Datainspektionen

Datum
2014-06-09

Diarienr
1838-2013

Seamless Payment AB
Sankt Eriksgatan 121
113 43 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) – Seamless Payment AB

Datainspektionens beslut

Ärendet avslutas.

Redogörelse för tillsynsärendet

Datainspektionen har genomfört en inspektion hos Seamless Payment AB (Seamless) den 15 november 2013. Inspektionen är en del i ett tillsynsprojekt där Datainspektionen har granskat hur fyra företag som tillhandahåller elektroniska betallösningar behandlar personuppgifter om kunder. Syftet med tillsynen har varit att kontrollera om bolagets personuppgiftsbehandling uppfyller personuppgiftslagens (1998:204) bestämmelser.

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

Betalning med SEQR-appen

Seamless tillhandahåller tjänsten SEQR som används för elektroniska betalningar. Betalningen sker med hjälp av en app som användarna laddar ned och installerar i sina mobiltelefoner. För att användarna ska kunna använda tjänsten för betalning krävs att de anger ett betalkonto. Vid inspektionen kunde användare endast välja Collector Credit AB (Collector) som kontoförare. På uppdrag av kontoföraren kontrollerar Seamless vid kontoansökan att det telefonabonnemang som används är knutet till användarens personnummer. Kreditkontroll utförs av kontoföraren.

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

SEQR kan användas för betalning i butik och vid köp över nätet. Betalningen görs genom att användaren skannar en s.k. QR-kod med appen och kameran i mobiltelefonen. SEQR kan även användas för betalning mellan två användare. Om betalningsmottagaren inte har ett SEQR-konto får denne ett sms med en beskrivning av hur man laddar ned appen. När betalningsmottagaren har laddat ner appen får den som ska skicka betalningen ett meddelande om att det går bra att överföra betalningen.

Rättslig grund för personuppgiftsbehandlingen m.m.

Seamless inhämtar personuppgifter om användaren dels från användaren själv, dels från samarbetspartners såsom handlare och betaltjänstleverantörer som är anslutna till tjänsten samt från centrala adressregister och liknande. De uppgifter som Seamless behandlar om användaren är namn, personnummer, adress, mobiltelefonnummer, bankkontouppgifter, transaktions- och kvittohistorik.

Seamless har vid inspektionen uppgett att ändamålet med att behandla användarnas personuppgifter är att administrera betalningar via SEQR. Därutöver kan användarnas personuppgifter komma att användas för att rikta marknadsföring baserad på användarnas inköpshistorik, lämna information om utvalda samarbetspartners varor och tjänster, anpassa och utveckla Seamless tjänster (marknads- och kundanalyser, för affärsuppföljning och affärs- och metodutveckling), presentera kvittoinformation samt för arkivering enligt bokföringslagens bestämmelser. Vid tidpunkten för inspektionen behandlade Seamless inte några uppgifter om användarnas inköpshistorik i syfte att rikta marknadsföring till användarna.

Seamless grundar sin behandling av användares personuppgifter på samtycke. Användarna får information om Seamless personuppgiftsbehandling i samband med att de registrerar sig. Datainspektionen har tagit del av den informationstext som Seamless använder för att informera de registrerade om sin behandling av personuppgifter.

Vidare behandlar Seamless telefonnummer till betalningsmottagare som inte är kunder till Seamless. Seamless anser att behandlingen har stöd i en intresseavvägning enligt 10 § f personuppgiftslagen.

Känsliga personuppgifter

När det gäller kvittoinformation från vissa typer av inköpsställen, exempelvis apotek, har Seamless gjort bedömningen att sådan information är känslig och att den därför inte ska samlas in. Om inköp vid andra inköpsställen, t.ex. en livsmedelsbutik, skulle medför att känsliga personuppgifter ändå samlas in

kommer Seamless inte att använda sådana uppgifter för andra ändamål än att visa kvittoinformation för användaren.

Gallring

Personuppgifter gallras när uppgifterna inte längre behöver bevaras enligt bokföringslagens regler (sju år). Användningen av personuppgifter under bevarandetiden begränsas med hänsyn till ändamålen med behandlingen.

Säkerhet för personuppgifter

Datainspektionen har granskat de säkerhetsåtgärder som Seamless har vidtagit rörande den fysiska säkerheten, behörighetstilldelning, autentisering, behandlingshistorik, åtgärder mot förlust av information, kommunikation inom Seamless samt kommunikationen mellan appen i användarens telefon och Seamless.

Skäl för beslutet

Datainspektionens tillsyn av Seamless personuppgiftsbehandling omfattar den behandling som utförs i samband med tillhandhållandet av tjänsten SEQR.

Tillämpliga bestämmelser

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

Rättslig grund för behandlingen vid betalning med SEQR

Datainspektionen konstaterar att behandlingen av personuppgifter vid betalning med SEQR sker efter det att användaren fått information om, och därefter lämnat sitt samtycke till behandlingen. Behandlingen har stöd i 10 och 15 §§ personuppgiftslagen.

Datainspektionen gör bedömningen mot följande bakgrund.

Av 10 § personuppgiftslagen framgår när det är tillåtet att behandla personuppgifter. Behandlingen är tillåten när den registrerade har samtyckt till behandlingen efter att ha fått information om den. Det är även tillåtet att behandla personuppgifter om det t.ex. är nödvändig för att ett avtal med den registrerade ska kunna fullgöras eller efter en s.k. intresseavvägning. För att behandlingen ska vara tillåten med stöd av en intresseavvägning krävs att den

är nödvändig för att ett berättigat intresse hos den personuppgiftsansvarige ska kunna tillgodoses och att detta intresse väger tyngre än den registrerades intresse av skydd mot kränkning av den personliga integriteten.

Seamless har uppgett att de insamlade personuppgifterna om användarna behandlas med stöd av användarnas samtycke som lämnas vid registreringen av SEQR-appen. Samtycket innefattar att användaren samtycker till att köprelaterad information används för riktad marknadsföring baserad på användarens inköpshistorik .

Av 15 § personuppgiftslagen framgår att det är tillåtet att behandla känsliga personuppgifter (t.ex. personuppgifter som rör hälsa) om den registrerade har lämnat sitt uttryckliga samtycke till behandlingen.

För att personuppgiftsbehandling ska vara tillåten med stöd av den registrerades samtycke krävs att denne har fått information om behandlingen innan behandlingen påbörjas. När det gäller behandling av känsliga personuppgifter ställs stora krav på tydlig information till den som ska lämna sitt uttryckliga samtycke.

Seamless lämnar information om den planerade personuppgiftsbehandlingen i villkoren som användarna godkänner vid registreringen. Av dessa villkor framgår att Seamless behandlar bl.a. uppgifter om inköpta varor och tjänster samt inköpsställe. Vidare kan noteras att Seamless har vidtagit åtgärder för att i möjligaste mån undvika att känsliga personuppgifter behandlas. Att viss kvittoinformation kan innehålla känsliga personuppgifter går dock inte att helt undvika. Det handlar emellertid om sådana inköpsuppgifter som vanligtvis generas vid alla former av kortbetalningar och andra elektroniska köp. Sådan registrering får anses vara allmänt känd. Användaren får därför anses ha fått tillräcklig information om behandlingen av de känsliga personuppgifter som kan komma att behandlas av Seamless. Seamless har därför stöd för behandlingen i användarnas samtycke.

Rättslig grund för behandlingen vid betalningsöverföring med SEQR

I de fall en användare använder SEQR-appen för att överföra betalning till en annan användare av appen behandlar Seamless uppgifter om mottagarens telefonnummer och bankkontonummer. Datainspektionen konstaterar att Seamless har stöd för behandlingen i användarnas samtycke.

Om mottagaren inte använder SEQR-appen får denne ett sms med en uppmaning om att ladda ned SEQR-appen för att kunna ta emot betalningen. I dessa fall anser Seamless att behandlingen av mottagarens telefonnummer sker med stöd av en intresseavvägning.

Datainspektionen konstaterar att det är fråga om behandling av relativt harmlösa uppgifter. Datainspektionen anser därför att Seamless har ett berättigat intresse av att behandla betalningsmottagarens telefonnummer och att detta intresse väger tyngre än de registrerades intresse av skydd för den personliga integriteten. Behandlingen är därför tillåten enligt 9 § f personuppgiftslagen.

Användning och bevarande av personuppgifter

Enligt 9 § första stycket i personuppgiftslagen ska den personuppgiftsansvarige se till att personuppgifter inte bevaras under längre tid än vad som är nödvändigt med hänsyn till ändamålen med behandlingen. Enligt 9 § första stycket e personuppgiftslagen ska de personuppgifter som behandlas vara adekvata och relevanta i förhållande till ändamålen med behandlingen.

Seamless har uppgett att de bevarar användarnas personuppgifter för bokföringsändamål i sju år enligt de krav som följer av bokföringslagen. Seamless har begränsat tiden för hur länge uppgifterna får användas för andra ändamål under denna tidsperiod. Datainspektionen anser därför att Seamless uppfyller de grundläggande kraven enligt 9 § första stycket personuppgiftslagen vad gäller användning och bevarande av personuppgifter.

IT-säkerhet

Enligt 31 § personuppgiftslagen ska den personuppgiftsansvarige vidta lämpliga tekniska och organisatoriska åtgärder för att skydda de personuppgifter som behandlas.

Datainspektionen anser, mot bakgrund av vad som framkommit i ärendet, att Seamless har vidtagit säkerhetsåtgärder som uppfyller kraven enligt 31 § personuppgiftslagen.

Övrigt

Datainspektionen finner ingen anledning att rikta kritik mot vad som i övrigt har framkommit i tillsynen mot Seamless personuppgiftsbehandling. Ärendet kan därför avslutas.

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