JUSTITSMINISTERIET
Civil- og Politiafdelingen

Folketinget
Retsudvalget
Christiansborg
1240 København K

Dato: 2. april 2009
Kontor: Færdsels- og våben-kontoret
Sagsnr.: 2009-150-1082
Dok.: LAR40186

Hermed sendes besvarelse af spørgsmål nr. 563 (Alm. del), som Folketingets Retsudvalg har stillet til justitsministeren den 9. marts 2009. Spørgsmålet er stillet efter ønske fra Karina Lorentzen Dehnhardt (SF).

Brian Mikkelsen

/

Anette Arnsted

Slotsholmsgade 10
1216 København K.

Telefon 7226 8400
Telefax 3393 3510

www.justitsministeriet.dk
jm@jm.dk

Spørgsmål nr. 563 fra Folketingets Retsudvalg (Alm. del):

> ”Hvordan kan man sikre pasmodellen mod misbrug fra kriminel, kommerciel eller statslig side?”

Svar:

Justitsministeriet har til brug for besvarelsen af spørgsmålet indhentet en udtalelse fra Rigspolitiet, der har oplyst følgende:

> ”Rigspolitiet har forstået spørgsmålet således, at det ønskes oplyst, hvordan det sikres, at der ikke sker misbrug af de oplysninger, som fremgår af passets personside eller er lagret på chippen i passet.
>
> Rigspolitiet kan oplyse, at udformningen af de danske pas, herunder lagringen af biometriske oplysninger, sker efter kravene i Rådets forordning nr. 2252/2004 af 13. december 2004 om standarder for sikkerhedselementer og biometriske identifikatorer i pas og rejsedokumenter med tilhørende tekniske specifikationer.
>
> Et væsentligt mål med forordningen og de tilhørende specifikationer er at sikre den nødvendige beskyttelse af borgernes oplysninger, herunder særligt at de biometriske kendetegn lagres, så der ikke kan skabes uautoriseret adgang.
>
> Specifikationerne kræver, at de lagrede oplysninger er beskyttet mod aflytning ved såkaldt Basic Access Control (BAC). Beskyttelsen sker rent praktisk ved, at oplysningerne i chippen er krypteret, og først kan læses, når den, der ønsker at få adgang til oplysningerne på chippen, har oplyst tre oplysninger, som tilsammen er unikke for det enkelte pas. De tre oplysninger er pasnummeret, indehaverens fødselsdato og passets udløbsdato. Selve overførslen af oplysningerne fra passet til myndighedernes paslæsere er ligeledes sikret ved kryptering, således at uvedkommende ikke kan aflytte kommunikationen.
>
> Det er derfor ikke muligt at få adgang til oplysningerne i passet, medmindre man fysisk har passet i hånden og dermed adgang til de tre nødvendige oplysninger. Tilsvarende er det ikke muligt at aflytte et pas, der befinder sig i pasindehaverens lomme.
>
> I tilknytning til den kommende implementering af fingeraftryk i de danske pas kræver de tekniske specifikationer, at selve fingeraftrykket beskyttes af såkaldt Extended Access Control (EAC). Det betyder, at fingeraftrykkene i de danske pas kun kan læses, hvis læseren er blevet autoriseret med et særligt certifikat fra de danske pasmyndigheder.”