Datainspektionen

Datum	Diarienr
2013-09-11	1612-2011

Nordea Bank 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 Nordea Bank AB:s (Nordea) 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 Nordea inte uppfyller sin skyldighet att självmant informera de registrerade om behandlingen av deras personuppgifter enligt 23-25 §§ personuppgiftslagen.

Datainspektionen konstaterade vidare att Nordea 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 Nordea 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 självmant 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

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

d) när åtgärderna under a) respektive b) kan vara vidtagna.

Nordea 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.

> För det första kommer Nordea att ändra appen så att det inmatade användarnamnet och PIN-koden inte visas på den smarta telefonens skärm.
>
> För det andra måste en användare 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 tvåfaktors autentiseringslösning.
>
> För det tredje införs en funktion i systemet som gör det möjligt för användaren att byta PIN-koden.
>
> För det fjärde informerar systemet användaren om när senaste inloggningen via appen har ägt rum.
>
> Nordea har gett in den information som banken avser att lämna till sina kunder i samband med nedladdningen av en uppdaterad version av sina appar. Apparna finns numera för nedladdning på relevanta marknadsplatser och bankens webbplats. Av informationen framgår att banken för att förhindra och utreda olika former av brottsliga attacker och incidenter loggar IP-adresser vid användande av mobilbanken som kunderna gör vid användningen av apparna.
>
> Nordea har gjort bedömningen att införandet av de nya funktionerna kommer att vara avslutad vid utgången av 2013.

Skäl för beslut

Föreläggande a) – information till de registrerade
Datainspektionen bedömer att den information till de registrerade som Nordea 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 servicekod kan den som är kund i Nordeas mobilbank se följande över ett öppet nät.

- Konton
- Kontonummer
- Saldo
- Disponibelt belopp
- Konto- och korttransaktioner (innehållande datum, namn och belopp)
- Datum och belopp på kommande betalningar
- Aviserade betalningar (förhandsaviserade autogiron)
- Datum och belopp på e-fakturor
- Aktie- och fondinnehav
- Kommande aktieaffärer (orderstatus)
- Uppgifter om tagna lån
- Pensions- och kapitalförsäkringar

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 en ökad risk för att någon obehörig lyckas komma åt inloggningsuppgifterna. Denne 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 realiseras 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.

De av Nordea föreslagna åtgärderna innebär att risken för att en obehörig person kan skaffa sig obemärkt åtkomst till integritetskänsliga personuppgifter minskar kraftigt.

Datainspektionen konstaterar att den av Nordea föreslagna autentiseringslösningen 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 Nordeas 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