Ministeren for videnskab, teknologi og udvikling

Udvalget for Videnskab og Teknologi
Folketinget
Christiansborg
1240 København K

Hermed fremsendes svar på spørgsmål nr. 198 og 199 (Alm. del) stillet af Udvalget for Videnskab og Teknologi den 20. juli 2010. Spørgsmålene er stillet efter ønske fra Per Clausen (EL).
.

Med venlig hilsen

Charlotte Sahl-Madsen

17. august 2010

Ministeriet for Videnskab
Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

Sagsnr.
Dok nr. 1473036

Spørgsmål nr. 198 og 199 (Alm. del) stillet af Udvalget for Videnskab og Teknologi den 20. juli 2010 til Ministeren for videnskab, teknologi og udvikling.

Spørgsmål 198

Kan ministeren bekræfte, at persondatalovens regler om samtykke og kryptering også gælder, når der anvendes sms i forbindelse med Nem id?

Svar

IT- og Telestyrelsen oplyser, at den pågældende anvendelse af sms er omfattet af persondataloven.

IT- og Telestyrelsen har til besvarelse af spørgsmålet indhentet følgende udtalelse om samtykke og kryptering fra DanID, som er den driftsansvarlige operatør på løsningen, og som i henhold til persondataloven må betragtes som den dataansvarlige:

" Det kan oplyses, at sms i nogle tilfælde anvendes til udsendelse af meddelelser til brugeren, herunder midlertidig adgangskode til aktivering af NemID. Det sker alene, når borgeren har angivet sit mobiltelefonnummer og er korrekt legitimeret eller kendt i systemet.

Borgeren vælger selv, om brugeren vil opgive et mobilnummer, og brugeren oplyses om, at supportfunktionen kan sende meddelelser, herunder en midlertidig adgangskode som sms til mobiltelefonen, hvis brugeren skulle få brug for det. Den midlertidige adgangskode kan kun benyttes en gang og skal erstattes af en af brugeren valgt ny kode. Den fremsendte midlertidige adgangskode indeholder ikke personnummer eller lignende oplysning om brugeren. Der udsendes således ikke fortrolige personoplysninger via sms. Der foretages ingen kryptering af disse sms'er.

Samtykkekravet i persondataloven i relation til udsendelse af meddelelser via sms anses opfyldt, når brugeren eksplicit vælger at angive mobiltelefonnummeret, hvis brugeren ønsker at modtage meddelelser på den måde.

Persondataloven indeholder ikke eksplicitte bestemmelser vedrørende kryptering, men § 41, stk. 3 foreskriver, at der skal træffes foranstaltninger til imødegåelse af, at data kommer i de forkerte hænder eller på anden måde forvanskes eller fortabes. Bestemmelsen gælder såvel dataansvarlige som databehandlere.

I praksis er reglen i persondataloven suppleret af bekendtgørelse nr. 528 af 15. juni 2000 om sikkerhedsforanstaltninger til beskyttelse af personoplysninger, som behandles for den offentlige forvaltning og den tilhørende vejledning nr. 37 af 2. april 2001. Reglerne for offentlige virksomheder har haft en afsmittende effekt for private virksomheder. Af bekendtgørelsen og vejledningen fremgår det:

Ministeriet for Videnskab
Teknologi og Udvikling
Bredgade 43
1260 København K
Telefon 3392 9700
Telefax 3332 3501
E-post vtu@vtu.dk
Netsted www.vtu.dk
CVR-nr. 1680 5408

”Hvis der er tale om transmission af fortrolige oplysninger, herunder personnummer, skal der som minimum foretages en kryptering.”

DanID har vurderet, at en sms, der indeholder en midlertidig adgangskode, ikke er fortrolige oplysninger i persondatalovens forstand, da den ikke indeholder oplysninger om borgeren.”

Jeg henholder mig til denne udtalelse fra DanID og fra IT- og Telestyrelsen.

Spørgsmål 199

Kan ministeren bekræfte, at det vil være nødvendigt med en backup på serveren med private kryptonøgler og at dette vil indebære, at samtlige nøgler vil kunne trækkes ud som software fra en sådan backup og at alle nøgler, som følge af dette vil kunne kompromiteres?

Svar

IT- og Telestyrelsen har til besvarelse af spørgsmålet indhentet følgende udtalelse fra DanID, som er den driftsansvarlige operatør på løsningen:

”DanID er underlagt de certifikatpolitikker, der gælder for udbydere af OCES-certifikater (Offentlige Certifikater til Elektronisk Service). I certifikatpolitikkerne stilles en række krav til udbyderens udstedelsesprocesser, nøglehåndtering, certifikathåndtering, anvendelse af algoritmer samt styring og drift af det tekniske miljø og de organisatoriske procedurer. For at opfylde disse krav er det bl.a. nødvendigt, at den server, som beskytter brugerens private kryptonøgler er dubleret, og at det er muligt at foretage kontrollerede og autoriserede kloner/backup af serveren. I den konkrete implementering af NemID opbevares nøglerne på specialdesignet hardware, der er placeret på to forskellige lokationer. Sikkerheden i serverne er blandt andet baseret på kryptografiske moduler, såkaldte Hardware Security Modules (HSM), der teknisk understøtter sikkerhedsprocedurer, hvor kloning/backup kun kan finde sted under kontrollerede forhold med deltagelse af flere betroede medarbejdere. En kloning/backup kræver således bl.a. anvendelse af to specifikke chipkort, der i DanID er placeret hos betroede medarbejdere i to forskellige organisatoriske enheder. Anvendelse af kontrollerede og autoriserede kloner/backup af HSM er gængs praksis for udbydere af certifikater.

Det bemærkes, at DanID er underlagt løbende ekstern systemrevision som en del af kravene fra certifikatpolitikken.

Det kan ikke afvises, at det, ved at omgå alle praktiske, tekniske og procedure-mæssige sikkerhedsforanstaltninger, som DanID via certifikatpolitikerne og DanID’s certificeringspraksis er underlagt, vil være muligt for DanID at lave en ren softwareklon/backup af serveren med brugernes private kryptonøgler. Dette vil dog forudsætte at flere uafhængige betroede personer hos DanID optræder i strid med certifikatpolitikernes krav og vil være et klart brud på de forpligtelser og krav, DanID er underlagt.

Det skal understreges, at selvom alle sikkerhedsforanstaltninger blev overtrådt, og der således i teorien er mulighed for at lave en softwareklon, vil dette ikke give DanID adgang til brugernes private nøgler, da disse er krypteret, og dermed utilgængelige uden anvendelse af brugerens selvvalgte adgangskode, der ikke kendes af DanID. Det samme gælder også, når DanID foretager kontrollerede og autoriserede kloner/backup i hardware."

Jeg henholder mig til denne udtalelse fra DanID.