Datainspektionen

Datum	Diarienr
2014-09-15	1275-2013

SJ AB
105 50 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) - personuppgiftsbehandling vid systemtester

Datainspektionens beslut

Datainspektionen konstaterar att SJ AB behandlat personuppgifter i strid med de grundläggande kraven i 9 § personuppgiftslagen genom att behandla personuppgifter för ett ändamål som är oförenligt med det för vilket uppgifterna samlades in samt genom att behandla fler personuppgifter än vad som varit nödvändigt med hänsyn till ändamålet med behandlingen.

Datainspektionen konstaterar vidare att SJ i strid med 31 § personuppgiftslagen inte vidtagit tillräckliga säkerhetsåtgärder för att skydda de personuppgifter som behandlats.

Då SJ AB vidtagit rättelse finner Datainspektionen att det saknas skäl att vidta ytterligare åtgärder. Ärendet avslutas.

Redogörelse för tillsynsärendet

Bakgrund

Datainspektionen har mottagit ett klagomål där det görs gällande att SJ AB (SJ) har behandlat personuppgifter i samband med att de har utfört tester i sina IT-system. Behandlingen har lett till att det felaktigt tagits en kreditupplysning på klaganden samt att denne vid ett antal tillfällen har fått biljetter och fakturor skickade till sig.

Med anledning av vad som anförts i klagomålet har inspektionen beslutat att inleda tillsyn mot bolaget. Bolaget har inkommit med yttranden i ärendet varvid det sammanfattningsvis har uppgett följande.

SJ:s redogörelse

Testsystemens uppbyggnad

SJ har ett antal system som möjliggör funktioner som försäljning av tågbiljetter och andra tjänster tillhandahållna av SJ. Innan nya funktioner eller system tas i bruk på bolagets webbplats måste de testas och verifieras. Testerna sker i en testmiljö i enlighet med de vedertagna processer och rutiner som finns framtagna för industrin. Samtliga tester sker i en testmiljö som är skild från produktionsmiljön där verkliga order genomförs. Kommunikation som normalt når kunden, e-post, utskick etc., är avstängda i testmiljön för att kunderna inte ska påverkas. Testerna utgörs av dels funktionella tester, dels prestandatester. Dessa olika typer av test förekommer i tre olika testfaser; systemtest, integrationstest och acceptanstest.

Vid utförandet av testerna använder SJ tre olika typer av uppgifter; fiktiva personuppgifter, produktionslika personuppgifter och verkliga personuppgifter.

- *Fiktiva personuppgifter* - är påhittade eller utgörs av fiktiva personnummer levererade av Skatteverket. För att de uppgifter som levereras från Skatteverket ska vara användbara i testerna krävs att de förädlas genom att ytterligare uppgifter adderas. Skatteverket kan tillhandahålla upp till ett par tusen fiktiva personnummer.
- *Produktionslika personuppgifter* - utgörs av personuppgifter som anställda hos SJ eller deras leverantörer har upplåtit för teständamål.
- *Verkliga personuppgifter* - utgörs av de uppgifter som SJ:s kunder har lämnat i den s.k. produktionsmiljön.

Vilka typer av personuppgifter som används i testerna beror på förutsättningarna i det enskilda fallet. SJ försöker så långt som möjligt att använda fiktiva eller produktionslika testdata i samband med test av IT-systemen. Ju senare i processen desto mer produktionslika testdata behövs. Det kan därför förekomma fall där det är nödvändigt att använda verkliga personuppgifter som testdata. I annat fall riskerar utfallen av testerna att inte bli tillförlitliga.

Under den första testfasen, systemtest, där ofta isolerade funktioner testas, är det tillräckligt att använda fiktiva eller produktionslika personuppgifter. Under de senare två testfaserna, integrationstest och acceptanstest, kan det dock vara nödvändigt att i vissa fall använda verkliga personuppgifter, särskilt i samband med att systemens prestanda och integrationer mot andra system testas.

Prestandatester syftar till att testa hur ett system beter sig när det belastas till fullo. Detta gör det nödvändigt att använda stora volymer av uppgifter. Uppgifterna måste dessutom se ut som i verkligheten, t.ex. måste flera olika fält vara ifyllda med olika uppgifter. SJ saknar möjligheter att producera eller köpa fiktiva uppgifter av den volym som krävs för att motsvara den egna kunddatabasen. I samband med att ett test ska utföras hämtas en kopia av hela eller delar av SJ:s kundsystem som finns i produktion. I kopian finns samtliga personuppgifter som kunderna lämnat till SJ. Vilka uppgifter som används är beroende av vilken funktion i systemet som ska testas. Uppgifterna i kopian är uppdaterade och aktuella och innehåller inga personuppgifter som har gallrats ur den s.k. produktionsmiljön.

Integrationstester syftar till att testa interaktion med system som finns hos tredje part. Dessa tester kräver i vissa fall att samma uppgifter finns representerade i både SJ:s egen och samarbetspartnerns testdatabas. För att kunna använda fiktiva personuppgifter i dessa fall är det nödvändigt att alla inblandade aktörer, som kreditupplysningsbolag, myndigheter m.fl., enats om en testdatabas. Då någon sådan testdatabas ännu inte existerar är det nödvändigt att även i dessa fall använda verkliga personuppgifter.

Det är SJ:s uppfattning att verkliga testdata är nödvändiga under en överskådlig framtid, även om användningen av verkliga testdata kan begränsas. Det är idag inte möjligt att helt utesluta verkliga testdata ur testmiljön om testerna ska uppfylla nödvändiga syften, i vart fall inte utan samordning med myndigheter och andra aktörer på marknaden och mycket betydande investeringar.

SJ behandlar inte känsliga personuppgifter för teständamål.

Uppgifter om personnummer används i vissa fall för att testa komplexa tjänster som involverar externa tjänsteleverantörer, exempelvis biljettbokningstjänster. Det är nödvändigt att personnumret har en riktig syntax och att den har en motsvarighet i den externa tjänstens testdata. Det kan därför vara nödvändigt att använda verkliga personnummer för teständamål.

Grundläggande krav på behandlingen

SJ framhåller att användning av personuppgifter för test av system, vars produktionsmiljö kunderna har begärt tillgång till genom att använda en viss funktionalitet på www.sj.se, måste anses vara ett ändamål som inte är oförenligt med de ursprungliga ändamålen. Det ursprungliga ändamålet med behandlingen är i första hand att fullgöra avtalen med kunderna.

Därtill är enligt SJ:s uppfattning teständamålet nödvändigt för de ursprungliga ändamålen. IT-system som introduceras för första gången, och därefter förvaltas och utvecklas, måste testas löpande för att säkerställa att den funktionalitet som slutligen erbjuds kunderna fungerar, håller en god kvalitet och prestanda samt möjliggör för SJ att fullgöra avtalen med kunderna.

SJ framhåller vidare att kunder i allmänhet förstår att tjänster som beställs och tillhandahålls via IT-system förutsätter att IT-systemen testas i samband med rättningar och utvecklingar.

Laglig grund för behandlingen

SJ anför i första hand att behandlingen av personuppgifter sker med stöd av 10 § a) personuppgiftslagen. Behandlingen av personuppgifter för teständamål är i förlängningen nödvändig för att SJ ska kunna fullgöra avtalen med kunderna.

I andra hand anför SJ att behandlingen kan ske efter en intresseavvägning enligt 10 § f) personuppgiftslagen. Det ligger i såväl SJ:s eget intresse som i kundernas intresse att funktionalitet och tjänster på www.sj.se, liksom övriga system som är nödvändiga för att fullgöra avtalen med kunderna, fungerar så väl som möjligt. För att leva upp till kundernas höga förväntningar är det nödvändigt att testa relevanta IT-system, till viss del med verkliga personuppgifter. SJ:s behov av behandling av personuppgifter för teständamål väger i detta fall, enligt SJ:s bedömning, tyngre än kundernas intresse av integritetsskydd.

SJ har beslutat att i framtiden inhämta kundernas samtycke till behandling av personuppgifter för teständamål.

Information till de registrerade

Den information om behandling av personuppgifter som idag lämnas till de kunder som registrerar sig, genom medlemskap, köp av biljett eller liknande, omfattar bland annat information om behandlingar för ändamålen att

fullgöra SJ:s åtaganden mot kunden samt för att förbättra SJ:s service och tjänster.

SJ kommer att justera informationstexterna på webbplatsen för att tydliggöra att kunduppgifter kan komma att användas för att förbättra och testa tjänsterna och de system de tillhandahålls i. I informationstexten ska teständamål inkluderas uttryckligen bland de behandlingar för vilka samtycke inhämtas.

Säkerhetsåtgärder och särskilt om klagandens fall
När verkliga testdata används ska en av huvuduppgifterna vara att uppgifterna inte förs över till produktionsmiljön. I klagandens fall har SJ av misstag gjort registreringar i produktionsmiljön istället för i testmiljön vilket har lett till den felaktiga kreditupplysningen och de felaktiga biljettbeställningarna. I testmiljön fanns felaktigt länkar ut till den korresponderande produktionsmiljön. Detta, i kombination med att vissa verkliga personuppgifter felaktigt användes för det aktuella funktionstestet, medförde att en bokning som rätteligen skulle gjorts i testmiljön genomfördes i produktionsmiljön. Utöver den drabbade kundens personuppgifter, användes endast testpersonalens egna personuppgifter, s.k. produktionslika personuppgifter, vid detta test. SJ har tagit bort klagandens personuppgifter ur testdatabasen och dementerat omfrågningen till kreditupplysningsbolaget.

SJ har vidare vidtagit följande åtgärder. SJ har uppdaterat instruktioner till testare och andra testdokument, internt och hos leverantör, för att säkerställa att endast fiktiva eller produktionslika personuppgifter används så långt det är möjligt. SJ har även vidtagit åtgärder för att testpersonal inte ska tro att de befinner sig i testmiljön när de faktiskt befinner sig i produktionsmiljön.

Skäl för beslutet

Vilka regler är tillämpliga?

Av den beskrivning SJ lämnat framgår att de ifrågavarande testerna görs i en testmiljö som är mycket lik den verkliga produktionsmiljön. Datainspektionen gör bedömningen att behandlingen i SJ:s testmiljö utgör en sådan automatiserad behandling av personuppgifter som omfattas av personuppgiftslagen, och att materialet är strukturerat på ett sådant sätt att de s.k. hanteringsreglerna är tillämpliga på den aktuella behandlingen (5-5 a §§ personuppgiftslagen).

Är behandlingen av personuppgifter förenlig med de grundläggande kraven i personuppgiftslagen?

Vid behandling av personuppgifter i strukturerat material måste de grundläggande kraven i 9 § personuppgiftslagen vara uppfyllda. Detta innebär bland annat att personuppgifter inte får behandlas för något ändamål som är oförenligt med det för vilket uppgifterna samlades in och att inte fler personuppgifter får behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen.

Vid bedömningen av om behandlingen av personuppgifterna är oförenlig med ändamålet med det för vilket uppgifterna samlades in kan man utgå från hur en registrerad typiskt sett skulle se på saken. Detta innebär att om den aktuella behandlingen rimligen kunde förväntas av den registrerade är det nya ändamålet inte att anse som oförenligt med det ursprungliga.

För att säkerställa att de uppgifter som finns i produktion behandlas på ett korrekt sätt och för att upptäcka och korrigera felaktiga personuppgifter kan det i vissa fall vara nödvändigt att behandla personuppgifter i testmiljön. En sådan behandling har också ett naturligt samband med det ursprungliga syftet med behandlingen, att tillhandahålla den ifrågavarande tjänsten. Behandling som är nödvändig för att säkerställa att personuppgifterna som finns i SJ:s produktionsmiljö är riktiga och att dessa behandlas på ett korrekt sätt kan därför enligt Datainspektionens mening i allmänhet inte anses oförenligt med den ursprungliga behandlingen.

I de fall personuppgifter behandlas för andra syften än ovan, till exempel i tester som görs i samband med utveckling av nya system och införande av nya funktioner i befintliga system, vill Datainspektionen lyfta fram följande. Sådana tester har, till skillnad från sådana kontroller som beskrivits ovan, i allmänhet ett svagare samband med den ursprungliga behandlingen av personuppgifterna. Att sambandet är svagare blir tydligt inte minst när behandlingen sker endast till syfte att utveckla systemen för framtida beställningar. Behandling av personuppgifter för sådant ändamål kan därför, enligt Datainspektionens mening, oftare än vad som är fallet med kontroller för att säkerställa korrekta uppgifter eller korrekt behandling vara att anse som oförenligt med det ändamål för vilket uppgifterna samlades in. Att det vid tester behövs en stor mängd uppgifter, till exempel i samband med prestandatester, medför enligt Datainspektionens mening inte automatiskt att behandling av verkliga personuppgifter är tillåten. Databaser där ett stort antal personuppgifter behandlas kan tvärtom medföra större ansvar för den personuppgiftsansvarige att hitta alternativa sätt att kontrollera systemens funktionalitet.

För att säkerställa att inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålet bör systemtester så långt det är möjligt utföras på ett sätt som inte innebär att personuppgifter behandlas. Av detta följer att om det finns alternativa sätt att testa systemen, till exempel med fingerade eller avidentifierade uppgifter ska dessa användas istället. Detta gäller även om ett sådant förfarande blir mer kostsamt än att använda en kopia av de uppgifter som finns i kunddatabasen. I de fall verkliga personuppgifter används är det vidare viktigt att inte fler personuppgifter behandlas än de som är nödvändiga för att utföra det aktuella testet. Personuppgifter får inte heller bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Personuppgifter som används för teständamål bör därför gallras en relativt kort tid efter behandlingen slutförts.

I förevarande fall har klagandens personuppgifter används vid testning av system vilket har medfört att det felaktigt tagits en kreditupplysning på klaganden samt att denne har fått biljetter och fakturor skickade till sig. SJ har själva uppgett att anledningen till att detta inträffade delvis berodde på att vissa verkliga personuppgifter felaktigt användes i det aktuella funktionstestet.

Klaganden torde inte ha haft att vänta sig att dennes uppgifter skulle användas för att beställa biljetter och kreditupplysningar i samband med att SJ testade sina system. Uppgifterna har i detta fall enligt Datainspektionens mening behandlats för ett ändamål som är oförenligt med det för vilket uppgifterna samlades in. Mot bakgrund av vad SJ uppgett är det även tydligt att fler personuppgifter använts än vad som varit nödvändigt för att utföra testet.

Har tillräckliga säkerhetsåtgärder vidtagits?

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en teknisk nivå som är lämplig med beaktande av de tekniska möjligheter 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.

När personuppgifter behandlas i testmiljön gäller samma regler för behandling som när det är fråga om behandling som sker i produktionsmiljön. Detta innebär att de rutiner som den personuppgiftsansvariga har i form av till exempel instruktioner till

användare, behörigheter, loggar, loggkontroller och IT-säkerhet ska gälla även för personuppgifter som behandlas i testmiljön.

Enligt Datainspektionens mening bör testmiljön och produktionsmiljön vara tydligt åtskilda och den personuppgiftsansvarige ska vidta nödvändiga åtgärder för att förhindra att testhandläggare av misstag utför åtgärder i produktionsmiljön avseende en verklig person.

I SJ:s testmiljö fanns tidigare länkar ut till den korresponderande produktionsmiljön. Detta har i klagandens fall bidragit till det misstag som har medfört att det tagits en kreditupplysning på klaganden och att det vid ett antal tillfällen skickats ut fakturor avseende biljetter som klaganden inte beställt. Datainspektionen konstaterar att detta tydligt visar att SJ inte vidtagit tillräckliga säkerhetsåtgärder för att skydda de uppgifter som behandlats i testmiljön.

SJ har vidtagit åtgärder

SJ har uppgett att klagandens personuppgifter felaktigt användes i det aktuella funktionstestet. SJ har vidare uppgett att bolaget har uppdaterat instruktioner och att de har vidtagit åtgärder för att testpersonal inte ska tro att de befinner sig i testmiljön när de faktiskt befinner sig i produktionsmiljön. Vidare är länkarna från produktionsmiljön till testmiljön borttagna.

Med anledning av att SJ har vidtagit dessa åtgärder väljer inspektionen att avsluta ärendet utan att vidta ytterligare åtgärder.

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 del av beslutet, annars kan överklagandet inte prövas. Datainspektionen sänder överklagandet vidare till Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Detta beslut har fattats av generaldirektören Kristina Svahn Starrsjö efter föredragning av juristen Evelin Asplund. Vid den slutliga handläggningen har även chefsjuristen Hans-Olof Lindblom, enhetschefen Catharina Fernquist och IT-säkerhetsspecialisten Adolf Slama deltagit.

Kristina Svahn Starrsjö

Evelin Asplund