Kopia till
a.arm@regeringskansliet.se

Arbetsmarknadsdepartementet
a.remissvar@regeringskansliet.se

Remiss av betänkandet Genomförande av plattformsdirektivet (SOU 2026:3)

Transportstyrelsens synpunkter

Transportstyrelsen tillstyrker förslagen och bedömningarna i betänkandet med följande synpunkter.

Avsnitt 7.5 Förbud mot behandling och insamling av vissa uppgifter.

Det saknas en diskussion om de cybersäkerhetsrisker som uppstår om plattformens mjukvara har för omfattande behörigheter i användarens enhet (t.ex. tillgång till mikrofon eller positionering i bakgrunden).

Konsekvens och åtgärd: För omfattande behörigheter skapar en kritisk sårbarhet för otillbörlig kartläggning av privatlivet, vilket kräver införande av tekniska spärrar och tidsstyrda behörigheter i plattformens arkitektur.

Avsnitt 7.6 Konsekvensbedömning avseende dataskydd

Det saknas en tydlig koppling till hur cybersäkerhetsincidenter (som kan påverka algoritmernas korrekthet) ska hanteras och kommuniceras till de som utför arbetet.

Konsekvens och åtgärd: Utan koppling till it-säkerhet kan algoritmer fatta felaktiga beslut baserat på manipulerat data, vilket innebär att konsekvensbedömningar (DPIA – data protection impact assessment) måste integrera specifika rutiner för incidenthantering.

Avsnitt 7.8 Mänsklig kontroll och utvärdering

Det saknas krav på loggning och spårbarhet som är tillräckligt robust för att en mänsklig granskare ska kunna verifiera att systemet inte har blivit komprometterat av en extern part.

Konsekvens och åtgärd: Brist på loggning och spårbarhet försvårar kontroll, revision och upptäckt av manipulation. Krav på säker loggning och revisionsbarhet bör därför införas.

Transportstyrelsen
Generaldirektör
601 73 Norrköping
Besöksadress
Olai Kyrkogata 35, Norrköping

Telefon 0771-503 503
Telefax 011-185 256

transportstyrelsen.se
kontakt@transportstyrelsen.se

Barbro Torstensson
barbro.torstensson@transportstyrelsen.se

Avsnitt 8.2.6 Sekretess för skyddsvärda uppgifter

Det saknas en analys av hur transparensreglerna i plattformsdirektivet förhåller sig till kraven på cybersäkerhet i andra regelverk, såsom NIS2-direktivet eller AI-förordningen.

Konsekvens och åtgärd: Alltför bred transparens riskerar att exponera tekniska sårbarheter för angripare, vilket kräver en analys för att balansera insynskraven mot säkerhetsregler i NIS2 och AI-förordningen.

Avsnitt 9.7 Kommunikationskanaler för personer som utför plattformsarbete

Det saknar krav på att dessa kommunikationskanaler ska vara skyddade mot avlyssning och dataexfiltrering genom modern cybersäkerhetsstandard (t.ex. TLS-krav eller flerfaktorsautentisering för åtkomst).

Konsekvens och åtgärd: Osäkra kanaler kan leda till dataläckage, avlyssning och nätfiske, vilket gör det nödvändigt att ställa krav på end-to-end-kryptering och säker multifaktorsautentisering (MFA)

———

Beslut i detta ärende har fattats av generaldirektör Jonas Bjelfvenstam. I den slutliga handläggningen av ärendet deltog avdelningsdirektör Kajsa Möller, IT-säkerhetsarkitekt Arju Ambin och utredare Barbro Torstensson, den senare föredragande.