

SJ AB

105 50 STOCKHOLM

## **Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av personuppgifter om tågresenärer med resekort i Mälardalen**

### **Datainspektionens beslut**

Datainspektionen bedömer att syftet med SJ:s behandling av resehistorik om identifierbara personer, att utföra kontroller vid reklamation från kund som använder resekortet, utgör ett berättigat ändamål. Datainspektionen anser att SJ:s bevarandetid av resehistorik ska tidsbegränsas till längst 90 dagar. Datainspektionen förutsätter att SJ avidentifierar lagrad reseinformation senast 90 dagar från avresedatum. Därefter ska det inte vara möjligt att återskapa hur en identifierbar kund rest med kortet.

Datainspektionen konstaterar att SJ:s information om personuppgiftsbehandling inte uppfyller kraven i 22-25 §§ personuppgiftslagen. SJ föreläggs att komplettera och förändra informationen i enlighet med vad som uttalas under skäl för beslutet.

### **Redogörelse för tillsynsärendet**

Datainspektionen har inlett tillsyn mot SJ AB för att kontrollera bolagets behandling av personuppgifter om tågresenärer som använder SJ Pendlarkort och TiM-kortet (resekort). Tillsynen är en fortsättning på tidigare genomförd tillsyn mot tre trafikhuvudmän för kollektivtrafik, vilka infört betal- eller biljettsystem baserade på samma resekortstandard som SJ introducerade för pendlarresenärer inom Mälardalen.

Ett resekort är ett kontaktlöst kort med ett chip som lämnar s.k. elektroniska spår varje gång resenären köper biljetter och reser med kortet. Information om resor och övriga korthistorik lagras centralt hos SJ.

Datainspektionen har sänt ett protokoll till SJ för eventuella synpunkter och begäran om kompletterande uppgifter samt utkast till beslut. SJ har inkommit med synpunkter och kompletterande uppgifter.

Vid inspektionen har i huvudsak framkommit följande.

#### *SJ resekort*

För tågresor i Mälardalen kan ett pendlarkort laddas med pengar och användas som resebörs att betala enkelresor med eller laddas för obegränsat resande under 30 dagar eller 10 resor under 30 dagar för vald tågsträcka.

SJ Pendlarkort innehåller RFID-chip, som kan kommunicera och lagra information. Varje gång kortet laddas och avläses registreras uppgifter om kortnummer, tidpunkt, resmål, biljetttyp, pris på resan och var resan är köpt. Kortet är inte personligt och kan användas av flera, t.ex. ett företagskort. Parallellt med Pendlarkortet kan TiM-kortet, som föregick Pendlarkortet, användas i automater och kortläsare i Mälardalen.

Ett Pendlarkort är giltigt i tre år med förlängning i treårsperioder. För ett Pendlarkort som innehåller e-börs kan kunden få sina insatta pengar återbetalda inom tre år efter den senast gjorda resan.

SJ kräver inte att den som köper ett Pendlarkort ska registrera kortet. För att kunna spärra kortet och få ersättning för förlorat kort ska kunden anmäla detta till SJ och uppge bl.a. kortnumret. En kund kan registrera sitt kort när som helst genom att lämna uppgifter om namn, adress och kortnummer. Kunden kan lämna ytterligare information, t.ex. telefon, e-postadress och reseprofil, dvs. vilken tågsträcka som kortet ska gälla för. Det är inte obligatoriskt att lämna personnummer. Av cirka 400 000 pendlarkort är i dag ungefär 5 000 registrerade.

SJ behandlar personuppgifterna med stöd av samtycke.

#### *Medlemskap i SJ PRIO*

SJ Prio är ett kundprogram för SJ:s frekventa resenärer. Den som har ett Pendlarkort kan välja att registrera sig som medlem och uppge sitt kortnummer för att samla poäng för sitt resande.

#### *Ändamål*

Insamlade personuppgifter om kunder med resekort används för att fullgöra SJ:s åtaganden gentemot kunden och för att förbättra SJ:s service och tjänster samt statistik.

För marknadsföringsändamål behandlas endast personuppgifter om Prio-kunder. Det finns ett spärregister för dem som inte vill ha direktreklam.

#### *Reklamationer*

Kunder som ansöker om ersättning enligt Restidsgarantin eller annan reklamation enligt normalvillkoren kan göra detta via SJ:s webbplats eller på pappersformulär. Vid en reklamation ska kunden alltid uppge personuppgifter medräknat kortnumret. Det innebär att den som inte

tidigare är registrerad hos SJ blir det i samband med en reklamation. Information om kunders reklamationer och andra klagomål registreras i ett ärendehanteringssystem. SJ använder uppgift om kortnumret för att kontrollera den reklamerade resan. SJ rekommenderar sina kunder att reklamera inom tre månader.

#### *Bevarande*

Resekortsinformation lagras centralt och är tillgänglig via SJ:s regionala säljsystem LOKA och gränssnittet smarty. Ingen rensning av resehistorik har gjorts i LOKA, men viss rensning av kunddata har gjorts.

På själva kortet lagras uppgifter om kortnummer, saldo, datum och tidpunkt för de senaste fem gjorda resorna samt ort för resans start och slut.

#### *Information om kortinnehåll på begäran av resenär*

En resenär som vill ha information om innehållet på ett pendlarkort kan få manuell information från säljstället, t.ex. resebutik, eller automatisk betjäning via en automat, som skriver ut ett kontoutdrag.

#### *SJ:s information till kunder om personuppgiftsbehandlingen*

Information om SJ:s personuppgiftsbehandling lämnas på webbplatsen och på det formulär som gäller för reklamationer för ersättning enligt restidsgarantin och via talsvar. En ansökan om s.k. registerutdrag hanteras efter en fastställd policy.

#### *IT-säkerhet*

Det regionala systemet TIM/LOKA startade 1996 och uppgraderades 2001. Smarty är ett gränssnitt och en vidareutveckling av LOKA systemet, som bygger på nordiska resekortföreningens standard för att möjliggöra ett samarbete med länstrafikbolag. Driften av LOKA sköts av Modulsystem AB och det finns ett skriftligt biträdesavtal.

SJ har dokumenterade krav för vem som har tillgång till systemen och till vilka uppgifter personen har behörighet. I dag samlas information om behörigheter i pärmar. SJ loggar inte vem som har haft åtkomst till uppgifter i systemen. Den som fått behörighet är utsedd för att få tillgång till informationen. Ett projekt om ett automatiserat system för loggar startar i juni 2008.

Behöriga användare (säljpersonal) kan koppla ihop lagrad reseinformation till en resenär via smarty/LOKA-systemet och via reklamationssystemet Siebel och har åtkomst till uppgifterna i längst 13 månader tillbaka i tiden.

Datainspektionen begärde att få åtkomst till historiken för ett visst pendlarkort och noterar att registrerade händelser gick tillbaka två år i tiden. Från köp och laddning av kortet den 12 maj 2006 till senaste registrerade händelsen i maj 2008. På datorskärmen visades samtidigt

information från reklamationsystemet om inkomna reklamationer för kortet.

Därefter har SJ uppgett bland annat följande.

#### *Bevarande och gallringsrutiner*

Databaser för uppgifter om kortens resetransaktioner har inte rensats på lagrad information om resor sedan starten 2000. Kort äldre än september 2005 ska nu markeras som utgångna.

SJ Pendlarkort infördes i september 2005 och det resekort som föregick detta kort var TiM-kortet. Uppgifter om namn, adress och personnummer kopplade till TiM-kortet kommer att gallras hösten 2008. Sökning av resor mot TiM-kortet via smarty ska därefter inte ge någon träff.

Uppgifter som gör att ett kort kan uppfattas som personuppgift via namn eller födelsedatum/personnummer har på senare tid endast förekommit via SJ företagsprogram. Dessa och äldre personuppgifter kopplade till TiM-kort/SJ Pendlarkort/SJ Fakturakort kommer att gallras eller ersättas under hösten 2008. När det gäller kvarstoden av de registrerade korten kommer SJ att analysera om kunduppgifterna måste finnas kvar. Målet är att rensa uppgifterna som sannolikt har låg kvalitet. Kunderna har de två senaste åren uppmanats att spara kortnummer och laddningskvitton på säker plats för att kunna hävda inbetalningar/fordringar för ej använda börsmedel vid förlust av kort etc.

Samtliga uppgifter om gjorda resor med resekortet kommer att finnas kvar i LOKA-systemet som statistiskt underlag men åtkomsten till uppgifterna begränsas.

Reseinformation överförs från LOKA-systemet till SJ biljettförsäljningssystem, men är då inte längre kopplad till en identifierbar person. Information om köp av kort och resor rapporteras dagligen till ekonomi/statistik-delen av SJ biljettförsäljningssystem. Uppgifterna rapporteras även till ett generellt statistiksystem.

Det är endast när kund med pendlarkort anmält sig till SJ-Prio som reseinformation överförs till SJ i identifierbar form.

SJ:s uppfattning om hur länge identifierbar resedata måste lagras för att SJ ska kunna handlägga eventuella reklamationer är att personuppgifterna sparas minst två månader efter det att preskriptionstiden enligt 1. kap. 5 § järnvägstrafiklagen har inträtt. Där anges bl.a. att den kortaste preskriptionstid som kan vara aktuell vid fordran på ersättning är ett år från det att fordringen uppkom.

I samband med att resenären reklamerar via en webbtjänst, görs ett anrop i systemet för att svara på om en resa genomförts/validerats enligt de uppgifter resenären påstår. Beslut om restidsersättning fattas

och sparas dels i Siebel, dels i databasen. Ärendesystemet sattes upp i november 2007 och det har inte beslutats om gallringsregler. Användningen av identifierbara personer vid reklamationshantering är nödvändig för att säkerställa korrektheten och att hanteringen endast görs en gång.

För den som reser i tjänsten och har ett pendlarkort i form av företagsresande "SJ Fakturakort", kan kortet vara både personligt och operativt.

#### *Åtkomst*

Det finns för närvarande 79 behöriga användare till smarty/LOKA. Huvuddelen av användarna tillhör "writers" och "readers", dvs. de kan söka och läsa information om kort samt skriva noteringar vid hantering av kundärenden eller endast söka och läsa information om kort. Användarna är personal på SJ Kundtjänst, SJ Säljstöd, SJ resebutik, SJ företagsförsäljning/inesälj och Servicedisk. Även databas- och systemadministratörer har tillgång till informationen.

Användares åtkomst till reseinformation via smarty/LOKA är i dag begränsad enligt "600 rader med resor" om ett kort-ID utan avseende på tid. SJ diskuterar en kompletteringsregel. SJ diskuterar för närvarande om användares åtkomst till LOKA/SJ-data via smarty och SJ reklamationssystem ska begränsas till maximalt 13 månader tillbaka i tiden. Tiden är vald med hänsyn till Restidsgarantin.

### **Skäl för beslutet**

#### *Vilka regler är tillämpliga?*

Personuppgiftslagen gäller i första hand sådan behandling av personuppgifter som är automatiserad. Med personuppgift menas all slags information som direkt eller indirekt kan hänföras till en person som är i livet (3 § personuppgiftslagen).

Varje gång resenären använder kortet sparar SJ uppgifter om kortnummer, datum och tid, vart kortinnehavaren reser, priset på resan och var den är köpt. Genom resekortets (chippets) unika serienummer (kortId) kan SJ hänföra den lagrade informationen om korttransaktioner (köp- och resehistorik) till en person som lämnat personuppgifter inklusive kortnumret till SJ för registrering. SJ:s behandling av kortinformation innefattar behandling av personuppgifter och omfattas därmed av personuppgiftslagens bestämmelser.

Resekortsinformation och kunddata lagras centralt i databaser och tillgång till uppgifterna har SJ via ett gränssnitt och ett ärendehanteringssystem. Vi bedömer att uppgifterna är strukturerade på ett sådant sätt att hanteringsreglerna är tillämpliga. Samtliga bestämmelser i personuppgiftslagen är därför tillämpliga på behandlingen (5 a § personuppgiftslagen).

*Är behandlingen av personuppgifter förenlig med personuppgiftslagen?*

I 10 § personuppgiftslagen regleras under vilka förutsättningar det är tillåtet att behandla personuppgifter. Utgångspunkten är att behandling är tillåten endast om den registrerade har lämnat sitt samtycke. Från den regeln finns undantag. Det anges bland annat att personuppgifter får behandlas om behandlingen är nödvändig för att ett avtal med den registrerade ska kunna fullgöras. Behandlingen kan också vara tillåten efter en intresseavvägning.

SJ har åberopat samtycke från de registrerade som rättslig grund för behandling av personuppgifter. Av personuppgiftslagens definitioner framgår att ett samtycke ska vara individuellt, frivilligt, särskilt, otvetydigt och informerat. För att ett samtycke enligt personuppgiftslagen ska vara giltigt förutsätts bland annat att den registrerade fått tillräcklig information. Datainspektionen har under en särskild rubrik nedan lämnat synpunkter på den information som SJ lämnar till kunder på webb och formulär i dag.

I 9 § personuppgiftslagen ställs ett antal grundläggande krav när det gäller behandling av personuppgifter. Den personuppgiftsansvarige ska se till att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål. Personuppgifterna får sedan inte behandlas för något ändamål som är oförenligt med dem för vilka uppgifterna samlades in. De personuppgifter som behandlas ska vara adekvata och relevanta i förhållande till ändamålen med behandlingen och fler uppgifter än nödvändigt med hänsyn till ändamålen får inte behandlas. Personuppgifter får inte heller sparas under längre tid än vad som är nödvändig med hänsyn till ändamålen med behandlingen.

SJ samlar in och lagrar information om tågresenärernas gjorda resor med resekortet. All resehistorik lagras dels som underlag för statistik, dels för eventuella reklamationer. SJ ersätter kortresenärer som på grund av en större försening reklamerat enligt Restidsgarantin, som är en del av SJ:s normalvillkor. Vid en reklamation ska kunden bland annat uppge sitt kortnummer. Den som begär ersättning ska reklamera senast inom tre månader. SJ uppger att användningen av uppgifter om identifierbara personer vid reklamationshandlingen är nödvändig för att säkerställa kontrollen av reklamationen och att den bara görs en gång.

Datainspektionen bedömer att SJ:s behandling av resehistorik om identifierbara personer, för att utföra kontroller vid reklamationer från kunder som använder resekort, kan utgöra ett berättigat ändamål. En förutsättning för att behandlingen ska betraktas som berättigad påverkas dock av hur länge uppgifterna sparas. Från integritetssynpunkt ökar risken för detaljerad kartläggning av kortinnehavarens resmönster ju längre tid reseinformationen lagras.

Det är tillåtet för SJ att behandla avidentifierade resetransaktioner för t.ex. statistik och trafikplanering. SJ har inte presenterat ett underlag som visar att det skulle finnas anledning för bolaget att behandla reseinformation om identifierbara personer för ändamålet statistik.

*Hur länge får uppgifterna sparas?*

Ett av de grundläggande kraven som ställs på behandling av personuppgifter är att den personuppgiftsansvarige ska se till att personuppgifter inte bevaras un-

der längre tid än vad som är nödvändigt för ändamålet. Det framgår av 9 § första stycket punkten i personuppgiftslagen. Om det finns bestämmelser om bevarande i annan lag eller förordning ska de bestämmelserna gälla.

Det är viktigt att den personuppgiftsansvarige noga överväger hur länge personuppgifter ska bevaras då information om enskilda behandlas. Uppgifter får inte samlas in och sparas bara för att de eventuellt kan komma till användning vid ett senare tillfälle och därför kan vara bra att ha.

Fram till i dag har SJ inte gjort några större rensningar av insamlade personuppgifter gällande resekortet. SJ kommer nu att hösten 2008 gallra en mängd äldre kunddata. Men SJ har bevarat all reseinformation och har inte för avsikt att gallra uppgifter om gjorda resor med kortet.

Datainspektionen anser att lagring av uppgifter om varje genomförd resa för identifierbara personer kan uppfattas som ett intrång i den personliga integriteten, då sådan information gör det möjligt att kartlägga personens resmönster. Datainspektionen anser därför att tiden för bevarande av reseinformation som kan kopplas till identifierbara personer bör begränsas. Bevarandetiden bör vara så kort som möjlig.

Datainspektionen har i tidigare tillsynsärenden som rör behandling av resekort i kollektivtrafiken beslutat att resehistoriken om identifierbara kunder får sparas centralt hos trafikhuvudmannen i ca 60 dagar för ändamålet att kontrollera reklamationer från kunder. Därefter ska uppgifterna avidentifieras, dvs. det inte vara möjligt att återskapa hur en identifierbar kund rest med kortet. I vårt beslut om bevarandetiden har vi vägt in att bolagen inte visat behov av att bevara resehistorik om identifierbara personer längre än cirka 60 dagar.

Att kunder har möjlighet att reklamera resan innebär inte med automatik att uppgifter om kunden får bevaras under den tid som reklamationsfristen löper.

SJ rekommenderar kunder att reklamera inom tre månader. I SJ AB normalvillkor i järnvägstrafik 13.2 anges följande ” Vill den resande påtala trafikstörning som avses i dessa normalvillkor, och begära ersättning för denna, bör han i första hand vända sig till tågpersonalen, eller till personal vid bemannat försäljningsställe, eller skriftligen senast inom 3 månader till SJ AB eller till den agent eller det ombud som sålt biljetten.” Av information enligt formulär för Restidsgaranti och andra ersättningar uppges att SJ behöver ha reklamationen inom tre månader från avresedatumet.

Mot bakgrund av att SJ:s reklamationsfrist om tre månader är väl inarbetad och accepterad av SJ:s resekortskunder anser Datainspektionen det rimligt att SJ får spara reseinformationen om en identifierbar kund i 90 dagar. Därefter ska uppgifterna avidentifieras, dvs. det ska inte vara möjligt att återskapa hur en identifierbar kund har rest med kortet. SJ:s hänvisning till järnvägstrafiklagens preskriptionsregler föranleder inte någon annan bedömning.

Om en reklamation har kommit in inom 90 dagar får SJ givetvis behålla personuppgifterna under handläggningen av reklamationsärendet.

*Uppfylls kraven på information till de registrerade?*

En viktig del av integritetsskyddet är att den registrerade får information om behandlingen av personuppgifter bland annat för att känna till vilka uppgifter som registreras och för att kunna tillvarata sina rättigheter.

Det är därför viktigt att de registrerade informeras om behandlingen av personuppgifter som sker i samband vid insamling av personuppgifter dels vid registrering av pendlarkortet, dels vid reklamationer. Informationen är nödvändig för att de registrerade ska kunna ta tillvara sina rättigheter.

Enligt 23-25 §§ personuppgiftslagen ska den personuppgiftsansvarige, i detta fall SJ, självant lämna information om behandlingen av personuppgifter till de registrerade.

Informationen bör innehålla:

- den personuppgiftsansvariges identitet (namn, adress, telefonnummer, organisationsnummer och i förekommande fall e-postadress),
- ändamålen med behandlingen av personuppgifter,
- all övrig information som behövs för att den registrerade ska kunna ta tillvara sina rättigheter i samband med behandlingen, såsom
  - vilka kategorier av uppgifter som behandlas,
  - hur länge uppgifterna sparas,
  - mottagare eller kategorier av mottagare av uppgifterna (dvs. till vilka uppgifterna kommer att lämnas ut),
  - rätten att gratis en gång årligen efter ansökan få information samt
  - rätten till rättelse

Datainspektionen kan konstatera att SJ:s information om personuppgiftsbehandlingen vid reklamationer och registrering på webbplatsen brister på följande punkter:

- Det saknas information om vilka uppgifter om resenären som behandlas, t.ex. att uppgifter om gjorda resor med kortet lagras hos SJ för att utföra kontroller vid reklamationer
- Det saknas information om hur länge personuppgifter inklusive resehistorik sparas
- Det saknas information om att ansökan om registerutdrag enligt 26 personuppgiftslagen är gratis en gång per år och att kunden har rätt till rättelse.

För att SJ ska få behandla personuppgifter med stöd av samtycke måste SJ komplettera och förändra informationen i enlighet med ovan.

*Uppfylls kravet på lämpliga säkerhetsåtgärder?*

Det ska finnas ett skriftligt avtal mellan den personuppgiftsansvarige och ett personuppgiftsbiträde, ett s.k. personuppgiftsbiträdesavtal. Avtalet ska reglera hur biträdet ska behandla uppgifterna och vilka säkerhetsåtgärder som ska vidtas (30 § personuppgiftslagen).

SJ har uppgett att bolaget har skriftliga avtal med de personuppgiftsbiträden som bolaget anlitar.

Den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att åstadkomma ett lämpligt skydd för de personuppgifter som behandlas. Vilken säkerhetsnivå som är lämplig avgörs av de tekniska möjligheter som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen och hur pass känsliga de behandlade uppgifterna är (31 § personuppgiftslagen).

SJ har dokumenterade krav för vem som har tillgång till systemen och till vilka uppgifter personen har behörighet. Den som fått behörighet är utsedd för att få tillgång till informationen. SJ loggar inte vem som har haft åtkomst till uppgifter i systemen. I dag samlas information om behörigheter i pärmar. Ett projekt om ett automatiserat system för loggar startar i juni 2008.

Datainspektionen bedömer att SJ:s vidtagna åtgärder ger ett lämpligt skydd för de personuppgifter som bolaget behandlar i databasen.

Med dessa påpekanden ska ärendet avslutas. Ärendet kan komma att följas upp.

### **Hur man överklagar**

Om ni vill överklaga beslutet skall ni skriva till Datainspektionen. Ange i skrivelsen vilket beslut som överklagas och den ändring som ni begär. Inspektionen måste ha fått ert överklagande inom tre veckor från den dag ni fick ta del av beslutet, annars kan överklagandet inte prövas. Datainspektionen sänder överklagandet vidare till Länsrätten i Stockholms län för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Leif Lindgren, teamledaren Catharina Fernquist, IT-direktören Jarl Hellberg och juristen Gunilla Öberg, föredragande.

Göran Gräslund

Gunilla Öberg

Kopia till:  
Personuppgiftsombud