|  |
| --- |
| Oversigt over databeskyttelsesretlige krav |

Indhold

[1. Databeskyttelsesretlige krav 3](#_Toc208696816)

[1.0 Generelle krav om overholdelse af databeskyttelsesretten og overblik over data 3](#_Toc208696817)

[1.1 Rimelighed og forebyggelse af ulovlig forskelsbehandling 4](#_Toc208696818)

[1.2 Transparens, forståelighed og systemtransparens 6](#_Toc208696819)

[1.3 Formålsbegrænsning 7](#_Toc208696820)

[1.4 Dataminimering og opbevaringsbegrænsning 8](#_Toc208696821)

[1.5 Datakvalitet 10](#_Toc208696822)

[1.6 Registreredes rettigheder 11](#_Toc208696823)

[1.7 Automatiske, individuelle afgørelser og profilering 12](#_Toc208696824)

[1.8 Robusthed og sikkerhed 15](#_Toc208696825)

[1.9 Governance og ansvarlighed 16](#_Toc208696826)

[2. Designprincipper vedrørende databeskyttelse 17](#_Toc208696827)

[2.1 Dataorienterede designprincipper 17](#_Toc208696828)

[2.2 Procesorienterede designprincipper 19](#_Toc208696829)

# Databeskyttelsesretlige krav

## Generelle krav om overholdelse af databeskyttelsesretten og overblik over data

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | Løsningen skal til enhver tid leve op til gældende ret, herunder særligt opfylde alle relevante krav i databeskyttelsesforordningen og databeskyttelsesloven. Dette indebærer bl.a., at løsningen skal leve op til forordningens grundlæggende principper samt kravet om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger. | Databeskyttelsesforordningen og databeskyttelsesloven |  |
|  | Løsningen skal til enhver tid kunne håndtere alle kategorier af personoplysninger i overensstemmelse med databeskyttelsesforordningen og databeskyttelsesloven. | Databeskyttelsesforordningen og databeskyttelsesloven |  |
|  | Løsningen skal understøtte, at der til enhver tid kan dannes et opdateret overblik over, hvilke data, herunder personoplysninger, der behandles i løsningen, herunder (1) træningsdata ved udvikling af systemet, (2) valideringsdata, (3) testdata ved test af systemet, (4) data i selve modellen, (5) inputdata ved anvendelse af systemet samt (6) outputdata ved anvendelse af systemet, f.eks. en afgørelse eller forudsigelse, herunder udledte personoplysninger. | Databeskyttelsesforordningens artikel 5, stk. 2, artikel 24-25 og 30 |  |
|  | Løsningen Løsningen skal understøtte, at der til enhver tid kan skabes et overblik over alle API’er og indbyggede tredjepartsløsninger, der giver tredjeparter adgang til personoplysninger. Der skal kunne gives et fuldt overblik over alle overførsler og videregivelser af personoplysninger til tredjeparter. | Databeskyttelsesforordningens artikel 5, stk. 2, artikel 24-25 og 30 |  |

## Rimelighed og forebyggelse af ulovlig forskelsbehandling

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | AI-systemet skal sikre, at der ikke sker direkte eller indirekte ulovlig forskelsbehandling af fysiske personer på grund af race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning, fagforeningsmæssigt tilhørsforhold, genetisk status eller helbredstilstand eller seksuel orientering.Med henblik på at understøtte løsningens rimelighed og forebygge ulovlig forskelsbehandling, skal træningen af modellen i AI-systemet ske ved at anvende passende matematiske eller statistiske procedurer, herunder ved brug af træningsdata, der er så repræsentative som muligt, i forhold til de borgere AI-systemet skal anvendes på.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |  |
|  | Modellen i løsningen skal udvikles, så den ikke ulovligt tillægger et eller flere bestemte kriterier en uforholdsmæssig stor eller lille vægtning.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |  |
|  | Løsningen skal understøtte udskiftning af træningsdata og genoptræning af modellen på ny, hvis tidligere træningsdata har givet anledning til fejl eller ulovlig forskelsbehandling.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |  |
|  | Løsningen skal understøtte, at modellen løbende kan overvåges på en transparent måde, så det er muligt at justere modellen. | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |  |
|  | *Hvis løsningen har en brugergrænseflade for borgerne:*Løsningen skal være brugercentreret og designet, så alle i målgruppen kan anvende den – uanset alder, etnicitet, køn, evner og egenskaber.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra a |  |

## Transparens, forståelighed og systemtransparens

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | Løsningens beslutningsprocesser skal være så transparente som muligt for at understøtte princippet om transparens. Løsningen skal designes, så dens beslutningsprocesser kan forklares, herunder hvordan løsningen når frem til (forslag til) beslutninger, logikken og de kriterier/data den lægger vægt på. Det skal sikres, at et menneske (1) kan forudsige, hvordan systemets output vil ændre sig, hvis input ændrer sig, (2) kan identificere de mest vigtige inputvariable og deres vægt og betydning for afgørelsens resultat, (3) identificere, hvornår outputtet sandsynligvis er forkert.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra a, artikel 13-15 og artikel 22 |  |
|  | Løsningen skal understøtte sporbarhed af løsningens beslutninger. Som følge heraf skal de metoder, der er blevet anvendt til design og udvikling af løsningens algoritme, dokumenteres. Hvis der er tale om et regelbaseret system, bør programmeringsmetoden eller den måde, systemet er bygget på, dokumenteres. Hvis der er tale om et læringsbaseret AI-system, bør der ske dokumentation af metoden til oplæring af algoritmen, herunder hvilke inputdata der er indsamlet og udvalgt, og hvordan dette er sket.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra a  |  |
|  | Inden endelig godkendelse, produktionssætning og ibrugtagning af AI-systemet skal leverandøren overdrage systemdokumentation for løsningen samt (hvis relevant) udførlige driftsvejledninger/brugsanvisninger til kommunen.  | Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, stk. 1 |  |
|  | *Hvis løsningen er baseret på en dynamisk (læringsbaseret) model:* Hvis ændringer i løsningens datagrundlag giver anledning til nye vægtninger eller anderledes afvejninger af kriterier, skal løsningen være i stand til at gøre sagsbehandlere opmærksomme herpå, f.eks. ved notifikationer ved udsving af en bestemt størrelse.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra a  |  |

## Formålsbegrænsning

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | Løsningen skal udvikles således, at der alene indsamles personoplysninger til udtrykkeligt angivne og legitime formål. | Databeskyttelsesforordningens artikel 5, stk. 1, litra b, og databeskyttelseslovens § 5, stk. 1 |  |
|  | Løsningen skal understøtte, at indsamlede personoplysninger ikke bliver viderebehandlet til formål, der er uforenelige med indsamlingsformålet. | Databeskyttelsesforordningens artikel 5, stk. 1, litra b, og databeskyttelseslovens § 5, stk. 1 |  |
|  | Løsningen skal understøtte mulighed for en klar opdeling af behandling af personoplysninger i miljøer for udvikling og anvendelse af modellen/systemet (data governance). | Databeskyttelsesforordningens artikel 5, stk. 1, litra b, og databeskyttelseslovens § 5, stk. 1 |  |

## Dataminimering og opbevaringsbegrænsning

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | Løsningen skal understøtte overholdelse af princippet om dataminimering ved udvikling (træning) og anvendelse af løsningen. Som følge heraf må AI-systemet ikke indsamle eller behandle flere personoplysninger, end hvad der er tilstrækkeligt, relevant og nødvendigt i lyset af løsningens formål. Løsningen skal understøtte, at der kan ske en periodisk evaluering af proportionaliteten i databehandlingen med henblik på at eliminere datakilder, der ikke længere er nødvendige i lyset af formålet. | Databeskyttelsesforordningens artikel 5, stk. 1, litra c |  |
|  | Løsningen skal understøtte brug af pseudonymisering, anonymisering og aggregering i videst muligt omfang, så systemet (også ved udvikling og træning) til enhver tid behandler så få personoplysninger som muligt i lyset af løsningens formål.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra c |  |
|  | Ved terminaladgang til eller løbende abonnement på oplysninger fra eksterne registre, skal løsningen understøtte, at der ved indsamling eller videregivelse ikke henholdsvis indsamles eller videregives flere oplysninger end nødvendigt. | Databeskyttelsesforordningens artikel 5, stk. 1, litra c |  |
|  | Løsningen skal understøtte sletning af træningsdata, valideringsdata og testdata, så snart de ikke længere er relevante, herunder i udviklingsmiljøer. | Databeskyttelsesforordningens artikel 5, stk. 1, litra c |  |
|  | Løsningen skal understøtte, at oplysninger kan slettes eller anonymiseres effektivt og uigenkaldeligt i løsningen, herunder i udviklings- og testmiljøer, efter en rimelig og på forhånd fastsat periode samt ved forlangende. | Databeskyttelsesforordningens artikel 5, stk. 1, litra e |  |
|  | *Hvis løsningen er baseret på en dynamisk (læringsbaseret) model:* Løsningen skal udgøre en stabil og pålidelig beslutningsmodel, hvorfor løbende sletning af personoplysninger ikke må forårsage markante praksisændringer for løsningens beslutninger.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra a og e |  |

## Datakvalitet

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | Med henblik på at overholde princippet om rigtighed skal løsningen navnlig sikre, at faktorer, der resulterer i unøjagtige personoplysninger, herunder ukorrekt output i form af f.eks. hallucinationer, bliver rettet, og at risikoen for fejl minimeres. Løsningen skal indeholde en beskrivelse af, hvordan alle personoplysninger, der anvendes til træning, test og anvendelse af AI-systemet, er så korrekte, relevante, repræsentative, komplette og ajourførte som muligt. | Databeskyttelsesforordningens artikel 5, stk. 1, litra d |  |
|  | Løsningen skal understøtte ændring, berigtigelse og ajourføring af registrerede personoplysninger, herunder både på kommunens eget initiativ og ved henvendelse herom fra den registrerede selv.  | Databeskyttelsesforordningens artikel 5, stk. 1, litra d |  |
|  | Løsningen skal understøtte et overblik over de kriterier (features) og deres vægtning, der indgår i modellen. Det skal være muligt at få indsigt i modellens nøjagtighed og træfsikkerhed samt at kunne beskrive dens begrænsninger. | Databeskyttelsesforordningens artikel 5, stk. 1, litra d |  |

## Registreredes rettigheder

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | Løsningen skal understøtte, at brugerne kan udøve deres rettigheder efter databeskyttelsesforordningen. Personoplysninger kan indgå i (1) træningsdata ved udvikling af systemet, (2) valideringsdata, (3) testdata ved test af systemet, (4) data i selve modellen, (5) inputdata ved anvendelse af systemet samt (6) outputdata ved anvendelse af systemet, f.eks. en afgørelse eller forudsigelse, herunder udledte personoplysninger i form af profiler, forudsigelser mv. De registreredes rettigheder skal kunne håndteres i forhold til alle disse anvendelser af personoplysninger. | Databeskyttelsesforordningens kapitel III |  |
|  | Løsningen skal understøtte, at den registrerede har mulighed for at få indsigt i personoplysninger i logfiler, såfremt løsningen gemmer sådanne oplysninger om løsningens drift og brug. | Databeskyttelsesforordningens artikel 15 |  |
|  | Løsningen skal understøtte, at den registrerede kan gives indsigt ved profilering og konsekvenserne heraf, herunder at der kan gives adgang til de oplysninger, der er anvendt som input til at oprette profilen, samt til oplysninger om profilen og de segmenter, som den registrerede er blevet placeret i.  | Databeskyttelsesforordningens artikel 15, smh. præambelbetragtning 60 |  |
|  | Løsningen skal understøtte, at den registrerede har ret til berigtigelse og fuldstændiggørelse af oplysninger. Retten til berigtigelse og sletning finder både anvendelse på ”inputdata” (de personoplysninger, der anvendes til at oprette profilen) og ”outputdata” (selve profilen eller ”scoren”, som personen er blevet tildelt). | Databeskyttelsesforordningens artikel 16 |  |

## Automatiske, individuelle afgørelser og profilering

|  |  |  |  |
| --- | --- | --- | --- |
| **Krav-ID** | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | Løsningen skal understøtte, at der kan foretages en løbende overvågning samt mulighed for menneskelig overvågning og indgriben før/efter AI-systemet har truffet en afgørelse. Ved den manuelle kontrol med outputtet af systemet skal der være adgang til relevant viden om, hvorvidt den forudsatte kvalitet af outputtet er tilstrækkelig og i overensstemmelse med fastsatte kvalitetskrav, f.eks. at der er en kvalitetsscore af outputtet tilgængelig for brugeren, der kan forklares. | Databeskyttelsesforordningens artikel 5, stk. 2, artikel 22 og 24 |  |
|  | Løsningen skal understøtte, at der kan foretages en klar og dokumenteret grænsedragning mellem automatiske, individuelle afgørelser og beslutningsstøtte, i de situationer hvor der anvendes en kombination af de to. | Databeskyttelsesforordningens artikel 5, stk. 2, artikel 22 og 24 |  |
|  | Hvis AI-systemet indebærer automatiske, individuelle afgørelser, herunder ved brug af profilering, skal løsningen understøtte, at den registrerede kan oplyses herom samt modtage meningsfulde oplysninger om logikken heri, herunder indsigt i den metode og de kriterier som kommunen har anvendt samt betydningen og de forventede konsekvenser af en sådan behandling for den registrerede. Den registrerede har også ret til indsigt i disse oplysninger.I stedet for at komme med en kompleks matematisk forklaring på, hvordan algoritmer eller maskinlæring fungerer, bør kommunen overveje at give oplysningerne til den registrerede på en måde, således at de er klare, letforståelige, lettilgængelige, kortfattede, fuldstændige og kontekstualiserede, således at den registrerede sættes i stand til at kontrollere, om oplysningerne er korrekte, og om der er en objektivt kontrollerbar sammenhæng og årsagsforbindelse mellem på den ene side den anvendte metode og de anvendte kriterier og på den anden side det resultat, som den automatiske afgørelse har ført til. Dette kan sikres ved f.eks. at oplyse om:* De kategorier af oplysninger, der er eller vil blive anvendt i forbindelse med profileringen eller beslutningstagningen,
* hvorfor disse kategorier anses for at være relevante,
* hvordan en profil, der anvendes i forbindelse med automatiske afgørelser, er opbygget, herunder eventuelle statistiske oplysninger, der er anvendt i analysen,
* hvorfor denne profil er relevant i forbindelse med automatiske afgørelser, og
* hvordan den anvendes til en afgørelse vedrørende den registrerede.
 | Databeskyttelsesforordningens artikel 5, stk. 1, litra a, artikel 12-15 og 22 |  |

## Robusthed og sikkerhed

|  |  |
| --- | --- |
| **Yderligere vejledning** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
| For identifikation og implementering af krav vedrørende AI-systemets robusthed og sikkerhed henvises til følgende yderligere vejledning: * Digitaliseringsstyrelsen, Erhvervsstyrelsen og Center for Cybersikkerhed: Vejledning: Tiltag til at sikre brugen af kunstig intelligens, januar 2020, som kan findes her: <https://www.sikkerdigital.dk/media/6839/vejledning-tiltag-til-at-sikre-brugen-af-kunstig-intelligens-2020.pdf>
* ISO/IEC 27001, Anneks A, som kan findes her (kræver licensbetaling): <https://www.ds.dk/da/om-standarder/ledelsesstandarder/iso-27001-informationssikkerhed?gclid=EAIaIQobChMIxq3E2P34_AIVEMbtCh3ZkgmIEAAYASAAEgKx6PD_BwE>
* ISO/IEC 29134:2023 og ISO/IEC 29151:2017, der i katalogform beskriver flere af de mulige sikkerhedsforanstaltninger, der kan benyttes. Standarderne kan findes her (kræver licensbetaling): <https://www.iso.org/standard/86012.html> og her: <https://www.iso.org/standard/62726.html>
* ENISA, Artificial intelligence and Cybersecurity research, juni 2023, beskriver flere mulige sikkerhedsforanstaltninger, der kan benyttes. Rapporten kan findes her: [Artificial Intelligence and Cybersecurity Research](https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research)
* ENISA, Cybersecurity and Privacy in AI – Medical Imaging Diagnosis, juni 2023, beskriver flere mulige sikkerhedsforanstaltninger ved brugen af AI i forbindelse med medicinsk billeddiagnostik. Rapporten kan findes her: [Cybersecurity and privacy in AI - Medical imaging diagnosis](https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis)
* ENISA, Securing Machine Learning Algorithms, december 2021, beskriver generelt maskinlæring og algortimer, som kan anvendes hertil. Rapporten afdækker også de trusler, der eksisterer ved brugen af maskinlæring. Rapporten kan findes her: [Securing Machine Learning Algorithms — ENISA (europa.eu)](https://www.enisa.europa.eu/publications/securing-machine-learning-algorithms?v2=1)
 |  |

## Governance og ansvarlighed

|  |  |  |  |
| --- | --- | --- | --- |
| Krav-ID | **Beskrivelse af krav** | **Kravets grundlag** | **Beskriv, hvordan kravet overholdes (”følg eller forklar”)** |
|  | Løsningen skal understøtte dokumentation, herunder versionering af løsningen, af valg og ændringer af AI-systemet, så kommunen altid kan dokumentere valg og fravalg under udvikling, drift og opdatering af systemet samt begrundelserne herfor.  | Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, stk. 1 |  |
|  | Løsningen skal understøtte, at kommunen selv eller en tredjepart kan gennemføre en stikprøvekontrol samt algoritmisk audit af AI-systemet, modellen eller kildekoden, det vil sige en audit for at påvise, at systemet rent faktisk fungerer efter hensigten og ikke giver diskriminerende, fejlagtige eller uberettigede resultater. | Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, stk. 1 |  |
|  | Løsningen skal understøtte, at der kan foretages en meningsfuld, reel menneskelig efterprøvelse og indgriben ved brug af AI-systemet som beslutningsstøtte. | Databeskyttelsesforordningens artikel 5, stk. 2, og artikel 24, stk. 1 |  |

# Designprincipper vedrørende databeskyttelse

## Dataorienterede designprincipper

Når et AI-system skal designes, kan der ofte hentes god inspiration til både mulige it-designprincipper og privatlivsfremmende foranstaltninger ved brug af følgende fem *dataorienterede* designprincipper, der også kan bruges til at nedbryde og tilpasse de ovennævnte databeskyttelsesretlige krav til den konkrete AI-løsning.[[1]](#footnote-1)

1. *Minimér og begræns*: Mængden af personoplysninger, der indsamles og behandles, skal være begrænset til, hvad der er lovligt og strengt nødvendigt (”select before you collect”). Derudover skal oplysningerne slettes, så snart de ikke længere er nødvendige for behandlingens formål.
2. *Skjul og beskyt*: Personoplysninger og deres interne sammenhænge skal hverken kommunikeres, behandles eller opbevares frit fremme. Dette designprincip kan f.eks. opfyldes ved brug af pseudonymisering, kryptering og aggregering af personoplysningerne.
3. *Separér*: Ved at adskille forskellige behandlinger af personoplysninger om samme person, mindskes muligheden for at oprette komplette profiler af vedkommende. Dette designprincip kan f.eks. opfyldes ved at gemme personoplysningerne i separate databaser, enheder og områder til forskellige formål. Dette designprincip understøtter også formålsbestemthed, idet personoplysninger til forskellige formål – f.eks. personoplysninger til brug for udvikling og anvendelse af AI-systemet – holdes adskilt.
4. *Aggregér*: Dette designprincip handler om at indsamle og behandle personoplysninger i så aggregeret form som muligt. Personoplysningerne skal være så begrænsede, ikke-detaljerede, ikke-fortrolige og ikke-følsomme som muligt – med respekt for behandlingens formål.
5. *Databeskyttelse gennem standardindstillinger*: AI-systemet skal som udgangspunkt være konfigureret med de mest privatlivsvenlige indstillinger som muligt, herunder navnlig at der ikke indsamles og opbevares flere personoplysninger end nødvendigt for behandlingen. Brugeren af løsningen skal dermed aktivt vælge at indstille mindre privatlivsvenligt.

Beskriv nedenfor, hvordan ovenstående dataorienterede designprincipper er blevet implementeret i AI-systemets design:

|  |  |
| --- | --- |
| **Princip** | **Beskriv, af hvordan princippet er blevet implementeret** |
| 1. Minimér og begræns |  |
| 2. Skjul og beskyt |  |
| 3. Separér |  |
| 4. Aggregér |  |
| 5. Databeskyttelse gennem standardindstillinger |  |

## Procesorienterede designprincipper

Udover de dataorienterede designprincipper kan følgende fire *procesorienterede* designprincipper ligeledes inddrages ved udformningen af AI-systemets design:[[2]](#footnote-2)

1. *Informér*: AI-systemet designes, så den registrerede bliver tilstrækkeligt informeret om, hvordan løsningen fungerer, samt hvordan vedkommendes personoplysninger bliver behandlet. Informationen tilpasses til brugergruppen. Hvis AI-systemet foretager profilering eller træffer automatiske afgørelser, skal den registrerede informeres om, hvordan dette foregår samt konsekvenserne for den registrerede.
2. *Kontrollér*: Den registrerede har ret til at kontrollere egne personoplysninger. Derudover har den registrerede ret til at kræve manuel behandling, i tilfælde hvor AI-systemet anvendes til at træffe fuldautomatiske afgørelser. AI-systemet skal som konsekvens heraf være indrettet, så den registrerede nemt er i stand til at udøve disse rettigheder.
3. *Håndhæv:* AI-systemet skal være designet, så det understøtter dokumentation af, hvordan det sikrer overholdelse databeskyttelsesreglerne (princippet om ansvarlighed). Dokumentationen skal i denne forbindelse dække ansvarsforhold, samt hvordan databeskyttelsesforordningen håndhæves, og den skal være tilgængelig ved revisioner eller inspektioner af AI-systemet.
4. *Demonstrér*: AI-systemet skal være designet og udviklet, så kommunen kan dokumentere og demonstrere, hvordan kravene i databeskyttelsesforordningen er blevet implementeret. Eksempelvis kan kommunen fremlægge dokumentation for udførte tests, rapporter fra sikkerhedsrevisioner, sårbarhedsscanninger og rapporter om håndtering af sikkerhedsbrud mv.

Beskriv nedenfor, hvordan ovenstående procesorienterede designprincipper er blevet implementeret i AI-systemets design:

|  |  |
| --- | --- |
| **Princip** | **Beskriv, af hvordan princippet er blevet implementeret** |
| 1. Informér |  |
| 2. Kontrollér |  |
| 3. Håndhæv |  |
| 4. Demonstrér |  |

1. Se Datatilsynet, Justitsministeriet og Digitaliseringsstyrelsen: Vejledning - Behandlingssikkerhed og databeskyttelse gennem design og standardindstillinger, juni 2018, side 25 f. og 30, smh. det norske datatilsyn: Software development with Data Protection by Design and by Default, version af 28. november 2017. [↑](#footnote-ref-1)
2. Se ovenfor. [↑](#footnote-ref-2)