysninger efter [artikel 9](#) eller af oplysninger om straffedomme og lovovertrædelser, og (c) systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Datatilsynets lister. Tilsynsmyndigheden udarbejder og offentliggør efter artikel 35, stk. 4, en liste over behandlingstyper, hvor DPIA altid kræves – Datatilsynet henviser selv til denne liste i sin vejledning. Efter stk. 5 kan der tilsvarende offentliggøres en liste over behandlinger, hvor DPIA ikke kræves. Præambelbetragtning 91 til forordningen peger på de typiske udlødere: omfattende behandling af meget store datamængder, omfattende brug af ny teknologi, profileringsbaserede afgørelser, biometriske og genetiske data, oplysninger om straffedomme samt omfattende overvågning af offentligt tilgængelige områder.

Særligt om høj restrisiko. Viser analysen, at behandlingen fortsat vil føre til høj risiko *i mangel af* foranstaltninger, der begrænser risikoen, må behandlingen ikke sættes i gang: den dataansvarlige skal først høre Datatilsynet efter [artikel 36, stk. 1](#). Tilsynet har op til otte uger – der kan forlænges med seks uger ved kompleks behandling – til at give skriftlig rådgivning og kan undervejs bruge alle sine beføjelser.

Politi, anklagemyndighed og kriminalforsorg. Uden for GDPR's område gælder en parallel – og på ét punkt strengere – ordning: [retshåndhævelseslovens § 25](#) kræver konsekvensanalyse ved høj risiko, og [§ 26](#) kræver

forudgående høring af tilsynsmyndigheden inden behandling i **nye registre**, både når analysen viser høj restrisiko, og når behandlingstypen i sig selv indebærer høj risiko ved brug af nye teknologier, mekanismer eller procedurer.

Undtagelsen for lovregulerede behandlinger. Har en behandling efter artikel 6, stk. 1, litra c eller e, hjemmel i EU-ret eller national ret, som regulerer netop de pågældende behandlingsaktiviteter, og er der allerede foretaget en generel konsekvensanalyse i forbindelse med vedtagelsen af retsgrundlaget, finder artikel 35, stk. 1-7, ikke anvendelse (artikel 35, stk. 10). I dansk lovgivningspraksis kan analysen efter Justitsministeriets *Vejledning om lov kvalitet* foretages i forbindelse med udformningen af et lovforslag eller en bekendtgørelse – men undtagelsen forudsætter, at analysen faktisk er lavet.

Frivilligt, men retssikrende. Er man i tvivl, er den dokumenterede **tærskelvurdering** (screening) den billige forsikring: ansvarlighedsprincippet i [artikel 5, stk. 2](#) kræver, at man kan *påvise* sine overvejelser – også når konklusionen blev, at DPIA ikke var nødvendig. Datatilsynet har i tilsynssager netop forudsat, at myndigheder afdækker, hvilke behandlingsaktiviteter der kræver konsekvensanalyse, og lægger en plan for at gennemføre dem. En frivillig DPIA er desuden ofte det bedste redskab til at dokumentere databeskyttelse gennem design efter [artikel 25](#).

Løbende pligt. DPIA'en er ikke et engangsdokument: den dataansvarlige skal foretage en fornyet gennemgang, i hvert fald når der sker en ændring af den risiko, behandlingsaktiviteterne udgør (artikel 35, stk. 11) – fx ved leverandørskifte, nyt modul, ny datakilde eller tilføjelse af AI-funktionalitet.

§ 2 Det skal dokumentet indeholde

1. En dokumenteret tærskelvurdering af, om behandlingen sandsynligvis indebærer høj risiko – inklusive begrundelsen, hvis konklusionen er, at DPIA ikke er påkrævet. Vurderingen skal kunne fremlægges over for Datatilsynet. (*Databeskyttelsesforordningen § 5, stk. 2*)
2. Analysen skal foreligge færdig forud for behandlingen og skal identificere den behandlingstype, den dækker; én analyse kan omfatte flere lignende behandlingsaktiviteter med lignende høje risici. (*Databeskyttelsesforordningen § 35, stk. 1*)
3. En systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen – herunder i givet fald de legitime interesser, den dataansvarlige forfølger. (*Databeskyttelsesforordningen § 35, stk. 7*)
4. En vurdering af, om behandlingsaktiviteterne er nødvendige og står i rimeligt forhold til formålene – dvs. om formålet kunne nås med færre oplysninger eller mindre indgribende midler. (*Databeskyttelsesforordningen § 35, stk. 7*)
5. En vurdering af risiciene for de registreredes rettigheder og frihedsrettigheder, hvor både sandsynlighed og alvor vurderes for hvert risikoscenarie – ikke kun risici for organisationen. (*Databeskyttelsesforordningen § 35, stk. 7*)
6. De foranstaltninger, der påtænkes for at imødegå risiciene, herunder garantier, sikkerhedsforanstaltninger og mekanismer, der kan sikre beskyttelsen og påvise overholdelse – med tydelig sammenhæng mellem den enkelte risiko og den enkelte foranstaltning samt en angivelse af restrisikoen. (*Databeskyttelsesforordningen § 35, stk. 7*)
- 7.

Dokumentation for, at databeskyttelsesrådgiveren er rådført, og hvad rådgivningen gik ud på, hvis en DPO er udpeget. (*Databeskyttelsesforordningen § 35, stk. 2*)

8. En stillingtagen til, om de registreredes eller deres repræsentanternes synspunkter skal indhentes om den planlagte behandling – og i givet fald resultatet heraf. (*Databeskyttelsesforordningen § 35, stk. 9*)
9. Inddragelse af eventuelle godkendte adfærdskodekser, der gælder for sektoren, ved vurderingen af behandlingens konsekvenser. (*Databeskyttelsesforordningen § 35, stk. 8*)
10. En udtrykkelig konklusion om, hvorvidt restrisikoen fortsat er høj, og dermed om Datatilsynet skal høres, før behandlingen påbegyndes – samt det materiale, der i så fald skal indgives (ansvarsfordeling, formål og hjælpemidler, foranstaltninger og garantier, DPO'ens kontaktoplysninger og selve konsekvensanalysen). (*Databeskyttelsesforordningen § 36, stk. 3*)
11. En plan for fornyet gennemgang: hvornår og på hvilken foranledning analysen revurderes, herunder i hvert fald ved ændringer i den risiko, behandlingsaktiviteterne udgør. (*Databeskyttelsesforordningen § 35, stk. 11*)
12. Dokumentet bør desuden være dateret og versionsstyret, angive hvem der har udarbejdet og godkendt det på ledelsesniveau, og henvise til den tilhørende artikel 30-fortegnelse og de relevante databehandleraftaler. Det er kutyme, men det er i praksis dét, der gør analysen til brugbar dokumentation.

LOV

Databeskyttelsesforordningen § 5, stk. 2

Databeskyttelsesforordningen § 35, stk. 1, 2, 7, 8, 9, 11

Databeskyttelsesforordningen § 36, stk. 3

§ 3 Tærskelvurderingen: hvornår er risikoen "høj"?

Ordlyden i artikel 35, stk. 1, er en sandsynlighedsvurdering: *vil* behandlingen sandsynligvis indebære en høj risiko? Vurderingen foretages på behandlingstypen – ikke på den enkelte registrerede – og de fire parametre er behandlingens karakter, omfang, sammenhæng og formål, med særlig vægt på brug af nye teknologier.

Ud over de tre formodningstilfælde i stk. 3 og Datatilsynets liste efter stk. 4 giver præambelbetragtning 91 de praktiske pejlemærker: meget store datamængder på regionalt eller nationalt plan, omfattende brug af ny teknologi, afgørelser truffet på grundlag af profilering, biometriske og genetiske data, oplysninger om straffedomme samt omfattende overvågning af offentligt tilgængelige områder. Datatilsynet peger i sin egen vejledning på de samme typer indgribende behandlinger – lokationsdata til kortlægning af personers adfærd, systematisk kontrolovervågning, profilering, automatiske afgørelser og samkøring af datasæt, der giver oplysninger ud over, hvad de registrerede med rimelighed kan forvente – og bemærker udtrykkeligt, at der er sammenfald med DPIA-pligten. De fælleseuropæiske retningslinjer (WP248), som Datatilsynet har lagt til grund i sin praksis, opstiller ni kriterier, og som tommelfingerregel peger to eller flere opfyldte kriterier på, at der skal laves en konsekvensanalyse.

Tærsklen er tydeligt lav på AI-området. I sagen om Uddannelses- og Forskningsstyrelsens AI-løsning til screening af SU-handicaptillæg lagde Datatilsynet vægt på store mængder følsomme data, en sårbar målgruppe og modellens evne til at finde sammenhænge ud over traditionel sagsbehandling – og fastslog, at der skal foretages en konsekvensanalyse efter artikel 35, stk. 1, før driften iværksættes. I sagen om det kommunale profileringsværktøj Asta blev profilering af ledige anset for så indgribende, at der stilles høje krav både til hjemmelsgrundlagets præcision og til beskyttelsesforanstaltningerne. Og da fodboldklubberne fik tilladelse til ansigtsgenkendelse efter [databeskyttelseslovens § 7, stk. 4](#), var det et udtrykkeligt vilkår, at

der skulle foreligge en konsekvensanalyse, der opfylder indholdskravene, før behandlingen måtte påbegyndes. Kontrolforanstaltninger over for medarbejdere – logning, tv-overvågning, GPS – ligger i samme felt; se den nærmere praksis i [oversigten om databeskyttelse i ansættelsesforhold](#).

LOV	Databeskyttelsesforordningen § 35, stk. 3, 4	Databeskyttelsesloven § 7, stk. 4	
PRAKSIS	Datatilsynet · Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere		16.07.2025
	Datatilsynet · Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre		03.07.2024
	Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger		12.06.2024
	Datatilsynet · Datatilsynets afvisning af webskrabning til biometrisk ansigtsgenkendelse		30.01.2024
	Datatilsynet · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta		18.05.2022

§ 4 Hvem gør hvad: dataansvarlig, DPO, leverandør og Datatilsynet

Den dataansvarlige er eneansvarlig for, at analysen bliver lavet, bliver lavet i tide og opfylder mindstekravene. Det er også den dataansvarlige, der træffer beslutningen om at gennemføre foranstaltningerne – og som ifalder ansvaret, hvis de udebliver.

DPO'en skal rådføres, når der foretages en konsekvensanalyse, jf. artikel 35, stk. 2, og det er en af rådgiverens lovbestemte kerneopgaver at rådgive om analysen og overvåge dens opfyldelse, jf. [artikel 39, stk. 1, litra c](#). DPO'en er samtidig tilsynets kontaktpunkt ved forudgående høring. Er der pligt til at have en DPO efter [artikel 37](#) – typisk for offentlige myndigheder og ved kerneaktiviteter med systematisk overvågning eller følsomme oplysninger i stort omfang – er de to pligter i praksis to sider af samme risikoprofil: den, der skal have en DPO, skal som regel også lave DPIA'er.

Databehandleren har ikke selv pligten, men skal efter [artikel 28](#) bistå den dataansvarlige med at overholde artikel 35 og 36 – en pligt, der bør stå eksplicit i databehandleraftalen, og som i statslige delegationsordninger er skrevet direkte ind i cirkulærerne om fælles dataansvar. Bistandspligten fritager ikke for egen stillingtagen: i AULA-tilsynene var det ikke nok at henvise til leverandørens materiale.

Datatilsynet har to roller. Rådgiveren i forhåndshøringen efter artikel 36 – og håndhæveren bagefter. Endelig kan **de registrerede** skulle høres efter artikel 35, stk. 9; på arbejdspladsen sker det naturligt gennem medarbejderrepræsentanter, hvilket AI-forordningen på sit område har gjort til en selvstændig informationspligt.

Husk sammenhængen til de øvrige dokumenter: DPIA'en trækker på [artikel 30](#)-fortegnelsen som datagrundlag, forudsætter gyldige databehandleraftaler for hver leverandør og ender ofte i konkrete ændringer af privatlivspolitikken og af, hvordan et samtykke indhentes.

LOV	Databeskyttelsesforordningen § 35, stk. 2	Databeskyttelsesforordningen § 37, stk. 1	
	Databeskyttelsesforordningen § 39, stk. 1		
PRAKSIS	Datatilsynet · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA		23.05.2024
	Datatilsynet · Alvorlig kritik og påbud til danske kommuner efter omfattende tilsyn med AULA		15.01.2024

§ 5 Metoden: fra beskrivelse til restrisiko og forhåndshøring

Artikel 35, stk. 7, er en minimumsstruktur, ikke en skabelon – men rækkefølgen er logisk og bør følges.

Først beskrives behandlingen systematisk: hvilke oplysninger, om hvem, hvorfra, til hvilke formål, hvor længe, med hvilke systemer og hvilke modtagere, herunder tredjelandsoverførsler. **Dernæst** prøves nødvendigheden og proportionaliteten: kan formålet nås med færre oplysninger, kortere opbevaring, pseudonymisering eller syntetiske data? Denne del er reelt en dokumentation af databeskyttelse gennem design efter artikel 25 og bliver ofte sprunget over. **Så** vurderes risikoen for de registrerede – scenarie for scenarie, med sandsynlighed og alvor, set fra borgerens synsvinkel og ikke fra organisationens. **Endelig** kobles hver risiko til de foranstaltninger, der skal nedbringe den, og restrisikoen efter foranstaltningerne opgøres.

Det er netop den sidste kobling, Datatilsynet efterprøver. I AULA-sagen mod Københavns Kommune anbefalede tilsynet, at risikovurderingerne struktureres, så de kan sammenlignes før og efter implementering af foranstaltningerne, og så sammenhængen mellem foranstaltninger og de enkelte risici fremgår tydeligt – kommunen havde ikke fuldt ud godtgjort, at der var implementeret passende foranstaltninger mod alle identificerede risici.

Er restrisikoen fortsat høj, indtræder høringspligten. Til Datatilsynet indgives efter artikel 36, stk. 3, ansvarsfordelingen mellem dataansvarlige, fælles dataansvarlige og databehandlere, den planlagte behandlingsformål og hjælpemidler, foranstaltninger og garantier, DPO'ens kontaktoplysninger, selve konsekvensanalysen og de yderligere oplysninger, tilsynet beder om. Tilsynet svarer inden for otte uger, der kan forlænges med seks; fristerne kan suspenderes, mens tilsynet afventer supplerende oplysninger. Sagen mod Nationalt Genom Center viser konsekvensen af at springe trinnet over: centret indsendte selv en konsekvensanalyse, der viste høj risiko og oplyste, at behandlingen allerede var i gang – tilsynet nedlagde midlertidigt forbud mod yderligere indsamling og endte med bødeindstilling og forbud mod andre formål end klinisk diagnostik, indtil en tilstrækkelig analyse forelå.

Er risikoen omvendt nedbragt til et acceptabelt niveau, er der ingen høringspligt – men analysen skal gemmes som dokumentation og revurderes ved ændringer.

LOV

Databeskyttelsesforordningen § 25, stk. 1

Databeskyttelsesforordningen § 35, stk. 7

Databeskyttelsesforordningen § 36, stk. 3

PRAKSIS **Datatilsynet** · Alvorlig kritik af Københavns Kommunes mangelfulde sikkerhed og risikovurdering i AULA 23.05.2024

Datatilsynet · Nationalt Genom Center indstilles til bøde på 600.000 kr. og modtager forbud mod behandling 25.03.2022

§ 6 Håndhævelsen: hvad det koster at springe analysen over

Danmark har ikke administrative bøder på databeskyttelsesområdet. Datatilsynet udtaler kritik eller alvorlig kritik, meddeler påbud og forbud – og politianmelder med en bødeindstilling, hvorefter bøden pålægges af domstolene. Hjemlen er [databeskyttelseslovens § 41](#), hvis stk. 1, nr. 1, netop kriminaliserer overtrædelse af den dataansvarliges og databehandlerens forpligtelser efter forordningens artikel 25-39 – dvs. både artikel 35 og artikel 36 – med bøde eller fængsel indtil 6 måneder. Bødeniveauet fastlægges efter kriterierne i [artikel 83, stk. 4](#), hvor rammen er 10 mio. EUR eller 2 % af den samlede globale årlige omsætning, og efter forordningens artikel 83, stk. 2, om overtrædelsens karakter, alvor og varighed. Også offentlige myndigheder kan straffes, jf. § 41, stk.

6 – bøden til Nationalt Genom Center blev fastsat under hensyn til de budgetmæssige rammer for offentlige myndigheder.

De to tungeste danske eksempler handler begge om konsekvensanalyse. Nationalt Genom Center blev indstillet til en bøde på 600.000 kr. og fik forbud mod behandling, fordi behandlingen af genetiske data var påbegyndt uden en fyldestgørende analyse og uden forudgående høring. Netcompany blev efter sikkerhedsbruddet på mit.dk politianmeldt og indstillet til den hidtil største danske bøde på 15 mio. kr., hvor det indgik, at der ikke var udarbejdet en konsekvensanalyse, selv om platformens formål, omfang og datakarakter indebar høj risiko. Tilsynet formulerede pointen skarpt: udarbejdelse af en konsekvensanalyse er ikke en formalitet, men en væsentlig retssikkerhedsgaranti, og analysen skal være lavet, inden behandlingen går i gang.

I tilsynssporet er reaktionen typisk alvorlig kritik og påbud: AULA-tilsynene med kommunerne endte med kritik og påbud for mangelfuld behandlingssikkerhed og manglende eller utilstrækkelige konsekvensanalyser – bl.a. over for Frederikshavn, Lolland, Esbjerg og Københavns Kommune. Datatilsynet anbefalede samtidig, at kommunerne udarbejder en **fælles** konsekvensanalyse for AULA, da behandlingsaktiviteterne er ens og indebærer lignende høje risici. Beslægtede sager om manglende risikovurdering før videregivelse og om utilstrækkelig test før idriftsættelse af Digital Post viser samme linje: risikoarbejdet skal ligge før driften. En bredere gennemgang findes i [oversigten over Datatilsynets afgørelser](#).

LOV	Databeskyttelsesforordningen § 83, stk. 4	Databeskyttelsesloven § 41, stk. 1
PRAKSIS	Datatilsynet · Alvorlig kritik til Digitaliseringsstyrelsen for utilstrækkelig sikkerhed ved brug af personoplysninger i testmiljøer	24.06.2025
	Datatilsynet · Alvorlig kritik og påbud til danske kommuner efter omfattende tilsyn med AULA	15.01.2024
	Datatilsynet · Netcompany politianmeldt og indstillet til bøde på 15 mio. kr. efter alvorligt sikkerhedsbrud på mit.dk	12.01.2024
	Datatilsynet · Alvorlig kritik af Frederikshavn Kommunes manglende behandlingssikkerhed og konsekvensanalyser	22.12.2023
	Datatilsynet · Alvorlig kritik og påbud til Lolland Kommune for mangelfuld behandlingssikkerhed og manglende konsekvensanalyser	22.12.2023
	Datatilsynet · Kritik af Esbjerg Kommune for utilstrækkelig dokumentation af risikovurderinger vedrørende behandlingssikkerhed	22.12.2023
	Datatilsynet · Nationalt Genom Center indstilles til bøde på 600.000 kr. og modtager forbud mod behandling	25.03.2022
	Datatilsynet · Alvorlig kritik af manglende risikovurdering ved videregivelse af personoplysninger	05.03.2020

§ 7 DPIA og AI-forordningens konsekvensanalyse for grundlæggende rettigheder (FRIA)

Fra den 2. august 2026 finder AI-forordningen anvendelse, jf. [artikel 113](#) (forpligtelserne knyttet til artikel 6, stk. 1, dog først fra 2. august 2027). Den introducerer et nyt dokument ved siden af DPIA'en: **konsekvensanalysen vedrørende grundlæggende rettigheder** (FRIA) i [AI-forordningens artikel 27](#). Pligten rammer idriftsættere, der er offentligretlige organer eller private enheder, som leverer offentlige tjenester, samt idriftsættere af højrisikosystemer til kreditvurdering og risikovurdering/prisfastsættelse i livs- og sygeforsikring – og den skal opfyldes **inden** idriftsættelse.

De to analyser overlapper, men er ikke identiske. FRIA'en kræver bl.a. en beskrivelse af idriftsætterens processer, anvendelsesperiode og -hyppighed, de berørte persongrupper, de specifikke risici for skade, gennemførelsen

af menneskeligt tilsyn og de foranstaltninger og klagemekanismer, der skal aktiveres, hvis risiciene opstår. Resultatet skal meddeles markedsovervågningsmyndigheden. Forholdet mellem de to dokumenter er reguleret udtrykkeligt: er nogle af FRIA-forpligtelserne allerede opfyldt gennem DPIA'en efter GDPR artikel 35, **supplerer** FRIA'en den analyse, jf. artikel 27, stk. 4 – og omvendt skal idriftsætteren efter [artikel 26, stk. 9](#) bruge udbyderens oplysninger efter artikel 13 til at opfylde sin DPIA-pligt. Den ene erstatter altså ikke den anden; i praksis bygges de mest hensigtsmæssigt som ét samlet dokument med to spor.

Datatilsynets praksis peger allerede i den retning: udvikling og drift af AI-løsninger indebærer ofte høj risiko og udløser DPIA-pligt, og tilsynet har samtidig understreget, at den dataansvarlige skal kunne påvise, at anvendelsen af personoplysninger til træning af algoritmer ikke overstiger det nødvendige. Se den samlede fremstilling i [oversigten om AI-systemer og GDPR](#).

LOV

AI-forordningen om harmoniserede regler for brug af kunstig intelligens § 26, stk. 9

AI-forordningen om harmoniserede regler for brug af kunstig intelligens § 27, stk. 1

Databeskyttelsesforordningen § 35, stk. 1

PRAKSIS	Datatilsynet · Vurdering af AI-løsning til sagsbehandling af SU-ansøgninger	12.06.2024
	Datatilsynet · Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	18.05.2022

§ 8 Typiske faldgruber

DPIA'en skrives efter idriftsættelsen. Den hyppigste og dyreste fejl. Artikel 35, stk. 1, kræver, at analysen foretages **forud for** behandlingen – og en analyse, der først færdiggøres, når systemet kører, kan pr. definition ikke bruges til at vælge foranstaltninger til. Datatilsynet indstillede Nationalt Genom Center til en bøde på 600.000 kr. og nedlagde forbud mod behandlingen, netop fordi behandlingen var påbegyndt, mens analysen stadig var uafsluttet, og det blev anset for skærpende, at man gik i gang med kendskab til, at de lovpligtige analyser ikke var færdige.

It-sikkerhedsrisikovurdering forveksles med konsekvensanalyse. En risikovurdering efter artikel 32 handler om sikkerhedsniveauet; en DPIA skal derudover indeholde formålsbeskrivelse, nødvendigheds- og proportionalitetsvurdering og en vurdering af konsekvenserne for de registreredes **rettigheder**. I AULA-tilsynene udtalte Datatilsynet kritik af Københavns Kommune, fordi konsekvensanalysen ikke opfyldte alle mindstekravene, og efterlyste bl.a., at sammenhængen mellem de enkelte risici og de enkelte foranstaltninger fremgik tydeligt.

Høj restrisiko – men ingen forhåndshøring. Mange stopper, når risikoen er beskrevet, og betragter høringspligten som frivillig. Er restrisikoen efter foranstaltningerne fortsat høj, er behandlingen retligt spærret, indtil Datatilsynet er hørt efter artikel 36. Tilsynet har udtrykkeligt fremhævet, at tilsidesættelse af høringspligten underminerer tilsynets mulighed for at kontrollere lovligheden af behandlinger med stor risiko for borgerne – og at der er tale om en væsentlig retssikkerhedsgaranti.

Leverandørens materiale genbruges ukritisk. En standardanalyse eller et risikokatalog fra systemleverandøren er input, ikke opfyldelse af pligten. I AULA-sagerne henviste kommuner til risikovurderingsmateriale fra KOMBIT, men Datatilsynet fastholdt, at dokumentationsforpligtelsen indebærer, at den dataansvarlige selv skal kunne fremlægge materiale, der viser, hvordan og på hvilket grundlag de databeskyttelsesretlige overvejelser er truffet, og hvad de konkret har givet anledning til.

Ingen dokumenteret tærskelvurdering. Når DPIA fravælges uden skriftlig begrundelse, kan man ikke påvise noget som helst, og bevisbyrden efter ansvarlighedsprincippet vendes reelt mod én selv. Datatilsynet har i tilsyn forudsat, at den dataansvarlige systematisk afdækker, hvilke behandlingsaktiviteter der skal laves konsekvensanalyser for, og lægger en plan for gennemførelsen – en tom mappe er i sig selv et kritikpunkt.

DPO'en inddrages ikke – eller først til sidst. Artikel 35, stk. 2, er en skal-bestemmelse: er der udpeget en databeskyttelsesrådgiver, skal denne rådføres, når der laves DPIA. Sker inddragelsen først, når analysen skal underskrives, mister rådgivningen sin funktion, og manglen kan i sig selv indgå i tilsynets vurdering – i AULA-sagen mod Københavns Kommune indgik netop DPO'ens interne tilsynsrapport i Datatilsynets undersøgelse.

Analysen opdateres aldrig. Nyt modul, ny underleverandør, ny datakilde, tilføjet AI-funktion eller migrering til ny platform ændrer risikobilledet – og udløser pligten til fornyet gennemgang efter artikel 35, stk. 11. En DPIA fra idriftsættelsesåret, der aldrig er rørt siden, dokumenterer i praksis kun, at man ikke har fulgt risikoen.

Man regner med, at lovhjemmel automatisk fritager. Undtagelsen i artikel 35, stk. 10, gælder kun, hvis retsgrundlaget faktisk regulerer de pågældende specifikke behandlingsaktiviteter, **og** der allerede er foretaget en generel konsekvensanalyse i forbindelse med vedtagelsen. At behandlingen har hjemmel i en lov er ikke i sig selv nok – og undtagelsen er kun relevant, hvis der ellers var DPIA-pligt efter stk. 1.

§ 9 Relaterede dokumenter

- [Artikel 30-fortegnelse](#) – Fortegnelsen over behandlingsaktiviteter – GDPR's interne keredokument og D atatilsynets første anmodning ved tilsyn
- [Databehandleraftale](#) – Den lovpligtige aftale mellem dataansvarlig og databehandler efter GDPR art. 28 – krav, indhold og faldgruber
- [Privatlivspolitik](#) – Oplysningspligten efter GDPR art. 13-14 omsat til ét dokument – hvad den skal indeholde, og hvad Datatilsynet slår ned på
- [Samtykkeerklæring \(GDPR\)](#) – Gyldigt samtykke som behandlingsgrundlag – frivilligt, specifikt, informeret og dokumenterbart (art. 4, nr. 11 og art. 7)
- [IT-kontrakt \(systemleverance/SaaS\)](#) – Kontrakten om softwareleverancer og cloud-drift – K-standarderne, agile leverancer, SLA'er og exit

REFERENCE Lovgrundlag

6 paragraffer

Databeskyttelsesforordningen § 35 stk. 1, 3, 7	Databeskyttelsesforordningen § 36 stk. 1
Databeskyttelsesforordningen § 83 stk. 4	Databeskyttelsesloven § 7 stk. 4
Databeskyttelsesloven § 41 stk. 1	Retshåndhævelsesloven § 25

MATERIALE Citerede afgørelser

14 afgørelser

DATATILSYNET · NÆVN / KLAGEINSTANS

14

16.07.2025	Fodboldklubber i Superligaen får grønt lys til ansigtsgenkendelse til bekæmpelse af karantæneramte tilskuere	2024-51-0014
24.06.2025	Alvorlig kritik til Digitaliseringsstyrelsen for utilstrækkelig sikkerhed ved brug af personoplysninger i testmiljøer	2023-442-0197
03.07.2024	Gyldighed af samtykke til ansigtsgenkendelse i fitnesscentre	2023-31-0028
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
15.01.2024	Alvorlig kritik og påbud til danske kommuner efter omfattende tilsyn med AULA	2023-420-0001
12.01.2024	Netcompany politianmeldt og indstillet til bøde på 15 mio. kr. efter alvorligt sikkerhedsbrud på mit.dk	
22.12.2023	Alvorlig kritik af Frederikshavn Kommunes manglende behandlingssikkerhed og konsekvensanalyser	2023-423-0004
22.12.2023	Kritik af Esbjerg Kommune for utilstrækkelig dokumentation af risikovurderinger vedrørende behandlingssikkerhed	2023-423-0006
22.12.2023	Alvorlig kritik og påbud til Lolland Kommune for mangelfuld behandlingssikkerhed og manglende konsekvensanalyser	2023-423-0007
18.05.2022	Datatilsynets vurdering af retsgrundlaget for kommunernes brug af AI-værktøjet Asta	2022-212-3676
25.03.2022	Nationalt Genom Center indstilles til bøde på 600.000 kr. og modtager forbud mod behandling	
05.03.2020	Alvorlig kritik af manglende risikovurdering ved videregivelse af personoplysninger	2019-441-3399