Datainspektionen

Datum	Diarienr
2012-05-16	1113-2010, 1823-2011

Taxi Stockholm 15 00 00 AB
Ombud:
Advokat NN
Sandart&Partners Advokatbyrå KB
Box 7131
103 87 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) – behandling av personuppgifter avseende en reklamationsdatabas

Datainspektionens beslut

Datainspektionen ser utifrån personuppgiftslagens bestämmelser inget principiellt hinder mot att Taxi Stockholm 15 00 00 AB (nedan bolaget) behandlar personuppgifter för att upprätthålla en reklamationsdatabas för klagomålshantering under förutsättning att inte fler än enstaka personuppgifter om lagöverträdelser behandlas. En sådan behandling har stöd av 1 § punkten d) Datainspektionens föreskrifter (DIFS 1998:3, omtryckt 2010:1) om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser.

Datainspektionen förelägger bolaget att upphöra med behandling av personuppgifter om lagöverträdelser i reklamationsdatabasen utöver de uppgifter om lagöverträdelser som inkommer i anledning av reklamationer och klagomål.

Bolaget föreläggs att kryptera skyddsvärda uppgifter över öppet nät, säkerställa mottagarens identitet vid åtkomst till skyddsvärda uppgifter över öppet nät med stark autentisering, införa rutiner för behandling av skyddsvärda uppgifter i e-post, införa loggning med systematisk uppföljning av åtkomst till skyddsvärda uppgifter samt förvara utskrifter med skyddsvärda uppgifter inlåsta.

Postadress: Box 8114, 104 20 Stockholm
Besöksadress: Drottninggatan 29, plan 5
Webbplats: www.datainspektionen.se
E-post: datainspektionen@datainspektionen.se
Telefon: 08-657 61 00
Telefax: 08-652 86 52

Bolaget förutsätts komplettera den information som man har för avsikt att lämna till förarna för att fullständig information ska lämnas enligt bestämmelserna i 23-25 §§ personuppgiftslagen.

Sammanfattning
Datainspektionen anser att bolaget har rättsligt stöd för att behandla personuppgifter i syfte att upprätthålla en reklamationsdatabas för klagomålshantering enligt 10 § punkten a) och punkten f) personuppgiftslagen (1998:204). Inom ramen för detta har bolaget stöd för att behandla enstaka inkommande personuppgifter om lagöverträdelser i anledning av klagomål och reklamationer enligt 1 § punkten d) Datainspektionens föreskrifter om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser m.m. (DIFS 1998:3, omtryckt 2010:1). Behandling därutöver, dvs. behandling av fler än enstaka personuppgifter om lagöverträdelser, kräver ett särskilt undantag från Datainspektionen efter ansökan i enlighet 21 § fjärde stycket personuppgiftslagen och 9 § personuppgiftsförordningen.

Så långt behandling av personuppgifter anses tillåten enligt detta beslut ska bolaget komplettera den information som lämnas till förarna. Vidare får uppgifterna sparas under hela avtalsförhållandet varefter de ska gallras men Datainspektionen utesluter inte att en del av uppgifterna även kan sparas en tid därefter. Erforderliga biträdesavtal förutsätts upprättas. Bolaget ska även vidta ett antal åtgärder för att höja säkerheten kring de behandlade uppgifterna för att uppnå en lämplig och godtagbar säkerhet i förhållande till uppgifternas känslighet. Några grundläggande principer när det gäller integritetsskydd är att inte samla in mer information än vad som behövs, inte ha den kvar längre än nödvändigt och inte använda den till något annat än vad man samlade in den för. För att leva upp till dessa principer krävs att man arbetar med inbyggd integritet i de IT-system som används för personuppgiftsbehandling.

Redogörelse för tillsynsärendet

Datainspektionen har genom flera klagomål uppmärksammats på att personuppgifter kan ha behandlats i strid med personuppgiftslagen i bolagets reklamationsdatabas.

På grund av vad som anförts i klagomålen har Datainspektionen beslutat att inleda tillsyn mot bolaget, i dess egenskap av personuppgiftsansvarig för den aktuella personuppgiftsbehandlingen. Tillsynen omfattar endast registrering och behandling av personuppgifter om förare.

Bolaget har i yttrande av den 19 augusti 2010 anfört i huvudsak följande.

Bolaget är ett företag som ägs av den ekonomiska föreningen Taxi Trafikförening u.p.a., vars medlemmar är de ca 900 fristående små och medelstora åkerier som samverkar under Taxi Stockholm-konceptet med ca 1 500 bilar, 4 200 förare och över 8 miljoner körningar per år i Storstockholmsområdet. Samtliga förare är anställda i åkerierna, något anställningsförhållande föreligger inte mellan bolaget och respektive förare. Bolaget tillhandahåller förarutbildning åt dem som har en taxiförarlegitimation utfärdad av Transportstyrelsen och bolaget utfärdar den särskilda Taxi Stockholm-legitimationen (nedan TS-legitimationen) till dem som önskar ansluta sig. Den förare som erhåller TS-legitimationen förbinder sig skriftligen att uppfylla de särskilda krav som uppställs i bolaget. Under utbildningen informeras de blivande förarna om att bolaget registrerar eventuella kundreklamationer och att allvarliga sådana kan leda till återkallelse av den särskilda legitimationen.

Bolaget har ett mycket starkt behov av att få information om eventuella klagomål. I första hand för att reparera den skadade kundrelationen, men även för att ta tillvara rättsliga anspråk. Bolaget upprätthåller ett databassystem för kundreklamationer gentemot förare. De uppgifterna används vid bedömningen av en förares lämplighet att inneha legitimation, vid återantagning av förare samt vid prövning av en förares ansökan om att bli åkare inom bolaget. En kunds klagomål specificeras i ett särskilt fält jämte chaufförens namn och legitimationsnummer. De klagomål som typiskt sett förekommer rör brister i bemötandet av en kund, överträdelser av trafikregler, sen ankomst samt i vissa fall krav på ekonomisk ersättning. Det förekommer också klagomål av mycket allvarlig natur som rör hot, våld, sexuella trakasserier och liknande.

Förarna erhåller skriftlig information när ett klagomål kommer in, dvs. i anslutning till att uppgifter om en förare förs in i databasen. Arbetsrättsliga åtgärder vidtas i anledning av klagomål. Endast en snäv krets medhjälpare på huvudkontoret har tillgång till databasen och säkerheten säkerställs bl.a. genom behörigheter.

Bolaget anser sig ha legitima och berättigade ändamål för behandlingen samt att denna är i överensstämmelse med god sed. Uppgifterna innehåller normalt inte några konkreta påstående om lagöverträdelser och i de sällsynta fall detta kan förekomma bör behandlingen anses falla under Datainspektionens undantag för tillvaratagande av företagets rättsliga anspråk i de enskilda fallen. Om Datainspektionen inte delar denna bedömning får bolaget överväga att ansöka om särskilt undantag. I samband med ansökan om den särskilda TS-legitimationen inhämtas sedan år 2002 förarens samtycke till att personuppgifter om denne får behandlas i samband med och för tjänstens utförande. Enligt bolagets uppfattning bör dess intresse av att behandla de aktuella personuppgifterna vara så starka att behandlingen är tillåten även utan samtycke

enligt 10 § f) personuppgiftslagen. Med hänsyn till att det råder någon form av kontraktuellt förhållande mellan bolaget och förarna genom utfärdandet av legitimationen och förarnas accept av villkoren för denna bör behandlingen även kunna anses tillåten enligt 10 § a) personuppgiftslagen.

Efter en inledande skriftväxling genomfördes en fältinspektion den 15 juni 2011 av bolagets behandling av personuppgifter avseende reklamationsförfarandet. Vid denna inspektion framkom bl.a. följande.

Totalt kommer ca 3 500 reklamationer in per år vilka registreras i bolagets reklamationsdatabas. Reklamationerna delas in i tre kategorier: enkla, allvarliga och mycket allvarliga förseelser. Endast en mindre del, knappt 10 procent, kategoriseras som allvarliga eller mycket allvarliga. En reklamation mot en förare kan ge upphov till olika slags påföljder och kan t.ex. resultera i en skriftlig varning eller att den särskilda TS-legitimationen återkallas. Reklamationerna kan också ligga till grund för poängavdrag enligt ”Stegen”, en modell som bolaget tagit fram för poängsättning av förarna i huvudsakligt syfte att förbättra servicen gentemot sina kunder. Uppgift om poängranking registreras i bolagets förarregister. Det finns skriftliga riktlinjer för handläggningen av kundreklamationer och bedömningar av förseelser och dess påföljder.

Klagomål kan lämnas via telefon, fax, e-post eller brev. Handläggarna i kundcenter och växeln har en särskilt framtagen digital blankett som skickas via e-post till reklamationsenheten för vidare hantering. Blanketten innehåller olika fält för bokningsnummer, händelsedatum, anmälare, taxinummer och förarnummer. Därtill finns ett fritextfält (händelsefält) där klagandens uppgifter återges och de har inte något system med koder eller förkortningar för att beskriva vissa händelser utan allt skrivs i klartext. Vid reklamationsenheten läggs ett ärende upp i reklamationsdatabasen och en bedömning görs slutligen hur ärendet ska klassificeras. I princip samtliga utredningsaktiviteter i ärendet dokumenteras i ett ytterligare fritextfält (anteckningsfält). Bild- eller ljudupptagningar förekommer inte i databasen.

Reklamationsdatabasen fungerar som ett ”track-record” vid återantagning av förare som ansöker på nytt om den särskilda TS-legitimationen för att utreda förarens lämplighet. Ytterst syftar registreringarna av uppgifter om påstådd misskötsamhet hos förarna till att skapa trygghet för bolagets kunder. En förare får t.ex. inte ha ”en dom på sig” de senaste fem åren. Bolaget understryker den speciella situation som föreligger i samband med taxiåkande och att kunden befinner sig i en utsatt position i förhållande till föraren varför man vill ha möjlighet att hindra en uppenbart olämplig förare från att beviljas den särskilda TS-legitimationen.

Bolaget anser sig vara personuppgiftsansvarigt för behandlingen av personuppgifter i reklamationsdatabasen. Bolaget har påbörjat en översyn av informationen som lämnas till förarna så att den ska uppfylla personuppgiftslagens krav. Bolaget har rutiner för registerutdrag och är noga med att den informationen enbart ska innehålla uppgifter om den registrerade. Bolaget har även påbörjat en översyn av rutinerna för gallring av personuppgifter i reklamationsdatabasen. Uppgifter ska gallras när de inte längre behövs, dock senast efter tre år efter det att uppgifterna registrerades. Uppgifter i reklamationsärenden som klassificeras som mycket allvarliga vill bolaget dock lagra utan tidsbegränsning.

Vid inspektionen framkom att det går att få fram samtliga registrerade reklamationer sedan 1998 på förarnivå. Det går vidare att söka på valfria ord i de båda fritextfälten. Vid kontrollslagning framgår att det finns uppgifter om att en förare har varit aktuell i ärende vid domstol med angivande av målnummer samt att trafiktillståndet har återkallats på grund av att denne dömts för i klartext angiven allvarlig brottslighet. Vid ytterligare kontrollslagning kan man få fram uppgifter om att en specifik förare har 17 registrerade anmälningar mot sig. Vid inspektionstillfället framkom även att reklamationsenheten förvarar utskrifter från reklamationsdatabasen i en för ändamålet avsedd papperslåda i anslutning till skrivbordet innan dokumenten görs oläsliga i dokumentförstörare.

Systemansvariga, leverantören och personer kopplade till efterbehandlingen i reklamationskedjan har tillgång till systemet. Tilldelning av behörigheter i reklamationsdatabasen utförs av tjänsteägare inom IT-avdelningen efter beslut från kundcenteransvarig. Borttagning av behörigheter sker vid avslutad tjänst eller ändrad befattning. Behörigheterna kan tilldelas på användarnivå eller rollnivå och behörighet ges i form av ”Nyupplägg” (Write), ”Titta”(Read) eller ”Full behörighet” (Read/Write/Modify). Loggning utav åtkomsten till databasen sker. Bolaget har för avsikt att se till att biträdesavtal tecknas med underleverantören som sköter servern med reklamationsdatabasen. Reklamationsdatabasen kan nås över Internet via en Citrix-lösning, som för närvarande hanteras lokalt av bolaget, och uppkopplingen är krypterad. För e-post används en webbaserad lösning som hanteras av Logica och e-postservern är fysiskt placerad utanför bolagets lokaler. Användarnamn och lösenord används för att logga in i såväl databasen som e-postsystemet. Det inkommer ca tio reklamationer via e-post per dag och några särskilda rutiner för att radera e-post finns inte.

Protokoll över inspektionen har upprättats och översänts till bolaget som har framfört synpunkter och förtydliganden i yttrande av den 19 augusti 2011.

Datainspektionen har uppmärksammat att bolaget genomför rutinmässiga kontroller mot Transportstyrelsens vägtrafikregister av samtliga förares innehav av taxiförarlegitimation. Detta behandlas i ett särskilt tillsynsärende (dnr 163-2012) vilket handläggs parallellt med detta ärende.

Skäl för beslutet

Vad avses med personuppgift?
Med personuppgift avses enligt 3 § personuppgiftslagen all slags information som direkt eller indirekt kan hänföras till en fysisk person som är i livet. Varje information som kan hänföras till en fysisk person är en personuppgift, även om informationen bara avser personen i egenskap av yrkesutövare. För att avgöra om en person är identifierbar ska man beakta alla hjälpmedel som i syfte att identifiera vederbörande rimligen kan komma att användas antingen av den personuppgiftsansvarige eller av någon annan. Även sådana i sig anonyma uppgifter som gör det möjligt med s.k. bakvägsidentifikation av en fysisk person omfattas av begreppet personuppgift.

I nu aktuell databas förekommer såväl direkta personuppgifter, namn och personnummer, som uppgift om taxinummer och förarlegitimation samt andra indirekta uppgifter, t.ex. mål- och ärendenummer, vilka utgör personuppgifter i lagens mening.

Är personuppgiftslagen tillämplig?
Enligt 5 § personuppgiftslagen gäller lagen för sådan behandling av personuppgifter som är helt eller delvis automatiserad och för annan, dvs. manuell, behandling av personuppgifter, om uppgifterna ingår i eller är avsedda att ingå i en strukturerad samling av personuppgifter som är tillgänglig för sökning eller sammanställning enligt särskilda kriterier såsom regelrätta register, databaser och ärende- och dokumenthanteringssystem.

Datainspektionen konstaterar att den behandling som utförs i reklamationsdatabasen är helt automatiserad på ett sådant sätt att personuppgiftslagens bestämmelser gäller.

Datainspektionen bedömer däremot att bolagets insamlande av ytterligare personuppgifter i form av t.ex. inhämtande av polisanmälningar och domar som sparas i manuella pärmar inte utgör sådan behandling av personuppgifter som omfattas av personuppgiftslagen. Uppgift om att dokument har inhämtats samt målnummer och liknande anges i anteckningsfältet. I ärendet har dock inte framkommit att personuppgifterna i pärmarna är sökbara på ett sådant kvalificerat sätt som avses i 5 § andra stycket personuppgiftslagen.

Strukturerad eller ostrukturerad behandling?
Enligt 5 a § personuppgiftslagen gäller en förenklad reglering för behandling av personuppgifter i ostrukturerat material utan koppling till en registerstruktur, t.ex. behandling av uppgifter i löpande text i ett dokument eller sedvanlig användning av datorstödd kommunikation som e-post. Sådana uppgifter får i princip behandlas fritt så länge det inte uppkommer en kränkning av den registrerades personliga integritet.

Datainspektionen konstaterar att personuppgifterna vid aktuell behandling i reklamationsdatabasen har strukturerats för att påtagligt underlätta sökning efter eller sammanställning av personuppgifter. Det rör sig därför om behandling av personuppgifter i så kallat strukturerat material. Det innebär att samtliga hanteringsregler i personuppgiftslagen måste beaktas, vilket även gäller beträffande de reklamationer som inkommer via e-post.

Grundläggande krav på personuppgiftsbehandling
Enligt de grundläggande kraven i 9 § personuppgiftslagen får personuppgifter bara behandlas om det är lagligt, på ett korrekt sätt och i enlighet med god sed samt får bara samlas in för särskilda, uttryckligt angivna och berättigade ändamål. Vidare ska personuppgifterna vara adekvata, relevanta, riktiga och aktuella. Dessutom får inte fler personuppgifter behandlas än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Alla rimliga åtgärder ska vidtas för att rätta, blockera eller utplåna sådana personuppgifter som är felaktiga eller ofullständiga och personuppgifter får inte bevaras under en längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Datainspektionen ser utifrån personuppgiftslagens bestämmelser inget principiellt hinder mot att bolaget behandlar personuppgifter för att upprätthålla en reklamationsdatabas för klagomålshantering. Det finns således ett berättigat ändamål för bolaget att behandla personuppgifter.

När behandling väl är tillåten enligt 9 § personuppgiftslagen ska den kunna hänföras till något av fallen i 10 § personuppgiftslagen. Därtill finns ytterligare begränsningar i 13-22 §§ personuppgiftslagen om behandlingen avser känsliga personuppgifter, personnummer och uppgifter om lagöverträdelser.

Tillåten behandling
I 10 § personuppgiftslagen finns en uttömmande uppräkning av i vilka situationer det är tillåtet att behandla personuppgifter. Personuppgifter får behandlas om den registrerade har lämnat sitt samtycke till behandlingen. Ett samtycke ska vara frivilligt, uttryckligt och informerat. I fråga om samtycke i arbetslivet måste man särskilt tänka på den beroendeställning som en arbets-

tagare ofta befinner sig i gentemot arbetsgivaren vid bedömning av kravet på om ett frivilligt samtycke är uppfyllt. Motsvarande bör gälla nu aktuellt avtalsförhållande.

Det samtycke som inhämtas i förevarande fall kan enligt vår mening inte anses frivilligt i den utsträckning som krävs, därtill kan registrerade aldrig samtycka till behandling av personuppgifter om lagöverträdelser, varför Datainspektionen bortser från detta som rättslig grund för aktuell behandling.

En annan rättslig grund för att behandla personuppgifter är 10 § punkten a) personuppgiftslagen. Det gäller om behandling är nödvändig för att ett avtal med den registrerade ska kunna fullgöras eller åtgärder som den registrerade har begärt ska kunna vidtas innan ett avtal träffas. När det gäller fullgörelse av avtal krävs det att den registrerade själv är avtalspart. En avtalspart kan behöva registrera uppgifter om olika slags försummelser som avtalsparten gjort sig skyldig till för att ha som grund för att avsluta avtalsförhållandet eller t.ex. kräva skadestånd. Det gäller särskilt i fråga om långvariga avtalsförhållanden, t.ex. anställningsavtal eller motsvarande, där det finns skyddsregler i lagstiftningen som begränsar möjligheterna till uppsägning vid enstaka avtalsbrott men som tillåter sådana åtgärder vid upprepade avtalsbrott. Arbetsrättsliga principer får anses till viss del tillämpliga i nu aktuell avtalssituation. I fråga om åtgärder som vidtas innan ett avtal träffas kan det t.ex. gälla kontroller och referensupptagning av en arbetssökande.

Förarna har vid erhållande av den särskilda TS-legitimationen skriftligen förbundit sig att följa bolagets policies i fråga om service och etik, trafiksäkerhetspolicy, alkohol- och drogpolicy, kvalitetspolicy och miljöpolicy. Bolagets behandling av personuppgifter i anledning av reklamationer avser därför såväl fullgörande av avtal i förhållande till förarna, som ett led i bolagets kvalitetssäkringsarbete med koppling till ”Stegen” och denna behandling kan enligt vår bedömning ha sitt stöd i 10 § punkten a) personuppgiftslagen.

Enligt 10 § punkten f) personuppgiftslagen är behandling av personuppgifter även tillåten om behandlingen är nödvändig för att ett ändamål som rör ett berättigat intresse hos den personuppgiftsansvarige ska kunna tillgodoses, om detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten. Vid intresseavvägningen väger åtgärder som betingas av säkerhetsskäl i allmänhet tyngre än åtgärder som betingas av t.ex. företagsekonomiska effektivitetsskäl. I vilka fall den personuppgiftsansvariges intresse väger över de registrerades intresse av att få ha sina personuppgifter i fred får avgöras efter en helhetsbedömning i det enskilda fallet.

Vid en sådan bedömning bör man ta hänsyn till bl.a. följande omständigheter:

- vilket slag av verksamhet som bedrivs
- eventuella överenskommelser som kan finnas i kollektivavtal
- branschpraxis, t.ex. Svenska Taxiförbundets kvalitetsnormer om God Taxitradition, enligt vilka taxiföretag bl.a. ska ha tillräckliga personalresurser och erforderlig kompetens för att snabbt och professionellt kunna behandla eventuella reklamationer
- regler och riktlinjer som har utfärdats av arbetsgivaren (t.ex. policies, regler för kvalitetssäkring, reklamationshantering enligt ”Stegen”)
- för vilket ändamål behandlingen ska utföras (t.ex. kontroll av efterlevnad av regler och policies)
- hur personuppgifterna behandlas och hur resultatet används
- om det finns fungerande rutiner för gallring av personuppgifterna och säkerheten (t.ex. att åtkomsten till personuppgifter begränsas till de personer som behöver uppgifterna för sina arbetsuppgifter)
- vilken information arbetstagarna har fått.

Aktuell behandling kan således ha sitt rättsliga stöd såväl enligt 10 § punkten a) personuppgiftslagen som av en intresseavvägning enligt 10 § punkten f) personuppgiftslagen.

Förbud mot att behandla personuppgifter om lagöverträdelser
Enligt 21 § första stycket personuppgiftslagen föreligger ett förbud mot att andra än myndigheter behandlar personuppgifter om lagöverträdelser som innefattar brott, domar i brottmål, straffprocessuella tvångsmedel eller administrativa frihetsberövanden. Av förarbetena till personuppgiftslagen framgår bl.a. att en uppgift om att någon har eller kan ha begått ett brott utgör en personuppgift om lagöverträdelse även om det inte finns någon dom eller motsvarande om brottet. En personuppgiftsansvarig som inte är en myndighet och som inte heller omfattas av ett undantag enligt tredje eller fjärde stycket samma lagrum får således inte behandla sådana uppgifter. Det förbudet kan heller inte upphävas med den registrerades samtycke.

Med stöd 21 § tredje stycket personuppgiftslagen och 9 § personuppgiftsförordningen (1998:1191) har Datainspektionen meddelat föreskrifter (DIFS 1998:3, omtryckt 2010:1) om undantag från förbudet för andra än myndigheter att behandla personuppgifter om lagöverträdelser m.m. Enligt 1 § punkten d) angivna föreskrifter får personuppgifter om lagöverträdelser behandlas utan hinder av förbudet i 21 § personuppgiftslagen om behandlingen avser endast enstaka uppgift som är nödvändig för att rättsliga anspråk ska kunna fastställas, göras gällande eller försvaras i ett enskilt fall, t.ex. ett skadeståndsanspråk.

I fråga om enstaka uppgift har Datainspektionen ansett att kravet på enstaka uppgift är uppfyllt när inkassoföretag registrerar sådana uppgifter om lagöverträdelser som åberopats av gäldenären i ett inkassoärende (dnr 376-2006). Däremot har kravet på enstaka uppgift inte ansetts vara uppfyllt när en arbetsgivare systematiskt skulle begära in uppgift från samtliga anställda om de dömts för brott (dnr 764-2007). Är det fråga om fler än enstaka uppgifter krävs att Datainspektionen beviljar ett särskilt undantag från förbudet i 21 § personuppgiftslagen med stöd av 21 § fjärde stycket personuppgiftslagen och 9 § personuppgiftsförordningen.

Bolaget kan inte på förhand veta vilka uppgifter som inkommer i anledning av reklamationer. Datainspektionen kan, efter genomförd fältinspektion, konstatera att bolaget behandlar en mängd olika personuppgifter, däribland personuppgifter om lagöverträdelser, i reklamationsdatabasen. Vi konstaterar även att bolaget vid den efterföljande behandlingen i anledning av reklamationer behandlar såväl direkta som indirekta personuppgifter om lagöverträdelser, t.ex. uppgift om mål- och ärendenummer.

För att behandlingen ska vara tillåten enligt ovan angivna föreskrifter krävs att behandlingen är nödvändig för att ta till vara rättsliga anspråk i ett enskilt fall. Personuppgifter får inte samlas in och lagras för framtida behov. En särskild bedömning ska därför alltid göras vid registrering av nu aktuella särskilt integritetskänsliga uppgifter. Behandlingen är endast tillåten så länge det avser uppgifter som har direkt betydelse för åtgärder gentemot en förare, såväl avtalsrättsliga som arbetsrättsliga, avseende ett konkret rättsligt anspråk. All behandling som sker måste också vara nödvändig i förhållande till detta anspråk. Enligt Datainspektionens uppfattning måste höga krav ställas på de situationer i vilka undantagen från det principiella förbud som finns mot att behandla personuppgifter om lagöverträdelser tillämpas (se t.ex. dnr 82-2005).

Det inkommer ca 3 500 reklamationer per år till bolaget varav ca 350 klassificeras som allvarliga eller mycket allvarliga. Såvitt vi har kunnat bedöma innehåller endast en del av dessa ärenden personuppgifter om lagöverträdelser. I anledning av reklamationer vidtar bolaget ett antal ytterligare åtgärder som innefattar behandling av personuppgifter. Reklamationsenheten registrerar alla utredningsåtgärder i anteckningsfältet, vilket kan innehålla bl.a. nödvändiga uppgifter om kontakter och korrespondens med t.ex. åkare och förare i anledning av klagomål till följd av förseelser. Reklamationsenheten kontaktar även t.ex. polismyndigheten för att bevaka ärenden i anledning av en del klagomål. Domar och beslut inhämtas från domstolar och myndigheter varvid bl.a. K-nummer respektive målnummer registreras i anteckningsfältet. Kopior av domar och beslut lagras dock manuellt i särskilt avsedda pärmar. I anteck-

ningsfältet förekommer bl.a. uppgift om att en förare dömts för allvarlig brottslighet samt uppgift om åtalsnedläggelse avseende en annan förare. Databasen innehåller inte endast personuppgifter i anledning av klagomål och i en del fall inkommande personuppgifter om lagöverträdelser, utan bolaget hämtar på eget initiativ in och registrerar ytterligare uppgifter om de förare som får ett klagomål mot sig, däribland integritetskänsliga uppgifter och personuppgifter om lagöverträdelser. Det är sammantaget fråga om en omfattande och systematisk behandling av personuppgifter om lagöverträdelser. Mot den bakgrunden finner vi att den behandling som sker i reklamationsdatabasen inte kan anses rymmas inom undantaget för behandling av enstaka uppgifter om lagöverträdelser enligt 1 § punkten d) Datainspektionens föreskrifter (DIFS 1998:3, omtryckt 2010:1). Inte heller något av de andra undantagen i angivna föreskrifter är tillämpligt på nu aktuell behandling. För att bolaget ska få behandla uppgifter om lagöverträdelser utöver de enstaka uppgifter som förekommer i anledning av reklamationer och klagomål krävs således att Datainspektionen efter ansökan beviljar undantag från förbudet i 21 § personuppgiftslagen i det enskilda fallet.

Datainspektionen förelägger därför bolaget att upphöra med behandling av personuppgifter om lagöverträdelser i reklamationsdatabasen utöver de uppgifter om lagöverträdelser som inkommer i anledning av reklamationer och klagomål.

Information till förarna
Enligt 23-25 §§ personuppgiftslagen är den personuppgiftsansvarige skyldig att självmant lämna information till de registrerade. Avser den personuppgiftsansvarige att samla in personuppgifter från såväl den registrerade själv som från någon annan genom klagomål och reklamationer, måste information lämnas i enlighet med både 23 och 24 §§. Lämpligen lämnas information om hela behandlingen av personuppgifter vid det tillfälle när information tidigast måste lämnas, t.ex. i samband med undertecknandet av förbindelsen. Förarna förutsätts då erhålla information om all annan personuppgiftsbehandling som avser förhållandet till förarna utöver den behandling som avser reklamationsdatabasen.

Informationen ska enligt 25 § personuppgiftslagen innehålla uppgift om

- den personuppgiftsansvariges identitet,
- ändamålen med behandlingen och
- all övrig information som behövs för att den registrerade ska kunna ta till vara sina rättigheter i samband med behandlingen.

Sådan övrig information är t.ex. information om vilka kategorier av uppgifter som behandlas, kategorier av mottagare av uppgifterna, hur länge uppgifterna bevaras samt rätten att gratis en gång om året efter ansökan erhålla informa-

tion om behandlade personuppgifter och rätten att få rättelse av felaktiga eller missvisande uppgifter.

Datainspektionen anser att delar av denna information saknas i den text som bolaget har presenterat i ett nytt förslag till informations- och samtyckeshandling avseende reklamationsdatabasen som förarna får underteckna i samband med erhållande av den särskilda legitimationen. Bolaget behöver därför göra följande:

- Komplettera och precisera ändamålen och ange de kategorier av uppgifter som behandlas.
- Tydligare redovisa kopplingen till bolagets poängrankingsystem ”Stegen” och ange de åtgärder som kan komma att vidtas i anledning av reklamationer och efter en bedömning av lämpligheten att inneha den särskilda TS-legitimationen.
- Ange hur länge uppgifterna bevaras.
- Komplettera informationen om de registrerades rätt till registerutdrag, varvid ledning till skrivning kan hämtas från 26 § personuppgiftslagen.

Datainspektionen förutsätter att bolaget kompletterar den information som man har för avsikt att lämna till förarna, enligt ovan redovisade punkter, för att fullständig information ska ges i enlighet med 23-25 §§ personuppgiftslagen. Det kan även vara lämpligt att upplysa om att information om behandling av personuppgifter lämnas då ett reklamationsförfarande inleds.

Gallring

Ett grundläggande krav enligt personuppgiftslagen är att personuppgifter inte ska bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålet med behandlingen. Uppgifter får alltså inte samlas in bara för att de eventuellt kan komma till användning vid ett senare tillfälle. Det är särskilt viktigt att den personuppgiftsansvarige funderar över hur länge personuppgifter ska bevaras då integritetskänslig information behandlas. Det är lämpligt att redan i samband med att behandlingen av personuppgifter påbörjas ta ställning till hur länge uppgifterna i normalfallet ska bevaras och när de ska tas bort. I arbetslivet gäller allmänt att personuppgifter om en anställd inte bör bevaras efter det att denne har slutat, men ibland måste vissa uppgifter bevaras under en längre tid om t.ex. andra lagar kräver det. Motsvarande bör gälla vid aktuellt avtalsförhållande med förarna.

Bolaget har uppgett att reklamationer ska gallras senast tre år efter registrering men vill samtidigt att allvarliga reklamationer ska få sparas utan tidsbegränsning. Av bolagets beskrivning av reklamationshantering enligt ”Stegen” framgår dock att ingen hänsyn ska tas till händelser eller poängavdrag som ligger längre tillbaka än 12 månader.

Datainspektionen har inget att erinra mot att nödvändiga avtalsrättsliga (och arbetsrättsliga) åtgärder vidtas med anledning av klagomål och reklamationer i enlighet med gällande lagstiftning för detta. Särskilt mot bakgrund av bolagets policies som varje förare har förbundit sig till som har koppling till den poängranking som används för kvalitetssäkring, ”Stegen”. Uppgifterna ska gallras så snart som möjligt efter att ändamålen med behandlingen har uppnåtts. Uppgifterna bör dock som längst kunna behållas under det aktuella avtalsförhållandet med förarna motsvarande en anställningstid. Efter det att förhållandet har upphört får rena faktauppgifter bevaras samt vissa uppgifter som krävs för administrativa ändamål, t.ex. uppgift om avsked men inte på vilken grund och uppgifter som krävs ur skatterättsligt hänseende. Datainspektionen utesluter inte att det undantagsvis kan finnas situationer som ger rättsligt stöd för ett, med hänsyn till ändamålet, nödvändigt bevarande av uppgifterna även efter att ett avtalsförhållande har upphört.

Biträdesavtal
Personuppgiftsansvarig är den som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandling av personuppgifter enligt 3 § personuppgiftslagen, normalt den juridiska personen. Enligt samma lagrum är personuppgiftsbiträde den som behandlar personuppgifter för den personuppgiftsansvariges räkning. Personuppgiftsbiträde kan vara antingen en fysisk eller en juridisk person. Ett skriftligt avtal som reglerar förhållandet mellan personuppgiftsbiträdet och den personuppgiftsansvarige ska enligt 30 § personuppgiftslagen upprättas och i avtalet ska säkerhetsåtgärderna vid behandlingen av personuppgifter regleras. Datainspektionen förutsätter att bolaget upprättar erforderliga biträdesavtal avseende den personuppgiftsbehandling som avser såväl reklamationsdatabasen som bolagets e-postserver.

IT-säkerhet
Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas. Åtgärderna ska åstadkomma en säkerhetsnivå som är lämplig med beaktande av de tekniska möjligheter som finns, kostnaden för åtgärderna, särskilda risker med behandlingen och hur pass känsliga uppgifterna är.

Skyddsvärdet hos uppgifter om lagöverträdelser är att jämställa med skyddsvärdet för känsliga personuppgifter enligt 13 § personuppgiftslagen ur säkerhetssynpunkt (se Datainspektionens allmänna råd, *Säkerhet för personuppgifter, s. 17-18*). När sådana personuppgifter görs tillgängliga för användare över Internet, ska användarnas identitet säkerställas med en teknisk funktion som ger en stark autentisering (se t.ex. Datainspektionens beslut dnr 1841-2010), exempelvis e-legitimation, engångslösenord eller motsvarande. Dessutom ska känsliga personuppgifter vara krypterade vid överföring över öppet nät. Syftet

är att säkerställa att endast avsedd mottagare kan ta del av uppgifterna. Endast de som behöver uppgifterna för att kunna utföra sitt arbete ska ha tillgång till dem, och det ska finnas en logg som är tillräckligt detaljerad för att kunna användas för att utreda otillåten åtkomst. Åtkomsten ska följas upp systematiskt i det syftet. Lämpliga säkerhetsåtgärder kan vara både fysiska och logiska och omfattar även skydd för lokalerna där uppgifter behandlas och skydd för t.ex. utskrifter i pappersform.

Datainspektionen kan konstatera att säkerhetsnivån vid aktuell behandling är låg i relation till personuppgifternas känslighet. Datainspektionen förelägger därför bolaget att vidta följande säkerhetsåtgärder för att uppnå en lämplig säkerhetsnivå:

1. Kryptera skyddsvärda uppgifter då de transporteras över öppet nät som t.ex. Internet.
2. Vid åtkomst till skyddsvärda uppgifter över öppet nät ska mottagarens identitet säkerställas genom stark autentisering.
3. Införa rutiner (med tillhörande instruktioner och uppföljning) för hur inkommande e-post med skyddsvärda uppgifter ska hanteras. Rutinerna ska även omfatta gallring.
4. Införa loggning av åtkomst till skyddsvärda personuppgifter. Loggen ska följas upp systematiskt och resultatet ska dokumenteras.
5. Utskrifter som innehåller skyddsvärda personuppgifter ska förvaras inlåsta.

För att kunna bedöma hur säkerhetsåtgärderna ska införas, i syfte att uppnå en lämplig säkerhetsnivå, bör bolaget genomföra en riskanalys vilket kan användas som ett verktyg i det fortsatta informationssäkerhetsarbetet.

Utöver dessa förelägganden har bolaget i övrigt att införa åtgärder för att säkerställa en god intrångssäkerhet digitalt och fysiskt (t.ex. skydd mot dataintrång utifrån och inbrott). Bolaget ansvarar för att upprätthålla ett strukturerat informationssäkerhetsarbete som ska omfatta bl.a. rutiner för loggning och uppföljning enligt ovan samt åtgärder för att öka kunskap och riskmedvetande kring informationssäkerhet hos berörda medarbetare. Kontroller och uppföljning ska därtill genomföras för att säkerställa att säkerhetsåtgärderna är verkningsfulla. Avslutningsvis påpekas att när skyddsvärda uppgifter (digitalt eller i utskrift samt säkerhetskopior) gallras ska de omgående förstöras så att de inte kan återskapas.

Övrigt

Användning av fritextfält är ofta förenat med integritetsrisker. Några grundläggande principer när det gäller integritetsskydd är att inte samla in mer information än vad som behövs, inte ha den kvar längre än man behöver och

inte använda den till något annat än vad man samlade in den för. För att leva upp till dessa principer krävs att man arbetar med inbyggd integritet i de IT-system som används för personuppgiftsbehandling. Den personuppgiftsansvarige ska uppmärksamma om det finns möjlighet att registrera fler uppgifter än vad som bedöms nödvändiga för ändamålen och i de fall det är möjligt bör en teknisk funktionalitet som medger att eventuellt onödig behandling tas bort alternativt att tydliga regler och rutiner tas fram för att registrering av personuppgifter i systemet sker i enlighet med lag och god sed. I så stor utsträckning som möjligt ska man använda sig av funktioner i användargränssnittet som begränsar möjligheten att skriva in sådant som inte får registreras, vilket minskar risken för otillåten och kränkande behandling av personuppgifter.

Detta beslut har fattats av generaldirektören Göran Gräslund i närvaro av chefsjuristen Hans-Olof Lindblom, tillsynschefen Britt-Marie Wester , IT-säkerhetsspecialisten Mikael Ejner samt juristen Jeanette Kronwall, föredragande.

Göran Gräslund

Jeanette Kronwall

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 Förvaltningsrätten i Stockholm för prövning om inspektionen inte själv ändrar beslutet på det sätt ni har begärt.

Kopia till:
Klagandena