TEKNOLOGI-RÅDET
THE DANISH BOARD OF TECHNOLOGY

Antonigade 4
DK - 1106 København

Tel. +45 33 32 05 03
Fax +45 33 91 05 09

www.tekno.dk
tekno@tekno.dk

Giro (1199) 8 51 07 68

Anbefalinger for brug af biometri i det danske samfund

1. Der skal udformes et sæt retningslinjer for anvendelse af biometri
I lyset af den teknologiske udvikling og digitaliseringen i almindelighed er de nuværende procedurer for vurdering og kontrol af biometriske systemer ikke tilstrækkelige. Den hastige udvikling af nye teknologier bevirker, at det ikke alene er nødvendigt med juridisk ekspertviden men også teknologisk ekspertise for at kunne vurdere, om et biometrisk system er hensigtsmæssigt konstrueret eller ej.
For det første anbefaler arbejdsgruppen, at personer med teknologisk indsigt bliver inddraget i vurderingen af systemerne, og at der løbende bliver ført kontrol med, at systemerne anvendes efter forskrifterne. For det andet anbefaler arbejdsgruppen, at personer og virksomheder, der ønsker at anvende systemer, hvor biometri indgår, får langt bedre adgang til både offentlig rådgivning og forhåndsgodkendelse i opstartsfasen, end de har i dag. For det tredje mener arbejdsgruppen, at fortolkningen af Persondataloven skal præciseres i lyset af den omfattende udvikling af biometriske teknologier og andre teknologier, der har fundet sted. I den forbindelse anbefaler arbejdsgruppen, at:

1.1 Datatilsynet tildeles flere ressourcer til kontrol og inddrager flere personer med teknologisk ekspertise i vurdering og godkendelse af biometriske systemer
Vurdering af nye teknologiske løsninger kræver stadig større teknisk ekspertise. Arbejdsgruppen anbefaler, at procedurerne for lovgivning om brugen af biometriske løsninger ændres, så personer med teknologisk indsigt bliver inddraget i vurderingen. Arbejdsgruppen anbefaler videre, at man i den forbindelse lader sig inspirere af den praksis, der er i Norge. En ændret praksis i Danmark vil kræve tilførsel af flere ressourcer, men arbejdsgruppen vurderer, at det er et helt nødvendigt tiltag, da man herved vil kunne sikre en mere kvalificeret vurdering af de enkelte sager.

1.2 Opstillere af biometri tilbydes rådgivning og mulighed for forhånds-godkendelse
Et stigende antal virksomheder og organisationer ønsker at opstille biometriske systemer. De kan på nuværende tidspunkt ikke få forhåndsgodkendt et system eller få teknisk rådgivning i opstartsfasen. På grund af de biometriske systemers kompleksitet kan det være vanskeligt at gennemskue, hvordan man mest hensigtsmæssigt konstruerer en løsning, der lever op til kravene om effektivitet og privatlivsbeskyttelse. Muligheden for rådgivning og for at få forhåndsgodkendt et system vil for det første skabe større sikkerhed for, at opstillere af et biometrisk system ikke senere i processen får påbud om at ændre i systemet. For det andet vil det medvirke til at sikre, at løsningerne opnår en højere kvalitet.

1.3 Præcisering af fortolkning af Persondataloven
En række teknologier udvikles i disse år markant og står overfor et massivt gennembrud. Biometri er en af disse teknologier, men også Radio Frequency Identification (RFID) og videoovervågning kan fremhæves. Der er behov for at præcisere, hvordan Persondataloven skal fortolkes i forhold til aktuelle teknologier og disses indflydelse på privatlivets fred. Arbejdsgruppen foreslår, at der bliver udarbejdet en vejledning, som med autoritet fortolker persondataloven og anviser,

hvordan teknologier skal anvendes i praksis, og hvilke privatlivsfremmende hensyn såsom Privacy Impact Assessment (PIA), Privacy Enhancing Technologies (PET) og Privacy by Design, der bør tages med i overvejelserne ved implementering af ny teknologi.

2 Biometri skal bruges til at opnå øget privatlivsbeskyttelse og til at sikre, at brugerne har kontrol med egne data

Biometri åbner for at styrke privatlivsbeskyttelsen, da teknologierne giver mulighed for sikker autentifikation (bekræftelse af adgangsrettigheder), uden at ens fulde identitet bliver afsløret. Man kan beskytte en række personfølsomme oplysninger ved hjælp af forskellige former for biometri kombineret med passwords. Arbejdsgruppen anbefaler, at man undgår at skabe biometriske systemer, hvor for eksempel et fingeraftryk og intet andet giver adgang til en lang række forskelligartede personfølsomme oplysninger. Arbejdsgruppen anbefaler videre, at der i relation til alle nye biometriske systemer bliver udarbejdet en privatlivsimplikationsanalyse (PIA), der sikrer en fornuftig balance mellem formålet med systemet, detaljeringsgraden af identifikation, de lagrede persondata og risikoen for datamisbrug og -tyveri. Privatlivsbeskyttelse og gennemsigtighed skal medtænkes, når systemerne bliver designet, og man bør udarbejde en plan for anvendelse af "Privacy Enhancing Technologies" (PET) – det er teknologier, som understøtter beskyttelse af borgernes privatliv. Samtidig bør etiske overvejelser om risici for social stigmatisering, social inklusion og social eksklusion medtænkes helt fra start. Arbejdsgruppen peger endvidere på, at jo mere der fra politisk hold bliver lagt vægt på at benytte biometri til at styrke privatlivsbeskyttelsen, jo mere accepteret vil biometri på sigt blive i offentligheden, da risikoen for misbrug herved minimeres.

2.1 Biometriske systemer skal konstrueres på en sådan måde, at de tager mest muligt hensyn til privatlivets beskyttelse

Man bør altid sikre, at målet med den biometriske løsning nås med mindst mulig indgriben i brugernes privatliv. En indledende vurdering med dette formål kan tage udgangspunkt i følgende spørgsmål:

1. Er systemet konstrueret på en sådan måde, at man i videst mulig omfang undgår at lagrepersonfølsomme oplysninger?
2. Er det muligt, for derved at undgå central lagring af personfølsomme oplysninger, at lagre data decentralt og sikre, at brugerne har kontrol over egne data – for eksempel ved brug af en såkaldt "system on card-løsning" eller en "match on card-løsning"?
3. Er det muligt at opfylde formålet med systemet, uden at brugerens identitet – for eksempel brugerens navn – bliver knyttet til biometriske data?
4. Er der alternative muligheder for brugere, som ikke kan eller ønsker at anvende biometri?
5. Er det muligt at anvende en pseudonymiseret, central database – det vil sige en database, hvor borgernes rigtige navne er erstattet af pseudonymer?
6. Er det biometriske system afsondret fra netværk?
7. Er der anvendt kryptering?
8. Er der fastlagt procedurer for, hvem der har adgang til de biometriske templates eller data knyttet til templates?
9. Slettes templates og tilknyttede data, som ikke længere anvendes?

2.2 Registrering af borgere og kunder skal ske på en sådan måde, at der bliver taget mest mulighensyn til privatlivets beskyttelse

De seneste år har en række diskoteker, fitnesscentre og andre søgt Datatilsynet om tilladelse til at anvende biometri. Disse henvendelser har ført til forskelligartede svar, som arbejdsgruppen ønsker at knytte følgende kommentarer til:

Restaurationsbranchen bør anvende "match on card-teknologi"

Arbejdsgruppen vurderer, at restaurationsbranchens ønsker til brug af biometri er uhensigtsmæssige. Branchens mål vil kunne opnås på mindre privatlivsindgribende vis, hvor restaurantgæster selv beholder deres biometri. Det kan for eksempel ske ved at udstede chipkort til gæsterne, hvorpå deres biometri lagres. På den måde vil man undgå den nuværende sammenknytning af navn, billede og biometri. Arbejdsgruppen vurderer, at lagring af såvel biometriske data som personens navn og billede i en central database repræsenterer et unødigt indgreb i den enkeltes privatliv. Målet kan i stedet nås ved brug af såkaldt "match on card-teknologi"– det vil sige en løsning, hvor de biometriske data i krypteret form er lagret på et plastikkort med chip. Ved adgang matches informationerne på chippen med resultatet af en aktuel scanning af gæstens fingeraftryk. Et alternativ kunne være brug af negativlister, hvor kun de uønskede gæster er registrerede. Udfordringen i den sammenhæng er, at uønskede personer vil kunne snyde nogle scannertyper ved fx at placere fingeren skævt på scannerenheden og derved opnå adgang alligevel. Derfor stiller både negativlister og selvbetjeningsløsninger større krav til scannerenhedernes beskaffenhed, så der kan tages højde for fejl. Generelt er det nødvendigt at etablere robuste systemer med læsere, der ikke kan snydes, og løbende følge den teknologiske udvikling og løbende opgradere sikkerheden.

Fitnesscentre bør anvende "match on card-teknologi"

Flere fitnesscentre har ansøgt om at måtte bruge biometri med det formål at undgå snyd og samtidig skabe nemmere adgang til centrene for medlemmerne. Datatilsynet har afvist at give disse fitnesscentre mulighed for at benytte et system med en tilhørende database, hvor medlemmernes biometri bliver lagret i krypteret form. Arbejdsgruppen vurderer, at de pågældende fitnesscentre bør have mulighed for at udstede medlemskort baseret på "match on card-teknologi" – en løsning, hvor de biometriske data i krypteret form er lagret på medlemskortets chip og ved adgang til fitnesscentret bliver matchet med resultatet af en aktuel scanning af brugerens fingeraftryk. Denne løsning vil betyde en merudgift for fitnesscentret, men systemet vil formentlig også mindske omfanget af snyd med medlemskort. Arbejdsgruppen anbefaler, at et sådant system skal være frivilligt og baseret på samtykke fra brugerne, ligesom det skal være muligt at vælge et alternativ, som ikke stiller brugerne dårligere, end hvis de benytter den biometriske løsning.

Erhvervslivet bør gå sammen om en fælles løsning, hvor brugerne bevarer kontrollen med egne data

I lyset af de ovenfor nævnte ønsker fra private virksomheder bør man undersøge mulighederne for, at private virksomheder i fællesskab designer et system, som både øger sikkerheden, gør brugen af serviceydelser mere bekvem og lader brugerne bevare kontrollen med egne data. En mulig egnet business case i denne sammenhæng, som bør undersøges nærmere, er biometrisk "match on card-teknologi" – eventuelt i kombination med en pinkode – som mulig erstatning for adgangskort, medlemskort, betalingskort mv.

3. Et fremtidigt biometrisk borgerservicekort skal baseres på "system on card-teknologi" eller lignende teknologier

Arbejdsgruppen mener, at et borgerkort med krypterede biometriske data, som er baseret på "system on card-teknologi" eller lignende teknologier, ud fra en sikkerhedsmæssig betragtning er en ønskelig løsning. "System on card" betyder, at brugeren ved hjælp af biometrisk identifikation har adgang til sit eget kort, som rummer en række koder/elektroniske nøgler til forskellige formål – blandt andet udveksling af informationer med det offentlige. Brugeren vil med denne teknologi have fuld kontrol over egne data, og systemet vil være mere privatlivsbeskyttende end for eksempel den nuværende digitale signatur. Arbejdsgruppen anbefaler, at et borgerservicekort baseres på decentral datalagring, og at borgeren via kortet kan aktivere en række forskellige koder/nøgler. Ved tyveri eller tab af kortet skal det være muligt at blokere det og oprette et nyt uden væsentlige omkostninger for hverken det offentlige eller brugeren. Prisen for et sådant system er dog på nuværende tidspunkt relativ høj, og det er blandt andet derfor værd at overveje alternativer til et borgerkortservicekort, som er udstedt og finansieret af staten. Arbejdsgruppen vurderer, at der på lidt længere sigt er potentiale i at anvende biometri i mobiltelefoner, PDA'er eller lignende, hvor adgang til de lagrede oplysninger, koder og nøgler kontrolleres af brugerne selv. Arbejdsgruppen peger på, at brug af mobiltelefon frem for et borgerservicekort vil have en række fordele:

- Brugerne er vant til at benytte mobiltelefonen
- Brugerne har (altid) mobiltelefonen med
- Brugerne betaler selv for den
- Mobiltelefonen har indbygget processor og kan derfor generere koder og nøgler
- Et stigende antal mobiltelefoner har både kamera, mikrofon og trykfølsomt display, hvilket potentielt giver mulighed for brug af følgende biometriske teknologier: Tastedynamik, irisscanning, ansigtsgenkendelse, signatur-analyse og stemmegenkendelse. Flere vil komme til i de kommende år.

4. Start med at definere formålet med den biometriske løsning

Hvis formålet med den biometriske løsning er tydeligt defineret på forhånd, kan man undgå urealistiske forventninger til løsningens formåen. Erfaringer fra udlandet viser, at manglende formålsspecifikationer har resulteret i biometriske løsninger, der ikke lever op til forventningerne hos hverken opstillerne eller brugerne. Arbejdsgruppen anbefaler derfor, at man allerede i udviklingsfasen skaber maksimal klarhed om den biometriske løsnings reelle formål og performance. Dette vil endvidere sætte fokus på potentielle faldgruber – for eksempel risikoen for såkaldt "function creep", hvilket vil sige, at data bruges til andet end det oprindelige formål. Arbejdsgruppen anbefaler, at man i en personalehåndbog eller lignende fastslår formålet med det biometriske system og samtidig formulerer præcist, hvad de opsamlede data bliver brugt til. Det vil give medarbejderne sikkerhed for, at data ikke bruges til andre formål end de tilsigtede. Det er arbejdsgruppens holdning, at en klar og tydelig formålsspecifikation vil skabe tryghed om den biometriske løsning hos medarbejdere/brugere. Samtidig vil det mindste risikoen for misbrug af data. Arbejdsgruppen fremhæver, at de mulige konsekvenser ved misbrug af data, som er opsamlet i en biometrisk løsning, afhænger af løsningens størrelse og omfang. De følgende anbefalinger er primært rettet mod større biometriske installationer:

5. Et biometrisk systems sikkerhed er betinget af sikkerheden i hele systemet
Et biometrisk systems sikkerhed er altid betinget af sikkerheden i hele den it-løsning, som biometrien er ét af mange elementer i. Arbejdsgruppen fremhæver derfor, at man altid skal se på helheden, når man vurderer et systems sikkerhed. Risikoen i et givet system for blandt andet "hacking" og "spoofing" – "spoofing" er, når en person udgiver sig for at være en anden ved for eksempel at anvende et falsk fingeraftryk – skal vurderes i alle de faser, en bruger skal gennemgå i forhold til registrering og øvrig brug af systemet. Arbejdsgruppen påpeger, at selve registreringsprocessen i et biometrisk system er en særligt sårbar fase. For eksempel skal der kun én uopmærksom medarbejder i kommunen til at skabe et lovligt udstedt pas, hvor de anvendte biometriske data passer sammen med en andens identitet.

6. Procedurerne for registrering af biometriske data skal standardiseres
For at sikre interoperabilitet på tværs af grænserne – interoperabilitet er produkters, systemers og forretningsprocessers evne til at arbejde sammen om løsningen af en fælles opgave – anbefaler arbejdsgruppen, at registrering af biometriske oplysninger standardiseres. Dette skal helst ske globalt, men i det mindste i EU. Arbejdsgruppen anbefaler, at en person, der skal registreres i en biometrisk løsning, skal oplyses om formålet med og omfanget af registreringen. Det skal endvidere være muligt for brugeren at se og kontrollere, om de registrerede oplysninger er korrekte. Registreringsproceduren skal derudover indeholde nogle klare, standardiserede procedurer for, hvordan man fjerner data om en bruger fra systemet. Veluddannet personale og transparente procedurer skal i det hele taget sikre fuld gennemskuelighed for de registrerede brugere. Der skal desuden udformes standardiserede procedurer for sletning af data.

7. Procedurerne for lagring og matchning af biometriske data skal standardiseres
Arbejdsgruppen anbefaler, at man, når det er muligt, undgår at anvende centrale databaser i forbindelse med biometriske løsninger. Hvis en biometrisk løsning alligevel baseres på en central database, skal datakvaliteten i denne være af højst mulig kvalitet og behandles af certificeret personale. Samtidig skal det være muligt for brugere at trække egne data tilbage eller rette i egne data, hvis brugerne finder, at der er fejl eller mangler i de registrerede data. Der skal ligeledes være en standardiseret klagemulighed, som fuldt ud respekterer individets suverænitet, og som understøtter procedurerne i et demokratisk samfund. Arbejdsgruppen anbefaler videre, at biometriske data aldrig lagres i råformat, hvilket for eksempel kan være et digitalt billede af et fingeraftryk. I stedet lagres data som krypterede templates. Dette vil reducere risikoen for identitetstyveri og misbrug af persondata betydeligt. Samtidig anbefaler arbejdsgruppen, at man undgår at udlicitere databehandling til tredjepart, da man derved forringer adgangen til at praktisere sikker kontrol med de lagrede oplysninger. Endelig anbefaler arbejdsgruppen øget standardisering på teknisk niveau i form af fælles algoritmer, kalibrering og interface og i forhold til uddannelse af certificeret personale. Standardiseringen på disse områder bør ske globalt og i det mindste på EU-niveau. Arbejdsgruppen anbefaler, at biometrisk matchning kun matcher de biometriske data og ikke forespørger de persondata, der er knyttet til de biometriske data. Det vil mindske risikoen betydeligt for, at personfølsomme oplysninger falder i forkerte hænder.

8. Der skal altid være sikre alternativer og "fall-back-procedurer"
Arbejdsgruppen peger på, at der især knytter sig to svagheder til biometrisk identifikation: Biometri kan aldrig blive 100 procent nøjagtigt, og biometriske

systemer vil altid både afvise og acceptere en andel ”forkerte” personer. Ikke alle har brugbare biometriske karakteristika – for eksempel kan et fingeraftryk være beskadiget, hvorfor det ikke kan registreres korrekt. Disse forhold gør, at det er umuligt at skabe et sikkert system, som udelukkende er baseret på biometri. Der vil derfor altid være behov for et eller flere klart definerede alternativer – såkaldte ”fall-back-procedurer”. Der bør endvidere i forbindelse med blandt andet automatiseret grænsekontrol uddannes operatører, der forstår at behandle både korrekt og forkert afviste personer på en anstændig måde, så der ikke foregår social stigmatisering og lignende.

9. Der er brug for flere test af biometriske systemer

Det er på nuværende tidspunkt meget vanskeligt at sammenligne forskellige biometriske systemers performance. De fleste af de tilgængelige test er fortaget af producenterne selv i laboratorier uden de fejlkilder, som findes i de miljøer, hvor systemerne bliver anvendt. En omfattende test af biometriske systemer fortaget af den britiske regering har vist en meget stor reel fejlrate for systemer, som er baseret på fingeraftryksscanning, irisgenkendelse eller ansigtsgenkendelse. Arbejdsgruppen anbefaler, at man indfører flere standardiserede test, og at der derigennem bliver skabt større åbenhed om de biometriske systemernes reelle formåen.

10. Berøringsfrie enheder bør benyttes i miljøer, hvor hensynet til hygiejne er vigtigt

Arbejdsgruppen anbefaler, at man benytter berøringsfrie scannere – hvor man for eksempel holder hånden i nogle centimeters afstand fra scanningspladen – på steder, hvor en høj grad af hygiejne er påkrævet. Det gælder eksempelvis på hospitaler. Arbejdsgruppen peger på, at iris- og venescanning i denne sammenhæng bør overvejes som gode alternativer til scanning af fingeraftryk.