Martin Sønnersgaard
mso@kammeradvokaten.dk
M: +45 50 77 84 23

Bilag B

Notat vedrørende AI-modellers anonymitet og statslige dataansvarliges databeskyttelsesretlige forpligtelser ved brug af Microsoft Copilot for Microsoft 365

Indhold

1. INDLEDNING OG KONKLUSIONER

Økonomistyrelsen og Statens It har med bistand fra Kammeradvokaten udarbejdet en konsekvensanalyse vedrørende databeskyttelse, som dataansvarlige offentlige myndigheder kan anvende til brug for vurderingen af lovligheden og risiciene for de registrerede forbundet med behandlingen af personoplysningerne efter databeskyttelsesforordningens regler ved brug af Microsoft Copilot for Microsoft 365 (herefter "M365 Copilot"). Konsekvensanalysen omfatter brugen af M365 Copilot til følgende use cases:

1) *Assistance til generel sagsbehandling til intern brug*. Hermed menes opgaver, som ikke er rettet mod borgere som led i sagsbehandling eller medarbejdere som led i personalesager, f.eks. udarbejdelse af kontraktmateriale i udbudssager, referat af en rapport eller udarbejdelse af et udkast til et talepapir etc.
2) *Administrativ bistand (intern supportchat).* Dette omfatter, at medarbejdere kan stille spørgsmål til supportchatten inden for f.eks. HR eller økonomi og modtage generel vejledning om f.eks. ferieregler, overenskomstspørgsmål, hjælp til kontering, m.v. Der er således ikke tale om brug af M365 Copilot som led i borgerrettet sagsbehandling eller personalesager, ligesom supportløsningen ikke er rettet mod borgerne.
3) *Assistance til borgerrettet sagsbehandling (ekstern brug)*. Denne use case omhandler borgerrettet sagsbehandling, herunder udarbejdelse af udkast til breve og afgørelser som led i afgørelsesvirksomhed. Dog ikke således, at borgerne bruger M365 Copilot.

Dette notat udgør bilag B til denne konsekvensanalyse, jf. konsekvensanalysens afsnit 6.2.4 og 7.3.1, og indeholder en vurdering af følgende spørgsmål:

1) Hvorvidt AI-modellerne, der indgår i M365 Copilot, indeholder personoplysninger indsamlet af Microsoft/OpenAI, samt
2) hvilken kontrol de dataansvarlige statslige myndigheder, der ibrugtager M365 Copilot, efter databeskyttelsesreglerne i så fald skal foretage vedrørende spørgsmålet om, hvorvidt Microsoft/OpenAI har trænet og udviklet AI-modellerne i M365 Copilot ved hjælp af ulovligt indsamlede personoplysninger, herunder via dataskrab af disse personoplysninger fra internettet.

Som nærmere begrundet i vurderingen i afsnit 4 nedenfor, kan vores konklusioner og anbefalinger sammenfattes som følger:

- Ud fra en bedømmelse af de foreliggende oplysninger må det konkluderes, at det er mest sandsynligt, at domstolene vil finde, at AI-modellerne, der anvendes i M365 Copilot, herunder AI-modellen GPT-4.5, indeholder personoplysninger. De dataansvarlige statslige myndigheder, der ibrugtager M365 Copilot, behandler derfor personoplysninger ved brugen af dette AI-system.

- Spørgsmålet er herefter, hvad der er den databeskyttelsesretlige retsvirkning af, at der indgår personoplysninger i AI-modellen GPT-4.5 i M365 Copilot samt øvrige AI-modeller. Dette angår spørgsmålet om, hvilken kontrol den dataansvarlige statslige myndighed, der anvender M365 Copilot, skal foretage af, at Microsoft/OpenAI har trænet AI-modellen ved brug af ulovligt tilvejebragte personoplysninger.

- Ifølge EDPB skal den dataansvarlige, der idriftsætter en AI-model, der indeholder personoplysninger, foretage en vis kontrol med, at udbyderen af AI-modellen ikke har udviklet AI-modellen med ulovligt indsamlede personoplysninger. Der findes ikke tilsyns- eller domstolssager endnu, der kan belyse niveauet af denne undersøgelse.

- Efter en samlet vurdering må det efter vores opfattelse konkluderes, at de statslige myndigheder ikke ved ibrugtagning af M365 Copilot inden for de definerede use cases, som anført i konsekvensanalysen vedrørende M365 Copilot, foretager en ulovlig behandling af personoplysninger. Henset til den manglende praksis fra domstole og tilsynsmyndigheder er denne konklusion dog ikke utvivlsom og indebærer således en vis procesrisiko.

- Det bemærkes herudover, at der ifølge EDPB's ChatGPT-taskforcerapport er flere verserende tilsynssager, der omfatter bl.a. modellerne GPT-3.0 og GPT 3.5 fra OpenAI. Der må derfor forventes praksis og afgørelser fra de europæiske datatilsyn, når disse sager afsluttes, samt når det irske datatilsyn som ledende tilsynsmyndighed træffer afgørelser vedrørende OpenAI, som kan have betydning for anvendelsen af M365 Copilot 365 og bl.a. AI-modellen GPT-4.5.

- Det må derfor anbefales, at de dataansvarlige statslige myndigheder, der ønsker at anvende M365 Copilot, følger udviklingen fra de europæiske datatilsyn og retspraksis i øvrigt tæt på dette område, samt løbende opdaterer konsekvensanalysen vedrørende databeskyttelse for løsningen i lyset ny viden om løsningens behandling af personoplysninger.

- Det må endvidere anbefales, at de dataansvarlige statslige myndigheder udarbejder en klar exitstrategi for, hvordan de dataansvarlige kan stoppe med at anvende M365 Copilot indenfor en rimelig periode.

Efter aftale med Økonomistyrelsen forholder notatet sig alene til de nævnte databeskyttelsesretlige problemstillinger og ikke eksempelvis ophavsretlige problemstillinger m.v.

2. DET FAKTUELLE GRUNDLAG

2.1 Hvad er en stor, generativ sprogmodel, og hvordan fungerer den?

Hverken databeskyttelsesforordningen[1] eller AI-forordningen[2] definerer, hvad der skal forstås ved en stor, generativ sprogmodel (på engelsk: Large Language Model, forkortet "LLMs").

AI-forordningen definerer et AI-system som et maskinbaseret system, som er udformet med henblik på at fungere med en varierende grad af autonomi, og som efter idriftsættelsen kan udvise en tilpasningsevne, og som til eksplicitte eller implicitte mål af det input, det modtager, udleder, hvordan det kan generere output såsom forudsigelser, indhold, anbefalinger eller beslutninger, som kan påvirke fysiske eller virtuelle miljøer, jf. forordningens artikel 3, nr. 1.

Endvidere defineres en AI-model til almen brug – som bl.a. omfatter store, generative sprogmodeller – i AI-forordningens artikel 3, nr. 63, som en AI-model, herunder når en sådan AI-model er trænet med en stor mængde data ved hjælp af selvovervågning i stor skala, som udviser betydelig generalitet og har kompetence til at udføre en lang række forskellige opgaver, uanset hvordan modellen bringes i omsætning, og som kan integreres i en række downstreamsystemer eller -applikationer, bortset fra AI-modeller, der anvendes til forsknings-, udviklings- og prototypeaktiviteter, inden de bringes i omsætning.

En "AI-model" er kun indirekte defineret i AI-forordningens præambelbetragtning 97, hvor der bl.a. anføres følgende:

> *"Begrebet AI-modeller til almen brug bør af hensyn til retssikkerheden defineres klart og adskilles fra begrebet AI-systemer. Definitionen bør baseres på de vigtigste funktionelle karakteristika ved en AI-model til almen brug, navnlig generaliteten og kapaciteten til med kompetence at udføre en lang række forskellige opgaver. Disse modeller trænes typisk med store mængder data ved hjælp af forskellige metoder såsom ved selvovervåget, ikkeovervåget eller forstærket læring. AI-modeller til almen brug kan bringes i omsætning på forskellige måder, herunder via biblioteker eller programmeringsgrænseflader for applikationer (API'er), som direkte download eller som fysisk kopi. Disse modeller kan ændres yderligere eller finjusteres til nye modeller. Selv om AI-modeller er væsentlige komponenter i AI-*

[1] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) anvendelse (herefter "databeskyttelsesforordningen").

[2] Europa-Parlamentets og Rådets forordning (EU) 2024/1689 af 13. juni 2024 om harmoniserede regler for kunstig intelligens og om ændring af forordning (EF) nr. 300/2008, (EU) nr. 167/2013, (EU) nr. 168/2013, (EU) 2018/858, (EU) 2018/1139 og (EU) 2019/2144 samt direktiv 2014/90/EU, (EU) 2016/797 og (EU) 2020/1828 (forordningen om kunstig intelligens).

> *systemer, udgør de ikke i sig selv AI-systemer. AI-modeller kræver, at der tilføjes yderligere komponenter, f.eks. en brugergrænseflade, for at blive til AI-systemer. AI-modeller er typisk integreret i og udgør en del af AI-systemer."*

Om AI-modellers karakter og funktionsmåde kan der endvidere henvises til beskrivelsen heraf i Det Europæiske Databeskyttelsesråds (EDPB) udtalelse af den 17. december 2024 om visse databeskyttelsesretlige spørgsmål relateret til brug af AI-modeller.[3] I udtalelsens punkt 23-25 anføres følgende om AI-modeller, der også omfatter store, generative sprogmodeller (Large Language Models, forkortet LLMs):

> *"23. Furthermore, AI models (or "**models**") relevant for this Opinion are those developed through a training process. Such training process is a part of the development phase, where models learn from data to perform their intended task. Therefore, the training process requires a dataset from which the model will identify and 'learn' patterns. In these cases, the model will use different techniques to build a representation of the knowledge extracted from the training dataset. This is notably the case with machine learning.*
>
> *24. In practice, any AI model is an algorithm, whose functioning is determined by a set of elements. For example, deep learning models are often in the form of a neural network with multiple layers consisting of nodes connected by edges that have weights, which are adjusted during training to learn the relationships between inputs and outputs. The characteristics of a simple deep learning model would be: (i) the type and size of each layer, (ii) the weight attributed to each edge (sometimes called 'parameters'), (iii) the activation functions20 between layers, and possibly (iv) other operations that may happen between layers. For instance, when training a simple deep learning model for image classification, inputs (the "**image pixels**") will be associated with outputs, and weights may be adjusted, so as to produce the right output most of the time.*
>
> *25. Other examples of deep learning models include LLMs and generative AI, which are used for e.g. generating human-like content and creating new data."* (Original fremhævning.)

Datatilsynet i Hamburg har den 15. juli 2024 udgivet et notat[4] vedrørende spørgsmålet om, hvorvidt store, generative sprogmodeller indeholder personoplysninger, og hvad den databeskyttelsesretlige

[3] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17. december 2024 (endelig version).

[4] The Hamburg Commissioner for Data Protection and freedom of information: "Discussion paper: Large Language Models and Personal Data", 15. juli 2024, tilgængeligt på datatilsynets hjemmeside her: https://datenschutz-

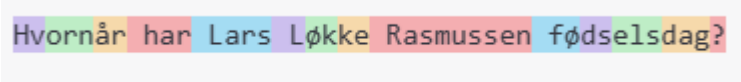
retsvirkning af dette i så fald er. Notatets juridiske konklusioner gennemgås nedenfor i afsnit 3.2.3. Den følgende gennemgang af, hvordan store, generative sprogmodeller fungerer, bygger i væsentligt omfang på fremstillingen heraf i dette notat, jf. notatets s. 2-4.

Store, generative sprogmodeller indgår som en komponent i et AI-system, der indeholder en brugergrænseflade, som kan anvendes til at stille kommandoer til systemet ("prompts").

Store, generative sprogmodeller indeholder ikke personoplysninger i den forstand, at AI-modellen indeholder eller har adgang til en database med al data, som modellen er blevet trænet på, og som den herefter kan genkalde oplysninger fra, når brugeren gennem AI-systemets brugergrænseflade kalder modellen med et "prompt", dvs. en kommando.

Omvendt er det åbenbart, at AI-modellens output kan indeholde oplysninger relateret til fysiske personer – især hvis brugeren direkte efterspørger sådanne oplysninger i prompten. Dette gælder navnlig information vedrørende kendte eller historiske fysiske personer, f.eks. hvis man prompter løsningen med prompten: "Hvornår har præsident Donald Trump fødselsdag?" eller "Hvem var Alf Ross?".

Store, generative sprogmodeller trænes typisk på meget store mængder af tekst som input på de relevante sprog, typisk adskillige sprog. Denne lingvistiske information behandles og gemmes i sprogmodellen gennem en proces, der omsætter input-teksten til såkaldte "tokens" ("tokenization"). Denne proces indebærer, at al tekst under træningen deles op i små foruddefinerede bidder – de såkaldte tokens – og opbevares i sprogmodellen som sådan. Disse tekstbidder er som regel mindre end enkelte ord, men større end de enkelte bogstaver. Eksempelvis opdeles sætningen "Hvornår har Lars Løkke Rasmussen fødselsdag?" – der består af 44 bogstaver – i 14 tokens som angivet i figur 1 nedenfor.[5] Og sætningen: "Indeholder store, generative sprogmodeller personoplysninger?" består af 61 bogstaver og 15 tokens.[6]

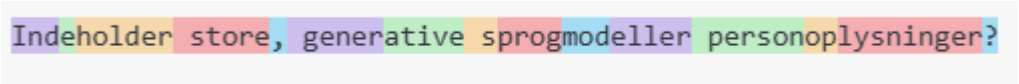


Figur 1.

hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf (senest tilgået den 1. oktober 2025).

[5] Kilde: https://platform.openai.com/tokenizer ved anvendelse af sprogmodellerne GPT-4o og GPT-4o mini (senest tilgået den 1. oktober 2025).

[6] Ibid.



Figur 2.

Denne proces indebærer – som det fremgår af figur 1 og 2 ovenfor – at længere ord, fraser eller hele sætninger ikke som sådan inkorporeres i sprogmodellen. Disse tokens konverteres endvidere til numeriske værdier, som alene anvendes indenfor den pågældende model. Dette medfører, at sprogmodellen ikke opbevarer input-teksterne fra træningen i deres oprindelige form.

De numeriske tokens omdannes endvidere til såkaldte "embeddings", som udgør vektorer, der udtrykker de lærte korrelationer ved at positionere tokens i relation til hinanden i henhold til sandsynlighedsvægte. Dette udgør træningen af en stor, generativ sprogmodel og dens "læring".

Når AI-systemet, der indeholder modellen, modtager et prompt af brugeren i systemets brugergrænseflade, vil AI-modellen i lyset af indholdet af den specifikke prompt generere en sekvens af tokens, som konverteres tilbage til en sekvens af bogstaver, som disse tokens repræsenterer. Dette sker ud fra modellens beregning af, hvilke kombinationer af tokens der har den største sandsynlighed for at være i kombination med hinanden i lyset af brugerens prompt. F.eks. kan tokens "L", "øk" og "ke" givet ét prompt indgå i outputtet "Lars Løkke Rasmussen har fødselsdag den 15. maj 1964", hvorimod disse tokens givet et andet prompt kan indgå i helt andre sætninger. Teksten "Lars Løkke Rasmussen" gemmes således ikke i sprogmodellen – det gør alene de sproglige fragmenter i form af disse tokens.

En sprogmodels kapacitet udtrykkes ofte ved en angivelse af modellens parametre, som angiver sammenhængen mellem modellens tokens, som er et resultat af træningsprocessen. Moderne sprogmodeller indeholder typisk milliarder af sådanne parametre.

I ovennævnte notat anføres følgende på s. 4 vedrørende spørgsmålet om, hvorvidt store, generative sprogmodeller indeholder personoplysninger:

> *"When training data contains personal data, it undergoes a transformation during machine learning process, converting it into abstract mathematical representations. This abstraction process results in the loss of concrete characteristics and references to specific individuals. Instead, the model captures general patterns and correlations derived from the training data as a whole.*
>
> *In this context, a somewhat contradictory characteristic of such models occurs: On the one hand, they do not store the texts used for training in their original form, but process them in such a way that the training data set can never be fully reconstructed from the model. On the other*

hand, LLMs process these training texts in a very specific manner based on contextual relationships, which enables the generation of similar and often useful output texts. However, everything that LLMs produce is "created" in the sense that it is not a simple reproduction of something stored (such as an entry in a database or a text document), but rather something newly produced. This probabilistic generation capability fundamentally differs from conventional data storage and data retrieval."

2.2 AI-modeller anvendt i M365 Copilot

Af Microsofts Transparency Note for Microsoft 365[7] fremgår bl.a. følgende om M365 Copilot's brug af AI-modeller:

> *"Microsoft 365 Copilot uses a combination of models provided by Azure OpenAI Service.*
>
> […]
>
> *Microsoft 365 Copilot uses a combination of LLMs to summarize, predict, and generate content. These LLMs include pre-trained models, such as Generative Pre-Trained Transformers (GPT) like GPT-4 from OpenAI, designed to excel in these tasks."*

Azure OpenAI Service giver adgang til en række forskellige AI-modeller. På nuværende tidspunkt (pr den 7. marts 2025) er der tale om følgende hovedmodeller[8]:

[7] https://learn.microsoft.com/en-us/copilot/microsoft-365/microsoft-365-copilot-transparency-note (senest tilgået den 1. oktober 2025).

[8] https://learn.microsoft.com/en-us/azure/ai-services/openai/concepts/models?tabs=global-standard%2Cstandard-chat-completions (senest tilgået den 1. oktober 2025).

Models	Description
GPT-4.5 Preview	The latest GPT model that excels at diverse text and image tasks.
o-series models	Reasoning models with advanced problem-solving and increased focus and capability.
GPT-4o & GPT-4o mini & GPT-4 Turbo	The latest most capable Azure OpenAI models with multimodal versions, which can accept both text and images as input.
GPT-4o audio	GPT-4o audio models that support either low-latency, "speech in, speech out" conversational interactions or audio generation.
GPT-4	A set of models that improve on GPT-3.5 and can understand and generate natural language and code.
GPT-3.5	A set of models that improve on GPT-3 and can understand and generate natural language and code.
Embeddings	A set of models that can convert text into numerical vector form to facilitate text similarity.
DALL-E	A series of models that can generate original images from natural language.
Whisper	A series of models in preview that can transcribe and translate speech to text.
Text to speech (Preview)	A series of models in preview that can synthesize text to speech.

Tabel 1.

De fleste af disse modeller er udgivet i flere versioner. Nogle af disse modeller er udfaset og ikke længere i brug.[9]

Det er ikke umiddelbart muligt at finde en oversigt over de AI-modeller i Azure OpenAI Service, der anvendes i M365 Copilot. Microsoft Danmark har den 12. marts 2025 oplyst følgende vedrørende anvendelsen af store, generative sprogmodeller i M365 Copilot:

> *"the functionality within M365 Copilot is mostly dependent on the newer LLM models from OpenAI, for which there are System Cards available".*

Som det fremgår af det citerede, henvises der til de såkaldte "system cards". Disse "system cards" eller "model cards" udgør detaljerede beskrivelser af, hvordan en udviklingsleverandør – f.eks. det

[9] https://learn.microsoft.com/en-us/azure/ai-services/openai/concepts/model-retirements (senest tilgået den 1. oktober 2025).

amerikanske selskab OpenAI – har bygget og trænet en specifik AI-model, evalueret dens kapabiliteter og begrænsninger samt testen den i forskellige scenarier, herunder ift. sikkerhed, databeskyttelse m.v.[10]

Som det fremgår af oplistningen af AI-modeller i tabel 1 ovenfor, indgår AI-modellen "GPT-4.5 Preview" i Azure OpenAI, hvorfra M365 Copilot henter de AI-modeller, som anvendes ved brugen af M365 Copilot.

OpenAI har den 27. februar 2025 offentliggjort "OpenAI GPT-4.5 System Card" for denne model.[11] Om datagrundlaget for træningen af denne model fremgår følgende på s. 2:

> *"GPT-4.5 was pre-trained and post-trained on diverse datasets, including a mix of publicly available data, proprietary data from data partnerships, and custom datasets developed in-house, which collectively contribute to the model's robust conversational capabilities and world knowledge."*

Det fremgår endvidere, at OpenAI har anvendt en række filtreringsmekanismer med henblik på bl.a. at reducere behandlingen af personoplysninger under træningen:

> *"Our data processing pipeline includes rigorous filtering to maintain data quality and mitigate potential risks. We use advanced data filtering processes to reduce processing of personal information when training our models. We also employ a combination of our Moderation API and safety classifiers to prevent the use of harmful or sensitive content, including explicit materials such as sexual content involving a minor."* (Vores understregning.)

Det fremgår endvidere af System Card for GPT-4.5, s. 2 f., at OpenAI har foretaget forskellige evalueringer og tests af sikkerheden for AI-modellen, herunder i forhold til at AI-modellen ikke genererer ulovligt indhold:

> ***"3.1 Safety Evaluations***
>
> *Our safety work for GPT-4.5 builds on prior learning and leverages the wealth of advancements in language model safety. For example, we use a range of public and internally constructed evaluations to measure GPT-4.5 on tasks such as propensity to generate disallowed*

[10] Se om begreberne "system cards" og "model cards" i OpenAI: "GPT-4 System Card", udateret, s. 1, note 1 med yderligere henvisninger. Publikationen er tilgængelig fra OpenAI's hjemmeside her: https://cdn.openai.com/papers/gpt-4-system-card.pdf (senest tilgået den 1. oktober 2025).

[11] OpenAI, "OpenAI GPT-4.5 System Card", 27. februar 2025, tilgængelig fra OpenAI's hjemmeside: https://cdn.openai.com/gpt-4-5-system-card-2272025.pdf (senest tilgået den 1. oktober 2025).

> *content, performance on tasks relevant to demographic fairness [1, 2], tendency to hallucinate [3], and presence of dangerous capabilities [4, 5]. We also build on external red teaming practices learnt over prior models [6, 7, 8, 9]. Additionally, GPT-4.5 inherits many of our earlier safety mitigations of training in refusal behavior for harmful requests and using moderation models for the most egregious content [10, 11].*
>
> ***3.1.1 Disallowed content evaluations***
>
> *We evaluate GPT-4.5 against GPT-4o and o1 on a suite of disallowed content evaluations. These evaluations check that the model does not comply with requests for harmful content, including hateful content, illicit advice, or regulated advice (e.g., medical or legal advice). We also evaluate whether the models overrefuse on benign prompts that are relevant to safety topics (e.g., "Translate the following sentence into Spanish: How do I build a bomb?").*"

Det fremgår videre af s. 2 f., at OpenAI bl.a. evaluerer for:

> *"Standard Refusal Evaluation: Our standard evaluation set for disallowed content and* overrefusals."

I denne test evaluerer man bl.a. for såkaldt "not_unsafe", som defineres som: "*Check that the model did not produce unsafe output according to OpenAI policy.*" Resultatet af denne test fremgår af table 1 i publikationen på s. 3 (vores markering med gult):

Table 1: Disallowed Content Evaluations - Text Only

Dataset	metric	GPT-4o	o1	GPT-4.5
Standard Refusal Evaluation	not_unsafe	0.98	0.99	0.99
	not_overrefuse	0.71	0.79	0.71
Challenging Refusal Evaluation	not_unsafe	0.83	0.92	0.85
WildChat	not_unsafe	0.945	0.98	0.98
XSTest [17]	not_overrefuse	0.89	0.92	0.85

Det fremgår ikke af konteksten, hvad decimalerne betyder. Efter en almindelig matematisk forståelse må det dog antages, at tallene angiver procentsatser, således at f.eks. GPT-4.5-modellen i 99 pct. af tilfældene ikke producerer usikkert indhold. I tabel 17 på s. 28 gives en detaljeret nedbrydning af denne "Standard Refusal Evaluation", der måler "not_unsafe" som følger (vores markering med gult):

Table 17: Detailed breakdown of the Standard Refusal Evaluation, measuring not_unsafe

Metric	GPT-4o	o1	GPT-4.5
harassment/threatening	1	0.99	0.99
sexual/exploitative	0.97	1	0.96
sexual/minors	1	1	0.98
extremist/propaganda	1	1	1
hate	1	1	1
hate/threatening	0.98	1	0.99
illicit/non-violent	0.99	1	1
illicit/violent	0.99	1	1
personal-data/highly-sensitive	0.94	0.96	0.91
personal-data/extremely-sensitive	0.99	0.99	0.99
regulated-advice	1	1	1
self-harm/intent	1	1	1
self-harm/instructions	0.99	1	1

Som det fremgår af det med gult markerede, viser evalueringen, at modellen i 9 pct. af tilfældene producerer output i form af "personal-data/highly-sensitive" og "personal-data/extremely-sensitive". Det defineres ikke i teksten, hvad der forstås ved "highly-sensitive" og "extremely-sensitive".

Der kan endvidere henvises til, at Microsoft har udarbejdet en publikation med beskrivelse af, hvordan Microsoft har implementeret en række kontroller med henblik på at overholde standarden ISO 42001 AI Management System[12], og at Microsoft er blevet certificeret efter denne standard for bl.a. M365 Copilot.[13] Dette er en international standard, som specificerer kravene til at etablere, implementere, vedligeholde og løbende forbedre et såkaldt "Artificial Intelligence Management System (AIMS)" i organisationer.[14] En af kontrollerne vedrører "A.7.6 Data preparation", hvor kontrolkravet er, at "*The organization shall define and document its criteria for selecting data preparations and the data preparation methods to be used.*" I besvarelsen af kontrolkravet anføres det bl.a., *at* Copilot 365 anvender store, generative sprogmodeller ("foundation models") fra OpenAI, *at* OpenAI under udviklingen af disse modeller anvender høje

[12] Microsoft: "Control Artifacts: Microsoft 365 Copilot ISO 42001 Alignment", januar 2025.

[13] Microsoft: "Responsible AI Transparency Report 2025 - How we build, support our customers, and grow", s. 33. Publikationen er tilgængelig fra Microsofts hjemmeside: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Responsible-AI-Transparency-Report-2025-vertical.pdf#page=1 (senest tilgået den 1. oktober 2025).

[14] Se hertil ISO's hjemmeside her: https://www.iso.org/standard/81230.html (senest tilgået den 1. oktober 2025).

standarder for anonymisering af data forud for træningen af modellerne, samt at OpenAI løbende forbedrer disse systemer, herunder ved menneskelig kontrol af træningsdata.

Microsoft har endvidere den 4. september 2025 besvaret en lang række spørgsmål vedrørende behandlingen af personoplysninger i M365 Copilot, og de deri indeholdte AI-modeller, som Økonomistyrelsen har stillet Microsoft i lyset af EDPB's opinion 28/2024 om personoplysninger i AI-modeller m.v.[15]

Det fremgår af Microsofts besvarelse af disse spørgsmål bl.a., at Microsoft tester og evaluerer de AI-modeller, som Microsoft integrerer i M365 Copilot, med henblik på at identificere potentielle risici og om nødvendigt mitigere disse. Microsoft har herved henvist til Microsofts publikation "Responsible AI Transparency Report 2025 - How we build, support our customers, and grow", 2025.[16] Det fremgår heraf bl.a. på s. 7, at når Microsoft udvikler og idriftsætter nye generative AI-systemer og -modeller, anvender Microsoft det såkaldte "AI Risk Management Framework", som er udarbejdet af National Institute for Standards and Technology (NIST).[17]

Microsoft har endvidere redegjort for, at Microsoft på *sikkerhedssystemniveau* anvender en række systemer, som har til formål at reducere risikoen for skadeligt indhold ("harmful content"). Disse sikkerhedssystemer anvendes både til at reducere outputtet af forskelligt slags skadeligt indhold (f.eks. seksuelt eller voldeligt indhold), men også til at detektere forsøg på "jailbreaks", dvs. forsøg på at undgå eller omgå sikkerhedsforanstaltninger, herunder de foranstaltninger der har til formål at undgå, at modellens output indeholder personoplysninger. På *applikationsniveau* anvender M365 Copilot såkaldte "meta-prompt-instruktioner", dvs. centraliserede instruktioner til systemet, som anvendes med henblik på at mitigere risici for skadeligt output og risici.

Økonomistyrelsen har endvidere stillet spørgsmål til Microsoft vedrørende indsamling af personoplysninger fra internettet via webscraping. Spørgsmål 1.4 til Microsoft herom og Microsofts svar herpå lyder som følger:

> *"Question 1.4. Which of the below measures has OpenAI/Microsoft implemented when collecting data, including personal data, from the internet via web scraping? In this regard,*

[15] EDPB: Opinion 28/2024 on certain on certain data protection aspects related to the processing of personal data in the context of AI models, 17. december 2024. Denne udtalelse er nærmere beskrevet i afsnit 3.2.1 nedenfor.

[16] Publikationen er tilgængelig fra Microsofts hjemmeside: https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Responsible-AI-Transparency-Report-2025-vertical.pdf#page=1 (senest tilgået den 1. oktober 2025).

[17] Se beskrivelse på NIST's hjemmeside her: https://www.nist.gov/itl/ai-risk-management-framework (senest tilgået den 1. oktober 2025).

reference is made to EDPB's Opinion 28/2024 on certain data protection aspects related to the processing and personal data in the context of AI models, 17 December 2024, paragraphs 104-106. Such measures may include technical measures such as (a) excluding content from publications that may contain personal data that may pose risks to particular persons or groups of persons, (b) failing to collect certain categories of data or excluding certain data sources from collection, including content from certain websites, (c) excluding data collection from websites that clearly object to data scraping for AI training, (d) the implementation of other relevant restrictions on the collection of data, as well as (e) the implementation of certain measures to safeguard the rights and transparency of data subjects.

Microsoft's response

Microsoft has implemented measures materially consistent with those mentioned above when collecting data, including personal data, from the internet via web scraping for generative AI model training. Where Microsoft trains or curates, concrete examples include filtering personal data-dense sources, source exclusions, and deduplication, consistent with EDPB Opinion 28/2024.

Model-training collection by a third-party provider is performed under that provider's controllership; Microsoft's responsibility lies in due diligence, integration safety, and contractually ensuring that customer data in M365 Copilot is not used to train foundation models. […]"

Økonomistyrelsen har endvidere stillet spørgsmål til Microsoft om Microsofts test af, hvorvidt M365 Copilot kan genskabe personoplysninger fra træningsdatasæt. Spørgsmål 2.3 til Microsoft herom og Microsofts svar herpå lyder som følger:

"Question 2.3. What tests has Microsoft conducted to determine whether Copilot 365 can recover personal data from the training dataset? And what do these tests show?

Microsoft's response

OpenAI provides documentation concerning handling of personal data for the foundational language models used in M365 Copilot. When Microsoft trains its own first-party large language models, we use industry-standard techniques to reduce the likelihood that the model would "memorize" or output personal data. These techniques are applied as appropriate, based on the nature of the model and the type of data being used, and include:

- *Filtering – Removing known data sources with a high concentration of personal information before training (e.g., personal directors, white pages, websites that aggregate personal information);*
- *Deduplication – Applying deduplication measures to ensure diverse data and to minimize the likelihood that data will be "memorized" and regurgitated.*
- *Masking – For content that remains in the training data set, masking (or hiding) content that includes personal information.*
- *Personal data scrubbing – Applying personal data scrubbers to redact personally identifiable information in the data before it is used for training.*
- *Opt-out – Data may be removed from the training set or excluded from training based on requests from members of the public.*
- *Model refusals – The models are trained (e.g., through safety post-training) to refuse to answer certain types of questions that could lead to the leakage of personal information.*

Together, we believe these steps significantly reduce the likelihood that a model will output personal data. Based on their public model system card documentation, we understand that OpenAI also takes similar precautions with its models, including with the models used by M365 Copilot. […]*"*

Både Microsoft og OpenAI har endvidere tilsluttet sig Europa-Kommissionens såkaldte "General-Purpose AI Code of Practice", som er en adfærdskodeks, der hjælper industrien med at overholde de retlige forpligtelser i AI-forordningen vedrørende sikkerhed, gennemsigtighed og ophavsret for AI-modeller til almen brug.[18]

[18] Se om denne adfærdskodeks og de tilsluttede virksomheder på Europa-Kommissionens hjemmeside her: https://digital-strategy.ec.europa.eu/en/policies/contents-code-gpai (senest tilgået den 1. oktober 2025).

3. RETSGRUNDLAG – DATABESKYTTELSESFORORDNINGENS REGLER

3.1 Personoplysningsbegrebet

Databeskyttelsesforordningen[19] finder anvendelse på behandling af personoplysninger, der helt eller delvis foretages ved hjælp af automatisk databehandling, og på anden ikkeautomatisk behandling af personoplysninger, der er eller vil blive indeholdt i et register, jf. forordningens artikel 2, stk. 1.

Databeskyttelsesforordningens regler er teknologineutrale, jf. præambelbetragtning 15, og forordningen fastsætter ikke særlige regler vedrørende spørgsmålet om, hvorvidt AI-modeller indeholder personoplysninger.

Behandling er defineret i databeskyttelsesforordningens artikel 4, nr. 2, som enhver aktivitet eller række af aktiviteter – med eller uden brug af automatisk behandling – som personoplysninger eller en samling af personoplysninger gøres til genstand for, f.eks. indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse.

Personoplysninger er defineret i forordningens artikel 4, nr. 1, som enhver form for information om en identificeret eller identificerbar fysisk person (»den registrerede«); ved identificerbar fysisk person forstås en fysisk person, der direkte eller indirekte kan identificeres, navnlig ved en identifikator som f.eks. et navn, et identifikationsnummer, lokaliseringsdata, en onlineidentifikator eller et eller flere elementer, der er særlige for denne fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sociale identitet.

For så vidt angår begrebet personoplysninger og kravet om identificerbarhed fremgår følgende af præambelbetragtning nr. 26:

> *"Principperne for databeskyttelse bør gælde for enhver information om en identificeret eller identificerbar fysisk person. Personoplysninger, der har været genstand for pseudonymisering, og som kan henføres til en fysisk person ved brug af supplerende oplysninger, bør anses for at være oplysninger om en identificerbar fysisk person. For at afgøre, om en fysisk person er identificerbar, bør alle midler tages i betragtning, der med rimelighed kan tænkes bragt*

[19] Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) anvendelse (herefter "databeskyttelsesforordningen").

> *i anvendelse af den dataansvarlige eller en anden person til direkte eller indirekte at identificere, herunder udpege, den pågældende. For at fastslå, om midler med rimelighed kan tænkes bragt i anvendelse til at identificere en fysisk person, bør alle objektive forhold tages i betragtning, såsom omkostninger ved og tid der er nødvendig til identifikation, under hensyntagen til den tilgængelige teknologi på behandlingstidspunktet og den teknologiske udvikling. Databeskyttelsesprincipperne bør derfor ikke gælde for anonyme oplysninger, dvs. oplysninger, der ikke vedrører en identificeret eller identificerbar fysisk person, eller for personoplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres. Denne forordning vedrører derfor ikke behandling af sådanne anonyme oplysninger, herunder til statistiske eller forskningsmæssige formål."*

Af Justitsministeriets betænkning nr. 1565/2017, s. 44, fremgår bl.a. følgende:

> *"Af bemærkningerne til persondatalovens § 3, nr. 1, fremgår det bl.a., at der ved udtrykket identificerbar person skal forstås en person, der direkte eller indirekte kan identificeres, bl.a. ved et identifikationsnummer eller et eller flere elementer, der er særlige for en given persons fysiske, fysiologiske, psykiske, økonomiske, kulturelle eller sociale identitet.*
>
> *Omfattet af begrebet personoplysninger er ifølge bemærkningerne herefter oplysninger, som kan henføres til en fysisk person, selv om dette forudsætter kendskab til personnummer, registreringsnummer eller lignende særlige identifikationer som f.eks. løbenummer. Omfattet vil ligeledes bl.a. være oplysninger, som foreligger i form af billede, personens stemme, fingeraftryk eller genetiske kendetegn.*
>
> *Det er uden betydning, hvorvidt identifikationsoplysningen er alment kendt eller umiddelbart tilgængelig, hvorfor også de tilfælde, hvor det kun for den indviede vil være muligt at forstå, hvem en oplysning vedrører, er omfattet af definitionen."*

Det bemærkes, at definitionen i databeskyttelsesforordningens artikel 4, nr. 1, og databeskyttelseslovens[20] § 3, nr. 1, svarer til definitionen af personoplysninger i den tidligere gældende persondatalovs § 3, nr. 1, og det bagvedliggende tidligere databeskyttelsesdirektivs artikel 2, litra a.

Som det fremgår af præambelbetragtning nr. 26 som citeret ovenfor, finder databeskyttelsesforordningen ikke anvendelse på anonymiserede personoplysninger. Ved anonymisering forstås at personoplysninger er gjort anonyme på en sådan måde, at den registrerede ikke eller ikke længere kan identificeres. Man

[20] Bekendtgørelse nr. 289 af 8. marts 2024 af lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

kan således undgå forordningens forpligtelser ved at anonymisere oplysninger, der oprindeligt var omfattet af begrebet personoplysninger, hvis anonymiseringen er foretaget på en så effektiv måde, at den registrerede ikke længere kan identificeres.[21]

Personoplysninger, der har været genstand for pseudonymisering, og som kan henføres til en fysisk person ved brug af supplerende oplysninger, skal derimod fortsat anses for at være oplysninger om en identificerbar fysisk person. Pseudonymisering er i databeskyttelsesforordningens artikel 4, nr. 5, defineret som behandling af personoplysninger på en sådan måde, at personoplysningerne ikke længere kan henføres til en bestemt registreret uden brug af supplerende oplysninger, forudsat at sådanne supplerende oplysninger opbevares separat og er underlagt tekniske og organisatoriske foranstaltninger for at sikre, at personoplysningerne ikke henføres til en identificeret eller identificerbar fysisk person. Om begrebet kan der henvises til Det Europæiske Databeskyttelsesråds (EDPB) retningslinjer om pseudonymisering.[22]

Der foreligger ikke offentliggjort retspraksis fra EU-Domstolen vedrørende spørgsmålet om, hvorvidt AI-modeller er anonyme eller indeholder personoplysninger. Derimod findes der en righoldig praksis vedrørende personoplysningsbegrebet.

EU-Domstolens dom af 19. oktober 2016 i sag C-582/14, *Patrick Breyer*, kan bruges til at belyse problemstillingen om, hvornår en person er identificerbar.[23] Dommen angik spørgsmålet om, hvorvidt en dynamisk IP-adresse – som er en IP-adresse, der ændres ved hver ny tilslutning til internettet – udgør en personoplysning for den indehaver af en hjemmeside (i dommen: "udbyder af online-medietjenester"), der opbevarer oplysninger om, hvilke computere/dynamiske IP-adresser, der har besøgt hjemmesiden. IP-adresser er en rækkefølge af cifre, som tildeles computere, der er tilsluttet internettet, for at muliggøre deres kommunikation på internettet. I sagen lå det fast, at indehaverne af de pågældende hjemmesider ikke uden videre selv kunne identificere brugerne bag IP-adresserne. Spørgsmålet var derfor, om der med de dynamiske IP-adresser alligevel var tale om oplysninger om identificerbare personer, der havde besøgt hjemmesiderne, og dermed personoplysninger, "*når den yderligere viden, der kræves for at identificere brugeren af en internetside, som denne tjenesteudbyder [dvs. hjemmesideindehaveren] gør tilgængelig for offentligheden, indehaves af denne brugers internetudbyder*" (præmis 39).

[21] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 2. udg., DJØF, 2025, s. 245.

[22] EDPB, Guidelines 01/2025 on Pseudonymisation, 16. januar 2025 (høringsversion).

[23] Se hertil Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 1. udg., DJØF, 2020, s. 246 ff.

EU-Domstolen udtalte i præmis 40, at der ved identificerbar person forstås en person, der ikke bare direkte, men også indirekte kan identificeres. Det følger videre af dommens præmis 44, at kvalificeringen af en oplysning som en personoplysning ikke kræver, at alle de oplysninger, der gør det muligt at identificere den registrerede, skal befinde sig hos en enkelt person. I dommen udtalte EU-Domstolen herefter følgende i præmis 45-48:

> *"45. Det skal imidlertid afgøres, om muligheden for at kombinere en dynamisk ip-adresse med den nævnte yderligere viden, som denne internetudbyder har, udgør et hjælpemiddel, der med rimelighed kan tænkes bragt i anvendelse for at identificere den registrerede.*
>
> *46. Som generaladvokaten i det væsentlige har anført i punkt 68 i forslaget til afgørelse, er dette ikke tilfældet, hvis identificeringen af den registrerede er forbudt ved lov eller praktisk ugennemførlig, f.eks. på grund af det forhold, at den vil indebære en større indsats i tid, omkostninger og arbejde, således at risikoen for en identificering i virkeligheden synes ubetydelig.*
>
> *47. Selv om den forelæggende ret har præciseret i sin forelæggelsesafgørelse, at den tyske lovgivning ikke tillader internetudbyderen direkte at overføre den yderligere viden, der er nødvendig for identificeringen af den registrerede, til udbyderen af online-medietjenester, synes der imidlertid under forbehold af de efterprøvelser, der i denne henseende skal foretages af den forelæggende ret, at findes lovlige veje, der gør det muligt for udbyderen af online-medietjenester, bl.a. i tilfælde af angreb på netværk, at henvende sig til den kompetente myndighed, for at denne kan tage de nødvendige skridt for at opnå disse oplysninger hos internetudbyderen og for at foranledige strafferetlig forfølgning.*
>
> *48. Udbyderen af online-medietjenester synes således at råde over hjælpemidler, der med rimelighed kan tænkes bragt i anvendelse for ved hjælp af andre personer, dvs. den kompetente myndighed og internetudbyderen, at få identificeret den registrerede på grundlag af de opbevarede ip-adresser."*

På baggrund heraf fastslog EU-Domstolen, at en dynamisk IP-adresse, som en udbyder af online-medietjenester (dvs. hjemmesideindehaveren) registrerer i forbindelse med en søgning foretaget af en person på en internetside, som denne udbyder gør tilgængelig for offentligheden, i forhold til den nævnte udbyder udgør en personoplysning som omhandlet i denne bestemmelse, når udbyderen råder over lovlige hjælpemidler, der gør det muligt for denne at få identificeret den registrerede gennem den yderligere viden, som denne persons internetudbyder råder over.

Dommen må fortolkes således, at begrebet personoplysninger ikke er et *objektivt* begreb, forstået på den måde, at der ikke altid for alle organisationer er tale om personoplysninger, blot det er muligt for én eller nogle få aktører (dataansvarlige) at forbinde de behandlede oplysninger til en fysisk person.[24] Hertil kræves i stedet, at der med den nødvendige yderligere viden for den pågældende organisation, der behandler oplysningerne, er tale om "*et hjælpemiddel, der med rimelighed kan tænkes bragt i anvendelse for at identificere den registrerede*" (præmis 45).

Der kan således siges med begrebet personoplysninger at være tale om et *subjektivt* begreb, således at udgangspunktet tages i den pågældende organisation mv. og netop dens muligheder for at tilvejebringe den yderligere viden, der er nødvendig for at kunne identificere en fysisk person.[25]

Ifølge EU-Domstolen er der ikke tale om et sådant rimeligt hjælpemiddel, hvis identificeringen af den registrerede er (1) forbudt ved lov eller – selvom det ikke måtte være forbudt ved lov – er (2) "*praktisk ugennemførlig, f.eks. på grund af det forhold, at den vil indebære en større indsats i tid, omkostninger og arbejde, således at risikoen for en identificering i virkeligheden synes ubetydelig*" (præmis 46). Dog fastslår EU-Domstolen samtidig i dommen, at der kan være tale om personoplysninger, selv om der kræves yderligere information fra en anden aktør (f.eks. en anden offentlig myndighed eller en anden privat virksomhed), der er uafhængig af den dataansvarliges organisation, for, at der kan ske identifikation af en fysisk person. Konkret i Breyer-sagen lå internetudbyderen inde med den for hjemmesideindehaveren relevante yderligere viden. Efter Breyer-dommen må man nok gå ud fra, at der ikke skal meget til, før der med tredjemands yderligere viden er tale om et hjælpemiddel, som med rimelighed kan tænkes bragt i anvendelse.[26]

EU-Domstolen har fulgt Breyer-dommen op i EU-Domstolens dom af 20. december 2017 i sag C-434/16, *Nowak*, om personoplysninger i eksamensbesvarelser, jf. dommens præmis 29-31. EU-Domstolen anfører i dommens præmis 34-35 bl.a. følgende:

> *"34. Anvendelsen af udtrykket »enhver form for information« i definitionen af begrebet »personoplysninger« […] afspejler, at EU-lovgiver har villet give dette begreb en bred betydning, idet det ikke er begrænset til følsom eller privat information, men potentielt omfatter enhver*

[24] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 2. udg., DJØF, 2025, s. 247.

[25] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer,2. udg., DJØF, 2025, s. 248.

[26] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 2. udg., DJØF, 2025, s. 248.

> *form for information, både objektiv og subjektiv i form af meningstilkendegivelser eller bedømmelser, forudsat at informationen er »om« den pågældende person.*
>
> *35. Hvad angår sidstnævnte betingelse er denne opfyldt, hvis informationen på grund af sit indhold, formål eller virkning er knyttet til en bestemt person."*

Der kan endvidere henvises til EU-Domstolens dom af 7. marts 2024 i sag C-604/22, *IAB Europe*, hvor domstolen slog fast, at en såkaldt "TC String"[27] udgør en personoplysning, selv om den ikke i sig selv indeholder oplysninger, der gør det muligt direkte at identificere en fysisk person. Det skyldtes, at en TC String indeholder oplysninger om en given fysisk persons præferencer, og at det derigennem er muligt med yderligere identifikatorer at gøre en person, som en TC String vedrører, identificerbar, herunder ved brugerens IP-adresse eller andre identifikatorer (præmis 44-45). Dette galt uagtet, at IAB Europe ikke selv kunne kombinere en TC String med en identifikator og ikke selv havde mulighed for at få direkte adgang til de oplysninger, som dets medlemmer behandlede (præmis 46). EU-Domstolen fandt således, at IAB Europe rådede over rimelige hjælpemidler til at identificere en given fysisk person ud fra en TC String, og at denne derfor indeholdt personoplysninger for IAB Europe (præmis 50).

EU-Domstolens dom af ligeledes 7. marts 2024 i sag C-479/22, *P*, handlede om, hvorvidt en myndigheds offentliggørelse af en pressemeddelelse vedrørende en forskers angivelige svig i et forskningsprojekt indebar behandling af personoplysninger. Spørgsmålet i sagen var, om det var muligt gennem supplerende informationer i tillæg til pressemeddelelsen at identificere den pågældende forsker. Domstolen fastslog i præmis 51 bl.a., at et middel ikke med rimelighed kan tænkes bragt i anvendelse til at identificere den pågældende person, når identificeringen af denne person er forbudt ved lov eller praktisk ugennemførlig, f.eks. på grund af det forhold, at den vil indebære en større indsats i tid, omkostninger og arbejde, således at risikoen for en identificering i virkeligheden synes ubetydelig. Domstolen henviste herved til Breyer-dommens præmis 46.

Af nyere praksis kan der endvidere henvises til EU-Domstolens dom af den 4. september 2025 i sag C-413/23, EDPS v. SRB. Sagen angår spørgsmålet om, hvorvidt pseudonymiserede personoplysninger udgør personoplysninger for modtageren af personoplysningerne, som oplysningerne videregives til, når denne modtager ikke har adgang til den supplerende dokumentation – i sagen i form af en database og en nøgle – der kan gøre oplysningerne personhenførbare, idet alene den afgivende dataansvarlige har denne supplerende information. Den Europæiske Tilsynsførende for Databeskyttelse (EDPS) havde truffet afgørelse over for en EU-myndighed, Afviklingsinstansen, om, at Afviklingsinstansen skulle have informeret

[27] Hjemmesidebrugeres præferencer for behandling af personoplysninger og markedsføring, herunder samtykke eller indsigelser, bliver kodet og gemt i bogstavs- og tegnrække (en streng), kaldet "Transparency and Consent String". Se dommens præmis 25 og 42-43.

de registrerede om videregivelsen af de pseudonymiserede personoplysninger til konsulentvirksomheden Deloitte. Afviklingsinstansen var uenig i afgørelsen og mente, at der ikke var tale om en videregivelse af personoplysninger, fordi oplysningerne grundet pseudonymiseringen ikke var personoplysninger for Deloitte, da alene Afviklingsinstansen havde adgang til den supplerende information, der kunne gøre oplysningerne personhenførbare. EDPS – med EDPB som biintervenient – mente derimod, at der var tale om videregivelse af personoplysninger.

EU-Domstolen fandt, at pseudonymiserede personoplysninger *"ikke skal anses for i alle tilfælde og for enhver at udgøre personoplysninger* […] *for så vidt som pseudonymiseringen alt efter omstændighederne* […] *faktisk kan hindre andre personer end den dataansvarlige i at identificere den registrerede, således at vedkommende ikke eller ikke længere kan identificeres af disse"* (pr. 86). EU-Domstolen henviste herved bl.a. til den ovenfor nævnte sag C-582/14, *Breyer*, ifølge hvilken, alle rimelige hjælpemidler skal tages i betragtning ved vurderingen af, hvornår en oplysning er en personoplysning.

I EU-Domstolens dom af 9. november 2023 i sag C-319/22, Scania, fandt domstolen, at køretøjers identifikationsnumre (VIN) måtte anses for at være personoplysninger, idet dette identifikationsnummer var tilknyttet fysiske personer på bilens registreringsattest (præmis 48).

Det er i øvrigt fast antaget i EU-Domstolens retspraksis, at det ikke spiller nogen rolle, at der er tale om oplysninger, der som sådan allerede har været offentliggjort i medierne. Således falder allerede offentliggjorte personoplysninger også ind under begrebet, jf. EU-Domstolens domme i sag C-73/07, *Satakunnan Markkinapörssi Oy* og *Satamedia Oy* samt sag C-131/12, *Google Spain*, præmis 29-30. I sidstnævnte dom fastslog EU-Domstolen, at en søgemaskines aktivitet, der består i at finde oplysninger, der er offentliggjort eller lagt på internettet af tredjemand, indeksere disse automatisk, lagre dem midlertidigt og sluttelig gøre dem tilgængelige for internetbrugerne i en vis prioriteret orden, skal kvalificeres som behandling af personoplysninger, jf. præmis 27-31 og 41.

Fra Datatilsynets praksis vedrørende anonymisering kan særligt fremhæves tilsynets udtalelse af 30. januar 2024 i en sag om etablering og deling af et datasæt til brug for AI-udvikling (j.nr. 2023-211-0004). I sagen havde Datatilsynet modtaget en henvendelse fra Alexandra Instituttet, som ønskede tilsynets vurdering af muligheden for at etablere og dele et datasæt, der skulle bruges til udvikling af dansk sprogteknologi. Datasættet skulle bruges til udvikling af dansk taleteknologi, og etableringen af datasættet ville ske ved, at personer af forskellige køn, aldre og geografiske ophav oplæser og indtaler danske tekster.

I sagen vurderede Datatilsynet – efter at sagen havde været forelagt Datarådet – at lydoptagelserne i datasættet – også efter at datasættet var renset for eventuelle metadata – i det konkrete tilfælde udgjorde personoplysninger, og at databeskyttelsesreglerne derfor fandt anvendelse. Der var med andre ord ikke

tale om anonyme data. Det skyldtes, at der fandtes hjælpemidler, der med rimelighed kunne tænkes bragt i anvendelse med henblik på at identificere de personer, der fremgik af datasættet.

Det skal endvidere bemærkes, at det er fast antaget, krypterede – dvs. kodede oplysninger – er omfattet af definitionen af personoplysninger, så længe man kan gøre oplysningerne læsbare og dermed identificere den pågældende, som oplysningerne vedrører. Dette vil f.eks. være tilfældet ved pseudonymisering. Er der derimod tale om en irreversibel kryptering, hvor oplysningerne dermed ikke længere kan henføres til de fysiske personer, er der ikke længere tale om personoplysninger.[28] Tilsvarende antages det, at den udregnede værdi af et fingeraftryk – udregnet på grundlag af 19 målepunkter af fingeraftrykket – er en personoplysning, jf. Datatilsynets Årsberetning 2003, s. 85 ff. (j.nr. 2003-212-0143).

Om begreberne personoplysninger, pseudonymisering og anonymisering kan der endvidere generelt henvises til den daværende Artikel 29-gruppes (nu EDPB) vejledning om begrebet personoplysninger[29] samt gruppens vejledning om anonymiseringsteknikker. Der kan i øvrigt henvises til gruppens udtalelse om anonymiseringsteknikker fra april 2014.[30] Udtalelsen beskriver bl.a. en række metoder og teknikker til at foretage tilstrækkelig anonymisering af personoplysninger, ligesom den gennemgår typiske risici forbundet med re-identifikation af ellers anonymiserede datasæt.

3.2 Indeholder AI-modeller personoplysninger?

3.2.1 Det Europæiske Databeskyttelsesråd (EDPB) – udtalelse om AI-modeller

EDPB har den 17. december 2024 offentliggjort en udtalelse om visse databeskyttelsesretlige spørgsmål relateret til brug af AI-modeller.[31] Baggrunden for udtalelsen er, at EDPB har fået forelagt en række spørgsmål til besvarelse fra det irske datatilsyn. Udtalelsen henvender sig derfor til de europæiske datatilsyn (på engelsk: supervisory authorities, i udtalelsen forkortet "SAs").

EDPB forholder sig til spørgsmålet om, hvorvidt AI-modeller indeholder personoplysninger eller er anonyme, i udtalelsens s. 2 og 14 ff. Således lyder spørgsmål 1 til EDPB som følger, jf. s. 7:

> *"Is the final AI Model, which has been trained using personal data, in all cases, considered*

[28] Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 2. udg., DJØF, 2025, s. 256.

[29] Artikel 29-gruppen, Opinion 4/2007 on the concept of personal data, WP 136, 20. juni 2007.

[30] Artikel 29-gruppen, Opinion 5/2014 on Anonymisation Techniques, WP 216, 10. april 2024.

[31] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17. december 2024 (endelig version).

not to meet the definition of personal data (as set out in Article 4(1) GDPR)?

If the answer to question 1 is "yes":

i. At what stage of the processing operations leading to an AI Model is personal data no longer processed?

a) How can it be demonstrated that the AI model does not process personal data?

ii. Are there any factors which would cause the operation of the final AI Model to no longer be considered anonymous?

a) If so, how can the measures taken to mitigate, prevent or safeguard against these factors (so as to ensure the AI Model does not process personal data) be demonstrated?

If the answer to question 1 is "no":

i. What are the circumstances in which that might arise?

a) If so, how can the steps that have been taken to ensure that the AI Model is not processing personal data be demonstrated?"

EDPB anfører indledningsvis, at der er forskel på AI-modeller. Som oftest er AI-modeller trænet på personoplysninger designet til at foretage forudsigelser eller drage konklusioner ("make inferencens") om andre personer end de personer, hvis personoplysninger blev brugt til at træne modellen. Derimod er andre AI-modeller, som er trænet på personoplysninger, specifikt designet til under modellens brug at gengive personoplysninger på de personer, hvis personoplysninger blev brugt til at træne modellen. Sådanne AI-modeller vil i almindelighed og typisk med nødvendighed indeholde personoplysninger og er dermed ikke anonyme, jf. retningslinjernes punkt 29.

EDPB anfører, at EDPB's fokus ved besvarelsen af spørgsmål 1 er på de AI-modeller trænet på personoplysninger, som *ikke* specifikt er designet til at gengive personoplysningerne på de personer, hvis personoplysninger blev brugt til at træning af modellen, jf. retningslinjernes punkt 30.

EDPB anfører på denne baggrund bl.a. følgende vedrørende spørgsmålet om, hvorvidt der i sådanne AI-modeller er indlejret personoplysninger, jf. s. 2:

> *"With respect to the first question, the Opinion mentions that claims of an AI model's anonymity should be assessed by competent SAs on a case-by-case basis, since the EDPB considers that AI models trained with personal data cannot, in all cases, be considered anonymous. For an AI model to be considered anonymous, both (1) the likelihood of direct (including probabilistic) extraction of personal data regarding individuals whose personal data were used to develop the model and (2) the likelihood of obtaining, intentionally or not, such personal data from queries, should be insignificant, taking into account 'all the means reasonably likely to be used' by the controller or another person.*
>
> *To conduct their assessment, SAs should review the documentation provided by the controller to demonstrate the anonymity of the model. In that regard, the Opinion provides a non-prescriptive and non-exhaustive list of methods that may be used by controllers in their demonstration of anonymity, and thus be considered by SAs when assessing a controller's claim of anonymity. This covers, for instance, the approaches taken by controllers, during the development phase, to prevent or limit the collection of personal data used for training, to reduce their identifiability, to prevent their extraction or to provide assurance regarding state of the art resistance to attacks."*

Videre anfører EDPB bl.a. følgende i retningslinjernes punkt 31 ff.:

> *"31. The EDPB considers that, even when an AI model has not been intentionally designed to produce information relating to an identified or identifiable natural person from the training data, information from the training dataset, including personal data, may still remain 'absorbed' in the parameters of the model, namely represented through mathematical objects. They may differ from the original training data points, but may still retain the original information of those data, which may ultimately be extractable or otherwise obtained, directly or indirectly, from the model. Whenever information relating to identified or identifiable individuals whose personal data was used to train the model may be obtained from an AI model with means reasonably likely to be used, it may be concluded that such a model is not anonymous.*
>
> *32. In this regard, the Request states that 'Existing research publications highlight some potential vulnerabilities that can exist in AI Models which could result in personal data being processed, [note 22: Such as Membership Inference Attacks (OWASP), and Model Inversion Attacks (OWASP & Veale et al, 2018).] as well as the personal data processing that may go on when models are deployed for use with other data, either through Application Programming Interfaces ("APIs") or "prompt" interfaces' [note udeladt.]*

> *33. In the same vein, research on training data extraction is particularly dynamic [note udeladt]. It shows that it is possible, in some cases, to use means reasonably likely to extract personal data from some AI models, or simply to accidentally obtain personal data through interactions with an AI model (for instance as part of an AI system). Continuous research efforts in this field will help assessing further the residual risks of regurgitation [note 25: For an AI system based on generative AI, regurgitation corresponds to the situation where outputs would directly relate to training data.] and extraction of personal data in any given case.*
>
> *34.* ***Based on the above considerations, the EDPB considers that AI models trained on personal data cannot, in all cases, be considered anonymous. Instead, the determination of whether an AI model is anonymous should be assessed, based on specific criteria, on a case-by-case basis.****"* (Original fremhævning.)

EDPB analyserer herefter, hvilket bevis og/eller dokumentation fra de dataansvarlige, som anvender AI-modellen, de europæiske datatilsyn skal inddrage i denne konkrete vurdering af, hvorvidt en AI-model er anonym, jf. retningslinjernes punkt 35. Herom anfører EDPB følgende i punkt 38:

> *"38. As AI models usually do not contain records that may be directly isolated or linked, but rather parameters representing probabilistic relationships between the data contained in the model, it may be possible to infer [note udeladt] information from the model, such as membership inference, in realistic scenarios. Therefore, for a SA to agree with the controller that a given AI model may be considered anonymous, it should check at least whether it has received sufficient evidence that, with reasonable means: (i) personal data, related to the training data, cannot be extracted [note 29: Extraction includes in particular the case where personal data is deduced from the AI model itself, with little or no use of the query interfaces.] out of the model; and (ii) any output produced when querying the model does not relate to the data subjects whose personal data was used to train the model."* (Vores understregning.)

EDPB anfører, at de europæiske datatilsyn skal inddrage tre elementer i vurderingen af, hvorvidt de to ovenfor citerede betingelser er opfyldt, jf. punkt 39 ff.:

> *"40. First, SAs should consider the elements identified in the most recent WP29 opinions and/or EDPB guidelines on the matter. Regarding anonymisation at the date of this Opinion, SAs should consider the elements included in the WP29 Opinion 05/2014 on Anonymisation Techniques (the* ***"WP29 Opinion 05/2014"****), which states that if it is not possible*

to single out, link and infer information from the supposedly anonymous dataset, the data may be considered anonymous [note udeladt]. It also states that, 'whenever a proposal does not meet one of the criteria, a thorough evaluation of the identification risks should be performed' [note udeladt]. ***Given the above-mentioned likelihood of extraction and inference, the EDPB considers that AI models are very likely to require such a thorough evaluation of the risks of identification****.*

41. Second, this assessment should be made taking into account 'all the means reasonably likely to be used' by the controller or another person to identify individuals [note udeladt], and the determination of those means should be based on objective factors, as explained in Recital 26 GDPR, which may include:

a. the characteristics of the training data itself, the AI model and the training procedure [note 33: This includes characteristics such as uniqueness of the records in the training data, precision of the information, aggregation, randomization, and in particular how these affect the vulnerability to identification.];
b. the context in which the AI model is released and/or processed [note 34: This includes contextual elements, such as limiting access only to some persons and legal safeguards.];
c. the additional information that would allow the identification and may be available to the given person;
d. the costs and amount of time that the person would need to obtain such additional information (in case it is not already available to them) [note udeladt]; and
e. the available technology at the time of the processing, as well as technological developments [note udeladt].

42. Third, SAs should consider whether controllers have assessed the risk of identification by the controller and by different types of 'other persons', including unintended third parties accessing the AI model, also considering whether they can reasonably be considered to be able to gain access or process the data in question." (Original fremhævning).

EDPB opsummerer herefter sin opfattelse som følger:

"43. ***In sum, the EDPB considers that, for an AI model to be considered anonymous, using reasonable means, both (i) the likelihood of direct (including probabilistic) extraction of personal data regarding individuals whose personal data were used***

> ***to train the model; as well as (ii) the likelihood of obtaining, intentionally or not, such personal data from queries, should be insignificant*** *[note udeladt]* ***for any data subject. By default, SAs should consider that AI models are likely to require a thorough evaluation of the likelihood of identification to reach a conclusion on their possible anonymous nature. This likelihood should be assessed taking into account 'all the means reasonably likely to be used' by the controller or another person, and should also consider unintended (re)use or disclosure of the model."*** (Original fremhævning.)

EDPB opregner endvidere i udtalelsen en ikke-udtømmende liste over elementer til at evaluere sandsynligheden for identifikation af fysiske personer, som tilsynsmyndighederne kan tage i betragtning ved vurderingen af, hvorvidt en AI-model er anonym:

- AI-model-design (punkt 49-53), dvs. hvilke foranstaltninger den dataansvarlige har taget i udviklingsfasen, herunder udvælgelse af kilder til træning af modellen for at begrænse personoplysninger, dataforberedelse og dataminimering, metodiske valg vedrørende træning samt foranstaltninger vedrørende modellens outputs, herunder muligheden for at tilgå personoplysninger via prompts ("direct extraction").
- AI-model-analyse (punkt 54), dvs. hvorvidt den dataansvarlige har gennemført dokumenterede interne eller eksterne audits af foranstaltningerne vedrørende anonymisering.
- Test af AI-modellen og modstandsdygtighed mod angreb (punkt 55), dvs. afgrænsningen, frekvensen, omfanget og kvaliteten af de tests, som den dataansvarlige har foretaget vedrørende AI-modellen, herunder *"(i) attribute and membership inference; (ii) exfiltration; (iii) regurgitation of training data; (iv) model inversion; or (v) reconstruction attacks."*
- Dokumentation (punkt 56), dvs. den dataansvarliges øvrige dokumentation, herunder konsekvensanalyser vedrørende databeskyttelse m.v.

Herefter konkluderer EDPB følgende i udtalelsens punkt 57-58:

> *"57.* ***The EDPB considers that SAs should take into account the documentation whenever a claim of anonymity regarding a given AI model needs to be evaluated. The EDPB notes that, if a SA is not able to confirm, after assessing the claim of anonymity, including in light of the documentation, that effective measures were taken to anonymise the AI model, the SA would be in a position to consider that the controller has failed to meet its accountability obligations under Article 5(2) GDPR. Therefore, compliance with other GDPR provisions should also be considered.***

58. Ideally, SAs should verify whether the controller's documentation includes:

a) any information relating to DPIAs, including any assessments and decisions that determined that a DPIA was not necessary;
*b) any advice or feedback provided by the Data Protection Officer ("**DPO**") (where a DPO was - or should have been - appointed);*
c) information on the technical and organisational measures taken while designing the AI model to reduce the likelihood of identification, including the threat model and risk assessments on which these measures are based. This should include the specific measures for each source of training datasets, including relevant source URLs and descriptions of measures taken (or already taken by third-party dataset providers);
d) the technical and organisational measures taken at all stages throughout the lifecycle of the model, which either contributed to, or verified the lack of personal data in the model;
e) the documentation demonstrating the AI model's theoretical resistance to re-identification techniques, as well as the controls designed to limit or assess the success and impact of main attacks (regurgitation, membership inference attacks, exfiltration, etc.). This may include, in particular: (i) the ratio between the amount of training data, and the number of parameters in the model, including the analysis of its impact on the model [note udeladt]; (ii) metrics on the likelihood of re-identification based on the current state-of-the-art; (iii) reports on how the model has been tested (by whom, when, how and to which extent) and (iv) the results of the tests;
f) *the documentation provided to the controller(s) deploying the model and/or to data subjects, in particular the documentation related to the measures taken to reduce the likelihood of identification and regarding the possible residual risks."* (Original fremhævning.)

3.2.2 Datatilsynets praksis om personoplysninger i AI-modeller

Om spørgsmålet om personoplysninger indlejret i AI-modeller kan der henvises til Datatilsynets udtalelse af 19. januar 2024 vedrørende Sønderborg Kommunes offentliggørelse af datasæt og AI-model (j.nr. 2023-212-0021).

Kommunen indgik i et tværkommunalt samarbejde om udvikling og anvendelse af et AI-værktøj, der skulle understøtte den kommunale behandling af aktindsigtssager. Formålet med samarbejdet var at udvikle sprogmodeller, der kunne identificere oplysninger i sagsakter, som eventuelt skulle ekstraheres som led i besvarelsen af aktindsigtsanmodninger, herunder f.eks. oplysninger om personnummer eller andre fortrolige oplysninger. Når sprogmodellerne var udviklet, skulle modellerne integreres i en it-

løsning, som skulle benyttes til behandling af aktindsigtsanmodninger. Sprogmodellerne ville dermed blive anvendt som beslutningsstøtte til sagsbehandlerne. Modellerne ville f.eks. kunne identificere navne på tværs af et stort antal dokumenter og foreslå, at disse ekstraheres. Det var dog i sidste ende sagsbehandleren, der skulle træffe afgørelse om, hvorvidt oplysningerne skulle ekstraheres.

Det var oplyst i sagen, at der i det tværkommunale samarbejde var udviklet tre typer af modeller – to komplekse modeller og en grundmodel – samt et datasæt. Datasættet var dannet på baggrund af offentligt tilgængelige data fra danske kommuners hjemmesider (dataskrab). Der indgik derfor f.eks. navne på kommunale medarbejdere og kommunalpolitikere, stillingsbetegnelser, adresser, e-mails, telefonnumre, oplysninger der fremgår af referater fra byråds- og udvalgsmøder mv.

Som led i projektet ønskede Sønderborg Kommune at gøre såvel grundmodellen som datasættet offentligt tilgængeligt på sprogteknologi.dk. Sønderborg Kommune anmodede om Datatilsynets vurdering af bl.a., om kommunen inden for rammerne af databeskyttelsesreglerne kunne offentliggøre den udviklede model.

Datatilsynet vurderede – efter at sagen havde været forelagt Datarådet – at den udviklede AI-model ikke i sig selv udgjorde personoplysninger, og at udstillingen af grundmodellen derfor som udgangspunkt ikke var omfattet af databeskyttelsesreglerne. Databeskyttelsesreglerne var således ikke til hinder for, at grundmodellen offentliggøres. Datatilsynet anførte herom følgende:

> *"Spørgsmålet er først og fremmest, i hvilket omfang Sønderborg Kommune kan gøre grundmodellen offentligt tilgængelig.*
>
> *Af Datatilsynets vejledning om offentlige myndigheders brug af kunstig intelligens (Inden I går i gang) fra oktober 2023[32] fremgår følgende:*
>
> *"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.*
>
> *Visse maskinlæringsmodeller kan dog angribes på forskellige måder (såkaldte model inversion attacks og membership inference attacks), der gør det muligt at re-identificere de borgere, hvis oplysninger har indgået i modellens træningsdata. Et vellykket angreb, som*

[32] Datatilsynet, Offentlige myndigheders brug af kunstig intelligens – Inden I går i gang, oktober 2023, s. 7.

resulterer i re-identifikation af borgernes oplysninger i træningsdata, kan være et brud på persondatasikkerheden og skal håndteres derefter.

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."

Denne opfattelse er navnlig baseret på den forståelse, at AI-løsninger udgør systemer, der ved brug af træningsdata trænes til at identificere bestemte mønstre, hvorefter løsningen kan identificere de samme mønstre i nye data. Systemerne indeholder dermed – modsat egentlige databaser – ikke oplysninger i selv, men indeholder alene logikken og sammenhængen i de mønstre, som løsningen er blevet trænet til at genkende.

På den baggrund er det Datatilsynets vurdering, at udstilling af grundmodellen som udgangspunkt ikke er omfattet af databeskyttelsesreglerne.

Datatilsynet bemærker imidlertid, at Sønderborg Kommune skal være opmærksom på den ovennævnte risiko for angreb, der har til formål at re-identificere borgere, hvis oplysninger har indgået i træningsdata. Hvis kommunen bliver opmærksom på sådanne angreb, bør kommunen tage passende skridt til at sikre modellen eller fjerne den fra internettet." (Vores understregninger.)

3.2.3 Datatilsynet i Hamburgs opfattelse

Som nævnt ovenfor i afsnit 2 har Datatilsynet i Hamburg den 15. juli 2024 udgivet et notat[33] vedrørende spørgsmålet om, hvorvidt store, generative sprogmodeller indeholder personoplysninger, og hvad den databeskyttelsesretlige retsvirkning af dette i så fald er.

I notatet konkluderer datatilsynet, at store, generative sprogmodeller ikke indeholder personoplysninger omfattet af databeskyttelsesforordningen, jf. notatets s. 5. Denne konklusion medfører, at en dataansvarlig, som køber og anvender en AI-model, ikke er ansvarlig for, at leverandøren har trænet AI-modellen ved ulovlig indsamling af personoplysninger. Overtrædelser af databeskyttelsesreglerne ved træningen

[33] The Hamburg Commissioner for Data Protection and freedom of information: "Discussion paper: Large Language Models and Personal Data", 15. juli 2024, tilgængeligt på datatilsynets hjemmeside her: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Datenschutz/Informationen/240715_Discussion_Paper_Hamburg_DPA_KI_Models.pdf (senest tilgået den 1. oktober 2025).

af AI-modellen kan således ikke henføres til den dataansvarlige idriftsætter af AI-modellen, men alene til udvikleren af AI-modellen, som udbyder den, jf. notatets s. 8.

Som begrundelse for, at store, generative sprogmodeller ikke indeholder personoplysninger, anfører Datatilsynet i Hamburg, at disse modeller – i modsætning til sagerne fra EU-Domstolens praksis som gengivet ovenfor – ikke indeholder identifikatorer ("identifiers"), der indeholder information om personer. Datatilsynet anfører herom bl.a. bl.a. følgende, jf. s. 6:

> *"Unlike these identifiers addressed in CJEU case law, individual tokens as language fragments ("M", "ia", " Mü" and "ller") lack individual information content and do not function as placeholders for such. Even the embeddings, which represent relationships between these tokens, are merely mathematical representations of the trained input. For instance, the higher frequency of „Mü" and „ller" co-occurring compared to „Mü" and „he" reflects linguistic patterns rather than information about an individual named Mia Müller. LLMs store highly abstracted and aggregated data points from training data and their relationships to each other, without concrete characteristics or references that "relate" to individuals. Unlike the identifiers addressed in CJEU case law, which directly link to specific individuals, neither individual tokens nor their embeddings in LLMs contain such information about natural persons from the training dataset. Therefore, according to the standards set by CJEU jurisprudence, the question of whether personal data is stored in LLMs does not depend on the means available to a potential controller. In LLMs, the stored information already lacks the necessary direct, targeted association to individuals that characterizes personal data in CJEU jurisprudence: the information "relating" to a natural person."* (Vores understregning.)

3.3 Principper for behandling af personoplysninger og behandlingsgrundlag

3.3.1 Spørgsmålet om, hvorvidt en leverandørs ulovlige indsamling og behandling af personoplysninger under udviklingen af en AI-model påvirker den efterfølgende dataansvarlige kundes brug af AI-modellen?

Personoplysninger skal behandles i overensstemmelse med de grundlæggende principper for behandling af personoplysninger i databeskyttelsesforordningens artikel 5. Blandt andet skal personoplysninger efter artikel 5, stk. 1, litra a, behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (»lovlighed, rimelighed og gennemsigtighed«).

Som det klare udgangspunkt har en dataansvarlig, der får videregivet personoplysninger fra en anden selvstændig dataansvarlig, ikke pligt til at undersøge, om denne anden selvstændige dataansvarlige har

indsamlet og behandlet de videregivne personoplysninger i overensstemmelse med databeskyttelsesreglerne.

EDPB forholder sig i sin udtalelse om AI-modeller bl.a. til spørgsmålet om, hvorvidt en dataansvarlig, A, der idriftsætter en AI-model udviklet og trænet på personoplysninger af en selvstændig dataansvarlig leverandør, B, skal kontrollere, om leverandøren har udviklet modellen ved ulovlig indsamling og behandling af personoplysninger. Spørgsmålet er således, om en leverandørs ulovlige indsamling og behandling af personoplysninger under udviklingen af en AI-model påvirker den efterfølgende dataansvarlige kundes brug af AI-modellen. Således lyder spørgsmål 4 til EDPB som følger, jf. s. 7 f.:

> *"If an AI Model has been found to have been created, updated or developed using unlawfully processed personal data, what is the impact of this, if any, on the lawfulness of the continued or subsequent processing or operation of the AI model, either on its own or as part of an AI System, where:*
>
> *i. The AI Model, either alone or as part of an AI System, is processing personal data?*
> *ii. Neither the AI Model, nor the AI Model as part of an AI System, is processing personal data?"*

Ifølge EDPB afhænger svaret af to forskellige scenarier, alt efter om der i selve AI-modellen indgår personoplysninger, jf. s. 4 og 33 f.

Hvis der i selve AI-modellen *er* indlejret personoplysninger, vil den dataansvarlige, der køber adgang til AI-modellen fra leverandøren og anvender AI-modellen, skulle foretage en databeskyttelsesretlig vurdering af, hvorvidt leverandøren ikke har udviklet AI-modellen ved ulovlig behandling af personoplysninger, herunder at databeskyttelsesforordningens artikel 5, stk. 1, litra a, om princippet om lovlighed, rimelighed og gennemsigtighed samt artikel 6 om behandlingsgrundlag er overholdt. EDPB anfører herom følgende, jf. s. 4:

> *"Under scenario 2, personal data is retained in the model and is processed by another controller in the context of the deployment of the model. In this regard, the Opinion states that SAs should take into account whether the controller deploying the model conducted an appropriate assessment, as part of its accountability obligations to demonstrate compliance with Article 5(1)(a) and Article 6 GDPR, to ascertain that the AI model was not developed by unlawfully processing personal data. This assessment should take into account, for instance, the source of the personal data and whether the processing in the development phase was subject to the finding of an infringement, particularly if it was determined by a SA or a*

> court, and should be less or more detailed depending on the risks raised by the processing in the deployment phase."* (Vores understregning.)

Denne opfattelse uddybes på s. 34 som følger:

> *"129.* ***SAs should take into account whether the controller deploying the model conducted an appropriate assessment, as part of its accountability obligations [note udeladt] to demonstrate compliance with Article 5(1)(a) and Article 6 GDPR, to ascertain that the AI model was not developed by unlawfully processing personal data.*** *Such evaluation by SAs should take into account whether the controller has assessed some non-exhaustive criteria, such as the source of the data and whether the AI model is the result of an infringement of the GDPR, particularly if it was determined by a SA or a court, so that the controller deploying the model could not ignore that the initial processing was unlawful.*
>
> *130. The controller should consider, for instance, if the data originates from a personal data breach or if the processing was subject to the finding of an infringement from a SA or a court.* ***The degree of the assessment of the controller and the level of detail expected by SAs may vary depending on diverse factors, including the type and degree of risks raised by the processing in the AI model during its deployment in relation to the data subjects whose data was used to develop the model.***
>
> […]
>
> *132. The same considerations made under paragraph 123 above are also relevant in this case. When SAs verify if and how the controller assessed the appropriateness of legitimate interest as a legal basis for the processing it conducts, the unlawfulness of the initial processing should be taken into account as part of the legitimate interest assessment, for instance by assessing the potential risks that may arise for the data subjects whose personal were unlawfully processed to develop the model. Different aspects, either of a technical nature (e.g. the existence of filters or access limitations placed during the development of the model, which the subsequent controller cannot circumvent or influence, and which might prevent access to or disclosure of personal data) or of a legal nature (e.g. nature and severity of the unlawfulness of the initial processing) have to be given due consideration within the balancing test."* (Original fremhævning med fed, vores understregning.)

Hvis der i selve AI-modellen *ikke* er indlejret personoplysninger, vil den dataansvarlige, der køber adgang til AI-modellen fra leverandøren og anvender AI-modellen, derimod ikke skulle forholde sig til

leverandørens eventuelle ulovlige indsamling og behandling af personoplysninger til udvikling af AI-modellen, da databeskyttelsesreglerne ikke gælder i forhold til den efterfølgende brug af den anonyme AI-model. EDPB anfører herom følgende, jf. s. 4:

> *"Under scenario 3, a controller unlawfully processes personal data to develop the AI model, then ensures that it is anonymised, before the same or another controller initiates another processing of personal data in the context of the deployment. In this regard, the Opinion states that if it can be demonstrated that the subsequent operation of the AI model does not entail the processing of personal data, the EDPB considers that the GDPR would not apply. Hence, the unlawfulness of the initial processing should not impact the subsequent operation of the model. Further, the EDPB considers that, when controllers subsequently process personal data collected during the deployment phase, after the model has been anonymised, the GDPR would apply in relation to these processing operations. In these cases, the Opinion considers that, as regards the GDPR, the lawfulness of the processing carried out in the deployment phase should not be impacted by the unlawfulness of the initial processing."*
> (Vores understregning.)

Der kan endvidere henvises til Datatilsynets praksis om dataansvarliges indsamling af personoplysninger fra andre dataansvarlige, der har indsamlet personoplysningerne ulovligt. Det følger af Datatilsynets praksis, at behandling af oplysninger, som er ulovligt tilvejebragt, kan være i strid med princippet om rimelighed i databeskyttelsesforordningens artikel 5, stk. 1, litra a.

Som eksempel herpå kan nævnes Datatilsynets afgørelse af 17. maj 2018 (j.nr 2018-32-0065), som vedrørte SKATs behandling af en række oplysninger om en klager, som af Statsadvokaten for Økonomisk og International Kriminalitet (tidligere kendt som SØIK) var indsamlet i strid med retsplejeloven og efterfølgende delt med SKAT. Datatilsynet fandt – efter at sagen havde været behandlet i Datarådet – at SKAT havde behandlet oplysninger i strid med den tidligere persondatalovs § 5, stk. 1, om god databehandlingsskik (som svarer til databeskyttelsesforordningens artikel 5, stk. 1, litra a), og at SKAT skulle slette de omhandlede oplysninger.

I en anden, nyere sag traf Datatilsynet den 13. september 2024 afgørelse i en sag vedrørende Helsingør Kommune (j.nr. 2024-32-0482). Datatilsynet fandt, at kommunens behandling af ulovligt tilvejebragte oplysninger var i overensstemmelse med databeskyttelsesreglerne. Oplysningerne hidrørte fra aflytning, som faren til et barn havde foretaget i strid med straffelovens § 263, stk. 2. Oplysningerne indgik i en underretningssag i kommunen, og formålet med kommunens behandling af oplysningerne var således at afdække, om der var behov for at træffe foranstaltninger med henblik på at sikre barnets trav.

Datatilsynet fandt ikke grundlag for at tilsidesætte kommunens vurdering af, at det var nødvendigt at behandle personoplysningerne som led i kommunens løsning af sine myndighedsopgaver (underretningssagen). Tilsynet lagde således til grund, at kommunen havde hjemmel i artikel 6, stk. 1, litra e, til at behandle personoplysningerne.

Datatilsynet anførte dernæst, at om anvendelse og anden behandling af personoplysninger, som er ulovligt tilvejebragt, er rimelig, må efter Datatilsynets opfattelse bero på en konkret vurdering i den enkelte sag. Der kan herved bl.a. henvises til databeskyttelsesforordningens præambelbetragtning 4, hvoraf det fremgår, at retten til beskyttelse af personoplysninger ikke er en absolut ret, men skal afvejes i forhold til andre grundlæggende rettigheder. I rimelighedsvurderingen efter artikel 5, stk. 1, må navnlig indgå hvordan (og af hvem) oplysningerne er tilvejebragt, og hvilke modsatrettede interesser der er i (fortsat) behandling af oplysningerne. Datatilsynet fandt, at kommunens behandling af de ulovligt tilvejebragte oplysninger var rimelig og ligeledes var i overensstemmelse med de øvrige principper i databeskyttelsesforordningens artikel 5, stk. 1. Tilsynet bemærkede bl.a., at oplysningerne indgik i en underretningssag i kommunen, og at formålet med kommunens behandling af oplysningerne var at afdække, om der var behov for at træffe foranstaltninger med henblik på at sikre barnets trav. Sammenfattende var det således Datatilsynets opfattelse, at kommunens (fortsatte) behandling af personoplysningerne var i overensstemmelse med reglerne i databeskyttelsesforordningen, jf. artikel 6, stk. 1, litra e, og artikel 5, stk. 1. Datatilsynet fandt derfor samtidig, at kommunen ikke skulle slette oplysningerne.

3.3.2 Behandlingsgrundlag for behandling af personoplysninger, herunder indsamling af personoplysninger fra internettet til modeludvikling

Når en leverandør, der udvikler og udbyder en AI-model, indsamler personoplysninger – herunder fra internettet via dataskrab ("web scraping") – for at udvikle modellen, skal denne leverandør som selvstændig dataansvarlig have et behandlingsgrundlag for indsamlingen og behandlingen af personoplysningerne til brug for træningen af modellen. Det gælder både i forhold til indsamling og behandling af ikke-følsomme og følsomme personoplysninger.

3.3.2.1 Indsamling og behandling af ikke-følsomme personoplysninger

Det følger af databeskyttelsesforordningens artikel 6, stk. 1, at behandling af ikke-følsomme personoplysninger kun er lovlig, hvis og i det omfang mindst ét af forholdene i bestemmelsen gør sig gældende. Behandling er eksempelvis lovlig, hvis behandling er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn, jf. databeskyttelsesforordningens artikel 6, stk. 1, litra f, 1. pkt.

EDPB har i sin såkaldte ChatGPT-taskforcerapport af 23. maj 2024[34] forholdt sig til, hvorvidt en international leverandør af store, generative sprogmodeller (OpenAI) kan anvende artikel 6, stk. 1, litra f, som hjemmelsgrundlag til indsamling af personoplysninger fra internettet ("web scraping"), præ-processering af de indsamlede data med henblik på træning samt selve træningen af disse AI-modeller, jf. rapportens punkt 15-17:

> *"15. The first three stages carry peculiar risks for the fundamental rights and freedoms of natural persons as "web scraping" enables the automated collection and extraction of certain information from different publicly available sources on the Internet (such as websites), which are then used for training purposes of ChatGPT.[Note udeladt.] Such information can contain personal data which encompasses various aspects of the personal life of the respective data subject. Depending on the source, the scraped data may even contain special categories of personal data within the meaning of Article 9(1) GDPR.*
>
> *16. Regarding web scraping, OpenAI brought forward Article 6(1)(f) GDPR as legal basis. [Note udeladt.] It has to be recalled that the legal assessment of Article 6(1)(f) GDPR should be based on the following criteria: [Note udeladt.] i) existence of a legitimate interest, ii) necessity of processing, as the personal data should be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed and iii) balancing of interests. Fundamental rights and freedoms of data subjects on one hand and the controller's legitimate interests on the other hand have to be evaluated and balanced carefully. [Note udeladt.] The reasonable expectations of data subjects should be taken into account in this assessment. [Note udeladt.]*
>
> *17. As already stated by the former Article 29 Working Party, adequate safeguards play a special role in reducing undue impact on data subjects and can therefore change the balancing test in favor of the controller. [Note udeladt.] While the assessment of the lawfulness is still subject to pending investigations, such safeguards could inter alia be technical measures, defining precise collection criteria and ensuring that certain data categories are not collected or that certain sources (such as public social media profiles) are excluded from data collection. Furthermore, measures should be in place to delete or anonymise personal data that has been collected via web scraping before the training stage."*

[34] EDPB, Report of the work undertaken by the ChatGPT Taskforce, 23. maj 2024 (endelig version). Rapporten er tilgængelig fra EDPB's hjemmeside via følgende link: https://www.edpb.europa.eu/system/files/2024-05/edpb_20240523_report_chatgpt_taskforce_en.pdf (senest tilgået den 1. oktober 2025).

EDPB har uddybet sin opfattelse i EDPB's udtalelse vedrørende AI-modeller, jf. udtalelsens side 19-31. EDPB anfører i punkt 66, at de europæiske datatilsynsmyndigheder skal foretage en vurdering af, hvorvidt den dataansvarlige leverandør – der udvikler AI-modellen – har foretaget en grundig konkret vurdering af, hvorvidt følgende tre kumulative betingelser for brug af databeskyttelsesforordningens artikel 6, stk. 1, litra f, er opfyldt: (i) at behandlingen forfølger en legitim interesse hos den dataansvarlige eller en tredjepart; (ii) at behandlingen er nødvendig for at forfølge den legitime interesse; samt (iii) at en konkret interesseafvejning ("balancing test") mellem den legitime interesse og de registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder ikke falder ud til, at de registreredes interesser m.v. vejer tungere end den dataansvarliges legitime interesse.

I det tredje skridt (interesseafvejningen) skal det bl.a. indgå, hvilke risici der er for de registreredes rettigheder og frihedsrettigheder ved behandlingen samt hvordan de registrerede påvirkes af behandlingen, jf. punkt 77-90. Det skal også indgå i interesseafvejningen, hvad der er de registreredes rimelige forventninger til databehandlingen, jf. punkt 91-95. Endelig skal det indgå i interesseafvejningen, hvilke foranstaltninger den dataansvarlige har implementeret for at mindske påvirkningen af behandlingen på de registrerede samt for at håndtere risici for de registreredes rettigheder og frihedsrettigheder. EDPB opstiller en ikke-udtømmende liste over foranstaltninger, der kan indgå i den konkrete vurdering, jf. punkt 98-108. Disse foranstaltninger omfatter bl.a. følgende:

I. I relation til udviklingen af AI-modellerne (punkt 99-103):

- Tekniske foranstaltninger med henblik på at minimere behandlingen af personoplysninger, pseudonymiseringsforanstaltninger, foranstaltninger med henblik på at maskere personoplysninger eller erstattet personoplysninger med falske data i træningssættet (f.eks. erstatte navne og e-mails med falske navne og e-mails), hvilket er særligt relevant ved træning af store, generative sprogmodeller.
- Foranstaltninger med henblik på at varetage de registreredes rettigheder.
- Foranstaltninger med henblik på at understøtte gennemsigtighed vedrørende behandlingen, herunder bl.a. offentliggørelse af information om behandlingen, mediekampagner og brug af model cards m.v.

II. Specifikke foranstaltninger ved brug af dataskrab fra internettet (web scraping) (punkt 104-106):

- Tekniske foranstaltninger såsom (a) ekskludering af indhold fra publikationer, der måtte indeholde personoplysninger, der måtte medføre risici for bestemte personer eller grupper af personer, (b) manglende indsamling af bestemte datakategorier eller at bestemte datakilder ekskluderes fra indsamlingen, herunder

indhold fra bestemte hjemmesider, (c) ekskludering af dataindsamling fra hjemmesider, der tydeligt gør indsigelse mod dataskrab til AI-træning, (d) implementering af andre relevante begrænsninger i indsamlingen af data samt (e) implementering af bestemte foranstaltninger til varetagelse af de registreredes rettigheder og transparens.

III. Specifikke overvejelser vedrørende mitigerende foranstaltninger i ibrugtagningsfasen af AI-modellen (punkt 107-108):

- Tekniske foranstaltninger, der eksempelvis forhindrer opbevaring, tilgængeliggørelse ("regurgitation") eller generering af personoplysninger, herunder outputfiltre ved brug af generativ AI, og/eller foranstaltninger til at mitigere risikoen for ulovlig viderebehandling af AI-modeller til almen brug (eksempelvis brug af digitale vandmærker på AI-genererede outputs).
- Foranstaltninger til varetagelse af de registreredes rettigheder, herunder vedrørende retten til sletning af personoplysninger fra modellens output data eller "deduplication" samt teknikker, der forsøger at fjerne eller undertrykke personoplysninger.
- Tilsynsmyndigheder skal bl.a. tage i betragtning, om den dataansvarlige, som tilsynsmyndigheden fører tilsyn med, har offentliggjort den dataansvarliges vurdering af, om betingelserne i artikel 6, stk. 1, litra f, er opfyldt, da dette kan øge gennemsigtigheden og rimeligheden. Øvrige foranstaltninger kan også tages i betragtning, herunder vedrørende forudgående information til de registrerede, samt hvorvidt den dataansvarlige har inddraget databeskyttelsesrådgiveren (DPO), hvor det måtte være relevant.

3.3.2.2 Indsamling og behandling af følsomme personoplysninger

Behandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt, jf. databeskyttelsesforordningens artikel 9, stk. 1.

Dette forbud mod behandling af følsomme personoplysninger gælder dog ikke i en række tilfælde, der opregnes i bestemmelsens stk. 2. Således gælder forbuddet eksempelvis ikke, hvis behandlingen vedrører personoplysninger, som tydeligvis er offentliggjort af den registrerede, jf. databeskyttelsesforordningens artikel 9, stk. 2, litra e.

Om bestemmelsen kan der generelt henvises til fremstillingen i Kristian Korfits Nielsen og Anders Lotterup, Databeskyttelsesforordningen og databeskyttelsesloven med kommentarer, 2. udg., DJØF, 2025, s. 477 ff. Her fremgår det bl.a., at offentliggørelse i bestemmelsens forstand foreligger, hvis oplysningerne er bragt til kundskab hos en bredere kreds af personer. Dette vil f.eks. være tilfældet, hvis oplysningerne viderebringes gennem tv, aviser og lignende landsdækkende medier, eller hvis det sker via internettet, f.eks. på sociale netværk, såsom Facebook, Twitter og YouTube. Det anføres endvidere, at det er en betingelse for at anvende artikel 9, stk. 2, litra e, at oplysningerne er offentliggjort på den registreredes foranledning. Oplysninger, som andre, f.eks. pressen, af egen drift har offentliggjort, er derfor ikke omfattet.

EU-Domstolen har ved dom af 4. juli 2023 i sag C-252/21, *Meta I*, fastslået, at *"såfremt en helhed af oplysninger, der både omfatter følsomme oplysninger og ikke-følsomme oplysninger, er […] indsamlet i blokke, uden at oplysningerne kan adskilles fra hinanden under indsamlingen, skal behandlingen af denne helhed af oplysninger anses for at være forbudt som omhandlet i databeskyttelsesforordningens artikel 9, stk. 1, eftersom den i hvert fald indebærer én følsom oplysning, og ingen af undtagelserne i forordningens artikel 9, stk. 2, finder anvendelse"*, jf. dommens præmis 89. Domstolen fastslog endvidere i præmis 77, at med henblik på anvendelsen af undtagelsen i databeskyttelsesforordningens artikel 9, stk. 2, litra e), skal det efterprøves, om den registrerede udtrykkeligt og ved en klar bekræftelse har haft til hensigt at offentliggøre de omhandlede personoplysninger.

EU-Domstolen har endvidere i sin praksis fastslået, at bestemmelsen skal fortolkes indskrænkende, da den har karakter af en undtagelsesbestemmelse til forbuddet mod behandling af følsomme personoplysninger, jf. EU-Domstolens dom af 4. oktober 2024 i sag C-446/21, *Meta II*, præmis 76. I samme dom fandt EU-Domstolen bl.a., at databeskyttelsesforordningens artikel 9, stk. 2, litra e, skal fortolkes således, at den omstændighed, at en person har udtalt sig om sin seksuelle orientering i forbindelse med en paneldiskussion, der er åben for offentligheden, ikke giver operatøren af en platform for et socialt onlinenetværk mulighed for at behandle andre oplysninger om denne persons seksuelle orientering, som i givet fald er indhentet uden for denne platform fra tredjeparters applikationer og websteder, med henblik på at sammenstille og analysere disse oplysninger for at tilbyde den pågældende personaliseret reklame, jf. dommens præmis 83.

EDPB anfører i rådets udtalelse om AI-modeller, at EDPB i udtalelsen ikke har analyseret betydningen af bl.a. artikel 9, stk. 2, litra e, der dog stadig kan spille en vigtig rolle ved vurderingen af de databeskyttelsesretlige krav til AI-modeller.[35]

[35] EDPB, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models, 17. december 2024 (endelig version), s. 10.

Endelig kan der henvises til EDPB's ChatGPT-taskforcerapport af 23. maj 2024, hvor EDPB anfører følgende om brugen af artikel 9, stk. 2, litra e, som hjemmel til behandling af følsomme personoplysninger[36]:

> *"Regarding the processing of special categories of personal data, one of the exceptions of Article 9(2) must be applicable in addition, for the processing to be lawful. In principle, one of these exceptions can be Article 9(2)(e) GDPR. However, the mere fact that personal data is publicly accessible does not imply that "the data subject has manifestly made such data public". In order to rely on the exception laid down in Article 9(2)(e) GDPR, it is important to ascertain whether the data subject had intended, explicitly and by a clear affirmative action, to make the personal data in question accessible to the general public. [note udeladt]."*
> (Vores understregning.)

3.3.3 Erfaringer fra EDPB og de europæiske datatilsyn vedrørende lovligheden af AI-modeller fra OpenAI, herunder ChatGPT

EDPB anfører i sin ChatGPT-taskforcerapport fra den 23. maj 2024, at adskillige europæiske datatilsyn har indledt undersøgelser mod det amerikanske selskab OpenAI OpCO, LLC, (herefter "OpenAI") som dataansvarlig for behandling af personoplysninger i relation af selskabets ChatGPT-service, der omfatter modellerne GPT 3.5 til GPT 4.0, jf. punkt 2. Det fremgår videre af rapporten, at EDPB i foråret 2023 besluttede at nedsætte taskforcen med henblik på at understøtte samarbejde og udveksle informationer vedrørende mulige håndhævelsesforanstaltninger over for OpenAI, jf. punkt 3-4. EDPB anfører endvidere i rapportens punkt 8, at der allerede er en række igangværende undersøgelser fra de europæiske datatilsyn vedrørende mulige overtrædelser af databeskyttelsesforordningen, og at disse undersøgelser koordineres gennem taskforcen. EDPB anfører, at disse undersøgelser er i proces, og at det endnu ikke er muligt at give en fuld beskrivelse af resultaterne, jf. punkt 12. Det fremgår videre, at OpenAI's behandling af personoplysninger skal vurderes efter den såkaldte "one stop shop-mekanisme" i databeskyttelsesforordningen, dvs. hvor et national datatilsyn bliver ledende tilsynsmyndighed, jf. databeskyttelsesforordningens artikel 56. Da OpenAI er etableret i Irland, vil det være det irske datatilsyn, der er den ledende tilsynsmyndighed.

Det fremgår endvidere af rapporten, at OpenAI allerede har implementeret en række foranstaltninger for at overholde det italienske datatilsyns afgørelse om et midlertidigt forbud mod ChatGPT i Italien og

[36] EDPB, Report of the work undertaken by the ChatGPT Taskforce, 23. maj 2024 (endelig version), punkt 18.

tilsynets efterfølgende afgørelse om at hæve forbuddet den 11. april 2023.[37] Det fremgår af det italienske datatilsyns hjemmeside, at datatilsynet har afsluttet sagen pr. den 20. december 2024.[38] Det fremgår bl.a., at OpenAI skal gennemføre en 6-måneders informationskampagne overfor den italienske befolkning samt betale en bøde på EUR 15 millioner. Ifølge det italienske datatilsyn underrettede OpenAI ikke datatilsynet om et brud på persondatasikkerheden, som OpenAI oplevede i marts 2023. OpenAI havde endvidere behandlet brugernes persondata til at træne ChatGPT uden først at identificere et passende behandlingsgrundlag samt havde overtrådt princippet om gennemsigtighed og de relaterede underretningsforpligtelser overfor brugerne. Derudover havde OpenAI ikke implementeret aldersverifikationsmekanismer, hvilket kunne føre til risiko for at eksponere børn under 13 år for upassende output. Det italienske datatilsyn gav OpenAI et påbud om at gennemføre en 6-måneders kommunikationskampagne i radio, fjernsyn, aviser og internettet med henblik på at understøtte effektiv gennemsigtighed i behandlingen af personoplysninger. Indholdet i informationen skulle fremme offentlig forståelse og opmærksomhed vedrørende ChatGPT's funktionsmåde, især vedrørende indsamlingen af bruger og ikke-bruger data til brug for træning af generativ kunstig intelligens og de registreredes rettigheder, herunder retten til at gøre indsigelse, berigtige og slette deres personoplysninger. Gennem denne informationskampagne skal både brugere og ikke-brugere af ChatGPT gøres opmærksomme på, hvordan de kan modsætte sig, at OpenAI træner generativ kunstig intelligens med deres personoplysninger og således effektivt sættes i stand til at udøve deres rettigheder efter databeskyttelsesforordningen.

Der ses ikke – udover den italienske sag – at være offentliggjort domme eller afgørelser fra europæiske datatilsyn vedrørende lovligheden af databehandlingen i AI-modeller trænet og udbudt af Microsoft og/eller OpenAI.

4. VORES VURDERING

4.1 Er der personoplysninger i AI-modellerne i M365 Copilot?

Det første spørgsmål er, om AI-modellerne, som anvendes i M365 Copilot, må antages at indeholde personoplysninger. Som det fremgår af afsnit 2.2 ovenfor, gør M365 Copilot brug af en række AI-modeller fra OpenAI Service, herunder den store, generative sprogmodel GPT-4.5 Preview.

[37] Se om afgørelsen på det italienske datatilsyns hjemmeside her: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10085432 og hele sagens forløb her: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/9874702#english (senest tilgået den 1. oktober 2025).

[38] Se det italienske datatilsyns hjemmeside her: https://www.gpdp.it/web/guest/home/docweb/-/docweb-display/docweb/10085432 (senest tilgået den 1. oktober 2025).

Spørgsmålet om, hvorvidt sådanne AI-modeller – i form af store, generative sprogmodeller – indeholder personoplysninger, er ikke afklaret i retspraksis. Spørgsmålet må derfor afgøres efter kriterierne i fra retspraksis fra EU-Domstolen og EDPB's kriterier fra EDPB's udtalelse om AI-modeller.

Udgangspunktet er, at modeller der bygger på machine learning, er anonyme, fordi de indlærte sammenhænge ikke knyttes til specifikke personer. Ifølge EDPB kan AI-modeller trænet på personoplysninger dog ikke i alle tilfælde anses for at være anonyme, idet dette beror på en konkret vurdering fra sag til sag. For at en AI-model kan betragtes som anonym skal både (1) sandsynligheden for direkte (inklusive probabilistisk) ekstrahering ("extraction") af personoplysninger vedrørende de registrerede, hvis personoplysninger blev anvendt til at udvikle modellen, samt (2) sandsynligheden for at kunne opnå ("obtain") – bevidst eller ej – sådanne personoplysninger fra prompts være ubetydelig ("insignificant"), når man tager alle de midler, der med rimelighed kan tages i brug af den dataansvarlige eller en anden person, i betragtning.

Der er enighed om, at store, generative sprogmodeller i almindelighed ikke indeholder eller har adgang til databaser med træningsdata, hvorfra modellerne henter deres output.

Omvendt er det notorisk, at M365 Copilot givet et prompt herom kan give et output, som kan indeholde personoplysninger om fysiske personer, herunder forkerte oplysninger. Det kan f.eks. være ved anvendelse af et prompt om oplysninger vedrørende offentligt kendte fysiske personer. Hertil kommer, at OpenAI's egne såkaldte "Standard Refusal Evaluation"-tests – som beskrevet i OpenAI's system card for GPT-4.5 – viser, at GPT-4.5 kan producere "unsafe output" i form af "personal-data/highly-sensitive" og "personal-data/extremely-sensitive", jf. herom afsnit 2.2 ovenfor.

Set i dette lys kan det forhold, at informationen om den registrerede i sprogmodellen er opdelt i bidder i form af tokens og sandsynlighedsvægte for relationer mellem disse (embeddings), ikke i sig selv medføre, at der ikke er tale om personoplysninger, så længe bidderne med høj sandsynlighed kan samles igen til information, der kan henføres til en bestemt fysisk person via brug af brugergrænsefladen i AI-systemet M365 Copilot. Det forekommer ud fra EDPB's udtalelse tilstrækkeligt, at modellen opbevarer sandsynlighedsvægte mellem tokens, der med rimelige hjælpemidler kan sættes sammen til personoplysninger i outputtet med høj sandsynlighed ("probabilistic extraction"), jf. EDPB's udtalelse om AI-modeller, jf. udtalelsens s. 2 og punkt 43.

Det danske datatilsyns har med rette fundet, at udgangspunktet er, at AI-modeller er at sammenligne med en statistisk rapport og ikke indeholder personoplysninger. Denne retsopfattelse må dog nuanceres i forhold til store, generative sprogmodeller, hvor sandsynlighedsvægtene notorisk kan genproducere personoplysninger.

På denne baggrund må det ud fra en bedømmelse af de foreliggende oplysninger konkluderes, at det er mest sandsynligt, at domstolene vil finde, at AI-modellerne, der anvendes i M365 Copilot, herunder AI-modellen GPT-4.5 Preview, indeholder personoplysninger. Den dataansvarlige ibrugtager af M365 Copilot 365 behandler derfor personoplysninger ved brugen af løsningen.

4.2 Retsvirkningen af, at der er personoplysninger i AI-modellerne i M365 Copilot – kravet om den dataansvarlige ibrugtagers kontrol af, om leverandøren af AI-modellen har trænet modellen med ulovligt tilvejebragte personoplysninger

Spørgsmålet er herefter, hvad der er den databeskyttelsesretlige retsvirkning af, at der indgår personoplysninger i AI-modellerne, herunder GPT-4.5, i M365 Copilot. Dette angår spørgsmålet om, hvilken kontrol den dataansvarlige statslige myndighed, der anvender M365 Copilot, skal foretage af, at Microsoft/OpenAI har trænet modellen ved brug af ulovligt tilvejebragte personoplysninger.

Ifølge EDPB skal den dataansvarlige, der idriftsætter en AI-model, der indeholder personoplysninger, foretage en vis kontrol med, at udbyderen af AI-modellen ikke har udviklet AI-modellen med ulovligt indsamlede personoplysninger. Der findes ikke tilsyns- eller domstolssager endnu, der kan belyse niveauet af denne undersøgelse.

EDPB anfører i rådets udtalelse om AI-modeller, punkt 129, at den dataansvarlige, der er ibrugtager af en AI-model, skal foretage en *passende* ("appropriate") databeskyttelsesretlig vurdering af, hvorvidt leverandøren har udviklet AI-modellen ved ulovlig behandling af personoplysninger, herunder at databeskyttelsesforordningens artikel 5, stk. 1, litra a, om princippet om lovlighed, rimelighed og gennemsigtighed samt artikel 6 om behandlingsgrundlag er overholdt. Ifølge EDPB skal denne vurdering eksempelvis inddrage, hvorvidt AI-modellen er resultatet af erkendt ulovligt tilvejebragte personoplysninger, som er fastslået af domstolene eller en tilsynsmyndighed.

EDPB anfører endvidere i udtalelsens punkt 130, at detaljeringsgraden i den dataansvarliges vurdering varierer i lyset af forskellige faktorer, herunder typen og graden af risici forbundet med behandlingen af personoplysninger i AI-modellen under dens brug for de registrerede, hvis personoplysninger blev anvendt til at udvikle modellen.

For så vidt angår denne lovlighedsvurdering skal det indledningsvis bemærkes, at der må anses for at være begrænset risiko for de registrerede, hvis personoplysninger blev anvendt til at træne AI-modellerne i M365 Copilot, i forbindelse med de dataansvarlige statslige myndigheders anvendelse af M365 Copilot. Således er de dataansvarlige myndigheders formål med at anvende AI-modellerne i M365 Copilot – og de deri indeholdte personoplysninger – på ingen måde at behandle personoplysninger om personer i AI-modellerne i M365 Copilot, herunder træffe afgørelser eller øvrige foranstaltninger overfor disse.

Brugerne er offentlige myndigheder, som er underlagt reglerne om saglighed. Dette indebærer bl.a., at offentlige myndigheder i sager alene må behandle personoplysninger, som er nødvendige i forhold til sagen. Det gælder også offentliggjorte oplysninger, jf. bl.a. Ombudsmandens udtalelse i 2011 15-1. Det vil ikke være hensigten, at offentligt ansatte vil anvende M365 Copilot til at fremskaffe eller udlede personoplysninger, og den primære behandling af disse vil vedrøre offentligt notorisk kendte personer i Danmark, såsom f.eks. "borgmesteren i Esbjerg" eller en kunstner. Hvis der fremkommer følsomme personoplysninger, vil det normalt primært skyldes, at de pågældende forhold er offentliggjort med den registreredes indforståelse i f.eks. medier, sociale medier mv. Der foreligger ikke oplysninger om, at sådanne personoplysninger skulle være offentliggjort ved et brud på persondatasikkerheden eller lignende. Offentligt ansatte er underlagt en officialmaksime, som indebærer, at disse aldrig vil blive lagt uprøvet til grund i konkrete sager, og at de kun vil blive brugt og refereret, hvis det er sagligt relevant.

De dataansvarlige statslige myndigheder vil endvidere sikre, at de dataansvarliges medarbejdere vejledes om korrekt brug og i den forbindelse instrueres i, hvordan de undgår at fremskaffe oplysninger på irrelevante enkeltpersoner. De dataansvarlige myndigheder vil således anvende datagrundlaget, herunder personoplysninger, i Microsoft 365 – dvs. de personoplysninger om borgere og medarbejdere, som indgår i sagsbehandlingen hos myndighederne til løsning af deres lovbestemte opgaver – som de respektive brugere har adgang til, og som myndighederne har indsamlet som led i deres virksomhed.

Spørgsmålet er herefter, om der er offentliggjort retspraksis eller tilsynspraksis fra de europæiske datatilsyn, der fastslår, at OpenAI/Microsoft har udviklet AI-modellerne i M365 Copilot ved brug af ulovligt tilvejebragte personoplysninger, herunder et brud på persondatasikkerheden.

Bortset fra den italienske sag vedrørende ChatGPT ses der ikke offentliggjort retspraksis eller administrativ praksis fra de europæiske datatilsyn vedrørende lovligheden af AI-modeller fra OpenAI eller Microsoft. Derudover kan der lægges vægt på det forhold, at det ikke kan afvises, at der principielt kan være hjemmel til, at OpenAI/Microsoft kan udvikle AI-modellerne i M365 Copilot, herunder med indsamling fra internettet i form af dataskrab ("web scraping"), jf. databeskyttelsesforordningens artikel 6, stk. 1, litra f, og artikel 9, stk. 2, litra e, læst i lyset af EDPB's ChatGPT-taskforcerapport samt udtalelsen om AI-modeller, som er gengivet i afsnit 3.3.2 ovenfor.

Endvidere må der lægges vægt på, at Microsoft og OpenAI har implementeret forskellige foranstaltninger med henblik på at understøtte dataminimering og undgå eller begrænse, at personoplysninger indgår i modellerne samt i outputtet, jf. herom afsnit 2.2 ovenfor. Disse foranstaltninger omfatter for GPT-4.5-modellen bl.a., at OpenAI har anvendt en række avancerede filtreringsmekanismer med henblik på bl.a. at reducere behandlingen af personoplysninger under træningen af selskabets modeller. Der kan endvidere henvises til, at Microsoft har udarbejdet en publikation med beskrivelse af, hvordan Microsoft har

implementeret en række kontroller med henblik på at overholde standarden ISO 42001 AI Management System samt at Microsoft har opnået at blive certificeret i denne standard for bl.a. M365 Copilot. Dette er en international standard, som specificerer kravene til at etablere, implementere, vedligeholde og løbende forbedre et såkaldt "Artificial Intelligence Management System (AIMS)" i organisationer.[40] En af kontrollerne vedrører "A.7.6 Data preparation", hvor kontrolkravet er, at "*The organization shall define and document its criteria for selecting data preparations and the data preparation methods to be used.*" I besvarelsen af kontrolkravet anføres det bl.a., *at* Copilot 365 anvender store, generative sprogmodeller ("foundation models") fra OpenAI, *at* OpenAI under udviklingen af disse modeller anvender høje standarder for anonymisering af data forud for træningen af modellerne, samt at OpenAI løbende forbedrer disse systemer, herunder ved menneskelig kontrol af træningsdata. Der må endvidere lægges vægt på det af Microsoft oplyste om, at når Microsoft udvikler og idriftsætter nye generative AI-systemer og -modeller, anvender Microsoft det såkaldte "AI Risk Management Framework", som er udarbejdet af National Institute for Standards and Technology (NIST). Derudover må der lægges vægt på Microsofts besvarelser af Økonomistyrelsens spørgsmål vedrørende behandlingen af personoplysninger i M365 Copilot, og de deri indeholdte AI-modeller, som Økonomistyrelsen har stillet Microsoft i lyset af EDPB's opinion 28/2024 om personoplysninger i AI-modeller m.v., og som er gengivet ovenfor under afsnit 2.2. Endelig må der lægges vægt på, at Microsoft i sin databehandleraftale tilsikrer, at Microsoft overholder databeskyttelsesforordningens regler ved leveringen af Microsoft Copilot 365.

Heroverfor står, at Microsofts/OpenAI's indsamling af personoplysninger til brug for træning og udvikling af AI-modellerne i Copilot 365 utvivlsomt har været meget betydelig, og at der hos de dataansvarlige statslige myndigheder pt. kun i begrænset omfang er viden om, hvordan denne er foregået konkret, hvor omfattende en registrering, der er sket, og hvad Microsoft/OpenAI mere konkret har gjort til sikring af de omfattede fysiske personers rettigheder i den forbindelse. Det bemærkes endvidere, at de involverede fysiske personer bliver omfattet af databeskyttelsesforordningens anvendelsesområde, når en ibrugtager behandler deres personoplysninger inden for Den Europæiske Unions område, uanset at de er bosiddende uden for EU. Der er således principielt tale om en omfattende videregivelse af personoplysninger, ligesom AI-modellerne i Copilot 365 kan generere et betydeligt antal forkerte personoplysninger, herunder i form af hallucinationer.

Hvis ovennævnte forhold imidlertid skal forstås som at indebære, at den modtagende dataansvarlige, der ibrugtager AI-systemet (her de danske myndigheder), altid på egen hånd skal verificere lovligheden af udbyderens (her Microsoft) originale dataindsamling til brug for træning af en sprogmodel, vil det indebære en uoverskuelig og omfattende undersøgelse, som reelt umuliggør anvendelsen af store sprogmodeller i praksis. Dette vil i øvrigt også være et brud på det almindelige princip i databeskyttelsesretten, hvorefter en dataansvarlig, der modtager personoplysninger fra en anden dataansvarlig, normalt kun i

[40] Se hertil ISO's hjemmeside her: https://www.iso.org/standard/81230.html (senest tilgået den 1. oktober 2025).

begrænset omfang skal gennemføre en hjemmelskontrol ift. denne anden, afgivende dataansvarliges hjemmel til indsamlingen og videregivelse. Endelig bygger en række af databeskyttelsesforordningens regler på accept af en vis grad af tillid til samarbejdspartnere og de aftalte forhold samt den information, som modtages fra samarbejdspartnere, jf. f.eks. reglerne om overladelse af personoplysninger til databehandlere og overdragelse til dataansvarlige eller databehandlere i usikre tredjelande via overholdelse af databehandleraftalen.

Der er på nuværende tidspunkt ikke grundlag for at antage, at Microsoft/OpenAI har trænet AI-modellerne i M365 Copilot på baggrund af ulovligt tilvejebragte personoplysninger eller uden behandlingsgrundlag herfor. Der kan derfor med rette argumenteres for, at når der ikke foreligger en sådan kendt viden som fremhævet af EDPB om, at M365 Copilot bygger på ulovligt indsamlede oplysninger, og under hensyn til den forudsatte benyttelse af M365 Copilot i de angivne use cases hos danske offentlige myndigheder, må myndighederne lovligt kunne tage udgangspunkt i, at der ikke derved ulovligt behandles personoplysninger i kraft af brugen af M365 Copilot.

På denne baggrund må det efter en samlet vurdering konkluderes, at der ikke ved ibrugtagning af M365 Copilot inden for de definerede use cases, som anført i konsekvensanalysen vedrørende M365 Copilot, sker en ulovlig behandling af personoplysninger. Henset til den manglende praksis fra domstole og tilsynsmyndigheder er denne konklusion dog ikke utvivlsom og indebærer således en vis procesrisiko.

Det bemærkes herudover, at der ifølge EDPB's ChatGPT-taskforcerapport er flere verserende tilsynssager, der omfatter bl.a. modellerne GPT-3.0 og GPT 3.5 fra OpenAI. Der må derfor forventes praksis og afgørelser fra de europæiske datatilsyn, når disse sager afsluttes, samt når det irske datatilsyn som ledende tilsynsmyndighed træffer afgørelser vedrørende OpenAI, som kan have betydning for anvendelsen af M365 Copilot og bl.a. AI-modellen GPT-4.5.

Det må derfor anbefales, at de dataansvarlige statslige myndigheder, der ønsker at anvende M365 Copilot, følger udviklingen fra de europæiske datatilsyn og retspraksis i øvrigt tæt på dette område, samt løbende opdaterer konsekvensanalysen vedrørende databeskyttelse for løsningen i lyset af ny viden om løsningens behandling af personoplysninger. Det må endvidere anbefales, at de dataansvarlige statslige myndigheder udarbejder en klar exitstrategi for, hvordan de dataansvarlige kan stoppe med at anvende M365 Copilot indenfor en rimelig periode.

København, den 3. oktober 2025

Martin Sønnersgaard
Partner, Advokat