Erklæring

Translations proofread by EDPB Members.
This language version has not yet been proofread.

Erklæring 1/2025 om alderssikring

Vedtaget den 11. februar 2025[1]

Det Europæiske Databeskyttelsesråd har vedtaget følgende erklæring:

1. BAGGRUND FOR OG FORMÅL MED DENNE ERKLÆRING

1. Den europæiske lovramme opfordrer til øget beskyttelse af børn i det digitale miljø. Som eksempler kan nævnes, at direktivet om audiovisuelle medietjenester[2], som medlemsstaterne har gennemført i deres nationale lovgivning, fremhæver muligheden for at gennemføre alderskontrolforanstaltninger (artikel 6a og 28b), GDPR indfører en minimumsalder for at kunne give samtykke til behandling af personoplysninger i forbindelse med informationssamfundstjenester (artikel 8), forordningen om digitale tjenester[3] henviser til alderskontrol som en risikobegrænsende foranstaltning (artikel 35, stk. 1), og en række medlemsstater har indført en minimumsalder for at kunne udføre retshandler, udøve visse rettigheder og få adgang til visse varer og tjenesteydelser i deres egen nationale lovgivning.

2. Desuden identificerer forskellige nationale og europæiske initiativer såsom strategien for et bedre internet for børn (BIK+) alderssikring som en løsning til at forbedre børns trivsel online gennem et sikkert, alderssvarende digitalt miljø i overensstemmelse med de europæiske digitale rettigheder og principper[4].

[1] Mindre rettelser af formateringen i dette dokument blev foretaget den 24. februar 2025. Der blev foretaget yderligere mindre ændringer af afsnit 16 og afsnit 22, punkt b), den 1. april 2025.
[2] Europa-Parlamentets og Rådets direktiv (EU) 2018/1808 af 14. november 2018 om ændring af direktiv 2010/13/EU om samordning af visse love og administrative bestemmelser i medlemsstaterne om udbud af audiovisuelle medietjenester (direktiv om audiovisuelle medietjenester) i betragtning af de ændrede markedsforhold, https://eur-lex.europa.eu/eli/dir/2018/1808/oj.
[3] Europa-Parlamentets og Rådets forordning (EU) 2022/2065 af 19. oktober 2022 om et indre marked for digitale tjenester og om ændring af direktiv 2000/31/EF (forordning om digitale tjenester) (EØS-relevant tekst), https://eur-lex.europa.eu/eli/reg/2022/2065/oj.
[4] Bedre internet for børn, vejledning til alderssikring, https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest.

3. Baseret på definitionen i forskningsrapporten *Mapping age assurance typologies and requirements*[5] vil "alderssikring" i dette dokument blive anvendt som *overordnet betegnelse for de metoder, der anvendes til at bestemme en persons alder eller aldersgruppe med varierende grad af tillid eller sikkerhed*. Samme rapport nævner tre primære kategorier af alderssikring, nemlig aldersvurdering, alderskontrol og egenerklæring.
4. Alderssikring indebærer specifikke risici for databeskyttelsen med potentiale til at have en negativ indflydelse på ikke blot fysiske personers ret til beskyttelse af deres personoplysninger, men også andre rettigheder og frihedsrettigheder[6] såsom retten til beskyttelse mod forskelsbehandling, retten til respekt for menneskets integritet, retten til frihed og sikkerhed samt retten til ytringsfrihed og oplysning.

5. I erkendelse af betydningen af en konsekvent tilgang på EU-plan til spørgsmålet om alderssikring ønsker Databeskyttelsesrådet at give specifik vejledning og fremlægge overordnede principper baseret på GDPR, som bør tages i betragtning, når personoplysninger behandles i forbindelse med alderssikring.

6. De foreslåede principper har til formål at forene beskyttelsen af børn og beskyttelsen af personoplysninger i forbindelse med alderssikring.

7. Der er givet prioritet til at imødekomme kravene vedrørende hovedprincipperne i artikel 5 i GDPR (lovlighed, rimelighed, gennemsigtighed, formålsbegrænsning, dataminimering, rigtighed, opbevaringsbegrænsning, fortrolighed, integritet og ansvarlighed) og til at sikre, at disse databeskyttelsesprincipper gennemføres korrekt og forbliver robuste over tid som fastsat i artikel 25 i GDPR, "Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger", og artikel 32 i GDPR, "Behandlingssikkerhed".

8. Denne erklæring fokuserer på de principper, der gælder for forskellige onlinebrugstilfælde, herunder når der er fastsat en minimumsalder ved lov eller på anden måde for køb af produkter, brug af tjenester, der kan skade børn, eller udførelse af retshandler, og når der er en omsorgspligt til at beskytte børn (f.eks. til at sikre, at tjenester udformes eller tilbydes på en alderssvarende måde).

9. Databeskyttelsesrådet kan også overveje – når det er relevant og i andre dokumenter – at udstede yderligere vejledning om specifikke brugstilfælde.

[5] Raiz Shaffique, M., og van der Hof, S. (2024): Mapping age assurance typologies and requirements. Forskningsrapport, del af projektet om bedre internet for børn (BIK), koordineret af European Schoolnet (EUN) og bestilt af Europa-Kommissionen.
[6] For yderligere oplysninger om alderssikrings potentielle indvirkning på rettigheder og frihedsrettigheder kan f.eks. henvises til: "Roadmap for age verification" (Australian eSafety Commissioner, 2023), https://www.esafety.gov.au/sites/default/files/2023-08/Age-verification-background-report.pdf?v=1731644498261, "A safe internet by default for children and the role of age verification" (AEPD, 2024), https://www.aepd.es/guides/technical-note-safe-internet-by-default-for-children.pdf, og "Trustworthy Age Assurance?", en undersøgelse bestilt af Verts/ALE-gruppen om grøn og social økonomi i Europa-Parlamentet (2024), https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance.

2. PRINCIPPER FOR UDFORMNING AF ALDERSSIKRING I OVERENSSTEMMELSE MED GDPR

2.1 Fuld og effektiv nydelse af rettigheder og friheder

Alderssikringen skal fuldt ud respektere fysiske personers grundlæggende rettigheder[7] og frihedsrettigheder, og barnets tarv skal komme i første række for alle parter, der er involveret i processen.

10. Når tjenesteudbydere gennemfører alderssikring, skal de sikre, at de ikke kun tager hensyn til indvirkningen på retten til beskyttelse af personoplysninger, men på alle fysiske personers grundlæggende rettigheder.

11. I det særlige tilfælde, som børn udgør, skal barnets tarv[8] være et primært hensyn for alle parter, der er involveret i alderssikring. Det er vigtigt at bemærke, at der ikke er noget hierarki med hensyn til vurdering af barnets tarv, og at der skal tages hensyn til alle børns rettigheder[9], herunder deres ret til beskyttelse af personoplysninger, til beskyttelse mod vold og alle andre former for udnyttelse, til at få adgang til oplysninger fra en række forskellige kilder og til at få deres synspunkter taget behørigt i betragtning.

2.2 Risikobaseret vurdering af proportionaliteten af alderssikring

Alderssikring bør altid gennemføres på en risikobaseret og forholdsmæssig måde, der er forenelig med fysiske personers rettigheder og frihedsrettigheder.

12. Tjenesteudbydere bør anlægge en risikobaseret tilgang, når de udformer og driver deres tjenester. Nødvendigheden og proportionaliteten af at anvende sikkerhedsforanstaltninger såsom alderssikring bør påvises, og der bør tages hensyn til de dermed forbundne risici. Nødvendigheden kan påvises ved at foretage en vurdering[10], der afdækker og evaluerer de risici, som en bestemt tjeneste udgør for børn[11], f.eks. eksponering for skadelig kontakt eller skadeligt indhold. Som led i denne vurdering kan tjenesteudbydere også tage hensyn til børns rettigheder, de muligheder, som det digitale miljø giver, børns synspunkter samt udviklingen i deres kompetencer med henblik på at sikre alderssvarende deltagelse[12].

---

[7] Navnlig verdenserklæringen om menneskerettigheder, den europæiske menneskerettighedskonvention og grundlæggende frihedsrettigheder, EU's charter om grundlæggende rettigheder og FN's konvention om barnets rettigheder.

[8] FN's Komité for Barnets Rettigheder har præciseret, at princippet om barnets tarv *"har til formål at sikre både fuld og effektiv nydelse af alle de rettigheder, der er anerkendt i konventionen, og barnets holistiske udvikling"*. Generel bemærkning nr. 14 (2013) om barnets ret til, at dets tarv kommer i første række (artikel 3, stk. 1), https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf.

[9] Generel bemærkning nr. 25 (2021) om børns rettigheder i forbindelse med det digitale miljø, FN's Højkommissariat for Menneskerettigheder, marts 2021.

[10] F.eks. en konsekvensanalyse vedrørende børns rettigheder, som kan, men ikke behøver at være en del af en konsekvensanalyse vedrørende databeskyttelse.

[11] Eksperter i børns rettigheder har fremhævet fordelene ved at anvende konsekvensanalyser vedrørende børns rettigheder som et effektivt redskab *"til at omsætte konventionen [om barnets rettigheder] og dens artikel 3 om prioritering af barnets tarv til praksis på en konkret og struktureret måde"* (i Mukherjee, S., Pothong, K., & Livingstone, S. (2021): Child Rights Impact Assessment: A tool to realise child rights in the digital environment. London: 5Rights Foundation). Desuden har FN's Komité opfordret staterne til at give mandat til at anvende konsekvensanalyser vedrørende børns rettigheder til at integrere børns rettigheder i reguleringen og udformningen af det digitale miljø.

[12] Generel bemærkning nr. 25 (2021) om børns rettigheder i forbindelse med det digitale miljø, FN's Højkommissariat for Menneskerettigheder, marts 2021.

13. Tjenesteudbyderne skal også respektere deres brugeres rettigheder og frihedsrettigheder, herunder retten til beskyttelse af deres personoplysninger, og afveje disse med behovet for sikkerhedsforanstaltninger, som altid bør være de mindst indgribende af dem, der er til rådighed, og som altid bør være effektive. I mange tilfælde udgør alderssikring en høj risiko for de registreredes rettigheder og frihedsrettigheder, hvilket derfor vil kræve, at der foretages en konsekvensanalyse vedrørende databeskyttelse (jf. artikel 35 i GDPR) forud for behandlingen under hensyntagen til behandlingens karakter, omfang, sammenhæng og formål. Konsekvensanalysen vedrørende databeskyttelse bør indeholde en systematisk beskrivelse af de planlagte behandlingsaktiviteter og formålene med behandlingen, herunder i givet fald de legitime interesser, der forfølges af den dataansvarlige. Den bør også indeholde en vurdering af nødvendigheden og proportionaliteten af behandlingen, afdække risici i forbindelse med behandling af personoplysninger med henblik på alderssikring og indeholde foranstaltninger til at afbøde disse risici[13].

14. Konsekvensanalysen vedrørende databeskyttelse bør være retningsgivende for udformningen og gennemførelsen af passende tekniske og organisatoriske foranstaltninger til overholdelse af databeskyttelsesreglerne. Denne risikobaserede tilgang er afgørende for at afveje det potentielle indgreb i fysiske personers rettigheder og frihedsrettigheder i forhold til det tilsigtede mål i denne særlige sammenhæng, nemlig børns sikkerhed. Omfanget, udstrækningen og intensiteten af dette indgreb med hensyn til indvirkning på rettigheder og frihedsrettigheder skal altid vurderes nøje[14]. En tjenesteudbyder, der behandler personoplysninger for at kontrollere alle sine brugeres alder, når de tilgår alt indhold eller alle tjenester, selv når indholdet eller tjenesterne er egnet til alle målgrupper og ikke indebærer nogen risiko, vil f.eks. ikke bestå nødvendigheds- og proportionalitetstesten.

2.3 Forebyggelse af databeskyttelsesrisici

Alderssikring bør ikke føre til unødvendige databeskyttelsesrisici for fysiske personer. Navnlig bør alderssikring ikke give tjenesteudbydere adgang til yderligere metoder til at identificere, lokalisere, profilere eller spore fysiske personer.

15. Tjenesteudbydere og enhver tredjepart, der er involveret i alderssikring, bør gennemføre effektive foranstaltninger og sikkerhedsforanstaltninger for at forhindre, at denne proces er årsag til unødvendige databeskyttelsesrisici såsom dem, der opstår som følge af identifikation, lokalisering, profilering eller sporing af fysiske personer. Behandlingen af personoplysninger med henblik på alderssikring bør ikke give adgang til yderligere metoder til at opfylde formål, der ikke er relateret til selve alderssikringen. Dette kræver valg af tilgange til alderssikring, der fuldt ud overholder princippet om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger (se afsnit 2.8), og gennemførelse af foranstaltninger, der garanterer princippet om rimelighed, og som sikrer, at personoplysninger ikke behandles på en måde, der er uberettiget skadelig, ulovligt diskriminerende, uventet eller vildledende for de registrerede.

[13] Databeskyttelsesrådets retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, https://ec.europa.eu/newsroom/article29/items/611236/en.
[14] EDPS' retningslinjer for vurdering af proportionaliteten af foranstaltninger, der begrænser de grundlæggende rettigheder til privatlivets fred og beskyttelse af personoplysninger, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

16. En fysisk person, der skal verificere sin alder for at få adgang til voksent indhold, forventer f.eks. ikke, at tjenesteudbyderen anvender alderssikring til at fastslå vedkommendes identitet eller præcise geografiske placering eller til at overvåge, evaluere eller udlede personlige aspekter af vedkommendes identitet. Dette forhold er særlig relevant for overholdelsen af databeskyttelsesprincipperne i artikel 5, stk. 1, i GDPR, herunder rimelighed, gennemsigtighed og formålsbegrænsning, og reglerne i artikel 6, stk. 4, i GDPR, vedrørende efterfølgende anvendelse af personoplysninger. I overensstemmelse med principperne om formålsbegrænsning og dataminimering i artikel 5, stk. 1, i GDPR, bør alderssikringsprocessen tilsvarende ikke muliggøre yderligere målretning mod eller profilering af brugere, herunder til både kommerciel (f.eks. personaliserede reklamer) og ondsindet målretning (f.eks. grooming, mobning, stalking eller chikane). Databeskyttelsesrådet minder om, at der i henhold til betragtning 75 i GDPR kan være særlige risici for databeskyttelsesrettigheder, når personoplysninger vedrører sårbare fysiske personer, navnlig børn. Generelt bør det ikke være muligt at finde ud af mere end nødvendigt om en fysisk person og dennes handlinger ved at profilere denne person på grundlag af de oplysninger, der anvendes i alderssikringsprocessen. Dette bør i videst muligt omfang sikres, også i tilfælde af brud på datasikkerheden.

17. Situationer med magtubalance bør undgås for at forhindre tjenesteudbydere i at tvinge enkeltpersoner til at stå over for unødvendige databeskyttelsesrisici på grund af manglende handling[15]. Når dette ikke er muligt, bør disse situationer identificeres og tages højde for med passende modforanstaltninger[16]. F.eks. bør brugere, der ikke kan eller ikke ønsker at anvende en bestemt alderssikringsmetode, tilbydes brugbare alternativer til at bevise deres alder. Desuden bør tjenesteudbydere regelmæssigt vurdere, om de udvalgte metoder og teknologier, herunder dem, der leveres af tredjeparter, fungerer i overensstemmelse med deres formål, og tilpasse dem for at sikre rimelighed i behandlingen. Tredjeparter, der er involveret i alderssikring, bør også stræbe efter at hjælpe tjenesteudbydere med at opfylde deres forpligtelser ved ikke at indføre unødvendige databeskyttelsesrisici og ved rettidigt at underrette om relevante ændringer af deres politikker, udformninger, tjenester osv.

2.4 Formålsbegrænsning og dataminimering

Tjenesteudbydere og enhver tredjepart, der er involveret i alderssikring, bør kun behandle de aldersrelaterede attributter, der er strengt nødvendige for deres udtrykkeligt angivne og legitime formål.

18. I de fleste tilfælde er formålet med alderssikring at træffe beslutninger om aldersrelateret adgangskontrol, forhindre onlineskader for børn, tilbyde et passende design eller en passende oplevelse afhængigt af alder osv. Uanset brugstilfældet bør formålet med behandlingen af personoplysninger være udtrykkeligt angivet (artikel 5, stk. 1, litra b), i GDPR). Når personoplysninger er indsamlet, må de ikke viderebehandles eller kombineres med yderligere

[15] F.eks. når de registrerede står over for automatiseret beslutningstagning uden ordentlige klagemekanismer, eller når samtykke ikke kan gives frivilligt. Begrebet "magtubalance" drøftes i Databeskyttelsesrådets udtalelse 08/2024 om gyldigt samtykke i forbindelse med giv samtykke eller betal-modeller, der anvendes af store onlineplatforme (afsnit 4.2.1.3), https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_da.pdf.

[16] Fra Databeskyttelsesrådets retningslinjer 03/2022 om mørke mønstre i sociale medieplatformes grænseflader, og hvordan man genkender og undgår dem (afsnit 2.3), version 2.0, https://www.edpb.europa.eu/system/files/2023-02/edpb_03-2022_guidelines_on_deceptive_design_patterns_in_social_media_platform_interfaces_v2_en_0.pdf.

oplysninger på en måde, der er uforenelig med disse formål. Tekniske foranstaltninger såsom teknologier til beskyttelse af privatlivet bør anvendes til at begrænse muligheden for at anvende personoplysninger til andre formål. Organisatoriske foranstaltninger såsom politikker og kontraktlige forpligtelser, der begrænser videreanvendelsen af personoplysninger[17], bør også anvendes.

19. En aldersrelateret attribut er enhver attribut, der angiver, at en fysisk person har en bestemt alder, er over eller under en bestemt alder eller er inden for en aldersgruppe. Formålsspecifikationen vil bestemme de relevante og nødvendige aldersrelaterede attributter, der skal indsamles. Dette vil også gøre det muligt for den dataansvarlige at vurdere proportionaliteten af alderssikringsprocessen. Fordelene ved denne proces bør ikke opvejes af ulemper i forbindelse med udøvelsen af de grundlæggende rettigheder[18] (se afsnit 2.2 ovenfor).

20. Den dataansvarlige bør derfor kun indsamle personoplysninger, der er nødvendige, tilstrækkelige og relevante for de formål, der tilstræbes. På denne måde bidrager dataminimering til at underbygge og operationalisere principperne om nødvendighed[19] og proportionalitet. For eksempel behøver tjenesteudbyderen måske kun at vide, om brugeren er over eller under en aldersgrænse. Dette kan opnås ved at gennemføre en tokeniseret tilgang baseret på deltagelse af en tredjepartsudbyder, hvor tjenesteudbyderen kun ser det funktionelle resultat af alderssikringsprocessen (f.eks. "over" eller "under" aldersgrænsen)[20]. Forskellige tilgange kan være relevante, når tjenesteudbyderen har brug for at vide, om brugeren er inden for en bestemt aldersgruppe eller født i et bestemt år.

2.5 Effektiviteten af alderssikring

Alderssikring bør påviseligt opnå et effektivitetsniveau, der er tilstrækkeligt til det formål, for hvilket alderssikringen udføres.

21. De metoder, hvormed alderssikringen udføres, bør være tilstrækkelige til at opfylde formålet med behandlingen. Navnlig bør effektiviteten af enhver lovbestemt alderssikringsforanstaltning betragtes som en forudsætning for at opfylde principperne om nødvendighed[21] og proportionalitet[22].

---

[17] Fra Databeskyttelsesrådets retningslinjer 4/2019 om artikel 25 – Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger, version 2.0, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_da.pdf.

[18] Fra EDPS' retningslinjer for vurdering af proportionaliteten af foranstaltninger, der begrænser de grundlæggende rettigheder til privatlivets fred og til beskyttelse af personoplysninger, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

[19] Fra EDPS' værktøjskasse til vurdering af nødvendigheden af foranstaltninger, der begrænser den grundlæggende ret til beskyttelse af personoplysninger, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

[20] En tredjepartsudbyder foretager en alderskontrol og giver brugeren en "alderstoken", som brugeren kan fremvise for tjenesteudbyderen uden at skulle bevise sin alder igen. En alderstoken kan indeholde forskellige brugerattributter og oplysninger om, hvornår, hvor eller hvordan alderskontrollen blev udført.

[21] EDPS' værktøjskasse til vurdering af nødvendigheden af foranstaltninger, der begrænser den grundlæggende ret til beskyttelse af personoplysninger, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

[22] Retningslinjer for vurdering af proportionaliteten af foranstaltninger, der begrænser den grundlæggende ret til privatlivets fred og til beskyttelse af personoplysninger, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

22. Effektiviteten af alderssikringen bør evalueres ud fra flere aspekter, herunder:

a) Tilgængelighed. Alderssikring bør være bredt tilgængelig for fysiske personer, så de kan bekræfte deres alder eller bevise, at de opfylder et aldersrelateret krav. Når visse kategorier af personer risikerer at blive forskelsbehandlet ved brug af en bestemt alderssikringsmetode, f.eks. fordi de ikke ejer et passende identitetsdokument eller en mobiltelefon eller på grund af et handicap, bør der, når det med rimelighed er muligt, stilles alternative metoder til alderssikring til rådighed med tilstrækkelige grader af privatliv, tryghed og sikkerhed. Alderssikringsløsninger bør også være i overensstemmelse med gældende lovgivning om tilgængelighed[23].
b) Pålidelighed I henhold til rigtighedsprincippet (artikel 5, stk. 1, litra d) i GDPR) bør enhver metode, der har til formål at afgøre, om en fysisk person opfylder et aldersrelateret krav, præstere en passende og konsekvent grad af rigtighed, når det afgøres, om vedkommende opfylder det pågældende krav eller ej. Der bør stilles passende klagemekanismer til rådighed, navnlig når brugerne kan blive væsentligt påvirket af automatiseret beslutningstagning, f.eks. når deres aldersrelaterede egenskaber ikke er blevet korrekt fastlagt (se afsnit 2.7 nedenfor).
c) Robusthed. Alderssikring bør være i stand til at håndtere uventede situationer og modstå rimeligt sandsynlige forsøg på at narre eller omgå systemet. Det skal bemærkes, at robusthed har ringe betydning i forbindelse med egenerklæring af en aldersrelateret attribut, da pålideligheden af en sådan metode hovedsagelig afhænger af brugerens gode vilje[24].

Desuden bør tjenesteudbydere, der gennemfører alderssikring, og eventuelle tredjeparter, der er involveret i processen, kunne påvise dens effektivitet og være gennemsigtige med hensyn til, hvordan de opnår passende niveauer af tilgængelighed, pålidelighed og robusthed (se afsnit 2.10).

2.6 Lovlighed, rimelighed og gennemsigtighed:

Tjenesteudbydere og enhver tredjepart, der er involveret i alderssikring, bør sikre, at behandlingen af personoplysninger med henblik på alderssikring er lovlig, rimelig over for og gennemsigtig for brugerne.

23. Tjenesteudbydere skal sikre, at de har et gældende retsgrundlag i henhold til artikel 6 i GDPR (og, hvis det er relevant, en gældende undtagelse fastsat i artikel 9, stk. 2) for at behandle personoplysninger i forbindelse med alderssikring. Det kan f.eks. være nødvendigt at anvende alderssikring for at overholde en retlig forpligtelse (artikel 6, stk. 1, litra c), i GDPR) under hensyntagen til, at alderssikringen skal stå i et rimeligt forhold til det legitime mål, der forfølges, og kravene i artikel 6, stk. 3, i GDPR.

[23] F.eks. er tilgængeligheden af den offentlige sektors websteder og mobilapplikationer og tilgængeligheden af produkter og tjenester fastsat i henholdsvis direktivet om webtilgængelighed og den europæiske lov om tilgængelighed. Alderssikringsløsninger skal sikre, at de overholder disse lovgivninger, ved at opfylde kravene i den harmoniserede europæiske standard for tilgængelighedskrav til IKT-produkter og -tjenester, EN 301 549 v3.2.1.

[24] Databeskyttelsesrådet har tidligere udtrykt alvorlig tvivl om effektiviteten af egenerklæring som en metode til alderskontrol i forbindelse med højrisikobehandling i bindende afgørelse 2/2023 om den tvist, som den irske tilsynsmyndighed har forelagt vedrørende TikTok Technology Limited (artikel 65 i GDPR), https://www.edpb.europa.eu/system/files/2023-09/edpb_bindingdecision_202302_ie_sa_ttl_children_en.pdf.

24. Desuden skal tjenesteudbydere være gennemsigtige over for brugerne med hensyn til, præcis hvordan deres personoplysninger anvendes og af hvem. Dette er især vigtigt, når der er flere parter involveret i alderssikringsprocessen. Før personoplysninger behandles med henblik på alderssikring, skal brugerne bl.a. informeres (i henhold til artikel 12, 13 og 14 i GDPR) om[25]:

- hvilke personoplysninger der vil blive behandlet og hvordan
- hvorvidt tredjeparter vil blive inddraget i processen, og i givet fald hvem de er, og hvem de dataansvarlige og databehandlerne er i dette scenarie
- hvorvidt deres oplysninger vil blive delt med andre eller overført til et tredjeland
- hvor længe deres personoplysninger vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier, der anvendes til fastlæggelse af opbevaringsperioden
- hvilke rettigheder de har i forbindelse med deres personoplysninger (artikel 15-22 i GDPR), herunder hvordan de kan anfægte en forkert afgørelse truffet som følge af alderssikring.

25. Gennemsigtighed i forbindelse med alderssikring er særlig vigtig, når det drejer sig om børn. Tjenesteydere skal sikre, at de, når det er relevant, formidler oplysninger om gennemsigtighed til børn på en måde, der er klar og letforståelig for dem.

26. Begrebet gennemsigtighed er grundlæggende forbundet med rimelighed. Hvis tjenesteudbydere ikke er klare og gennemsigtige med hensyn til, hvordan de behandler fysiske personers oplysninger med henblik på alderssikring, er det usandsynligt, at denne behandling kan betragtes som rimelig, hvilket igen gør det usandsynligt, at behandlingen er lovlig. Navnlig hvis en udbyder tilbyder forskellige metoder for brugerne til at bekræfte deres alder, bør udbyderen være gennemsigtig med hensyn til den indvirkning, som hver metode har ud fra et databeskyttelsesperspektiv.

2.7 Automatiske afgørelser

Enhver forekomst af automatiseret beslutningstagning i forbindelse med alderssikring bør være i overensstemmelse med GDPR. Hvis det er relevant, bør tjenesteudbydere og enhver involveret tredjepart træffe passende foranstaltninger til at beskytte fysiske personers rettigheder og frihedsrettigheder samt legitime interesser.

27. EU-lovgiveren har valgt en bred definition af automatiseret beslutningstagning, der kræver undersøgelse fra sag til sag[26]. Automatiserede beslutninger kan inddrages på forskellige stadier i alderssikringsprocessen, enten for at få adgang til indholdet eller tjenesten eller gennem de metoder, der anvendes til at bevise alder.

[25] Se Artikel 29-Gruppens retningslinjer om gennemsigtighed i henhold til forordning 2016/679, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_da.pdf.

[26] Sag C-634/21, SCHUFA Holding (Scoring): Domstolens dom (Første Afdeling) af 7. december 2023 – OQ mod Land Hessen (anmodning om præjudiciel afgørelse fra Verwaltungsgericht Wiesbaden – Tyskland) (Præjudiciel forelæggelse – beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger – forordning (EU) 2016/679 – artikel 22 – automatiske individuelle afgørelser – kreditoplysningsbureauer – automatisk fastsættelse af en sandsynlighedsværdi vedrørende en persons evne til at opfylde sine betalingsforpligtelser i fremtiden ("scoring") – tredjemænds anvendelse af denne sandsynlighedsværdi), https://eur-lex.europa.eu/legal-content/DA/ALL/?uri=CELEX%3A62021CA0634.

28. Fuldautomatisk alderssikring kan have retsvirkninger for de pågældende fysiske personer – f.eks. for udøvelsen af deres ytringsfrihed – eller kan som minimum påvirke dem betydeligt på en lignende måde[27]. Virkningen af automatisk alderssikring på fysiske personers rettigheder kan variere afhængigt af typen af indhold eller tjenester, der er tale om.

29. Derfor bør tjenesteudbydere og enhver tredjepart, der er involveret i alderssikring, stille retsmidler og passende klagemekanismer til rådighed for brugere, hvis aldersrelaterede egenskaber ikke er korrekt fastlagt. Afhængigt af strukturen i alderssikringsprocessen skal de identificere, hvem den registrerede skal kontakte for at udøve sine rettigheder[28].

30. Tjenesteudbydere og enhver involveret tredjepart bør være særligt opmærksomme, når det drejer sig om børn. Som anført i betragtning 71 i GDPR gælder det, at *"en afgørelse […] som alene bygger på automatisk behandling, og som har retsvirkning eller som på tilsvarende vis betydeligt påvirker den pågældende […] bør ikke omfatte et barn"*. Undtagelser fra denne regel bør fortsat gælde under begrænsede omstændigheder, f.eks. hvor det er nødvendigt *"for at beskytte deres velfærd"*[29]. Under alle omstændigheder bør tjenesteudbydere og enhver involveret tredjepart gennemføre passende foranstaltninger – f.eks. brugbare alternativer, klagemekanismer og, hvor det er relevant, menneskelig indgriben – med oplysninger, der er tilpasset børn, når det drejer sig om dem.

2.8 Databeskyttelse gennem design og databeskyttelse gennem standardindstillinger

Alderssikring bør udformes, gennemføres og evalueres under hensyntagen til de mest privatlivsbevarende tilgængelige metoder og teknologier med henblik på at opfylde kravene i GDPR og effektivt beskytte de registreredes rettigheder.

31. I henhold til artikel 25 i GDPR bør dataansvarlige, der er involveret i alderssikring, gennemføre passende tekniske og organisatoriske foranstaltninger og nødvendige garantier for at sikre en effektiv gennemførelse af alle databeskyttelsesprincipper og dermed de registreredes rettigheder og frihedsrettigheder. Kravet om, at dataansvarlige som standard skal tage hensyn til databeskyttelse i designfasen af enhver behandlingsaktivitet vedrørende personoplysninger, gælder også for databehandlere og i hele en behandlingslivscyklus.

32. I betragtning af, hvor mange forskellige risici der er forbundet med alderssikringssystemer, og alvorligheden af dem, navnlig når identitetsdokumenter eller særlige kategorier af personoplysninger såsom biometriske data behandles, bør der lægges størst mulig vægt på at undgå unødvendig adgang til og behandling, deling og lagring af personoplysninger. Alderssikringssystemer og ethvert retligt eller teknisk instrument, der fastsætter krav til sådanne systemer, bør også revideres og ajourføres regelmæssigt, hvis det er nødvendigt, for

[27] Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, https://ec.europa.eu/newsroom/article29/items/612053/en.

[28] Som anført i Databeskyttelsesrådets retningslinjer (ovennævnte): *"kan disse rettigheder gøres gældende over for den dataansvarlige, der opretter profilen, og den dataansvarlige, der træffer en automatisk afgørelse om en registreret (med eller uden menneskelig indgriben), hvis disse enheder ikke er de samme"*.

[29] Fra retningslinjerne om automatiske individuelle afgørelser og profilering i henhold til forordning (EU) 2016/679: *"Der kan dog være visse situationer, hvor dataansvarlige er nødt til at træffe afgørelser, der alene er baseret på automatisk behandling, herunder profilering, som har retsvirkning for eller på tilsvarende vis betydeligt påvirker børn, f.eks. for at beskytte deres velfærd"*.

at tage hensyn til det hurtigt skiftende landskab af teknologier til beskyttelse af privatlivet inden for digital identitetsstyring.

33. Som nævnt i Databeskyttelsesrådets retningslinjer for databeskyttelse gennem design og databeskyttelse gennem standardindstillinger[30] pålægger henvisningen til "det aktuelle tekniske niveau" i forbindelse med artikel 25 i GDPR de dataansvarlige en forpligtelse til at tage hensyn til de nuværende teknologiske fremskridt, der er tilgængelige på markedet, når de fastlægger ovennævnte passende tekniske og organisatoriske foranstaltninger. Standarder, bedste praksis og adfærdskodekser, der anerkendes af relevante interessenter, kan være nyttige ved fastlæggelsen af sådanne foranstaltninger. Hensigtsmæssigheden af disse foranstaltninger bør dog verificeres for hver enkelt behandlingsaktivitet.

34. Databeskyttelsesrådet anbefaler derfor, at der på grundlag af det aktuelle tekniske niveau inden for alderssikring på det tidspunkt, hvor dette dokument blev udarbejdet, tages behørigt hensyn til teknologier og arkitekturer, der favoriserer brugerholdte data og sikker lokal behandling (enhedsbaseret), hvilket giver mulighed for egenskaber såsom uforbindelighed[31] (fra forskellige parters synspunkt og selv i tilfælde af hemmelige aftaler eller brud på datasikkerheden) og selektiv videregivelse[32] af personoplysninger, der er under den registreredes kontrol. Hertil kommer, at brugen af tilgange såsom dem, der er afhængige af batchudstedelse[33] af legitimationsoplysninger til engangsbrug eller kryptografiske protokoller såsom zero-knowledge proofs[34], bør stilles til rådighed for de registrerede i tilfælde, hvor alderssikring kan indebære store risici for deres privatliv.

2.9 Sikkerhed ved alderssikring

Tjenesteydere og enhver tredjepart, der er involveret i alderssikring, bør gennemføre passende tekniske og organisatoriske foranstaltninger for at sikre et sikkerhedsniveau, der svarer til risikoen.

35. Databeskyttelsesforordningen kræver, at både dataansvarlige og databehandlere har indført passende tekniske og organisatoriske foranstaltninger til at sikre et sikkerhedsniveau, der står i et rimeligt forhold til risikoen for de personoplysninger, der behandles (betragtning 83 og artikel 32). Arten, følsomheden og mængden af personoplysninger, der kan være involveret i alderssikring, illustrerer tydeligt den potentielle negative virkning, som et brud på datasikkerheden kan medføre.

36. Tillidsmodeller er afgørende for at forhindre databrud i forbindelse med alderssikring, da de definerer, hvordan de forskellige parter kan verificere hinandens identitet og integritet. De fremmer sikker kommunikation og dataudveksling mellem deltagere, der måske ikke har

[30] Databeskyttelsesrådets retningslinjer 4/2019 om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger i henhold til artikel 25, version 2.0, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_da.pdf.

[31] Egenskaben uforbindelighed indebærer, at det er umuligt at knytte eller korrelere forskellige dataelementer, handlinger eller transaktioner til en bestemt registreret.

[32] Selektiv videregivelse er en funktion ved tokens, legitimationsoplysninger og attestationer, der gør det muligt for de registrerede kun at dele de oplysninger, de ønsker, med bestemte parter i hvert enkelt tilfælde.

[33] Batchudstedelse handler om at besvare én anmodning om legitimationsoplysninger fra den registrerede med et sæt eller en gruppe af legitimationsoplysninger udarbejdet på samme tid.

[34] Et zero-knowledge proof er en protokol, hvor én part (bevisføreren) kan demonstrere over for en anden part (verifikatoren), at en given erklæring er sand, uden at formidle nogen oplysninger til verifikatoren ud over den blotte kendsgerning, at erklæringen er sand.

tidligere relationer. Desuden kan pseudonymisering og kryptering af personoplysninger være nyttige foranstaltninger til at afbøde de mulige negative virkninger af databrud. Opfyldelse af princippet om opbevaringsbegrænsning og anvendelse af korte opbevaringsperioder kan også være afgørende for sikkerheden i forbindelse med alderssikring, idet eksponeringsfladen reduceres. En politik om at undlade at logge kan betragtes som en værdifuld sikkerhedsforanstaltning: Når brugerens alder er blevet verificeret, vil de personoplysninger, der blev brugt til alderssikringsprocessen, ikke længere blive opbevaret.

37. I praksis, givet det stigende retlige pres for at gennemføre alderssikring og antallet af udbydere, der kan være underlagt sådanne regler, bør brud på sikkerheden imødeses. Det bør undersøges, om alle passende teknologiske beskyttelsesforanstaltninger og organisatoriske foranstaltninger er blevet gennemført, for omgående at kunne fastslå, om et brud på persondatasikkerheden har fundet sted, hvilket efterfølgende afgør, om anmeldelsesforpligtelsen finder anvendelse[35]. Et centralt element i enhver datasikkerhedspolitik er så vidt muligt at kunne forhindre brud på datasikkerheden og reagere rettidigt, hvis det sker. Derfor bør muligheden for straks at genoprette tilgængeligheden af alderssikring efter et sikkerhedsbrud også betragtes som afgørende. På samme måde er det afgørende at sikre alderssikringsøkosystemets modstandsdygtighed ved at fremme eksistensen af forskellige alternativer og løst sammenkoblede parter[36], der ikke er så afhængige af hinanden, at en fejl eller et nedbrud hos én af dem ville medføre betydelige adgangsbegrænsninger.

38. Selv om sikkerhedsforanstaltninger er af allerstørste betydning i forbindelse med alderssikring, garanterer de ikke, at autoriseret eller uautoriseret adgang til personoplysninger ikke vil påvirke fysiske personers rettigheder. De kan ikke erstatte anvendelsen af principperne om nødvendighed, proportionalitet eller databeskyttelse gennem design og databeskyttelse gennem standardindstillinger.

2.10 Ansvarlighed

Tjenesteudbydere og enhver involveret tredjepart bør indføre forvaltningsmetoder, der gør det muligt for dem at være ansvarlige for deres tilgang til alderssikring og at påvise deres overholdelse af databeskyttelsesforordningen og andre retlige krav.

39. I betragtning af de forskellige interessenter, der er involveret, spiller forvaltning af alderssikring en afgørende rolle for ansvarligheden. Alderssikring bør fungere inden for en forvaltningsramme, der sikrer, at alle processer og systemer udformes, gennemføres, revideres, dokumenteres, vurderes, anvendes, vedligeholdes, testes eller auditeres på en måde, der opfylder databeskyttelsesbestemmelserne og andre lovkrav. Denne ramme bør som minimum omfatte databeskyttelsespolitikkerne (artikel 24, stk. 2, i GDPR) og de prioriterings- og beslutningsprocesser, der er nødvendige for at nå overholdelsesmålene og styre risiciene på passende vis i hele alderssikringens livscyklus.

[35] Fra Databeskyttelsesrådets retningslinjer 9/2022 om anmeldelse af brud på persondatasikkerheden i henhold til GDPR, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_da.pdf.

[36] Parterne er så lidt afhængige af hinanden som muligt, hvilket mindsker omfanget af virkningerne i tilfælde af ændringer eller fejl.

40. For eksempel bør forvaltningsrammen afgrænse, hvem der fra en dataansvarligs/databehandlers perspektiv er ansvarlig, og hvordan, for præcis hvilke aktiviteter eller operationer i forbindelse med behandlingen. Den bør også sikre, at alderssikringen kan auditeres effektivt af myndigheder og relevante interessenter. Forvaltningsrammen er afgørende for ansvarligheden, men også for gennemsigtigheden af og tilliden til alderssikring. De registrerede vil formentlig have større tillid til metoder, der er gennemsigtige med hensyn til deres aktiviteter, beslutningstagning osv.

41. Desuden omfatter en del af forvaltningsrammen sikring af effektivitet (afsnit 2.5), databeskyttelse gennem design og databeskyttelse gennem standardindstillinger (afsnit 2.8) og sikkerhed (afsnit 2.9) i forbindelse med alderssikring.

På Det Europæiske Databeskyttelsesråds vegne

Formand

(Anu Talus)