Datum: 2026-10-16
Diarienummer S2026/01273
Socialpartementet
s.remissvar@regeringskansliet.se

Remissvar betänkandet SOU 2026:35 "En åldersgräns för barns tillgång till sociala medier"

DFRI, Föreningen för Digitala Fri- och Rättigheter, har tagit del av betänkandet SOU 2026:35 "En åldersgräns för barns tillgång till sociala medier". Vi kommenterar inte åldersgränsen som sådan — vi kritiserar enbart den tekniska konstruktion som valts. Vår utgångspunkt är att om en åldersgräns väl införs, bör den utformas så att den inte i sig skapar nya integritetsrisker.

Vi föreslår att en ny bestämmelse införs i dataskyddslagen (2018:218) som uttryckligen anger att endast dubbelblinda metoder är tillåtna och att åldersverifiering aldrig får vara en orsak till insamling av personuppgifter.

Avslutningsvis förklarar vi varför vi anser att en obligatorisk åldersverifiering för åtkomst till medier och tjänster på Internet grovt kränker individers rättigheter till fri och öppen kommunikation, barn såväl som vuxna. Det finns andra metoder som kan uppnå syftet att skydda barn från skadligt innehåll, med färre ingrepp i privatlivet hos hela befolkningen.

Barnets rätt att inte bli spårbart

Barnet skyddas bäst genom att inte bli spårbart. Uppgifter insamlade före myndighetsåldern blir i praktiken permanenta och ger upphov till förutsägelsemodeller som fortsätter in i vuxenlivet. Barn saknar dessutom förutsättningar att lämna giltigt samtycke till sådan behandling.

Betänkandets 3 § förbjuder "inloggat läge" för barn under 15 år utan metodkrav (s. 191). Metodvalet är fritt, vilket i praktiken tillåter identifieringsbaserade eller biometriska metoder — i strid med GDPR:s principer om dataminimering.

SOU:n redogör inte heller för IMY:s restriktiva praxis rörande biometri (*Vägledning om ansiktsigenkänning och GDPR*) — en metodneutral 3 § tillåter just den typ av metoder som IMY är restriktiv till (IMY omnämns som tillsynsmyndighet, s. 244–246).

Dubbelblind verifiering som lösning

Med *dubbelblind åldersverifiering*, får plattformen endast uppgift om huruvida åldersgränsen är uppnådd, och varken plattformen eller utfärdaren får ytterligare kännedom om den andra parten. Barnet lämnar inga personuppgifter. Betänkandet redogör för flera EU-rättsliga instrument som möjliggör ett bindande metodkrav i 3 §:

- *EU-kommissionens riktlinjer till artikel 28.1 i Digital Services Act, EU-förordning 2022/2065, punkt 46*; uppmanar leverantörer att använda dubbelblinda metoder för ålderskontroll (s. 112, s. 228).
- *EDPB-uttalande 1/25 om åldersstyrkande* (antaget 11 februari 2025) bekräftar samma krav (s. 110–111).

- *EU-kommissionens rekommendation C(2026) 4225 final* (29 april 2026) är ett separat ramverk riktat till medlemsstater (s. 148–149).
- *Förordningen 2024/1183 (eIDAS 2.0)* ålägger medlemsstater att senast den 21 november 2026 erbjuda en europeisk digital identitetsplånbok med stöd för åldersattribut och Zero-Knowledge-Proof enligt öppna standarder (OpenID for Verifiable Credentials, ISO 18013-7) (s. 145–147).
- *EU-kommissionens Age Verification App* har publicerats som referensimplementation med öppen källkod klar i april 2026 (s. 148).

Författningsförslag

Vi föreslår att följande bestämmelse införs i dataskyddslagen (2018:218), 2 kap. 4 a §

> *Åldersverifiering som krävs enligt svensk författning får aldrig vara en orsak till insamling av personuppgifter. Metoden ska vara dubbelblind, och endast den binära uppgiften om huruvida en åldersgräns är uppnådd får göras tillgänglig.*
>
> *1. Identifiering, biometrisk behandling (såsom ansiktsigenkänning, röstigenkänning, iris-skanning eller fingeravtryck) och upprättande av centraliserade databaser över verifierade användare är otillåtna.*
>
> *2. Personuppgifter som behandlas i samband med verifiering får inte användas för andra ändamål, inklusive profilering, beteendeanalys, AI-träning, riktad reklam eller tredjepartsöverföring, och får inte lagras längre tid än vad som krävs för att konstatera att åldersgränsen är uppnådd.*
>
> *3. Överträdelse av denna bestämmelse ska vid Integritetsskyddsmyndighetens bedömning av administrativa sanktionsavgifter enligt artikel 83 i EU:s dataskyddsförordning anses utgöra en allvarlig överträdelse.*

Bestämmelsen stänger luckan i GDPR artikel 8, som skyddar barns samtycke men inte reglerar *hur* åldersverifiering får genomföras. Bestämmelsen kan införas utan övergångstid eftersom digital åldersverifiering inte var lagstadgad innan. Plattformar som frivilligt tillämpar identifieringsbaserad verifiering idag saknar rättsligt skydd för sin metod och deras frivilliga val ger ingen rätt att motsätta sig ny lagstiftning.

DFRI väljer att ändra i dataskyddslagen istället för den nya sociala medier-lagen, så att samma skydd även applicerar vid digital åldersverifiering enligt alkohollagen (2010:1622), tobakslagen (2010:1882), marknadsföringslagen (2008:486) och lagen om handel med vissa receptfria läkemedel (2009:730).

Vi rekommenderar vidare att regeringen på EU-nivå verkar för att en motsvarande bestämmelse även införs i GDPR, i syfte att säkerställa enhetliga förutsättningar för plattformar verksamma i flera medlemsstater.

Bakgrund: Andra åtgärder än åldersverifiering är mer önskvärda för att skydda barns exponering för skadligt innehåll

DFRIs åsikt är att en obligatorisk åldersverifiering för åtkomst till medier och tjänster på Internet grovt kränker individers rättigheter till fri och öppen kommunikation, barn såväl som vuxna. Det kan också leda till identifiering av individers besök i mycket större skala än avsett. Det finns andra metoder som kan uppnå syftet att skydda barn från skadligt innehåll, med färre ingrepp i privatlivet hos hela befolkningen.

Om åldersverifiering införs, med följden att individers besök på olika tjänster kan lagras, finns det hög risk för ändamålsglidning, oförutsedd analys av identifierade individers beteenden samt ett ökat cybersäkerhetshot.
Obligatorisk åldersverifiering på sociala medier riskerar att göra hela internet mindre privat för att hantera problem som borde lösas mer riktat. Den kan skapa nya säkerhetsrisker, försvåra anonym kommunikation, utestänga legitima användare och ge begränsad effekt om de bakomliggande problemen kvarstår. Innan sådana krav införs bör man därför visa att de faktiskt fungerar, att mindre ingripande åtgärder inte räcker och att nyttan står i proportion till kostnaderna för individens frihet och integritet.
EU:s dataskyddsstyrelse, EDPB, framhåller att åldersbedömning måste skydda barn samtidigt som den använder så lite integritetskänslig information som möjligt. EU-kommissionens riktlinjer från 2025 betonar också att plattformar bör bedöma om ålderskontroll verkligen behövs eller om mindre ingripande åtgärder kan ge tillräckligt skydd.
Exempel på problem och hur de kan hanteras:

- Om problemet är skadliga rekommendationer, åtgärda rekommendationssystemen.
- Om problemet är trakasserier, förbättra moderering och möjligheterna att blockera användare.
- Om problemet är olämpligt vuxeninnehåll, överväg riktade kontroller för just det innehållet i stället för generella krav för hela internet.

Det är naivt att tro att innehåll, algoritmer eller trakasserier som bedöms som skadligt skulle sluta vara skadligt för att en åldersgräns passeras. Det finns inget enkelt sätt att lösa dessa problem. Det som krävs är långsiktigt arbete och tillräckliga resurser sätts till för att utföra detta arbete.

Det existerar redan teknik för att kontrollera barns exponering i digitala medier.

Smarta telefoner och andra enheter har redan möjligheter för föräldrar att blockera tjänster och innehåll, köp och begränsa kommunikation. Många föräldrar använder redan detta. Istället för att tvinga hela befolkningen att identifiera sig för åtkomst till Internettjänster så kan myndigheter, skolor och andra instanser hjälpa och utbilda föräldrar att använda dessa kontroller.

Åldersverifiering för vissa tjänster kan leda till total identifiering för att alls få åtkomst till Internet

Unga människor har mycket kreativ förmåga att runda kontroller. Exempel på detta är att meddelande-chattar i tjänster som inte räknas som sociala medier används för tillfällig kommunikation mellan unga. I takt med att detta blir synligt så kan resultatet bli att all tillgång till Internet kräver identifiering. Flera länder överväger redan detta.

Med åldersverifiering, och som följd någon form av identifiering av användare, ökar risken för ändamålsglidning.

Genom att myndigheter och/eller tredjepartsaktörer kan identifiera vilka besök individer gör, kan denna information användas för syften som inte är avsedda idag. Exempelvis felaktigt identifiera personer som hot i någon form, identifiera personer med riskbeteenden eller identifiera personer med misstänksamma relationer. En kommersiell aktör kan använda uppgifterna för att analysera och negativt påverka individers möjligheter till försäkringar, anställningar eller annat. På ett sätt som inte kan förutses.

Genom lagring av befolkningens identifierade uppgifter, ibland samlat med besöksdata, ökar risken markant för cyberattacker och dataläckage

Om befolkningens besöksdata, eller indirekt besöksdata (metadata), finns lagrat hos myndighet eller kommersiell aktör, blir känsliga uppgifter mer tillgängliga för attack och läckage till främmande makt, bedragare och andra illvilliga aktörer. Denna information kan exempelvis användas för

utpressning av högprofilerade individer, såsom politiker, säkerhetspersonal och makthavare inom affärsvärlden.

Föreningen för Digitala Fri- och Rättigheter, DFRI

Christian Häggström, styrelseledamot DFRI

Övriga delaktiga i författandet av remissvaret har varit
Bengt Jonsson, medlem i DFRI
Börje Ohlman, generalsekreterare i DFRI
Ulrika Vincent, ordförande i DFRI

https://dfri.se , e-post styrelse@dfri.se