Datainspektionen

Datum	Diarienr
2014-06-09	1822-2013

Trustly Group AB
N.N.
St. Göransgatan 63
112 38 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) av Trustly Group AB

Datainspektionens beslut

1. Datainspektionen konstaterar att Trustly Group AB:s avtal med Zendesk inte uppfyller kraven på personuppgiftsbiträdesavtal i 30 § andra stycket och 31 § andra stycket personuppgiftslagen.

   Datainspektionen förelägger Trustly Group AB att vidta åtgärder för att antingen teckna ett personuppgiftsbiträdesavtal med Zendesk som uppfyller bestämmelserna i personuppgiftslagen eller att upphöra med behandling av kundernas personuppgifter med hjälp av Zendesks tjänster.

2. Datainspektionen konstaterar att Trustly inte genomför någon prövning av hur länge personuppgifter får bevaras för olika ändamål. Uppgifter kan därmed komma att bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

   Datainspektionen förutsätter att Trustly Group AB utarbetar rutiner för gallring av personuppgifter. Sådana rutiner bör även innefatta vilka ändamål personuppgifterna får användas för.

Redogörelse för tillsynsärendet

Datainspektionen har inspekterat Trustly Group AB (Trustly). Inspektionen är en del i ett tillsynsprojekt där Datainspektionen har granskat hur fyra företag som tillhandahåller elektroniska betallösningar behandlar personuppgifter om kunder. Syftet med inspektionen har varit att kontrollera Trustlys personuppgiftsbehandling i samband med att tjänsten Trustly Direktbetalning upp-

fyller personuppgiftslagens (1998:204) bestämmelser.. Protokoll över inspektionen har upprättats och översänts till Trustly, som har yttrat sig.

Vid inspektionen och senare skriftväxling med bolaget har bl.a. följande framkommit.

Företaget

Trustly är ett Stockholmsbaserat bolag med cirka 40 anställda och med dotterbolag i Spanien och Malta samt ett vilande dotterbolag i Sverige, Trustly Sverige AB. Trustly tillhandahåller bl.a. tjänsten Direktbetalning via annonstjänsten Blocket. Trustly är ett betalningsinstitut med tillstånd från Finansinspektionen.

Tjänsten Direktbetalning

Tjänsten Direktbetalning gör det möjligt för användaren att utföra en onlinebetalning direkt från sitt bankkonto. Tjänsten som är tekniskt integrerad i Blocket är en s.k. Payment Account Access Service av typen Payment Intiation Service vilket innebär att användaren interagerar med sin bank via ett användargränssnitt som tillhandhålls i tjänsten (s.k. overlay). Tjänsten har utvecklats för att motverka nätbedrägerier och innefattar bl.a. ett bedrägeriskydd för användarna. Tjänsten innebär att både säljare och köpare identifieras genom anslutning till deras internetbanker.

Betalning med tjänsten Direktbetalning går till på följande sätt. Vid betalning väljer köparen Direktbetalning i annonsen på Blocket. I ett särskilt formulär får köparen ange vad denne och säljaren har överenskommit angående leveranssätt och pris. Köparen får även fylla i kontaktuppgifter samt vilken bank denne avser att använda vid betalningen. Köparen godkänner i detta skede ”Allmänna villkor för användning av betaltjänst” som tillhandahålls via en länk. På nästa sida anger köparen sitt personnummer och godkänner ”Allmänna villkor och bestämmelser för Trustly” som finns tillgängliga via en länk. Därefter autentiserar sig köparen gentemot sin bank med BankID på sin mobil eller genom dosa med engångskod. Om köparen kan använda flera bankkonton visas en lista med dessa. Efter köparens godkännande förs betalningen över till Trustlys klientmedelskonto.

Säljaren får därefter ett meddelande via e-post om att någon vill köpa den utannonserade varan. Med detta meddelande finns ett transaktionsnummer, vilket säljaren anger i tjänsten Direktbetalning. Efter att ha tagit del av de uppgifter som köparen lämnat anger säljaren sitt personnummer och loggar in på sin internetbank via tjänsten på motsvarande sätt som köparen gjort enligt

ovan. Genom inloggningen på sin internetbank identifierar säljaren sig och accepterar köparens betalning.

Normalt utbetalas beloppet till säljaren så snart denne har identifierat sig. För transanktioner som bedöms ha hög risk fördröjs utbetalningen med tio dagar. Säljaren har tio dagar på sig att leverera varan. Om säljaren inte levererar varan ersätter Trustly köparen under förutsättning att köparen gjort en polisanmälan. Säljaren kan också välja att inte acceptera köparens betalning. I sådana fall avbryts betalningen och köparen får meddelande om detta.

Personuppgiftsbehandling

Trustly samlar in personuppgifter (namn, personnummer, kontaktuppgifter och uppgifter om bankkontonummer) från köpare och säljare i samband med att de använder tjänsten. Vidare inhämtas viss teknisk information om användarnas utrustning. Vid kommunikation med användarens internetbank samlas dennes inloggningsuppgifter in och vidarebefordras till internetbanken utan att sparas av Trustly. Om användaren ska välja bankkontonummer sparas endast det valda kontonumret.

Kontroll av inhämtade personuppgifter görs mot SPAR. Kontroll av om användaren har betalningsanmärkning eller skuldsaldo hos Kronofogdemyndigheten görs i Bisnodes tjänst ”Spärrkatalog” i syfte att förbygga brott mot penningtvättslagen, bedrägerier eller liknande brottslighet.

Trustly behandlar personuppgifter i syfte att genomföra transaktioner, att förhindra bedrägerier och liknande brottslighet samt att uppfylla rättsliga skyldigheter, t.ex. enligt lagen (2009:62) om åtgärder mot penningtvätt och finansiering av terrorism (penningtvättslagen) och lagen (2010:751) om betaltjänster (betaltjänstlagen). Enligt Trustlys allmänna villkor för användning av betaltjänsten (p. 12.4) har Trustly rätt att använda bl.a. transaktionshistorik och information om köpbeteende för kommersiell efterbearbetning, såsom exempelvis riktad marknadsföring till användare. Trustly har dock uppgett att någon sådan behandling inte sker i dagsläget.

Gallring

Trustly bevarar personuppgifter enligt de krav som följer av lagstiftning bl.a. enligt bokföringslagen, penningtvättslagen och betaltjänstlagen.

E-post i kundtjänsten

Trustly har efter inspektionen upphört med att behandlar personuppgifter om slutanvändaren i Google Apps. Hanteringen sker numera i ett separat sup-

porthanteringssystem vilket tillhandahålls av det amerikanska företaget Zendesk. Trustly har uppgett att företagets personuppgiftspolicy kommer att kompletteras med ett förbud mot att behandla personuppgifter om slutanvändare internt via e-post.

Skäl för beslutet

Tillämpliga bestämmelser

Trustlys behandling av personuppgifter i samband med tillhandahållandet av tjänsten Direktbetalning omfattas av personuppgiftslagen. Datainspektionen bedömer att personuppgifterna har struktureras på ett sådant sätt att flertalet av bestämmelserna i personuppgiftslagen är tillämpliga.

Trustly är ett betalningsinstitut enligt betaltjänstlagen och bolagets verksamhet omfattas av penningtvättslagen.

Enligt 4 kap. penningtvättslagen får verksamhetsutövare behandla personuppgifter under vissa förutsättningar i syfte att förhindra att finansiell verksamhet och annan näringsverksamhet utnyttjas för penningtvätt eller finansiering av terrorism. Bestämmelserna i penningtvättslagen ger bl.a. stöd för att behandla personuppgifter om lagöverträdelser i särskilda register.

Enligt 6 kap. betaltjänstlagen har en betaltjänstleverantör eller den som ansvarar för ett betalningssystem rätt att, under vissa förutsättningar, behandla personuppgifter om misstänkta bedrägerier. Bestämmelserna motsvarar i huvudsak de som finns i penningtvättslagen.

Information för inhämtande av användarnas samtycke

Datainspektionen bedömer att Trustlys behandling av personuppgifter har stöd i 10 § personuppgiftslagen då de registrerade har samtyckt till behandlingen. Inspektionen anser dock att det är önskvärt att den information som lämnas till de registrerade innan de samtycker till behandlingen görs mer lättillgänglig.

Datainspektionen gör bedömningen mot följande bakgrund.

Personuppgifter får behandlas endast om den registrerade har lämnat sitt samtycke. Därutöver får personuppgifter behandlas i viss andra närmare angivna situationer (10 § personuppgiftslagen). För att få behandla personuppgifter med stöd av samtycke av den registrerade krävs att denne har fått information om behandlingen (3 § personuppgiftslagen).

Trustly behandlar personuppgifter om användarna med stöd av deras samtycke. Information om personuppgiftsbehandlingen lämnas i de allmänna villkor som användaren accepterar vid användning av tjänsten. Informationen lämnas dels i Allmänna villkor för användning av betaltjänsten (p. 12 ”Personuppgifter”), dels i Allmänna villkor och bestämmelser för Trustly (p. 7 ”Integritetspolicy och behandling av personuppgifter”).

Av punkten 7 (sista stycket) i de sistnämnda villkoren framgår att i vissa fall kan särskilda villkor gälla i tillägg till dessa villkor och att vid motstridigheter gäller vad som stadgas i de särskilda villkoren avseende behandling av personuppgifter. Datainspektionen utgår från att de andra särskilda villkor som användaren accepterar – allmänna villkoren för användning av betaltjänsten – är sådana särskilda villkor som har företräde vid motstridigheter.

Datainspektionen konstaterar att den information som Trustly behöver lämna för att inhämta användarens samtycke framgår av de båda villkorsbilagorna. Trustly har därför stöd för behandlingen i det samtycke som har lämnats av användaren. Det är dock önskvärt att informationen görs mer lättillgänglig för användaren t.ex. genom att den samlas på ett ställe.

Datainspektionen vill betona att de grundläggande kraven gäller även om användarna samtycker till behandlingen. Det är t.ex. inte tillåtet att behandla personuppgifter som inte är relevanta i förhållande till ändamålet med behandlingen, även om de registrerade har samtyckt till detta. De grundläggande kraven har särskild betydelse när den personuppgiftsansvarige inhämtar samtycke till omfattande behandling av kunders personuppgifter.

Behandling av personuppgifter i kontakt med användarens bank

Datainspektionen har inget att erinra mot den personuppgiftsbehandling som sker vid Trustlys kontakter med användarens bank.

Enligt de allmänna villkor och bestämmelser för Trustly, som finns tillgängliga via en länk när användaren fyller i sitt personnummer, godkänner användaren att Trustly vidarebefordrar inloggningsuppgifter till användarens internetbanks gränssnitt (punkten 7). I avtalet lämnas information bl.a. om att Trustly är personuppgiftsansvarig, för vilka ändamål som personuppgifterna kommer att behandlas och till vilka uppgifterna kommer att lämnas ut.

Behandling av inloggningsuppgifter och kontouppgifter från bankerna sker således med användarnas samtycke. Behandlingen omfattar inte fler uppgifter än vad som behövs för att utföra tjänsten. Inloggningsuppgifterna sparas inte heller av Trustly längre än vad som behövs för inloggningen. Vidare har Trustly vidtagit tillräckliga åtgärder för skydda de personuppgifter som behandlas.

Behandling av personuppgifter i Trustlys kundtjänst

Datainspektionen konstaterar att Trustly Group AB:s avtal med Zendesk inte uppfyller kraven på personuppgiftsbiträdesavtal i 30 § andra stycket och 31 § andra stycket personuppgiftslagen.

Datainspektionen förelägger Trustly Group AB att vidta åtgärder för att antingen teckna ett personuppgiftsbiträdesavtal med Zendesk som uppfyller bestämmelserna i personuppgiftslagen eller att upphöra med att behandla kundernas personuppgifter med hjälp av Zendesks tjänster.

Datainspektionen gör bedömningen mot följande bakgrund.

Trustly använder i sin kundtjänst en s.k. molntjänst för hantering av e-post. Tjänsten tillhandahålls av det amerikanska företaget Zendesk Inc (Zendesk).

Datainspektionen har förståelse för att det kan finnas fördelar med att använda molntjänster såväl vad avser funktion, effektivitet och ekonomi. När sådana tjänster används för att behandla personuppgifter är det dock väsentligt att skyddet för de registrerades integritet inte försämras. Av personuppgiftslagen följer också att den personuppgiftsansvarige är skyldig att se till att den som behandlar personuppgifter för dennes räkning vidtar de åtgärder som lagen kräver.

Av 31 § första stycket personuppgiftslagen framgår att den personuppgiftsansvarige ska vidta lämpliga organisatoriska säkerhetsåtgärder för att skydda de personuppgifter som behandlas. Att genomföra en risk- och sårbarhetsanalys är ett exempel på en sådan organisatorisk säkerhetsåtgärd.

Behandling av personuppgifter i molntjänster som tillhandahålls över internet av globala molntjänstleverantörer kan medföra vissa specifika risker som den personuppgiftsansvarige måste beakta innan en planerad behandling av personuppgifter inleds. Riskerna hänför sig framför allt till bristande kontroll över de personuppgifter som behandlas i molntjänsten och bristande insyn i personuppgiftsbiträdets behandling av personuppgifterna ifråga. För att en personuppgiftsansvarig ska kunna bedöma om det är möjligt att behandla personuppgifter i en molntjänst måste den ansvarige först genomföra en grundlig risk- och sårbarhetsanalys. Analysen ska genomföras bland annat med beaktande av vilka personuppgifter som ska behandlas och vilken säkerhet molntjänstleverantören erbjuder. Därefter måste den personuppgiftsansvarige kontrollera om det, i förhållande till personuppgiftslagen och/eller annan tillämplig integritetsskyddslagstiftning, är tillåtet att behandla personuppgifter i molntjänsten, en s.k. laglighetsprövning. Risk- och sårbarhetsana-

lysen och laglighetsprövningen är ofta tätt sammanlänkade och kan med fördel genomföras inom ramen för samma utredning.

Mot bakgrund av att många molntjänstleverantörer erbjuder sina kunder standardiserade avtalsvillkor är det av avgörande betydelse att den personuppgiftsansvarige utför en laglighetsprövning av avtalsvillkoren i förhållanden till den planerade personuppgiftsbehandlingen. Endast på detta sätt kan den ansvarige kontrollera om behandlingen av personuppgifterna i molntjänsten är tillåten enligt lag.

Datainspektionen konstaterar att Trustly inte har genomfört någon risk- och sårbarhetsanalys av den tjänst som tillhandahålls av Zendesk.

Av 30 § första stycket personuppgiftslagen framgår att Trustly som personuppgiftsansvarig är skyldig att se till att ett personuppgiftsbiträde och de personer som arbetar under biträdets ledning endast får behandla personuppgifter i enlighet med instruktioner från Trustly. För detta syfte är Trustly, enligt 30 § andra stycket personuppgiftslagen, skyldig att teckna ett skriftligt avtal med personuppgiftsbiträdet (biträdesavtal). I ett sådant avtal ska det särskilt föreskrivas att biträdet får behandla personuppgifter bara i enlighet med instruktioner från den personuppgiftsansvarige och att biträdet är skyldigt att vidta de säkerhetsåtgärder som följer av 31 § första stycket personuppgiftslagen.

Datainspektionen har tidigare ansett att kraven på personuppgiftsbiträdesavtal enligt 30 och 31 §§ personuppgiftslagen innebär att villkoren i avtalet ska vara urskiljbara från övriga villkor som gäller mellan parterna och att villkoren i biträdesavtalet inte ensidigt ska kunna ändras av personuppgiftsbiträdet. Vidare har Datainspektionen ansett att av bestämmelserna i 30 och 31 §§ följer att biträdesavtalet ska

- föreskriva att personuppgiftsbiträdet är skyldigt att tillämpa svensk lagstiftning eller bestämmelserna i EU:s dataskyddsdirektiv när det gäller behandlingen av personuppgifter från den personuppgiftsansvarige,
- säkerställa att personuppgiftsbiträdet inte behandlar personuppgifter för andra ändamål än dem som den personuppgiftsansvarige anlitat biträdet för,
- säkerställa att den personuppgiftsansvarige har kännedom om vilka underleverantörer till ett personuppgiftsbiträde som kan komma att behandla personuppgifter från den personuppgiftsansvarige, var dessa underleverantörer är lokaliserade och vad som utgör deras huvudsakliga uppgift enligt avtalet med personuppgiftsbiträdet,

- säkerställa att den personuppgiftsansvarige på lämpligt sätt har möjlighet att följa upp att personuppgiftsbiträdet och dennes underleverantörer lever upp till den personuppgiftsansvariges krav på personuppgiftsbehandlingen och vidtar lämpliga säkerhetsåtgärder,
- säkerställa att det finns tekniska och praktiska förutsättningar att utreda misstankar om att någon hos personuppgiftsbiträdet eller dennes underleverantörer haft obehörig åtkomst till personuppgifterna,
- garantera att säker radering av personuppgifterna, samt
- säkerställa att parterna vet vilka åtgärder som ska vidtas vid avtalets upphörande så att personuppgiftsbiträdet inte har åtkomst till personuppgifterna därefter.

Trustly har inte tecknat ett specifikt biträdesavtal med Zendesk. I det standardavtal som Trustly har godkänt genom att använda tjänsten regleras vissa frågor om personuppgiftsbehandling under punkten ”3. Data privacy and security; confidentiality”. I punkten 3.4 anges följande.

> “We collect certain information about You, Agents and End Users as well as Your and their respective devices, computers and use of the Service. We use, disclose, and protect this information as described in Our Privacy Policy, the then-current version of which is available at www.zendesk.com/privacy and is incorporated into the Terms.”

I den nämnda privacy policyn finns ytterligare villkor om Zendesks behandling av personuppgifter. Det anges bl.a. att Zendesk har anslutit sig till US-EN Safe Harbor och att Zendesk ”do not own, control or direct the use of the information stored or processed on our platform at the direction of our customers […] and only access such information as authorized by our customers or as required by law. Det anges även att Zendesk ”are only the ”data processors” and not the “data controllers” of the information on our platform for the purposes of the EU Directive on Data Protection (Directive 95/46/EC). Av policyn framgår även att Zendesk får dela med sig av personuppgifterna till underleverantörer (”third-party service providers”).

Avtalet innehåller dock flera brister i förhållande till de krav på biträdesavtal som följer av 30 och 31 §§ personuppgiftslagen. I avtalet saknas bl.a. instruktioner som förbjuder att Zendesk behandla personuppgifterna för egna ändamål (se bl.a. ”research purposes” i Privacy Policy). Avtalet föreskriver att tvister med anledning avtalet ska lösas enligt federal och delstatslagstiftning i Kalifornien (punkt 18). Avtalet ger dessutom inte Trustly som personuppgiftsansvarig, förutsättningar för att få kännedom om vilka andra personuppgiftsbiträden som kan komma att behandla personuppgifter från Trustly (punkt 12.1). Vidare saknas det i avtalet bestämmelser som ger Trustly möjlighet att

följa upp att Zendesk och Zendesks underleverantörer lever upp till Trustlys krav på personuppgiftsbehandlingen och vidtar lämpliga säkerhetsåtgärder. Den ”Privacy Policy” som avtalet hänvisar kan dessutom ensidigt ändras av Zendesk (punkt 12.2 och Privacy Policy).

Trustly kan inte styra över vilken information som deras kunder skickar med e-post till Trustlys kundtjänst. Det ställer höga krav på den säkerhet som ska omgärda personuppgiftsbehandlingen.

Mot den bakgrunden ska därför Trustly föreläggas att åtgärda de påtalade bristerna i avtalet med Zendesk eller att upphöra att använda tjänsten.

Gallring av personuppgifter

Datainspektionen konstaterar att Trustly inte genomför någon prövning av hur länge personuppgifter får bevaras för olika ändamål. Perseonuppgifter kan därmed komma att bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

Datainspektionen förutsätter att Trustly Group AB utarbetar rutiner för gallring av personuppgifter. Sådana rutiner bör även innefatta vilka ändamål personuppgifterna får användas för.

Datainspektionen gör bedömningen mot följande bakgrund.

Enligt de grundläggande kraven för personuppgiftsbehandling, som anges i 9 § första stycket personuppgiftslagen, ska den personuppgiftsansvarige bl.a. se till att personuppgifter samlas in bara för särskilda, uttryckligt angivna och berättigade ändamål (c), att de personuppgifter som behandlas är adekvata och relevanta i förhållande till ändamålen med behandlingen (e), att inte fler personuppgifter behandlas än som är nödvändigt med hänsyn till ändamålen med behandlingen (f) och att personuppgifter inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen (i).

När personuppgifter, som i Trustlys fall, samlas in för flera ändamål medför de angivna kraven att personuppgifterna får användas för respektive ändamål så länge som de är adekvata och relevanta för vart och ett av dessa ändamål. Därefter ska uppgifter gallras såvida de inte får användas för något annat berättigat ändamål. När uppgifterna inte längre behövs för *något* av de ändamål som de samlades in för ska de gallras. Vad som är adekvata och relevanta uppgifter och hur länge uppgifterna är nödvändiga att bevara avgörs för Trustlys personuppgiftsbehandling till viss del av krav i lagstiftning och myndighetsföreskrifter.

Enligt de bestämmelser i författningar och andra föreskrifter som Trustly har att tillämpa i sin verksamhet – bl.a. bokföringslagen, penningtvättslagen och betaltjänstlagen – gäller vanligtvis skyldigheten att bevara uppgifter under viss angiven tid. Däremot reglerar dessa bestämmelser inte när uppgifterna ska gallras. Detta följer i stället av de grundläggande kraven i 9 § första stycket personuppgiftslagen. Som nämnts ovan gäller enligt denna bestämmelse att personuppgifter inte ska bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen.

De personuppgifter om namn, personnummer, adress m.m. som sparas i Trustlys system är inte i sig särskilt integritetskänsliga. En omfattande användning av tjänsten kan dock göra det möjligt att kartlägga en användares levnadssätt med hjälp av uppgifter om bl.a. var och när användaren har handlat. Mot den bakgrunden är det särskilt viktigt att Trustly ser till att inte bevara uppgifter om sina kunder längre än vad som är nödvändigt med hänsyn till de ändamål som Trustly får behandla uppgifterna för.

För att säkerställa att Trustly inte behandlar personuppgifter i strid med personuppgiftslagen bör Trustly noggrant utreda vilka författningsreglerade skyldigheter de har att bevara personuppgifter och för vilka ändamål bevarade uppgifter får användas. I de fall det inte anges någon bevarandetid i de författningar som Trustly har att följa måste Trustly göra en egen bedömning av hur länge uppgifterna är nödvändiga att bevara för de angivna ändamålen. Trustly bör även utreda om de författningsreglerade skyldigheterna innebär att samtliga personuppgifter måste bevaras. Om det finns kategorier av uppgifter som inte behöver sparas enligt t.ex. bokföringslagen får dessa uppgifter enbart lagras om det krävs för något annat berättigat ändamål.

Övrig behandling av personuppgifter

Mot bakgrund av vad som har kommit fram i ärendet finner Datainspektionen ingen anledning att rikta kritik mot Trustlys hantering av personuppgifter i övrigt.

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.

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

Kristina Svahn Starrsjö

Martin Brinnen