Tågföretagen

Datum
2026-10-01

Era diarienr: Ju2026/01011

Mottagare
ju.remissvar@regeringskansliet.se
ju.L4@regeringskansliet.se

Tågföretagens remissyttrande avseende betänkandet ’Tillgång till passageraruppgifter i brottsbekämpningen’ (SOU 2026:28)

Tågföretagen är bransch- och arbetsgivarorganisation med cirka 90 medlemmar som har närmare 19 000 medarbetare. Bland medlemmarna finns de flesta av Sveriges aktiva tågoperatörer och ett flertal järnvägsinfrastrukturföretag.

Sammanfattande ställningstagande

Tågföretagen har tagit del av Justitiedepartementets remiss av betänkandet *Tillgång till passageraruppgifter i brottsbekämpningen (SOU 2026:28)* och lämnar följande synpunkter.

Tågföretagen avstyrker att förslaget om en trafikslagsneutral PNR-lagstiftning genomförs i sin nuvarande form.

Tågföretagen delar ambitionen att ge brottsbekämpande myndigheter effektiva verktyg för att förebygga, förhindra och bekämpa allvarlig och gränsöverskridande brottslighet. Det kan finnas legitima behov av att ge behöriga myndigheter tillgång till passageraruppgifter som transportföretagen redan samlar in inom ramen för sin normala verksamhet.

Det är positivt att förslaget inte innebär någon generell skyldighet för transportföretagen att samla in nya uppgifter, utan endast att överföra sådana uppgifter som redan finns tillgängliga i den normala verksamheten. För järnvägens del innebär detta exempelvis att uppgifter om biljetter som säljs ombord och där efterfrågade person- eller bokningsuppgifter inte samlas in normalt inte bör omfattas av rapporteringsskyldigheten.

Förslaget innehåller emellertid flera oklarheter som behöver hanteras innan en reglering kan genomföras. Det gäller särskilt vem som ska ansvara för rapporteringen när den som utför den gränsöverskridande trafiken inte är samma aktör som har sålt biljetten och innehar uppgifterna. Det gäller också avsaknaden av gemensamma standarder, underskattade införande- och förvaltningskostnader samt ansvaret för informationssäkerhet och cybersäkerhetsrisker. Utredningen analyserar dessutom inte tillräckligt vilka nya sårbarheter som uppstår när stora mängder passageraruppgifter systematiskt ska överföras mellan privata och offentliga aktörer genom nya digitala gränssnitt. För järnvägssektorn, som i stor utsträckning bedriver samhällsviktig

verksamhet, behöver frågor om cybersäkerhet, motståndskraft och kontinuitetshantering ges en mer framträdande plats i den fortsatta beredningen.

Gränsöverskridande järnvägstrafik bedrivs på en gemensam europeisk marknad och är beroende av gemensamma och förutsebara regler och tekniska standarder. Sverige bör därför undvika att införa nationella särlösningar som riskerar att behöva ändras eller ersättas när en EU-gemensam reglering eller standardisering utvecklas.

Sammanfattning

Tågföretagen anser att:

1. **Skyldigheten även fortsättningsvis tydligt ska begränsas till befintliga uppgifter.** Järnvägsföretagen ska endast behöva överföra sådana uppgifter som de redan samlar in inom ramen för sin normala verksamhet. Regleringen får inte direkt eller indirekt tvinga företagen att börja samla in nya personuppgifter.
2. **Rapporteringsansvaret måste förtydligas.** Den aktör som utför den gränsöverskridande trafiken är inte alltid samma aktör som har sålt biljetten eller innehar bokningsuppgifterna. Det måste tydligt framgå vilken aktör som ansvarar för rapporteringen och vilka skyldigheter som gäller när uppgifterna finns hos en återförsäljare, distributör eller annan transportör.
3. **Avgränsningen till gränsöverskridande tågtrafik ska framgå tydligt.** Förslaget omfattar inte inrikes tågtrafik, vilket måste avspeglas tydligt i lagstiftning, föreskrifter och tekniska krav.
4. **Gemensamma standarder måste utvecklas.** Det behövs standardiserade och långsiktigt hållbara lösningar för myndigheters förfrågningar om passageraruppgifter.
5. **Inrikes resenärer ska inte omfattas** av regleringen men om dylika förfrågningar kommer nationellt behöver de följa samma process samt uppgifter.
6. **Kostnaderna har underskattats.** Utredningens konsekvensanalys är otillräcklig när det gäller kostnaderna för utveckling, systemintegration, informationssäkerhet, cybersäkerhet, testning, drift, förvaltning och regelefterlevnad.
7. **Kravspecifikationerna måste tas fram tillsammans med företagen.** Järnvägsföretagen behöver involveras tidigt i utvecklingsarbetet.
8. **Överföringen bör ske genom ett standardiserat API.** En säker och standardiserad API-lösning bör vara utgångspunkten.
9. **Sverige bör undvika nationella särlösningar.** Kraven bör samordnas med den internationella och europeiska utvecklingen.
10. **Regleringen måste föregås av en fördjupad cybersäkerhetsanalys.** Innan ett nationellt system införs bör hotbild, sårbarheter, ansvarsfördelning och konsekvenser för samhällsviktig verksamhet analyseras. Kraven bör utformas enligt principerna om säkerhet genom design och säkerhet som standard.

Mot denna bakgrund anser Tågföretagen att förslaget inte bör genomföras i sin nuvarande form. Om regeringen går vidare krävs ett fortsatt beredning- och utvecklingsarbete i nära dialog med järnvägsföretagen.

Endast uppgifter som företagen redan samlar in

Tågföretagen ser positivt på att rapporteringsskyldigheten enligt förslaget ska begränsas till uppgifter som transportföretaget samlar in inom ramen för sin normala verksamhet.

Denna princip måste upprätthållas och tydliggöras i den fortsatta beredningen. En skyldighet att överföra befintliga uppgifter får inte i praktiken utvecklas till en skyldighet att samla in nya uppgifter.

För järnvägens del innebär detta exempelvis att biljetter som säljs ombord utan insamling av efterfrågade boknings- eller personuppgifter inte bör generera någon rapporteringsskyldighet avseende uppgifter som företaget inte har.

Den föreslagna ordningen måste också ta hänsyn till att järnvägens försäljningsmodeller varierar. Vissa biljetter är personliga och kopplade till en bokning, medan andra biljetter kan vara opersonliga eller säljas utan fullständiga kontakt- och identitetsuppgifter. Ett och samma järnvägsföretag kan använda flera olika försäljningskanaler och biljettyper.

Det behövs därför ett tydligt klargörande av att frånvaro av en viss uppgift inte är en brist i rapporteringen när uppgiften inte samlas in i företagets normala verksamhet.

Vem ska ansvara för rapporteringen?

En central oklarhet i förslaget gäller vem som ska rapportera uppgifterna.

Enligt förslaget läggs skyldigheten på det transportföretag som bedriver den gränsöverskridande trafiken. Den aktör som utför trafiken är emellertid inte alltid samma aktör som har sålt biljetten eller innehar boknings- och betalningsuppgifterna.

Biljetten kan exempelvis ha sålts av:

- ett annat järnvägsföretag,
- en oberoende biljettåterförsäljare,
- en digital distributionsplattform,
- en resebyrå eller reseagent,
- ett företag som säljer en sammanhållen resa med flera transportörer,
- en regional kollektivtrafikmyndighet eller dess försäljningssystem.

I vissa fall kan uppgifter vara fördelade mellan flera aktörer. Det utförande järnvägsföretaget kan ha information om tåget och transporten, medan återförsäljaren har bokningsrelaterade, kontakt- och betalningsuppgifterna.

Tågföretagen anser därför att det måste tex behöver klargöras är:

1. vilken aktör som har den rättsliga rapporteringsskyldigheten,
2. om skyldigheten följer den operativa trafiken, biljettförsäljningen eller innehavet av uppgifterna,
3. hur ansvaret ska fördelas när flera aktörer innehar olika delar av informationen,
4. om ett järnvägsföretag kan fullgöra sin skyldighet genom att rapportera enbart de uppgifter som företaget faktiskt innehar,
5. om och på vilken rättslig grund uppgifter ska överföras mellan kommersiella aktörer före rapporteringen till myndigheten,
6. vem som ansvarar för felaktiga, ofullständiga eller för sent överförda uppgifter.

Det bör inte krävas att ett utförande järnvägsföretag samlar in uppgifter från andra försäljnings- eller distributionsaktörer endast i syfte att kunna rapportera dem vidare. En sådan ordning skulle skapa ytterligare behandling och överföring av personuppgifter, oklar ansvarsfördelning och nya informationssäkerhetsrisker.

Informationssäkerhet och cybersäkerhet

En systematisk överföring av passagerar-, bokningsrelaterade, kontakt- och betalningsuppgifter skapar betydande informationssäkerhets- och cybersäkerhetsrisker.

Den föreslagna ordningen innebär att stora mängder personuppgifter samlas, bearbetas och överförs mellan flera privata och offentliga aktörer genom nya tekniska gränssnitt och integrationslösningar. Därmed skapas också en ny digital infrastruktur för informationsutbyte som riskerar att bli ett attraktivt mål för cyberangrepp, dataintrång och andra antagonistiska handlingar. Varje nytt gränssnitt, integrationspunkt eller central mottagningsfunktion innebär en potentiell sårbarhet som kan utnyttjas för att få tillgång till känsliga uppgifter, påverka datakvaliteten eller störa verksamhet som är av betydelse för samhället.

För järnvägssektorn är detta särskilt relevant eftersom flera aktörer bedriver samhällsviktig verksamhet och redan omfattas av omfattande krav på informationssäkerhet, kontinuitetshantering och cybersäkerhet. Ett nytt nationellt rapporteringssystem måste därför utformas så att det stärker, och inte försvagar, sektorns samlade motståndskraft.

Mot denna bakgrund måste cybersäkerhet genom hela informationskedjan utgöra en grundläggande del av systemets utformning redan från början.

Kraven måste också samordnas med andra tillämpliga regelverk om dataskydd, informationssäkerhet, cybersäkerhet och säkerhetsskydd. Företagen bör inte bära ett otydligt eller

obegränsat ansvar för risker som uppstår i myndigheternas system eller i den gemensamma infrastrukturen. Ansvarsfördelningen mellan myndigheter, systemleverantörer och transportföretag måste vara tydlig innan några tekniska eller rättsliga skyldigheter träder i kraft.

Otillräcklig konsekvensanalys och underskattade kostnader

Tågföretagen anser att utredningens konsekvensanalys är otillräcklig.

Utredningen konstaterar att förslaget kommer att innebära kostnader och administration för transportföretagen och bedömer att en del eller hela kostnadsökningen kan komma att bäras av konsumenterna. Denna övergripande bedömning är inte tillräcklig för att ligga till grund för ett beslut om nya och tekniskt omfattande skyldigheter.

Utredningen analyserar inte heller tillräckligt de kostnader och risker som följer av ökade cybersäkerhetskrav. För att uppfylla lagstiftningens krav kommer företagen sannolikt att behöva investera i säkerhetsarkitektur, logghantering, övervakning, incidenthantering, säkerhetsgranskningar, penetrationstester, kontinuitetsåtgärder och löpande anpassningar till förändrade hotbilder. För verksamheter som bedöms som samhällsviktiga kan dessa investeringar vara betydande.

Harmonisering inom EU

Tågföretagen anser att Sverige bör verka för en gemensam europeisk reglering och standardisering. Ett nationellt regelverk riskerar annars att avvika från kommande europeiska regler och standarder och leda till att järnvägsföretagen måste utveckla flera parallella rapporteringslösningar.

Om flera medlemsstater inför olika nationella krav blir situationen svårhanterlig för järnvägsföretag som bedriver trafik över nationsgränserna. Ett företag kan då behöva rapportera olika uppgifter, vid olika tidpunkter och genom olika tekniska lösningar för samma internationella tågresa.

För Tågföretagen
Lina Lagerroth
Senior Näringspolitisk expert