DATATILSYNET

Den norske Bank ASA, Filial Danmark
CVR-nr.: 19-13-63-02
Højbro Plads 21, 1.
1200 København K

Att.: Hilde Knoph Fallang

26. november 2002

Datatilsynet
Borgergade 28, 5.
1300 København K

CVR-nr. 11-88-37-29

Telefon 3319 3200
Fax 3319 3218

E-post
dt@datatilsynet.dk
www.datatilsynet.dk

J.nr. 2002-711-0030
Sagsbehandler
Nils Rasmussen
Direkte 3319 3234

Vedrørende uvedkommendes adgang til data i Valus

På baggrund af en konkret henvendelse anmodede Datatilsynet ved brev af 23. oktober 2002 Den norske Bank om en redegørelse vedrørende uvedkommendes mulige adgang til personoplysninger på www.valus.dk i perioden efter at betalingssystemet Valus var blevet sat i produktion.

Den norske Bank har ved brev af 6. november 2002 oplyst om formålet med og opbygningen af betalingssystemet Valus samt redegjort for bankens håndtering af konstaterede angreb på Valus i maj måned 2002.

Banken har endvidere ved e-post af 25. november 2002 besvaret Datatilsynets uddybende spørgsmål om eventuel lukning af Valus i forbindelse med hændelsen den 22. maj 2002.

Det oplyses af Den norske Bank, at Valus er udviklet af Den norske Bank, Accenture og Netaxept. Systemet ejes af Den norske Bank og forvaltes af Netaxept. Den norske Bank og Netaxept er henholdsvis dataansvarlig og databehandler i persondatalovens forstand.

Det oplyses endvidere, at Valus består af et **informationssystem** og et **betalingssystem**. I bankens redegørelse af 6. november 2002 oplyses det om angreb, som fandt sted mod **betalingssystemet** den 22. maj 2002,

- at uvedkommende i en kort periode efter systemets åbning har kunnet se enkelte anonyme betalingstransaktioner og enkelte testtransaktioner stammende fra en forudgående pilotperiode. Transaktionerne indeholdt navne på medarbejdere fra de tre virksomheder, som står bag udviklingen af Valus,
- at det ikke på noget tidspunkt har været muligt for uvedkommende at modificere i Valus, hverken persondata eller transaktionsdata,
- at hændelsen skyldes en programmeringsfejl, som blev konstateret den 22. maj 2002, og at fejlen blev rettet i produktionsmiljøet den 23. maj 2002 kl. 8 efter gennemførelse af korrektion og test,
- at fejlen ikke var blevet afdækket på grund af en fejl i testscripts og testbetingelser, og fordi en særskilt test ikke blev gennemført igen,

- at rutiner vedrørende gennemgang af testplaner, testbetingelser og relaterede processer er blevet skærpet,
- at interne rutiner ikke vurderes at have været overtrådt, samt
- at systemet efter rettelse af fejlen jævnligt har været genstand for angreb, uden at angrebene er lykkedes.

Om konsekvensen af den konstaterede fejl i betalingssystemet oplyser banken - at det ved at ændre en transaktions-ID i en URL - for en lovlig pålogget bruger var muligt at se andre brugeres transaktioner, uden at disse transaktioner dog kunne henføres til en bestemt person.

Det fremhæves endvidere af banken, at oplysninger om brugernes betalingskortnumre ikke gemmes i Valus-systemet, og at de derfor ikke var tilgængelige ved hændelsen i maj.

Om de angreb, som fandt sted den 23. maj 2002, og som blev omtalt på Computerworlds debatsider samme dag, oplyses det i bankens brev af 6. november 2002, at disse angreb rettede sig mod Valus' **informationssider**, som ikke indeholder transaktions- og persondata.

Det fremgår af bankens redegørelse, at banken løbende kontrollerer, i hvilket omfang systemet er udsat for angreb, og at man vurderer, om disse angreb lykkes.

På Datatilsynets forespørgsel om eventuel lukning af betalingssystemet i forbindelse med hændelserne den 22. maj 2002 har banken oplyst, at systemet ikke blev lukket umiddelbart efter at fejlen blev opdaget, idet det var bankens vurdering, at fejlen havde minimale konsekvenser, da informationen hovedsagelig var anonym. Banken vurderede endvidere, at en lukning ville have været til større ulempe for forbrugere og kunder, end konsekvensen af den fortsatte drift. Banken oplyser endvidere, at man i perioden fra kl. 03.00 til kl. 15.45 den 23. maj 2002 lukkede systemet for at sikre spor i logfiler og for at gennemgå data. Gennemgangen afdækkede efter det oplyste ingen unormale forhold.

Sammenfattende anfører Den norske Bank, at det er bankens opfattelse, at der er truffet de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt kunne tilintetgøres, fortabes eller forringes, samt mod, at disse oplysninger kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven.

Det er endvidere bankens opfattelse, at Netaxept som databehandler kan træffe de i persondataloven § 41, stk. 3-5, nævnte tekniske og organisatoriske sikkerhedsforanstaltninger, og at banken har påset, at dette skete.

Datatilsynets udtalelse
Lov nr. 429 af 31. maj 2000 om behandling af personoplysninger (persondataloven) gælder i følge lovens § 1 bl.a. for behandling af personop-

lysninger, som helt eller delvis foretages ved hjælp af elektronisk databehandling.

Af persondatalovens § 41, stk. 3, fremgår, at den dataansvarlige skal træffe de fornødne tekniske og organisatoriske sikkerhedsforanstaltninger mod, at oplysninger hændeligt eller ulovligt tilintetgøres, fortabes eller forringes, samt mod, at de kommer til uvedkommendes kendskab, misbruges eller i øvrigt behandles i strid med loven. Tilsvarende gælder for databehandlere.

Datatilsynet har noteret sig Den norske Banks oplysninger.

Da **informationssiderne** efter det oplyste ikke indeholder personoplysninger, falder disse sider udenfor persondatalovens område.

I Valus' **betalingssystem** har der været adgang for uvedkommende til et begrænset antal testtransaktioner samt betalingstransaktioner, som var anonyme for den uvedkommende læser. I denne sammenhæng må Datatilsynet således konstatere, at der ikke i overensstemmelse med persondatalovens § 41, stk. 3, har været truffet de fornødne foranstaltninger mod, at oplysninger kunne komme til uvedkommendes kendskab.

Under hensyn til konsekvensen og omfanget af den konstaterede brist og bankens håndtering af de nævnte hændelser finder Datatilsynet efter en samlet vurdering ikke grundlag for at udtale kritik af Den norske Bank. Datatilsynet foretager sig herefter ikke yderligere i sagen.

Kopi af dette brev er d.d. sendt til Forbrugerstyrelsen, som har anmodet om at blive orienteret om udfaldet af denne sag. Datatilsynet forventer endvidere at omtale sagen på sin hjemmeside.

Med venlig hilsen

Ib Alfred Larsen
IT-chef