

Västrafik AB

Box 123
541 23 SKÖVDE

Tillsyn enligt personuppgiftslagen (1998:204) – Behandling av personuppgifter i kollektivtrafiken; elektroniska biljetter m.m.

Datainspektionens beslut

Västrafik AB (VT) lagrar information om varje gjord resa med Västrafik-kortet. Datainspektionen bedömer att VT:s behandling av uppgifter om resehistorik utgör sådan behandling av personuppgifter som innebär att personuppgiftslagen blir tillämplig.

Datainspektionen bedömer att syftet med behandlingen av resehistorik om identifierbara personer, att utföra kontroller vid reklamationer eller andra klagomål från kunden, utgör ett berättigat ändamål. Datainspektionen anser att bevarande av resehistorik om identifierbara personer ska tidsbegränsas till cirka 60 dagar. Därefter ska uppgifterna avidentifieras, dvs. det ska inte vara möjligt att återskapa hur en identifierbar kund rest med kortet. Datainspektionen förutsätter att VT avidentifierar resehistoriken efter denna tid.

Datainspektionen förutsätter att VT följer informationsskyldigheten enligt 25 § personuppgiftslagen samt fullföljer sin plan att under hösten 2007 komplettera informationen till kund vid registrering av kortet och till befintlig kund som registrerat sitt kort. VT ska informera enligt vad som anges i skälen nedan. Datainspektionen förutsätter att sådan information lämnas innan kunden samtycker till behandlingen.

Datainspektionen förutsätter att VT inför rutiner för att kontrollera åtkomsten till resehistoriken om identifierbara personer.

Datainspektionen kan komma att följa upp ärendet.

Redogörelse för tillsynsärendet

I kollektivtrafiken pågår en utveckling som innebär att det införs biljettsystem där resenärerna använder smartkort, som laddas med elektroniska biljetter och elektroniska pengar. Med hjälp av RFID-teknik kontrolleras kortens innehåll av särskilda kortläsare i trafiken. Varje gång resenären använder kortet lämnar han eller hon s.k. elektroniska spår, t.ex. information om när och var han eller hon steg på en buss eller passerade en automatspärren och ibland även information om avstigningen (resehistorik). Vissa trafikföretag erbjuder personligt anpassade tjänster till kunder som registrerar sina personuppgifter hos dem.

Datainspektionen har genomfört inspektioner hos tre trafikhuvudmän, bland annat VT, för att kontrollera hur de behandlar personuppgifter om kunder som reser med elektroniska biljetter och/eller för att få tillgång till tjänster, t.ex. en personlig webbsida.

Datainspektionen har sänt ett inspektionsprotokoll till VT för eventuella synpunkter och en begäran om kompletterande uppgifter. VT har även fått tillfälle att yttra sig över vår preliminära bedömning. VT har inkommit med synpunkter och svar.

I ärendet har bl.a. framkommit följande.

Nya Västtrafikkortet är ett kontaktlöst kort med ett programmerbart chip som kan kommunicera och lagra information. Kortet kan laddas med olika typer av biljetter (områdesladdningar) och/eller en börs (pengar). Varje kort innehåller ett unikt serienummer. Via kortläsare avläses förutom uppgift om kortnumret bland annat datum, klockslag, linje, tur, hållplats och ibland även uppgifter om när kunden stiger av fordonet. Transaktionerna överförs från kortläsare till att lagras centralt i en databas (Betalsystemet).

Registrering av kortet

VT erbjuder sina kunder att registrera kortet för att de ska kunna spärra kortet och få ersättning för resterande värde på ett borttappat eller stulet kort. En registrerad kortägare får också tillgång till en personlig webbsida på bolagets webbplats, där kunden får aktuell information och verktyg för att t.ex. spärra kort, aktivera reklamspärren och avregistrera kortet.

VT behandlar uppgifter om den som registrerar kortet med stöd av samtycke. Kunden lämnar följande obligatoriska uppgifter; kortnummer, personnummer, namn och adress. Om en kund inte fyllt i uppgift om personnummer kontaktar VT numera kunden, som ombeds att själv komplettera uppgiften. Det är frivilligt att lämna uppgift om personligt kortnamn samt uppgift om att kortanvändaren är samma som ägare, minderårig, annan person eller husdjur. En person kan registrera flera kort som denne kan lämna ut till olika användare. VT samlar in uppgifterna via sin webbplats eller OCR-blanketter. Insamlade kunduppgifter lagras i en databas (Kundsystemet) för administration av kundförhållandet och marknadsföring.

Anonymt resande

En kund kan resa anonymt genom att betala kontant eller använda ett kort som inte är registrerat. Ett registrerat kort kan användas av andra än den som registrerat kortet.

Resehistorik på individnivå

VT anser sig behöva granska resehistorik med samtidig kunskap om vem som är registrerad vid reklamation/förfrågan från kunden själv. För att kunna bemöta en eventuell reklamation från en kund gällande ett visst korts förehavande i systemet är det nödvändigt att kunna lista samtliga transaktioner. Genom att jämföra kundens uppgifter med de uppgifter som finns i systemet kan man konstatera om reklamationen är relevant eller inte och om så är fallet också kompensera kunden. VT behöver tillgång till varje individuellt kortnummer vid bearbetning av information som används till att fördela och periodisera försäljningsintäkter. VT har även använt resehistoriken när en viss produkt inte fungerade på ett korrekt sätt i betalsystemet, vilket fick till följd att kunden inte fick korrekt antal giltighetsdagar. De kort som innehöll en felaktig produkt har bolaget sedan letat upp i kundregistret för att på så vis informera och kompensera drabbade kunder.

Bevarande

VT lagrar uppgifter om resehistorik respektive uppgifter om vem som registrerat ett kort i två olika system/databaser som inte har någon interaktiv koppling till varandra. Resehistorik är tillgänglig på två sätt i betalsystemet. Via en applikation är informationen tillgänglig i max 120 dagar efter att transaktionen genomförts. Denna applikation används vid uppföljning av reklamationer. Samtliga kundservicemedarbetare har tillgång till denna applikation. Resehistorik finns även tillgänglig via rådata direkt i databasen. Den informationen är endast tillgänglig för systemadministratörer.

VT kommer att lagra information som är max 12 månader gammal. Information äldre än 12 månader kommer att arkiveras. Den arkiverade information kommer inte vara lagrad i ett läsbart format, men kommer att kunna vara möjlig att återskapa om det skulle anses vara nödvändigt. Det finns för närvarande ingen funktionalitet i betalsystemet att radera enbart delar av den information som är lagrad i databasen, såsom kortnummer (s.k. avidentifiering).

Själva kortet innehåller maximalt två områdesladdningar och en kontoladdning (e-börs) samt information om senast gjord resa.

Information och samtycke

VT lämnar skriftlig information om personuppgiftsbehandlingar på webbplatsen och på OCR-blanketten. VT behandlar uppgifter om kunder som registrerat sitt kort med stöd av samtycke. Information, som lämnas till kunden vid registrering, kommer att kompletteras under hösten 2007. Informationen kommer även att kompletteras så att det tydligt framgår hur länge informationen sparas, dvs. 12 månader följt av arkivering. Även de kunder som redan har registrerat sitt kort kommer att informeras.

Marknadsföring och reklamspärr

De personuppgifter som kan komma att användas i marknadsföringssyfte, även vid gemensamma reklamkampanjer med t.ex. Pressbyrån, kommer alltid att ha VT som avsändare. Personuppgifterna kommer aldrig att lämnas ut eller säljas till någon av VT:s samarbetspartners. En kund som registrerat sitt kort och motsätter sig direktreklam kan via webben själv aktivera reklamspärr eller via kontakt med kundtjänst få reklamspärr.

Biträdesavtal

VT har upprättat biträdesavtal med anlitat tryckeri och DM-byrå.

Behörighet och åtkomstkontroll

System- och betaldatacontrollern beslutar om vem som ska ha tillgång till betalsystemets olika applikationer. Innan årets slut beräknar VT ha genomfört skriftliga rutiner för vilka kriterier som ska gälla.

Förutom kundservicepersonal är det inga andra anställda inom bolaget som har tillgång till båda systemen. Kontroll av vilken användare som varit inne vid vilket tillfälle i betalsystemet eller kundsystemet genomförs inte löpande. Det finns för närvarande ingen möjlighet att i detalj se vad respektive användare gjort under en inloggningssession i systemen.

Skäl för beslutet

Datainspektionen har bedömt följande frågor:

1. Är resehistorik personuppgifter?
2. Är de s.k. hanteringsreglerna i personuppgiftslagen tillämpliga på VT:s behandling av personuppgifter?
3. Vad krävs för att VT ska uppfylla de grundläggande kraven i 9 § PuL?
4. Vad innebär ett samtycke?
5. Vilken information måste VT lämna till kunderna?
6. Vilka säkerhetsåtgärder måste VT vidta?

1. Är resehistorik personuppgifter?

Enligt 5 § personuppgiftslagen omfattas behandling av personuppgifter som är helt eller delvis automatiserad av lagens bestämmelser. Med personuppgifter avses enligt 3 § personuppgiftslagen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet.

VT samlar in information om varje gjord resa med Västtrafikkortet.

Resetransaktioner för varje kort lagras på kortnumret i en central databas. Varje kort har ett unikt serienummer, som leder till att resehistoriken kan hänföras till en person, såsom en resenär som registrerat sitt kort och då uppgett sitt kortnummer. Kortnumret tillsammans med övriga kunduppgifter lagras i en kunddatabas. Datainspektionens bedömer att VT:s behandling av resehistorik innefattar behandling av personuppgifter och personuppgiftslagen är därmed tillämplig.

2. Är de s.k. hanteringsreglerna i personuppgiftslagen tillämpliga på VT:s behandling av personuppgifter?

Vilka regler i personuppgiftslagen som måste tillämpas beror på hur uppgifterna hanteras. Ska uppgifterna ingå i en strukturerad samling av personuppgifter såsom i en databas eller ett ärendehanteringssystem måste i princip alla regler i personuppgiftslagen beaktas (de s.k. hanteringsreglerna). Är det däremot fråga om behandling av personuppgifter i ostrukturerat material utan koppling till en registerstruktur behöver man inte tillämpa alla regler i personuppgiftslagen.

Datainspektionens bedömning är att uppgifterna behandlas på ett sådant sätt att de s.k. hanteringsreglerna i personuppgiftslagen ska tillämpas.

3. Vad krävs för att uppfylla de grundläggande kraven i 9 § PuL?

I 9 § personuppgiftslagen finns grundläggande krav som all personuppgiftsbehandling måste uppfylla. Det innebär bland annat att den personuppgiftsansvarige ska se till att personuppgifter bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Uppgifterna får därefter inte behandlas för något ändamål som är oförenligt med det för vilka uppgifterna samlades in. Den personuppgiftsansvarige får inte heller behandla fler personuppgifter än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Personuppgifter får inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Datainspektionens målsättning är att värna integriteten vid behandling av personuppgifter utan att användningen av teknik onödigt hindras eller försvåras.

Å ena sidan möjliggör teknikutvecklingen effektivare kollektivtrafiksystem. Å andra sidan innebär den registreringen som sker vid användningen av Västtrafikkortet att genomförda resor med kortet registreras i detalj. När en resenär använder kortet skapas elektroniska spår i stor omfattning och VT får då tillgång till detaljerad resinformation för varje enskilt kort. I de fall resenären väljer att uppge sitt kortnummer kan lagrad resehistorik hänföras till personen. Uppgifter om hur enskilda personer reser med kollektivtrafik är inte att betrakta som känsliga enligt personuppgiftslagens definition. Datainspektionen anser att lagring av uppgifter om varje genomförd resa för en identifierbar person får godtas för att VT ska kunna utföra kontroller vid reklamationer eller andra klagomål från kunden. Däremot kan uppgifterna uppfattas som ett intrång i den personliga integriteten, eftersom sådan information kan sammanställas och göra det möjligt att kartlägga personens resmönster. Datainspektionen bedömer därför att tiden för bevarande av resehistoriken kopplat till identifierbara personer bör begränsas. Bevarandetiden bör vara så kort som möjlig, men med hänsyn till det behov som finns att bevara uppgifterna för att kunna kontrollera reklamationer och klagomål från kunder anser Datainspektionen det rimligt att uppgifterna får sparas i cirka 60 dagar. Därefter ska uppgifterna avidentifieras dvs. det ska inte vara möjligt att återskapa hur en identifierbar kund har rest med kortet.

Det är alltid tillåtet för VT att behandla avidentifierade resetransaktioner för t.ex. statistik, analyser och trafikplanering.

4. Vad innebär samtycke?

Det är tillåtet att behandla personuppgifter om den registrerade har lämnat sitt samtycke till behandlingen (10 §). Av definitionen framgår att samtycket ska vara en frivillig, särskild och otvetydig viljeyttring genom vilken den registrerade, efter att ha fått information, godtar behandling av personuppgifter som rör honom eller henne (3 §).

VT behandlar personuppgifter om resenärer med stöd av samtycke.

Att ett samtycke ska vara frivilligt kan sägas innebära att resenären måste ha ett fritt val att avgöra om hans eller hennes uppgifter ska få behandlas. Den som vill resa anonymt med VT kan göra det genom att inte registrera sitt Västtrafik-kort och genom att betala kontant. Datainspektionen vill framhålla att frivilligheten kan ifrågasättas om resenärer som registrerar sitt kort erbjuder tjänster som är så prismässigt förmånliga att det framstår som särskilt ofördelaktigt att inte registrera kortet.

För att ett samtycke ska vara giltigt enligt personuppgiftslagen krävs också att VT lämnar tillräcklig information om personuppgiftsbehandlingen.

5. Vilken information måste VT lämna till kunderna?

Information till de registrerade om behandling av personuppgifter är en viktig del av integritetsskyddet. Bestämmelserna finns i 23 – 25 § personuppgiftslagen. Kunder som registrerar sitt kort och/eller registrerar sig för att få tillgång till en personlig webbsida har rätt att få veta:

- vilka uppgifter om dem som registreras,
- hur uppgifterna används,
- hur länge de sparas,
- vilka rättigheter de har enligt personuppgiftslagen,
- vilket företag som är ansvarigt för att personuppgiftslagen följs.
- om uppgifter om kunderna kan komma att lämnas ut och i så fall vilka uppgifter som lämnas ut, till vilka mottagare eller kategorier av mottagare och för vilka ändamål. (25 § PuL).

De rättigheter enligt personuppgiftslagen som kunderna ska informeras om är rätten att säga nej till reklam, att efter ansökan få information om vilka uppgifter om honom eller henne som finns registrerade och att få rättelse om uppgifter har behandlats i strid med personuppgiftslagen (11 §, 26 § och 28 §).

VT lämnar i dag information om personuppgiftsbehandling i samband med att en kund registrerar sitt kort. Datainspektionen konstaterar att informationen brister i fråga om att VT lagrar uppgifter om kundens resehistorik. Datainspektionen noterar att VT kommer att komplettera information till kunder som registrerar sitt kort till hösten 2007. Då ska tydligt framgå hur

länge informationen sparas. Även kunder som redan registrerat sitt kort kommer att informeras.

Datainspektionen förutsätter att VT följer informationsskyldigheten enligt 25 § personuppgiftslagen. Den som väljer att registrera sitt kort ska innan han eller hon samtycker ha fått tydlig information om att resehistorik sparas, vilka uppgifter som registreras, hur uppgifterna används och hur länge de sparas.

7. Vilka säkerhetsåtgärder måste VT vidta?

Personuppgiftsbiträdesavtal

Ett personuppgiftsbiträde får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige. Ett skriftligt avtal som reglerar förhållandet mellan personuppgiftsbiträdet och den personuppgiftsansvarige ska enligt 30 § personuppgiftslagen upprättas.

Datainspektionen konstaterar att VT har upprättat personuppgiftsbiträdesavtal med tryckeri och DM-byrå och förutsätter att VT kommer att upprätta skriftliga avtal när det blir aktuellt att anlita någon utanför den egna organisationen, som får behandla personuppgifter enligt den personuppgiftsansvariges instruktioner.

Behörighet och uppföljning av loggar

Av 31 § personuppgiftslagen framgår att den personuppgiftsansvarige ska vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av bl.a. de tekniska möjligheterna som finns, vad det skulle kosta att genomföra åtgärderna, de särskilda risker som finns med behandlingen av personuppgifterna och hur pass känsliga de behandlade personuppgifterna är.

VT har uppgett att system- och betaldatacontrollern beslutar om vem som ska ha tillgång till betalsystemets olika applikationer och att man beräknar att ha skriftliga rutiner för vilka kriterier som ska gälla innan årets slut.

VT har uppgett att förutom kundservicepersonal är det inga andra anställda inom bolaget som har tillgång till båda systemen. Kontroll av vilken användare som varit inne vid vilket tillfälle i betalsystemet eller kundsystemet genomförs inte löpande. Det finns för närvarande ingen möjlighet att i detalj se vad respektive användare gjort under en inloggningssession i systemen. Datainspektionen anser att endast behöriga användare ska kunna ta del av personuppgifterna. Endast den som har behov av resedetaljerna för att kunna utföra sina arbetsuppgifter i verksamheten får ha åtkomst till informationen. För att åtkomsten ska kunna kontrolleras ska det finnas en behandlingshistorik som visar vem som haft åtkomst till uppgifterna (logg). En behandlingshistorik har också en förebyggande funktion förutsatt att användarna informeras om loggen och kontrollen av åtkomst.

Datainspektionen förutsätter att VT inför rutiner för att kontrollera åtkomsten till personuppgifter om resehistoriken.

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