

Uttalande



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

Uttalande 1/2025 om åldersstyrkande

Antaget den 11 februari 2025¹

Europeiska dataskyddsstyrelsen har antagit följande uttalande:

1. UTTALANDETS BAKGRUND OCH SYFTE

1. EU vill med sitt regelverk se till att barn får ett bättre skydd i den digitala miljön. Direktivet om audiovisuella medietjänster², som medlemsstaterna har införlivat i sin nationella lagstiftning, framhåller till exempel möjligheten att genomföra åtgärder för ålderskontroll (artiklarna 6a och 28b), dataskyddsförordningen inför ålderskrav för samtycke till behandling av personuppgifter i samband med informationssamhällets tjänster (artikel 8), rättsakten om digitala tjänster³ hänvisar till ålderskontroll som en riskbegränsande åtgärd (artikel 35.1) och ett antal medlemsstater har i sin nationella lagstiftning infört ålderskrav för att utföra rättshandlingar, utöva vissa rättigheter eller få tillgång till vissa varor och tjänster.
2. Olika nationella och europeiska initiativ, såsom bättre internet för barn (BIK+), anser dessutom att åldersstyrkande är en lösning som ökar barnens välbefinnande på nätet i och med att den digitala miljön görs säker och åldersanpassad, i linje med de europeiska digitala rättigheterna och principerna⁴.

¹ Den 24 februari 2025 gjordes mindre rättelser av detta dokumentets formatering. Ytterligare mindre ändringar av punkterna 16 och 22 b gjordes den 1 april 2025.

² Europaparlamentets och rådets direktiv (EU) 2018/1808 av den 14 november 2018 om ändring av direktiv 2010/13/EU om samordning av vissa bestämmelser som fastställs i medlemsstaternas lagar och andra författningar om tillhandahållande av audiovisuella medietjänster (direktivet om audiovisuella medietjänster), mot bakgrund av ändrade marknadsförhållanden, <https://eur-lex.europa.eu/eli/dir/2018/1808/oj>.

³ Europaparlamentets och rådets förordning (EU) 2022/2065 av den 19 oktober 2022 om en inre marknad för digitala tjänster och om ändring av direktiv 2000/31/EG (förordningen om digitala tjänster), <https://eur-lex.europa.eu/eli/reg/2022/2065/oj>.

⁴ Better Internet for Kids, Guide to age assurance, <https://better-internet-for-kids.europa.eu/en/age-assurance-guide-oldest>.

3. Baserat på definitionen i forskningsrapporten *Mapping age assurance typologies and requirements*⁵ kommer begreppet "åldersstyrkande" i detta dokument att användas som en paraplyterm för de metoder som används för att fastställa en persons ålder eller åldersintervall vid olika konfidens- eller säkerhetsnivåer. I samma rapport nämns följande tre huvudsakliga kategorier av åldersstyrkande: åldersuppskattning, ålderskontroll och egen försäkran.
4. Åldersstyrkande medför särskilda risker för dataskyddet och kan ha en negativ inverkan på inte bara fysiska personers rätt till skydd av sina personuppgifter utan även på andra rättigheter och friheter⁶ såsom rätten till icke-diskriminering, rätten till personlig integritet, rätten till frihet och säkerhet samt rätten till yttrandefrihet och information.
5. EDPB erkänner vikten av en konsekvent strategi på EU-nivå när det gäller åldersstyrkande och vill därför, med dataskyddsförordningen som utgångspunkt, tillhandahålla särskild vägledning och principer på hög nivå vilka bör beaktas när personuppgifter behandlas i samband med ett sådant styrkande.
6. Syftet med de föreslagna principerna är att se till att såväl barn som personuppgifter skyddas i samband med åldersstyrkande.
7. Prioritet har getts åt de krav som följer av huvudprinciperna i artikel 5 i dataskyddsförordningen (laglighet, korrekthet och öppenhet, ändamålsbegränsning, uppgiftsminimering, riktighet, lagringsminimering, konfidentialitet, integritet och ansvarsskyldighet) och att säkerställa att dessa dataskyddsprinciper genomförs korrekt och förblir stabila över tid, i enlighet med artikel 25 i dataskyddsförordningen, "Inbyggt dataskydd och dataskydd som standard", och artikel 32 i samma förordning, "Säkerhet i samband med behandlingen".
8. Detta uttalande handlar främst om de principer som är tillämpliga vid olika fall av användning online, som när en lag eller något annat föreskriver en minimiålder vid produktköp, vid användningen av tjänster som kan skada barn eller för att utföra rättshandlingar, samt när det finns en skyldighet att skydda barn (t.ex. att se till att tjänsterna utformas eller erbjuds på ett åldersanpassat sätt).
9. EDPB kan också överväga att – när så är relevant och i andra dokument – utfärda ytterligare vägledning om specifika användningsfall.

⁵ Raiz Shaffique, M., & van der Hof, S. (2024). *Mapping age assurance typologies and requirements*. Forskningsrapport, en del av projektet bättre internet för barn (BIK) som samordnas av Europeiska skoldatanätet och som har beställts av Europeiska kommissionen.

⁶ Mer information om hur åldersstyrkande kan inverka på rättigheter och friheter finns i t.ex. *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> och *Trustworthy Age Assurance?*, en studie beställd av klustret för en grön och social ekonomi vid Europaparlamentets grupp De gröna/Europeiska fria alliansen (2024) <https://www.greens-efa.eu/en/article/document/trustworthy-age-assurance>.

2. PRINCIPER FÖR UTFORMNINGEN AV ETT ÅLDERSSTYRKANDE SOM ÄR FÖRENLIGT MED DATASKYDDSFÖRORDNINGEN

2.1 Ett fullständigt och faktiskt åtnjutande av rättigheter och friheter

Åldersstyrkandet måste respektera fysiska personers alla grundläggande rättigheter⁷ och friheter, och alla parter som deltar i processen bör beakta barnets bästa i första hand.

10. När tjänsteleverantörerna genomför åldersstyrkande bör de säkerställa att de inte bara beaktar hur rätten till skydd av personuppgifter påverkas utan hur alla de grundläggande rättigheterna för fysiska personer påverkas.
11. När det gäller just barn bör alla parter som är delaktiga i åldersstyrkandet beakta barnets bästa⁸ i första hand. Det är viktigt att notera att det inte finns någon hierarki när det gäller hänsyn till barnets bästa och att hänsyn bör tas till barns alla rättigheter⁹, inbegripet deras rätt till skydd av personuppgifter, skydd mot våld och alla andra former av utnyttjande, att få tillgång till information från en rad olika källor samt att deras åsikter tillmäts vederbörlig betydelse.

2.2 Riskbaserad bedömning av proportionaliteten hos åldersstyrkandet

Åldersstyrkandet bör alltid genomföras på ett riskbaserat och proportionerligt sätt som är förenligt med fysiska personers rättigheter och friheter.

12. Tjänsteleverantörerna bör tillämpa en riskbaserad metod när de utformar och bedriver sina tjänster. Nödvändigheten och proportionaliteten i att använda säkerhetsåtgärder såsom åldersstyrkande bör påvisas och de risker som är förknippade med detta beaktas. Nödvändigheten kan påvisas med hjälp av en bedömning¹⁰ i vilken man identifierar och utvärderar¹¹ de risker som en viss tjänst medför för barn, såsom exponering för skadlig kontakt eller skadligt innehåll. Som en del av denna bedömning kan tjänsteleverantörerna också beakta barnets rättigheter, de möjligheter som den digitala miljön erbjuder, barnens åsikter samt barns utveckling av sina förmågor, för att säkerställa att deltagandet är åldersanpassat¹².
13. Tjänsteleverantörerna måste också respektera sina användares rättigheter och friheter, däribland deras rätt att få sina personuppgifter skyddade, och väga dessa mot behovet av säkerhetsåtgärder, vilka alltid bör vara de minst inkräktande av de som är tillgängliga och alltid

⁷ Särskilt den allmänna förklaringen om de mänskliga rättigheterna, den europeiska konventionen om skydd för de mänskliga rättigheterna och de grundläggande friheterna, Europeiska unionens stadga om de grundläggande rättigheterna och FN:s konvention om barnets rättigheter.

⁸ FN:s kommitté för barnets rättigheter har klargjort att "[s]yftet med begreppet 'barnets bästa' är att säkerställa både fullt och faktiskt åtnjutande av alla de rättigheter som erkänns i konventionen och barnets helhetsutveckling". Allmän kommentar nr 14 (2013) om barnets rätt att i första hand få beaktat vad som bedöms vara barnets bästa (artikel 3.1), https://www2.ohchr.org/English/bodies/crc/docs/GC/CRC_C_GC_14_ENG.pdf.

⁹ Allmän kommentar nr 25 (2021) om barnets rättigheter i relation till den digitala miljön, OHCHR, mars 2021.

¹⁰ Till exempel en konsekvensbedömning avseende barnets rättigheter, som kan men inte måste vara en del av en konsekvensbedömning avseende dataskydd.

¹¹ Experter på barns rättigheter har lyft fram fördelarna med att använda konsekvensbedömningar avseende barnets rättigheter som ett bra verktyg när det gäller att på ett konkret och strukturerat sätt omsätta konventionen om barnets rättigheter, och dess artikel 3 om att prioritera barnets bästa, i praktiken (i Mukherjee, S., Pothong, K. och Livingstone, S. [2021]. *Child Rights Impact Assessment: A tool to realise child rights in the digital environment*. London: SRights Foundation). FN-kommittén har även uppmanat stater att föreskriva användningen av sådana konsekvensbedömningar för att integrera barns rättigheter i regleringen och utformningen av den digitala miljön.

¹² Allmän kommentar nr 25 (2021) om barnets rättigheter i relation till den digitala miljön, OHCHR, mars 2021.

ändamålsenliga. Åldersstyrkande utgör ofta en hög risk för de registrerades rättigheter och friheter och då måste en konsekvensbedömning avseende dataskydd (artikel 35 i dataskyddsförordningen) genomföras före behandlingen, med beaktande av behandlingens art, omfattning, sammanhang och ändamål. Konsekvensbedömningen avseende dataskydd bör innehålla en systematisk beskrivning av den planerade behandlingen och behandlingens syften, inbegripet, när det är lämpligt, den personuppgiftsansvariges berättigade intresse. Den bör också innehålla en bedömning av behovet av och proportionaliteten hos behandlingen, identifiera risker som uppstår till följd av behandlingen av en persons uppgifter i syfte att styrka dennes ålder och innehålla åtgärder för att minska dessa risker¹³.

14. Konsekvensbedömningen bör ligga till grund för utformningen och genomförandet av lämpliga tekniska och organisatoriska åtgärder för efterlevnad av dataskyddet. Denna riskbaserade metod är avgörande för avvägningen mellan det potentiella ingreppet i fysiska personers rättigheter och friheter och det mål som eftersträvas i detta sammanhang, det vill säga barns säkerhet. Ingreppets tillämpningsområde, omfattning och intensitet måste alltid bedömas noggrant med avseende på vilken inverkan det har på rättigheter och friheter¹⁴. En tjänsteleverantör som behandlar personuppgifter för att kontrollera alla användares ålder för att de ska få tillgång till allt leverantörens innehåll eller alla dess tjänster skulle till exempel inte klara nödvändighets- och proportionalitetstesterna om innehållet eller tjänsterna är lämpliga för alla målgrupper och inte medför några risker.

2.3 Hur förebygger man dataskyddsrisiker?

Åldersstyrkande bör inte leda till onödiga risker för skyddet av fysiska personers uppgifter. I synnerhet bör åldersstyrkande inte ge tjänsteleverantörer fler möjligheter att identifiera, lokalisera, profilera eller spåra fysiska personer.

15. Tjänsteleverantörer och alla tredje parter som deltar i åldersstyrkandet bör genomföra ändamålsenliga åtgärder och skyddsåtgärder för att förhindra att processen orsakar onödiga dataskyddsrisiker, till exempel sådana som uppstår när fysiska personer identifieras, lokaliseras, profileras eller spåras. Behandlingen av personuppgifter i syfte att styrka någons ålder bör inte skapa fler möjligheter att uppfylla ändamål som inte har med själva åldersstyrkandet att göra. Man måste därför välja strategier för att styrka åldern som är helt förenliga med principen om inbyggt dataskydd och dataskydd som standard (se avsnitt 2.8) och genomförandeåtgärder som garanterar principen om korrekthet och säkerställer att personuppgifter inte behandlas på ett sätt som är omotiverat missgynnande, olagligt diskriminerande, oväntat eller vilseledande för de registrerade.
16. Fysiska personer som måste bekräfta sin ålder för att få tillgång till innehåll för vuxna förväntar sig till exempel antagligen inte att tjänsteleverantören använder åldersstyrkandet för att fastställa deras identiteter eller deras exakta geografiska plats eller för att övervaka, utvärdera eller dra slutsatser om personliga aspekter av deras identiteter. Detta är särskilt relevant för efterlevnaden av dataskyddsprinciperna i artikel 5.1 i dataskyddsförordningen, däribland korrekthet, öppenhet och ändamålsbegränsning, och bestämmelserna i artikel 6.4 i dataskyddsförordningen om efterföljande behandling av personuppgifter. I enlighet med

¹³ EDPB:s riktlinjer om konsekvensbedömning avseende dataskydd och fastställande av huruvida behandlingen "sannolikt leder till en hög risk" i den mening som avses i förordning 2016/679, <https://ec.europa.eu/newsroom/article29/items/611236/sv>.

¹⁴ EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

principerna om ändamålsbegränsning och uppgiftsminimering enligt artikel 5.1 i dataskyddsförordningen bör processen för åldersstyrkande inte heller möjliggöra utökad målinriktning eller profilering av användare, vare sig det gäller kommersiell (t.ex. individanpassad reklam) eller skadlig målinriktning (t.ex. grooming, mobbning, stalkning eller trakasserier). EDPB erinrar om att det enligt skäl 75 i dataskyddsförordningen kan finnas synnerliga risker för dataskydds rättigheterna när personuppgifterna rör sårbara fysiska personer, framför allt barn. I allmänhet bör det inte vara möjligt att få mer information än nödvändigt om fysiska personer och deras handlingar genom att profilera dem på grundval av den information som används i processen för åldersstyrkande. Detta bör i största möjliga utsträckning säkerställas, även vid en uppgiftsincident.

17. Situationer där maktobalanser förekommer bör undvikas för att tjänsteleverantörer inte ska kunna tvinga enskilda personer att lida onödiga dataskyddsrisiker på grund av att de saknar handlingsmöjligheter¹⁵. Om det inte går bör dessa situationer erkännas och åtgärdas med hjälp av lämpliga motåtgärder¹⁶. Till exempel bör användare som inte kan eller inte vill använda en särskild metod för åldersstyrkande erbjudas genomförbara alternativ för att bevisa sin ålder. Tjänsteleverantörerna bör dessutom regelbundet bedöma om de utvalda metoderna och teknikerna, även de som tillhandahålls av tredje parter, fungerar i linje med sina ändamål och anpassa dem för att säkerställa korrekt behandling. Tredje parter som deltar i åldersstyrkandet bör också sträva efter att hjälpa tjänsteleverantörerna att fullgöra sina skyldigheter genom att inte skapa onödiga dataskyddsrisiker och genom att i god tid informera om alla relevanta ändringar de gjort av sina policyer, utformningar, tjänster med mera.

2.4 Ändamålsbegränsning och uppgiftsminimering

Tjänsteleverantörer och alla tredje parter som deltar i åldersstyrkandet bör endast behandla de åldersrelaterade attribut som är absolut nödvändiga för det särskilda, uttryckligt angivna och berättigade ändamålet.

18. I de flesta fall är ändamålet med åldersstyrkandet att fatta åldersrelaterade beslut om åtkomstkontroll, förhindra att barn skadas online, erbjuda en lämplig och åldersanpassad utformning eller upplevelse och så vidare. Oavsett användningsfall bör ändamålet med behandlingen av personuppgifter vara särskilt och uttryckligt angivet (artikel 5.1 b i dataskyddsförordningen). När personuppgifterna väl har samlats in får de inte behandlas ytterligare eller kombineras med fler uppgifter på ett sätt som är oförenligt med dessa ändamål. Tekniska åtgärder såsom integritetsfrämjande teknik bör användas för att begränsa möjligheten att ändra användningen av personuppgifterna. Organisatoriska åtgärder som begränsar vidareutnyttjandet av personuppgifter¹⁷ bör också vidtas, såsom policyer och avtalsförpliktelser.

¹⁵ Till exempel när registrerade ställs inför automatiserat beslutsfattande utan lämpliga prövningsmekanismer eller när samtycke inte kan ges frivilligt. Begreppet "maktobalans" diskuteras i EDPB:s yttrande 08/2024 om giltigt samtycke inom ramen för modeller för samtycke eller betalning som används av stora onlineplattformar (avsnitt 4.2.1.3), https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_sv.pdf.

¹⁶ Ur EDPB Guidelines 03/2022 on Deceptive design patterns in social media platform interfaces: how to recognise and avoid them (avsnitt 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.

¹⁷ Ur EDPB:s riktlinjer 4/2019 om artikel 25 Inbyggt dataskydd och dataskydd som standard, version 2.0, https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_sv.pdf.

19. Åldersrelaterade attribut är alla attribut som anger att en fysisk person är en viss ålder, över eller under en viss ålder, eller inom ett åldersintervall. Specifikationen av ändamålet kommer att avgöra vilka åldersrelaterade attribut som är relevanta och nödvändiga och ska samlas in. Detta kommer också att göra det möjligt för den personuppgiftsansvarige att bedöma proportionaliteten hos processen för åldersstyrkande. Fördelarna med denna process bör inte uppvägas av eventuella nackdelar när det gäller utövandet av de grundläggande rättigheterna¹⁸ (se avsnitt 2.2 ovan).
20. Den personuppgiftsansvarige bör därför bara samla in personuppgifter som är nödvändiga, adekvata och relevanta för de ändamål som de är tänkta att användas för. På så sätt bidrar uppgiftsminimering till att konkretisera och omsätta principerna om nödvändighet¹⁹ och proportionalitet i praktiken. Tjänsteleverantören kanske till exempel bara behöva veta om användaren är över eller under en åldersgräns. Detta skulle kunna genomföras genom en informationsbärande strategi som bygger på en tredjepartsleverantörs deltagande och där tjänsteleverantören bara ser det användbara resultatet av processen för åldersstyrkande (t.ex. "över" eller "under" åldersgränsen)²⁰. Olika strategier kan vara relevanta när tjänsteleverantören behöver veta om användaren befinner sig inom ett visst åldersintervall eller är född ett visst år.

2.5 Åldersstyrkandets ändamålsenlighet

Det bör gå att påvisa att åldersstyrkandet är tillräckligt effektivt för det ändamål för vilket det utförs.

21. Åldersstyrkanden bör utföras på sätt som är lämpliga för att uppnå ändamålet med behandlingen. I synnerhet bör det vara en förutsättning att alla lagstadgade åldersstyrkande åtgärder är ändamålsenliga för att principerna om nödvändighet²¹ och proportionalitet²² ska uppfyllas.
22. Åldersstyrkandets ändamålsenlighet bör utvärderas med avseende på flera aspekter, bland annat följande:
 - a) Tillgänglighet. Åldersstyrkandet bör vara allmänt tillgängligt för fysiska personer så att de kan bekräfta sin ålder eller bevisa att de uppfyller ett åldersrelaterat krav. Om vissa kategorier av personer riskerar att diskrimineras genom en särskild metod för åldersstyrkande, till exempel på grund av att de inte innehar rätt identitetshandlingar eller mobiltelefon eller på grund av en funktionsnedsättning, bör alternativa metoder för åldersstyrkande som erbjuder tillräcklig integritet, trygghet och säkerhet göras

¹⁸ Ur *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

¹⁹ Ur *EDPS Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

²⁰ En tredjepartsleverantör utför ålderskontrollen och ger användaren ett "åldersmärke" (en bärare av information om ålder) som denne kan visa för tjänsteleverantören utan att behöva bekräfta sin ålder på nytt. Åldersmärket kan innehålla olika användarattribut och uppgifter om när, var eller hur ålderskontrollen utfördes.

²¹ *EDPS, Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit*, https://www.edps.europa.eu/sites/default/files/publication/17-06-01_necessity_toolkit_final_en.pdf.

²² *Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data*, https://www.edps.europa.eu/sites/default/files/publication/19-02-25_proportionality_guidelines_en.pdf.

tillgängliga, när detta rimligen är genomförbart. Lösningar för åldersstyrkande bör också vara förenliga med all gällande lagstiftning om tillgänglighet²³.

- b) Tillförlitlighet. Enligt principen om korrekthet (artikel 5.1 d i dataskyddsförordningen) bör alla metoder vars ändamål är att avgöra om en fysisk person uppfyller ett åldersrelaterat krav hålla en lämplig och stabil nivå av korrekthet för att det ska gå att avgöra om de uppfyller detta krav eller inte. Lämpliga provningsmekanismer bör göras tillgängliga, i synnerhet när användarna i hög grad kan påverkas av ett automatiserat beslutsfattande, som när deras åldersrelaterade attribut inte har blivit korrekt fastställda (se avsnitt 2.7 nedan).
- c) Robusthet. Åldersstyrkandet bör inte påverkas av oväntade situationer och det bör, inom rimliga gränser, kunna stå emot troliga försök att lura eller kringgå systemet. Det bör noteras att robusthet inte har särskilt stor betydelse i samband med egen försäkran av ett åldersrelaterat attribut, eftersom tillförlitligheten hos en sådan metod främst beror på användarens goda vilja²⁴.

Tjänsteleverantörer som genomför åldersstyrkandet, liksom eventuella tredje parter som deltar i processen, bör även kunna visa att det är ändamålsenligt och vara öppna med hur de gör för att uppnå lämpliga nivåer av tillgänglighet, tillförlitlighet och robusthet (se avsnitt 2.10).

2.6 Laglighet, korrekthet och öppenhet

Tjänsteleverantörer och alla tredje parter som deltar i åldersstyrkande bör säkerställa att behandlingen av personuppgifter i åldersstyrkande syfte är laglig, korrekt och öppen för användarna.

- 23. Tjänsteleverantörerna måste säkerställa att de har en tillämplig rättslig grund i enlighet med artikel 6 i dataskyddsförordningen (och, i förekommande fall, det tillämpliga undantaget i artikel 9.2) för behandlingen av personuppgifter i samband med åldersstyrkandet. De kan till exempel behöva införa åldersstyrkande för att fullgöra en rättslig förpliktelse (artikel 6.1 c i dataskyddsförordningen), med beaktande av att åldersstyrkandet måste stå i proportion till det legitima mål som eftersträvas och kraven i artikel 6.3 i dataskyddsförordningen.
- 24. Dessutom måste tjänsteleverantörerna vara öppna inför användarna om exakt hur deras personuppgifter används och av vem. Detta är särskilt viktigt när flera parter deltar i processen för åldersstyrkande. Innan personuppgifter behandlas med ändamålet att styrka användarnas ålder måste användarna (i enlighet med artiklarna 12, 13 och 14 i dataskyddsförordningen) bland annat informeras om²⁵

- vilka personuppgifter som kommer att behandlas och hur,

²³ Exempelvis regleras tillgängligheten hos den offentliga sektorns webbplatser och mobila applikationer och produkters och tjänsters tillgänglighet genom direktivet om webbtillgänglighet respektive det europeiska tillgänglighetsdirektivet. Lösningar för åldersstyrkande måste säkerställa att de efterlever sådan lagstiftning genom att uppfylla kraven i den harmoniserade europeiska standarden för tillgänglighetskrav för IKT-produkter och IKT-tjänster, EN 301 549, version 3.2.1.

²⁴ EDPB har tidigare, i sitt bindande beslut 2/2023 om den tvist som hänskjutits av den irländska tillsynsmyndigheten angående TikTok Technology Limited (artikel 65 i dataskyddsförordningen), uttryckt allvarliga tvivel om att egen försäkran är effektivt som en metod för ålderskontroll i samband med behandlingar där risken är hög, https://www.edpb.europa.eu/system/files/2024-11/edpb_bindingdecision_202302_ie_sa_tti_children_sv_0.pdf.

²⁵ Se artikel 29-arbetsgruppens riktlinjer om öppenhet enligt förordning (EU) 2016/679, https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_sv.pdf.

- huruvida tredje parter kommer att delta i processen och, om så är fallet, vilka de är och vilka personuppgiftsansvariga och personuppgiftsbiträden som deltar i detta scenario,
 - om deras uppgifter kommer att delas med andra eller överförs till ett tredjeland,
 - hur länge deras personuppgifter kommer att lagras eller, om detta inte är möjligt, kriterierna för att fastställa lagringstiden,
 - vilka rättigheter de har i fråga om sina personuppgifter (artiklarna 15–22 i dataskyddsförordningen), inbegripet hur de kan överklaga ett felaktigt beslut som fattats till följd av åldersstyrkandet.
25. Öppenhet i samband med åldersstyrkande är särskilt viktigt när det gäller barn. Tjänsteleverantörerna måste se till att de förmedlar information om öppenhet till barn, när de berörs, på ett sätt som är tydligt och lätt att förstå.
26. Begreppet öppenhet är i grunden kopplat till korrekthet. Om tjänsteleverantörerna inte är tydliga och öppna med hur de behandlar fysiska personers information i syfte att styrka deras ålder kan behandlingen troligen inte anses vara korrekt, vilket i sin tur innebär att den troligen inte är laglig. Leverantörerna bör i synnerhet vara öppna med vilken inverkan varje metod har ur ett dataskyddsperspektiv om de erbjuder användarna olika metoder att bekräfta sin ålder.

2.7 Automatiserat beslutsfattande

Alla fall av automatiserat beslutsfattande i samband med åldersstyrkande bör vara förenliga med dataskyddsförordningen. I tillämpliga fall bör tjänsteleverantörer och alla berörda tredje parter vidta lämpliga åtgärder för att skydda fysiska personers rättigheter och friheter och berättigade intressen.

27. EU-lagstiftaren har valt en bred definition av automatiserat beslutsfattande som kräver granskning i varje enskilt fall²⁶. Automatiserade beslut kan fattas i olika skeden av processen för åldersstyrkande, antingen för att få tillgång till innehållet eller tjänsten eller genom de metoder som används för att bevisa åldern.
28. Ett helt automatiserat åldersstyrkande kan få rättsliga följder för de berörda fysiska personerna – till exempel när det gäller utövandet av deras yttrandefrihet – eller åtminstone i betydande grad påverka dem på liknande sätt²⁷. Det automatiska åldersstyrkandets följder för de fysiska personernas rättigheter kan variera, beroende på vilken typ av innehåll eller tjänster det rör sig om.
29. Tjänsteleverantörer och alla tredje parter som deltar i åldersstyrkande bör därför erbjuda användarna avhjälpande åtgärder och lämpliga prövningsmekanismer om deras åldersrelaterade attribut inte har blivit korrekt fastställda. Beroende på hur processen för

²⁶ Mål C-634/21, SCHUFA Holding (Scoring): Domstolens dom (första avdelningen) av den 7 december 2023 (begäran om förhandsavgörande från Verwaltungsgericht Wiesbaden – Tyskland) – QQ mot Land Hessen (Begäran om förhandsavgörande – Skydd för fysiska personer med avseende på behandling av personuppgifter – Förordning (EU) 2016/679 – Artikel 22 – Automatiserat individuellt beslutsfattande – Kreditupplysningsföretag – Automatiserat fastställande av ett sannolikhetsvärde om en persons framtida återbetalningsförmåga ("Scoring") – Tredje parts användning av detta sannolikhetsvärde), <https://eur-lex.europa.eu/legal-content/SV/ALL/?uri=CELEX%3A62021CA0634>.

²⁷ Riktlinjer om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679, <https://ec.europa.eu/newsroom/article29/items/612053/en>.

åldersstyrkande är uppbyggd ska de ange vem den registrerade bör kontakta för att utöva sina rättigheter²⁸.

30. Tjänsteleverantörer och alla berörda tredje parter bör vara särskilt uppmärksamma när barn berörs. Såsom anges i skäl 71 i dataskyddsförordningen bör åtgärder som "enbart grundas på automatiserad behandling och medför rättsverkan [...] eller på liknande sätt i betydande grad påverkar [den registrerade] [...] inte gälla för barn". Undantag från denna regel bör under begränsade omständigheter kvarstå, till exempel när det är nödvändigt "för att skydda deras välbefinnande"²⁹. Under alla omständigheter bör tjänsteleverantörer och alla berörda tredje parter genomföra lämpliga åtgärder – till exempel genomförbara alternativ, provningsmekanismer och, i tillämpliga fall, mänskligt ingripande – med information som är anpassad för barn, när de berörs.

2.8 Inbyggt dataskydd och dataskydd som standard

Åldersstyrkandet bör utformas, genomföras och utvärderas med beaktande av de mest integritetsbevarande metoder och tekniker som är tillgängliga för att uppfylla kraven i dataskyddsförordningen och på ett ändamålsenligt sätt skydda de registrerades rättigheter.

31. I enlighet med artikel 25 i dataskyddsförordningen bör personuppgiftsansvariga som arbetar med åldersstyrkande genomföra lämpliga tekniska och organisatoriska åtgärder och nödvändiga skyddsåtgärder för att säkerställa ett ändamålsenligt genomförande av alla dataskyddsprinciper och därmed de registrerades rättigheter och friheter. Kravet på att personuppgiftsansvariga ska ha dataskydd som standard i utformningsskedet av all behandling av personuppgifter gäller även personuppgiftsbiträden och under hela behandlingens livscykel.
32. Med tanke på att riskerna med systemen för åldersstyrkande kan se olika ut och vara allvarliga, särskilt när det är identitetshandlingar eller särskilda kategorier av personuppgifter såsom biometrisk data som behandlas, bör man göra allt man kan för att undvika onödig åtkomst till och onödig behandling, delning och lagring av personuppgifter. Systemen för åldersstyrkande och alla rättsliga eller tekniska instrument som fastställer kraven för sådana system bör också regelbundet ses över och vid behov uppdateras i syfte att ta hänsyn till det snabbt föränderliga landskapet vad gäller integritetsfrämjande teknik på det digitala identitetshanteringsområdet.
33. Såsom nämns i dataskyddsstyrelsens riktlinjer om inbyggt dataskydd och dataskydd som standard³⁰ medför hänvisningen till "den senaste utvecklingen" i samband med artikel 25 i dataskyddsförordningen en skyldighet för personuppgiftsansvariga att beakta de aktuella framsteg på teknikområdet som är tillgängliga på marknaden vid fastställandet av de tidigare nämnda lämpliga tekniska och organisatoriska åtgärderna. Standarder, bästa praxis och uppförandekoder som erkänns av berörda parter kan vara till hjälp vid fastställandet av

²⁸ EDPB anger i sina riktlinjer (se ovan) att "dessa rättigheter [kan] åberopas gentemot den personuppgiftsansvarige som skapar profilen och den personuppgiftsansvarige som fattar ett automatiserat beslut om en registrerad (med eller utan mänskligt ingripande), om dessa inte är en och samma person eller enhet."

²⁹ Ur riktlinjerna om automatiserat individuellt beslutsfattande och profilering enligt förordning (EU) 2016/679: "Det kan dock finnas situationer där det är nödvändigt för personuppgiftsansvariga att använda sig av enbart automatiserat beslutsfattande, inbegripet profilering, som har rättsliga eller på liknande sätt betydande följder för barn, t.ex. för att skydda deras välbefinnande."

³⁰ EDPB:s riktlinjer 4/2019 om artikel 25 Inbyggt dataskydd och dataskydd som standard, version 2.0,

https://www.edpb.europa.eu/system/files/2021-04/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_sv.pdf.

sådana åtgärder. Vid varje enskild behandling bör det dock bekräftas att dessa åtgärder är lämpliga.

34. Följaktligen rekommenderar EDPB, på grundval av den senaste utvecklingen på området åldersstyrkande när detta dokument utarbetades, att vederbörlig hänsyn tas till teknik och strukturer som framför allt nyttjar uppgifter som innehas av användaren samt säker lokal (enhetsbaserad) behandling, vilket möjliggör egenskaper såsom olänkbarhet³¹ (ur olika parter synvinkel och även vid otillåten samverkan eller dataintrång) och selektivt utlämnande³² av personuppgifter som den registrerade kontrollerar. Dessutom bör användningen av metoder som till exempel bygger på grupputfärdande³³ av engångsuppgifter eller krypteringsprotokoll såsom nollkunskapsbevis³⁴ göras tillgängliga för de registrerade när åldersstyrkandet kan medföra stora integritetsrisker för dem.

2.9 Åldersstyrkandets säkerhet

Tjänsteleverantörer och alla tredje parter som deltar i åldersstyrkande bör vidta lämpliga tekniska och organisatoriska åtgärder för att säkerställa att säkerhetsnivån är lämplig i förhållande till risken.

35. Enligt dataskyddsförordningen ska både personuppgiftsansvariga och personuppgiftsbiträden ha infört lämpliga tekniska och organisatoriska åtgärder för att säkerställa en säkerhetsnivå som är lämplig i förhållande till risken som de behandlade personuppgifterna utgör (skäl 83 och artikel 32). Känsligheten hos och arten och omfattningen av de personuppgifter som kan användas i åldersstyrkandet visar att en personuppgiftsincident skulle kunna få skadliga effekter.
36. Tillitsmodeller är avgörande för att förhindra dataintrång i samband med åldersstyrkande, eftersom de anger hur de olika parterna kan bekräfta varandras identiteter och integritet. De underlättar en säker kommunikation och ett säkert datautbyte mellan deltagare som kanske inte har haft några tidigare förbindelser. Pseudonymisering och kryptering av personuppgifter kan också bidra till att mildra de eventuella skadliga effekterna av ett dataintrång. För ett säkert åldersstyrkande kan man även behöva tillämpa principen om lagringsminimering och använda korta lagringstider, eftersom man på så vis minskar exponeringsytan. En policy om att inte föra några loggar kan anses vara en värdefull skyddsåtgärd: När användarens ålder väl har bekräftats sparas inga av de personuppgifter som använts i åldersstyrkandesprocessen.
37. Eftersom det rättsliga trycket att styrka någons ålder ökar, liksom antalet leverantörer som kan omfattas av sådana regler, bör man i praktiken förvänta sig att säkerhetsincidenter kommer att inträffa. Man bör fastställa om alla lämpliga tekniska skyddsåtgärder och alla lämpliga organisatoriska åtgärder har vidtagits för att omedelbart fastställa om en incident har ägt rum, vilket i sin tur är avgörande för om anmälningsskyldigheten ska fullgöras³⁵. Ett

³¹ Olänkbarhet innebär att det inte går att koppla eller korrelera olika dataposter, åtgärder eller transaktioner till en specifik registrerad person.

³² Selektivt utlämnande är en egenskap hos märken (informationsbärare), referenser och intyg som gör att de registrerade kan dela endast den information de vill dela med specifika parter från fall till fall.

³³ Grupputfärdande bygger på att man svarar på en begäran om referenser från den registrerade med en uppsättning eller en grupp av referenser som tagits fram samtidigt.

³⁴ Ett nollkunskapsbevis är ett protokoll där en part (sändaren) kan visa en annan part (kontrollanten) att ett visst påstående är sant, utan att kontrollanten får någon annan information än att påståendet är sant.

³⁵ Ur EDPB:s riktlinjer 9/2022 om anmälan av personuppgiftsincidenter enligt den allmänna dataskyddsförordningen, https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202209_personal_data_breach_notification_v2.0_sv.pdf.

centralt inslag i alla datasäkerhetspolicyer är att man om möjligt ska kunna förhindra en incident och, om den inträffar, reagera i god tid. Det bör därför också anses vara avgörande att man efter en säkerhetsincident snabbt kan göra åldersstyrkandet tillgängligt igen. Likaså är det mycket viktigt att säkerställa motståndskraften i ekosystemet för åldersstyrkande och främja förekomsten av olika alternativ och löst kopplade parter³⁶ som inte är så beroende av varandra att ett misslyckande eller ett haveri hos den ena orsakar betydande begränsningar i åtkomsten.

38. Det är förvisso oerhört viktigt att vidta säkerhetsåtgärder vid åldersstyrkande, men de garanterar inte att vare sig tillåten eller otillåten åtkomst till personuppgifter inte kommer att påverka fysiska personers rättigheter. De kan inte ersätta tillämpningen av principerna om nödvändighet, proportionalitet eller inbyggt dataskydd och dataskydd som standard.

2.10 Ansvarsskyldighet

Tjänsteleverantörer och alla tredje parter som deltar bör införa styrningsmetoder som gör att de kan vara ansvariga för sin strategi för åldersstyrkande och för att visa att de efterlever dataskyddsförordningen och andra rättsliga krav.

39. Eftersom olika intressenter deltar spelar styrningen av åldersstyrkandet en avgörande roll för ansvarsskyldigheten. Åldersstyrkande bör ske inom ramen för en styrning som säkerställer att alla processer och system utformas, genomförs, ses över, dokumenteras, bedöms, används, underhålls, testas eller granskas på ett sätt som uppfyller såväl dataskyddsbestämmelser som andra rättsliga krav. Denna ram bör åtminstone omfatta de strategier för dataskydd (artikel 24.2 i dataskyddsförordningen) och de prioriterings- och beslutsprocesser som krävs för att uppnå efterlevnadsmålen och hantera riskerna på ett lämpligt sätt under hela åldersstyrkandets livscykel.
40. I styrningsramen bör man till exempel avgränsa vem som ur en personuppgiftsansvarigs/personuppgiftsbiträdes perspektiv är ansvarig, och på vilket sätt, för exakt vilka verksamheter och åtgärder som genomförs vid behandlingen. Ramen bör också säkerställa att myndigheter och berörda parter kan granska åldersstyrkandet som sig bör. Styrningsramen är avgörande för ansvarsskyldigheten, men också för öppenheten i och förtroendet för åldersstyrkandet. De registrerade är mer benägna att lita på metoderna när man är öppen med hur de fungerar, hur beslutsfattandet går till och så vidare.
41. En del av styrningsramen avser också säkerställandet av ändamålsenlighet (avsnitt 2.5), inbyggt dataskydd och dataskydd som standard (avsnitt 2.8) och säkerhet (avsnitt 2.9) vad gäller åldersstyrkandet.

För Europeiska dataskyddsstyrelsen

³⁶ Parter som i minsta möjliga utsträckning är beroende av varandra, vilket innebär att konsekvenserna blir mindre vid förändringar eller fel.

Ordförande

(Anu Talus)