



Datum: 2026-09-28

Vårt ärendenr: SJ-2026-0097

Ert diariernr: Ju2026/01011

Handläggare:

Gunnar Alexandersson

Gunnar.Alexandersson@sj.se

Mottagare:

ju.remissvar@regeringskansliet.se

ju.L4@regeringskansliet.se

Tillgång till passageraruppgifter i brottsbekämpningen (SOU 2026:28) – yttrande från SJ AB

SJ AB (SJ) har tagit del av Justitiedepartementets remiss av SOU 2026:28 *Tillgång till passageraruppgifter i brottsbekämpningen* och lämnar synpunkter i detta yttrande. Yttrandet fokuserar på valda delar av betänkandets förslag. SJ hänvisar i övrigt till det yttrande som lämnas av Tågföretagen.

1. Övergripande synpunkter

SJ välkomnar ambitionen att ge brottsbekämpande myndigheter effektiva verktyg för att förebygga, förhindra och bekämpa allvarlig och gränsöverskridande brottslighet. När befintlig lagstiftning för luftfarten nu föreslås utvidgas till fler trafikslag är det särskilt viktigt att få ett regelverk som tydliggör skyldigheter och ansvarsförhållanden, samtidigt som man undviker att införa system som medför betydande kostnadsökningar och/eller ökade risker exempelvis vad gäller cybersäkerhet. Dessa delar utvecklas närmare nedan.

2. Utlämnande av personuppgifter

SJ välkomnar att förslagen till ny lagstiftning för *gränsöverskridande resor* innebär att transportföretagen även fortsättningsvis endast ska tillhandahålla de personuppgifter de redan har tillgång till i sin ordinarie verksamhet. Med den föreslagna utvidgning av vilka uppgiftstyper som omfattas, är det av central betydelse att denna begränsning kvarstår i järnvägssektorn.

Den nya skrivningen i exempelvis polislagen (1984:387) om att *"Det som sägs om transportföretag gäller även andra företag som yrkesmässigt får tillgång till transportföretagets uppgifter om transporter"*, tolkar SJ som att exempelvis även rese-



byråer och andra tredjepartssäljare omfattas av skyldigheterna. Här är det viktigt att bringa klarhet i vad som gäller om en tredjepartssäljare har tillgång till vissa typer av uppgifter medan det utförande transportföretaget har tillgång till andra uppgiftstyper. Vidare bör dubbelrapportering undvikas.

När det gäller *inrikes resor* motsätter sig SJ starkt utredningens bedömning att frågan om utlämnande av passageraruppgifter bör lämnas oreglerad och överlåtas till transportföretagen att hantera frivilligt. SJ förespråkar inte ett system med kontinuerligt och obligatoriskt utlämnande av samtliga passageraruppgifter i inrikes trafik, men det är emellertid nödvändigt att det i lag regleras i vilken omfattning, under vilka förutsättningar och hur, sådana uppgifter **ska** lämnas ut till brottsbekämpande myndigheter.

Det nuvarande tillståndet i Sverige innebär en betydligt större inskränkning av resenärernas fri- och rättigheter än vad utredningen beskriver. Brottsbekämpande myndigheter begär redan i dag ut uppgifter om inrikes resor i betydande utsträckning. För SJs del rör det sig om uppskattningsvis 50 procent av den totala mängden passageraruppgifter som efterfrågas. Dessa förfrågningar hanteras på rent frivillig basis, med stöd av 2 kap. 5 § lagen (2018:218) med kompletterande bestämmelser till EU:s dataskyddsförordning, och i regel utan annat underlag än ett påstående om att uppgifterna behövs för att förebygga eller utreda brott. Resenärer saknar därmed helt möjlighet att förutse när deras personuppgifter kan komma att delas med brottsbekämpande myndigheter.

Dagens situation skapar därutöver en oskälig riskexponering för transportföretagen, som tvingas navigera mellan risken att kritiseras för godtyckliga utlämnanden på (formellt sett) frivillig basis och att utsättas för påtryckningar från brottsbekämpande myndigheter vid avslag. Det är lagstiftarens – inte transportföretagens – uppgift att göra den proportionalitetsbedömning som krävs enligt 2 kap. 20–21 §§ regeringsformen och fastställa under vilka förutsättningar utlämnande ska ske.

3. Cybersäkerhetsrisker och kostnadskonsekvenser

Utredningen föreslår att transportföretag som bedriver passagerartrafik med tåg, buss eller färja inför varje resa som ankommer till eller avgår från Sverige ska överföra PNR-uppgifter (*Passenger Name Record*) till den s.k. enheten för passagerarinformation. Denna enhet används i dag för hantering av sådana uppgifter från flygbolagen, där de samlas i PNR-systemets databas.

Att bygga nya automatiserade gränssnitt mellan järnvägsföretagens system och myndigheter innebär i praktiken att man skapar nya permanenta angreppsytor mot system som hanterar stora mängder person- och reseinformation. I dagens säkerhetsläge, där cyberangrepp blir allt mer avancerade och AI gör det möjligt att automatisera och skala attacker, menar SJ att dessa sakförhållanden behöver väga betydligt tyngre i bedömningen.



För järnvägen är IT och cybersäkerhet en central del av sektorns förmåga att bedriva en robust och tillförlitlig samhällsviktig verksamhet. Utgångspunkten bör därför vara att minimera externa gränssnitt, behörigheter och beroenden – inte att skapa fler.

Utredningen konstaterar dessutom själv att behandlingen innebär ett allvarligt ingrepp i rätten till privatliv och skyddet för personuppgifter. Den konstaterar också att tåg- och bussföretag får både initiala och löpande IT-kostnader, samtidigt som de faktiska kostnaderna är svåra att bedöma.

SJ menar att det inte bara handlar om kostnaden för att bygga ett tekniskt gränssnitt. Det krävs säkerhetsarkitektur, riskanalyser, autentisering, loggning, övervakning, tester, incidenthantering och kontinuerlig förvaltning. Därtill kommer kraven från dataskyddsregelverket och riskbaserade cybersäkerhetsprinciper enligt NIS2-direktivet. I betänkandets konsekvensutredning tonas effekterna för transportföretagen ned med att "eventuella kostnadsökningar kan [...] vara möjliga att övervältra på konsumenterna, dvs. alla som köper resor" (sid 373). Det är ett synsätt som inte tar hänsyn till sektorns konkurrenskraft. SJ är också tveksamt till utredningens bedömning att hanteringen av andra ärenden kan komma att minska.

Det finns därtill en viktig undanträngningseffekt. Samma begränsade IT- och cybersäkerhetskompetens som behövs för att bygga och förvalta dessa lösningar behövs för att säkra och utveckla järnvägens kärnverksamhet. SJ och andra aktörer riskerar alltså att behöva flytta resurser från driftsäkerhet och motståndskraft i tågtrafiken till administration och tekniska integrationer för ett annat samhällsuppdrag.

Om staten bedömer att denna informationsöverföring är nödvändig anser SJ därför att staten också bör ta huvudansvaret för en central, standardiserad och säker teknisk lösning, inklusive relaterade kostnader.

SJs tydliga rekommendation är därför att förslaget inte genomförs i nuvarande form innan cybersäkerhetsriskerna, påverkan på järnvägens samhällsviktiga verksamhet och den fullständiga livscykelkostnaden har analyserats betydligt djupare.

Jonas Abrahamsson

VD