Regeringskansliet,
Infrastrukturdepartementet

Ett nationellt biljettsystem för all kollektivtrafik (SOU 2020:25)

Datainspektionen har granskat förslaget huvudsakligen utifrån myndighetens uppgift att arbeta för att människors grundläggande fri- och rättigheter skyddas i samband med behandling av personuppgifter.

Med anledning av det antal frågor som behandlats i betänkandet har Datainspektionen valt att begränsa sitt yttrande till frågor av väsentlig betydelse för enskildas personliga integritet.

Datainspektionen lämnar följande synpunkter.

Sammanfattning

Datainspektionen kan se att det finns ett behov av ett nationellt biljettsystem för att göra det enklare för människor att resa kollektivt i hela Sverige, men anser att det finns viktiga delar kvar att utreda vad gäller den personuppgiftsbehandling som får utföras i det nationella biljettsystemet. Till exempel behöver det utredas vilken personuppgiftsbehandling som aktualiseras av förslaget, vilka personuppgifter som får behandlas och i vilken mån känsliga personuppgifter kan komma att behandlas.

Datainspektionen saknar även en närmare analys av hur förslagen förhåller sig till dataskyddsförordningen, och efterfrågar i det fortsatta beredningsarbetet en fullständig integritetsanalys. I integritetsanalysen ska de risker och konsekvenser förslagen kan innebära för den personliga integriteten kartläggas och behovet av skyddsåtgärder och alternativa lösningar bedömas. För att uppfylla kraven i ett konkret lagstiftningsärende måste behandlingen vara proportionell, vilket innebär att det intrång som

sker i den enskildes privata sfär måste vara befogat och inte större än nödvändigt.

Då förslaget innebär att en databas kommer att inrättas som omfattar större delen av befolkningen, och där resenärer riskerar att få sina resvanor kartlagda och sitt beteendemönster övervakat, anser Datainspektionen att den föreslagna behandlingen av personuppgifter i det nationella biljettsystemet omfattas av grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen. Det innebär att frågor som är centrala för avvägningen av integritetsintrånget och skyddet för den enskildes personliga integritet måste regleras i lag. Enligt Datainspektionen kan det därför inte överlåtas på berörda myndigheter att själva skapa regelverk och vidta lämpliga skyddsåtgärder.

Enligt Datainspektionen är de författningsförslag som lämnas i betänkandet som rör personuppgiftsbehandlingen mycket knapphändiga och bristfälligt utformade. Datainspektionen kan därför inte heller tillstyrka de föreslagna författningsförslagen.

Inledning

Betänkandet innehåller ett omfattande förslag till inrättandet av ett nationellt biljettsystem för all kollektivtrafik i Sverige. Förslaget innebär att ett nytt register kommer att skapas, och att en stor mängd personuppgifter kommer att samlas in i det. Eftersom de flesta vid åtminstone något tillfälle kan tänkas komma att resa kollektivt, kommer registret att omfatta så gott som hela befolkningen. Det är även många aktörer, bland annat Trafikverket, de regionala kollektivtrafikföretagen, privata företag och tredjepartsförsäljare, inblandade i hanteringen.

Förslaget i betänkandet består i korthet av att regeringen ska tillsätta en särskild utredning som analyserarar behovet av en statlig organisation för en nationell digital infrastruktur inom mobilitetsområdet. I betänkandet talas det om en genomförandekommitté som får ansvar för att förbereda införandet av den digitala infrastrukturen för biljettsystemet. Betänkandet innehåller även vissa författningsförslag.

Utgångspunkten för detta yttrande är innehållet i avsnitt 8.2 En digital infrastruktur för ett nationellt biljettsystem och författningskommentaren.

Innehållet i det nationella biljettsystemet

I betänkandet beskrivs det att det nationella biljettsystemet ska utgå från de regionala kollektivtrafikmyndigheternas egna biljettsystem, och att staten

ska se till att det finns en s.k. biljettväxel med tillhörande programmeringsgränssnitt (API- Application Programming Interface). Den IT-lösning som föreslås är IDF-baserad, vilket innebär att resenären skapar ett konto hos sitt kollektivföretag och får ett färdbevis i form av en identifikator (IDF). Det är alltså kollektivtrafikföretagen och tredjepartsförsäljarna som ställer ut IDF. För att hantera de fordringar som uppstår mellan parterna när biljetter förmedlas genom biljettväxeln och då resenärer reser med sin identifikator föreslås även en nationell avräkningsfunktion upprättas.

Datainspektionen noterar att den digitala infrastruktur som beskrivs avser en lösning med öppna API:er, och konstaterar att förslaget inte innehåller någon fullständig beskrivning av biljetthanteringen. Det går således inte att utläsa vilken information som biljettsystemet kommer att innehålla eller hur det är tänkt att informationen ska utbytas i systemet. Att förstå hur informationen kommer att flöda i biljettsystemet är dock viktigt för att kunna kartlägga den personuppgiftsbehandling som aktualiseras genom förslaget. Datainspektionen anser mot denna bakgrund att underlaget bör kompletteras dels med en beskrivning av informationsflödet, dels en kartläggning av den personuppgiftsbehandling som är tänkt att utföras i systemet.

Förhållandet till Dataskyddsförordningen

Kompletterande nationell reglering
Det nationella biljettsystemet ska enligt förslaget regleras i ett nytt kapitel 3 a i lagen (2010:1065) om kollektivtrafik och två nya bestämmelser 4 a och 5 a §§ i förordningen (2011:1126) om kollektivtrafik. Utöver de nya bestämmelserna föreslås även vissa följdändringar.

Dataskyddsförordningen utgör det primära regelverket för behandling av personuppgifter inom EU. Enligt artikel 6.2 i dataskyddsförordningen får medlemsstaterna behålla eller införa mer specifika bestämmelser för att anpassa tillämpningen av bestämmelserna i förordningen med hänsyn till behandling för att följa artikel 6.1 c och e. Detta innebär att kompletterande nationell reglering av personuppgiftsbehandling endast kan ske i den mån dataskyddsförordningen medger det och inom de ramar förordningen sätter. När nationella bestämmelser föreslås räcker det således inte att konstatera att det finns ett utrymme för sådana bestämmelser i dataskyddsförordningen utan det måste även utredas om innehållet i förslagen överensstämmer med förordningens krav. Dessa krav framgår bl.a. av artiklarna 5, 6 och 9 i dataskyddsförordningen.

Datainspektionen konstaterar att det inte framgår av betänkandet hur författningsförslagen förhåller sig till dataskyddsförordningen. Mot denna bakgrund anser Datainspektionen att utrymmet för nationell lagstiftning behöver analyseras vidare. Datainspektionen efterfrågar därför i det fortsatta beredningsarbetet en närmare analys av hur förslagen förhåller sig till dataskyddsbestämmelserna.

Enligt Datainspektionen kan det till exempel ifrågasättas huruvida den föreslagna bestämmelsen i 3 a kap. 5 § 1 st lagen (2010:1065) om kollektivtrafik, som anger att personuppgifter endast får behandlas om det är nödvändigt för att bedriva det nationella biljettsystemet för kollektivtrafik, är i överensstämmelse med den grundläggande principen om ändamålsbegränsning (se artikel 5.1 b i dataskyddsförordningen) då ändamålet är mycket vidsträckt reglerat.

Datainspektionen anser även att den nämnda bestämmelsen är vilseledande, då den ger ett intryck av att självständigt reglera behandlingen av personuppgifter. Enligt Datainspektionen bör bestämmelser om hur personuppgifter får behandlas alltid innehålla en uttrycklig hänvisning till Dataskyddsförordningen.

Personuppgiftsansvarig
I författningskommentaren till den föreslagna bestämmelsen i 3 a kap. 5 § lagen (2010:1065) om kollektivtrafik anges det att behandlingen av personuppgifter kommer att ingå i den ansvariga myndighetens uppgifter att tillhandahålla ett nationellt biljettsystem för kollektivtrafik. (se s.399)

I den föreslagna bestämmelsen i 4 a § förordningen (2011:1126) om kollektivtrafik anges det att det är Trafikverket, som ska ansvara för att tillhandahålla det nationella biljettsystemet.

Datainspektionen konstaterar att det inte framgår klart av underlaget om det också är tänkt att Trafikverket ska vara personuppgiftsansvarig för behandlingen av personuppgifter i det nationella biljettsystemet. Detta även om det antyds i betänkandet att det är det som är avsikten (se t.ex. s.283). Eftersom vem som är personuppgiftsansvarig får anges i lag eller förordning, anser Datainspektionen att förslaget för det fallet att Trafikverket ska vara personuppgiftsansvarig bör kompletteras med en sådan reglering. Om Trafikverket inte ska vara personuppgiftsansvarig bör det utredas vem eller vilka som är personuppgiftsansvariga för de personuppgiftsbehandlingar som kommer att utföras i det nationella biljettsystemet.

Datainspektionen noterar vidare att det av den föreslagna bestämmelsen i 4 a § förordningen (2011:1126) om kollektivtrafik framgår att Trafikverket får överlåta uppgiften att tillhandahålla det nationella biljettsystemet till en enskild juridisk person. Datainspektionen vill erinra om att den som är personuppgiftsansvarig förvisso kan överlåta en faktisk behandling av personuppgifter, men att personuppgiftsansvaret aldrig kan överlåtas. Om Trafikverket ska vara personuppgiftsansvarig anser Datainspektionen att det även behöver utredas vad det innebär ur en ansvarssynpunkt om uppgiften att tillhandahålla det nationella biljettsystemet ska kunna överlåtas till en enskild juridisk person.

Personuppgifter som får behandlas
När det gäller vilka personuppgifter som får behandlas i det nationella biljettsystemet noterar Datainspektionen att det i den föreslagna bestämmelsen i 3 a kap. 5 § 2 st lagen(2010:1065) om kollektivtrafik anges att regeringen eller den myndighet som regeringen bestämmer får meddela föreskrifter om begränsningar av vilka personuppgifter som får behandlas för ändamålet.

I betänkandet anges att utredningen anser att regleringen av vilka personuppgifter som får behandlas är beroende av systemets mer detaljerade utformning som den föreslagna genomförandekommittén kommer att utarbeta. Utredningen föreslår därför att kommittén även får i uppdrag att återkomma till regeringen eller den myndighet regeringen bestämmer med ett underlag till bestämmelser avseende dataskydd för det nationella biljettsystemet. Enligt utredningen bör det i detta underlag klargöras om känsliga personuppgifter kan förekomma i det nationella biljettsystemet och föreslås särskilda åtgärder (se s.297 f).

Som Datainspektionen påpekat ovan är det viktigt att kartlägga den personuppgiftsbehandling som ett förslag aktualiserar. Innan en sådan kartläggning har utförts går det enligt Datainspektionen inte att ta ställning till vilket behov det finns av att behandla personuppgifter i systemet, och än mindre vilka begränsningar som kan behöva införas och i vilken författningsform.

Integritetskänslig behandling - särskilt fokus på avräkningsfunktionen
För att ett förslag ska uppfylla kraven i ett konkret författningsärende måste det intrång som sker i den enskildes privata sfär vara befogat och inte större än nödvändigt. Det ska också mötas av integritetshöjande bestämmelser till förmån för den enskilde vars uppgifter behandlas.

Av artikel 6.3 i dataskyddsförordningen framgår att när grunden för en behandling fastställs i nationell rätt, ska den uppfylla ett mål av allmänt intresse och vara proportionell mot det legitima mål som eftersträvas. Det innebär att integritetsriskerna med en viss personuppgiftsbehandling ska vägas mot de fördelar som behandlingen bidrar med till det ändamål som förslagen avser att uppfylla. Om ett förslag är av sådan karaktär att den omfattas av grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen måste förslaget även prövas mot denna bestämmelse. När det gäller känsliga personuppgifter som till exempel uppgifter om hälsa är sådan behandling som utgångspunkt förbjuden om inte ett av undantagen i artikel 9 är tillämpligt.

I betänkandet anges att avräkningsfunktionen hanterar underlag med information om rörelsemönster för resenärer vid användning av kollektivtrafik som bedrivs av kollektivtrafikföretag som resenären inte har ett direkt avtal med. Enligt utredningen utgör det dock en begränsad del av resenärens resande, vilket gör att ingen komplett bild av resemönstret kan avläsas. (se s. 295). Som framgår kommer information om resenärers rörelsemönster att behandlas i avräkningsfunktion. Detta öppnar, enligt Datainspektionens uppfattning, upp för möjligheten att kartlägga resenärer och övervaka deras beteendemönster, och gäller oavsett om systemet ger en komplett bild av resemönstret eller inte.

Av betänkandet framgår vidare att det framförallt är behandlingen i den s.k. avräkningsfunktionen som kan vara integritetskänslig, eftersom den hanterar aggregerade data från olika kollektivtrafikföretag som går att härleda till resenärer (se s.297). Med beaktande av att det är möjligt att koppla information som hanteras i avräkningsfunktionen till resenärer anser Datainspektionen att det inte kan uteslutas att även känsliga personuppgifter om t.ex. funktionsnedsättningar (hälsa) kan komma att behandlas. Även om sådana uppgifter inte behandlas direkt, så kan de komma att behandlas indirekt genom att vissa biljetter förbehålls särskilda kategorier av resenärer. Att känsliga personuppgifter kan komma att behandlas har också uppmärksammats av utredningen, som i betänkandet föreslår att genomförandekommittén ska få i uppdrag att klargöra om känsliga personuppgifter kan komma att behandlas (se ovan). Datainspektionen anser att det i det fortsatta beredningsarbetet även bör analyseras vilket undantag i artikel 9 i dataskyddsförordningen som i så fall är tillämpligt.

Datainspektionen noterar i sammanhanget att betänkandet inte behandlar frågan om biljetter som utställs för resor med färdtjänst ska ingå i det

nationella biljettsystemet. Enligt Datainspektionen behöver även detta klargöras i det fortsatta beredningsarbetet.

I betänkandet anges vidare att utredningen har bedömt att det finns ett särskilt behov av dataskydd för hanteringen av den information som kommer avräkningsfunktionen till del. Enligt utredningen är det angeläget att berörda myndigheter skapar regelverk och vidtar skyddsåtgärder som står i proportion till och motverkar de risker som föreligger i hanteringen med avräkningsfunktionen, t.ex. regler om utlämnande av information, att skapa funktioner för pseudonymisering samt upprätta regler för gallringsrutiner (se s.297).

Datainspektionen, som konstaterar att utredaren vill överlåta till berörda myndigheter att själva skapa regelverk och vidta lämpliga skyddsåtgärder, vill i detta avseende framhålla att dataskyddsförordningen innehåller bestämmelser om att den personuppgiftsansvarige ska göra en bedömning av behandlingens konsekvenser för skyddet för personuppgifter innan särskilt riskfyllda behandlingar påbörjas, så kallad konsekvensbedömning avseende dataskydd, artikel 35. Enligt Datainspektionen är det sannolikt att den behandling av personuppgifter som skulle följa på förslaget kan leda till att en konsekvensbedömning krävs.

Datainspektionen vill understryka att en konsekvensbedömning så långt det är möjligt med fördel kan genomföras inom ramen för lagstiftningsarbete, trots att man inte har de tekniska förutsättningarna och därmed kanske inte heller behovet av konkreta säkerhets- och skyddsåtgärder helt klart för sig. Det gör kommande tillämpning förutsägbar och ger även en grund för den konsekvensbedömning som den personuppgiftsansvarige sedan behöver göra för att kunna minimera eventuella höga risker. Datainspektionen anser därför att en fördjupad s.k. integritetsanalys bör utföras inom ramen för det fortsatta beredningsarbetet.

Förhållandet till 2 kap 6 § regeringsformen

Förutom att registret kommer att omfatta personuppgifter om en stor del av befolkningen, så tycks den föreslagna lösningen även öppna upp för en potentiell möjlighet att kartlägga resenärer och övervaka deras beteendemönster. Dessutom är det troligt att registret, åtminstone i viss omfattning, kan komma att innehålla s.k. känsliga personuppgifter om resenärerna. Som Datainspektionen förstår så finns det ingen valmöjlighet, utan alla som vill resa kollektivt kommer att behöva köpa biljetter genom det nationella biljettsystemet. Det torde i praktiken även vara svårt att kunna inhämta ett giltigt samtycke till behandlingen. Enligt Datainspektionen är

det mot denna bakgrund mycket som talar för att den föreslagna behandlingen av personuppgifter i det nationella biljettsystemet är av sådan karaktär att den omfattas av grundlagsskyddet i 2 kap. 6 § andra stycket regeringsformen.

Enligt 2 kap. 6 § andra stycket regeringsformen är var och en gentemot det allmänna skyddad mot betydande intrång i den personliga integriteten, om det sker utan samtycke och innebär övervakning eller kartläggning av den enskildes personliga förhållanden. I förarbetena ges ett flertal exempel på vad som kan utgöra kartläggning respektive övervakning. Det konstateras bland annat att en del åtgärder som innebär kartläggning samtidigt utgör övervakning, och att det därför inte är möjligt att göra en tydlig gränsdragning mellan åtgärderna samt att dagens snabba tekniska utveckling medför att nya metoder kommer att utvecklas som möjliggör övervakning och kartläggning i andra former än vad som för närvarande är möjligt Det konstateras vidare att behovet av ett utökat integritetsskydd gör sig starkast gällande i förhållande till åtgärder som innebär kartläggning eller övervakning av enskildas personliga förhållanden (jfr prop. 2009/10:80 s. 179-181).

Datainspektionen anser att enbart det faktum det föreslagna systemet möjliggör en kartläggning och övervakning av resenärerna är tillräckligt för att det ska krävas en noggrannare reglering i lag. Detta även om syftet med registret inte primärt är att kartlägga och övervaka resenärerna. Inspektionen vill i sammanhanget även framhålla att riksdagen vid flera tillfällen uttalat sig om att befolknings- och myndighetsregister som innehåller ett stort antal registrerade och har ett känsligt innehåll bör regleras särskilt i lag.

Vad gäller en begränsning av rättigheterna i 2 kap. 6 § andra stycket regeringsformen krävs det, för att den ska vara tillåten, att den är stadgad i lag och att den inte gå utöver vad som är nödvändigt med hänsyn till det ändamål som har föranlett den, se 2 kap. 20 och 21 §§ regeringsformen. Detta innebär alltså att åtgärder som får sådana effekter som anges i paragrafen får vidtas bara om det finns föreskrifter i lag som medger det. Det innebär i sin tur att frågor som är centrala för avvägningen av integritetsintrånget och skyddet för den enskildes personliga integritet måste regleras i lag.

Datainspektionen ifrågasätter mot denna bakgrund utredningens förslag att överlåta till berörda myndigheter att själva skapa regelverk och vidta lämpliga skyddsåtgärder.

Inbyggt dataskydd

Datainspektionen hänvisar till artikel 25.1 i dataskyddsförordningen som handlar om inbyggt dataskydd (privacy by design), och vill framhålla att det är viktigt att hänsyn tas till dataskyddsbestämmelserna redan vid planeringen och utformningen av ett nationellt biljettsystem. Att integrera nödvändiga skyddsåtgärder i IT-systemet är nämligen ett sätt att säkerställa att kraven i dataskyddsförordningen uppfylls och att de registrerades rättigheter skyddas.

Datainspektionen anser att det i uppdraget till genomförandekommittén även bör ingå att identifiera och föreslå lämpliga skyddsåtgärder som kan byggas in i IT-systemet.

Detta beslut har fattats av enhetschefen Malin Blixt efter föredragning av juristen Pernilla Andersson. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom och juristen Mattias Sandström medverkat.Malin Blixt, 2020-10-16 (Det här är en elektronisk signatur)