

Svenska Handelsbanken AB
NN
106 70 Stockholm

Tillsyn enligt personuppgiftslagen (1998:204) – bankers användning av s.k. appar

Datainspektionens beslut

Ärendet avslutas.

Redogörelse för tillsynsärendet

Datainspektionen har inspekterat Svenska Handelsbanken AB:s (Handelsbanken) personuppgiftsbehandling i appen för smarta telefoner med operativsystemen iOS från Apple (iPhone) och Android från Google som banken tillhandahåller sina kunder.

Datainspektionen konstaterade i beslut den 12 september 2012 att Handelsbanken inte uppfyller sin skyldighet att självant informera de registrerade om behandlingen av deras personuppgifter enligt 23-25 §§ personuppgiftslagen.

Datainspektionen konstaterade vidare att Handelsbanken inte levde upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen genom att man via bankens appar kommer åt integritetskänsliga personuppgifter efter autentisering med enbart användarnamn och lösenord.

Datainspektionen förelade Handelsbanken att komma in med en skriftlig åtgärdsplan. I åtgärdsplanen skulle banken redogöra för

- a) vilka konkreta åtgärder banken avser att vidta för att uppfylla sin skyldighet att självant informera de registrerade enligt 23-25 §§ personuppgiftslagen,
- b) vilka konkreta åtgärder banken avser att vidta för att leva upp till kraven på säkerhetsåtgärder enligt 31 § personuppgiftslagen,

- c) på vilka grunder banken bedömer att åtgärderna under b) är verkningsfulla och tillräckliga samt
- d) när åtgärderna under a) respektive b) kan vara vidtagna.

Handelsbanken har därefter kommit in med ett konkret lösningsförslag, sin grund för bedömningen att åtgärden är verkningsfull och tillräcklig för att höja säkerheten, tidplan för när åtgärden kan genomföras samt ett förslag på information till den registrerade. Av yttrandet framgår i huvudsak följande.

Förslaget går ut på att man måste aktivera appen efter nedladdningen innan man kan använda den. Aktiveringen av appen förutsätter en stark autentisering av användaren.

Vid aktiveringen knyter systemet appen till en specifik telefon. Det innebär att för att kunna komma åt integritetskänsliga personuppgifter med hjälp av appen krävs dels att man kan PIN-koden, dels att man måste ha telefonen till vilken appen är knuten. Därmed skapar man en autentiseringslösning med två faktorer.

Handelsbanken har gett in den information som banken avser att lämna till sina kunder och som är en del av bankens villkor för mobiltjänsten. Av informationen framgår att banken av säkerhets- och utredningsskäl loggar den IP-adress från vilken kundens inloggning sker.

Handelsbanken har gjort bedömningen att testning, implementering och utrullning till samtliga kunder av den nya säkerhetsfunktionen kommer att vara avslutad vid utgången av 2014.

Skäl för beslut

Föreläggande a) – information till de registrerade

Datainspektionen bedömer att den information till de registrerade som Handelsbanken har gett in uppfyller bankens skyldighet att självmant informera de registrerade enligt 23-25 §§ personuppgiftslagen.

Föreläggande b-c) – säkerhetsåtgärder

Av 31 § personuppgiftslagen följer 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 hur pass känsliga de behandlade personuppgifterna är, riskerna som finns med behandlingen av personuppgifterna, de tekniska möjligheter som finns tillgängliga på marknaden samt vad det kostar att genomföra åtgärderna.

Genom att logga in i appen med hjälp av sitt personnummer och en fyrsiffrig PIN-kod kan den som är kund i Handelsbankens internetbank se följande över ett öppet nät.

- Kontonamn
- Kontonummer
- Saldo
- Kommande, stoppade och genomförda transaktioner (innehållande kontonummer, belopp och datum, egna anteckningar, meddelande till mottagaren)
- Fördefinierade mottagare/mottagarkonton
- E-fakturor

Enligt Datainspektionens allmänna råd är uppgifter om enskildas personliga och ekonomiska förhållanden inom bankväsendet normalt att anse som integritetskänsliga. Ett uttryck för att det är fråga om integritetskänsliga uppgifter är att uppgifterna omfattas av tystnadsplikt eller sekretess.

Särskilt med tanke på att appar ofta används på offentliga platser finns det skäl att anta att det föreligger en ökad risk för att en obehörig person lyckas komma åt inloggningsuppgifter. En sådan person skulle därefter, genom att enkelt ladda ner bankens app till sin egen smarta telefon, kunna logga in i appen och obehörigen ta del av en stor mängd uppgifter, utan att den behörige användaren märker det.

Datainspektionen anser att det kan medföra stora risker för den enskildes personliga integritet om någon obehörig får tillgång till t.ex. uppgifter om konton, transaktioner med namn på mottagaren eller avsändaren och skuldsättning. Uppgifterna skulle kunna användas till att kartlägga, inte bara stora delar av en persons ekonomiska förhållanden, utan även var denne har befunnit sig och dennes inköpsvanor. Uppgifterna om transaktioner kan dessutom innehålla känsliga uppgifter i personuppgiftslagens mening, t.ex. genom att avslöja den enskildes vårdgivare.

Risken för dataintrång om man använder sig av lösenord för autentisering är betydligt högre än om man använder sig av stark autentisering. Stark autentisering, också kallat multifaktorautentisering, kan realiserars på olika sätt. Det kan ske exempelvis med e-legitimation, men även andra tekniska funktioner för asymmetrisk kryptering samt vissa lösningar för engångslösenord och liknande kan användas. Den ökade risken beror naturligtvis på att det är lättare att komma åt enbart ett lösenord, än att skaffa sig åtkomst till exempelvis en koddosa och ett lösenord. Dessutom är det lättare för en användare att upptäcka att man har blivit av med till exempel koddosan eller sin smarta

telefon med den nedladdade e-legitimationen, än att någon obehörig har lyckats avslöja lösenordet.

Datainspektionen konstaterar att den av Handelsbanken föreslagna lösningen innebär att autentiseringen av användaren sker med två faktorer – PIN-koden och telefonen till vilken appen är knuten – det vill säga stark autentisering.

Förutsatt att implementeringen av den föreslagna lösningen sker på ett korrekt sätt, bedömer Datainspektionen att säkerheten för åtkomst till integritetskänsliga personuppgifter via appen kommer att höjas till en nivå som är tillräcklig för att uppfylla kraven på säkerhetsåtgärderna enligt 31 § personuppgiftslagen. Ärendet ska därför avslutas, men kan komma att följas upp.

Föreläggande d) – tidplan

Datainspektionen har inga synpunkter på Handelsbankens tidplan.

Detta beslut har fattats av generaldirektören Kristina Svahn Starrsjö i närvaro av chefsjuristen Hans-Olof Lindblom, juristen Malin Fredholm och IT-säkerhetsspecialisten Adolf Slama, föredragande.

Kristina Svahn Starrsjö

Adolf Slama