RÅDET FOR DIGITAL SIKKERHED

Information og anbefalinger nr. 4

Digital vækst med tillid som fundament

12. november 2014

Resumé

Regeringen planlægger i efteråret 2014 at lancere en vækstplan med en række konkrete initiativer, som skal fremme den digital vækst i Danmark. Rådet for Digital Sikkerhed støtter ambitionen om at gøre digital vækst til et centralt fokus, både i forhold til dansk erhvervspolitik og i forhold til det danske samfunds udvikling som helhed.

Danmark har aktuelt meget store uudnyttede muligheder for at drage fordel af og være med til at forme den globale digitale vækst. I det globale perspektiv er Danmark med helt i front, når det gælder digitalisering, både i den private og i den offentlige sektor. Derfor er det vigtigt, at vi udvikler eksempler til efterfølgelse, hvor digitale løsninger etableres med tillid som en afgørende del af fundamentet. Fremover bør både it-sikkerhed og individets ret til privatlivsbeskyttelse derfor være en integreret del i alle nye it-projekter. Det er ifølge Rådets vurdering en forudsætning for sund, stabil og langsigtet digital vækst.

Der bør arbejdes for at etablere et dansk cluster med fokus på sund digital vækst, hvor globalt førende forskere bringes sammen med de virksomheder, der er aktive inden for området. En fremsynet statslig politik på dette område vil give muligheder for at etablere en internationalt succesfuld dansk indsats på linje med fx høreapparat- og vindmølleindustrierne. Det er i denne sammenhæng afgørende at sikre sammenhængen med offentligt igangsat digital infrastruktur, fx CPR og systemer til elektronisk identifikation (eID), at sørge for gode rammebetingelser og at udforme offentlige udbudskrav, så de understøtter satsningen.

Inden for sundhedsforskningen og generelt i den offentlige sektor er der behov for konsekvent implementering af *privacy by design*, således at datalækager stoppes, og så danskere borgeres privatlivsoplysninger bliver beskyttet. Der er i høj grad brug for formidling og dokumentation af, hvilke metoder forskere og andre kan anvende til pseudonymisering og anonymisering af persondata.

Sund digital vækst er afhængig af, at danske borgere bevarer tilliden til de digitale løsninger. Fremadrettet vil digitalisering af kommunikationen mellem myndigheder, borgere og virksomheder få stigende indflydelse på borgernes generelle tillid til det offentlige og til staten som sådan. Rådet mener derfor, at der uden yderligere udsættelse bør gennemføres en grundig revision af CPR-systemet, og at dette bør ske i sammenhæng med udformningen af afløseren for det nuværende NemID-system. Det centrale princip bør være, at offentligt ansatte og andre databehandlere kun har adgang til det minimum af persondata, som faktisk er nødvendige for at løse en konkret opgave. Det bør således fremover være muligt ved hjælp af CPR og en eID-løsning at verificere en borgers ret til en bestemt ydelse, uden at borgerens identitet blotlægges. Det bør også være muligt at pseudonymisere sundhedsdata, så det vil være op til den enkelte borger, om vedkommende vil orienteres om evt. sygdomsrisici, der afdækkes i forskningsmæssig sammenhæng.

Som led i den foreslåede ambitiøse satsning på sund digital vækst, bør Danmark have en national databeskyttelsesmyndighed, som kan leve op til og også være med til at udforme fremtidens *best practice*, når det gælder national databeskyttelse. Placeret under Folketinget, skal denne myndighed kunne vejlede, stille krav og udføre kontroller i et helt andet omfang end hidtil, både i forhold til offentlige og private aktører.

Anbefalinger

Rådet for Digital Sikkerhed anbefaler følgende som led i en samlet indsats:

- at regeringen fortsætter og intensiverer sit arbejde for at udnytte de muligheder, som ligger i brug af *big data (data mining)* i forhold til eksisterende og fremtidige data om den danske befolkning.
- at regeringen etablerer de nødvendige rammer for at skabe et stærkt og globalt førende erhvervsorienteret forskningsmiljø inden for *big data* og privatlivsbeskyttelse.
- at regeringen og myndigheder generelt stiller offentligt generede data frit og gratis til rådighed for virksomheder og forskere, som vil være i front ift. udvikling af ny smart teknologi og smarte tjenester.
- at regeringen fastlægger et grundlæggende princip om, at borgerne fremadrettet skal have kontrol med hvilke identificerbare persondata, der deles med hvem. I offentligt regi vil det betyde, at en borgers data kun kan tilgås i forbindelse med et konkret arbejdsmæssigt behov. I forskningssammenhæng vil det betyde, at borgere selv har mulighed for at bestemme, hvorvidt de ønsker at indgå i forskning, og om de ønsker at blive adviseret om evt. viden om deres personlige sundhedsrisici, som afdækkes via forskning.
- at regeringen fastlægger retningslinjer for, hvorledes privatlivsbeskyttelse opretholdes i forbindelse med udvidet brug af *big data*, *data mining* osv., herunder at der skabes nem adgang til viden om, hvordan data kan pseudonymiseres og anonymiseres, i praksis for eksempel via vejledning udarbejdet af Erhvervsstyrelsen og den nationale databeskyttelsesmyndighed.
- at regeringen stiller krav og etablerer rammebetingelser, som sikrer etablering af danske digitale systemer, der skaber maksimal tillid og tryghed for borgere, virksomheder og myndigheder, herunder en gennemgribende og sammenhængende revision af CPR- og det danske eID-system (aktuelt NemID).
- at regeringen sikrer, at Danmark får en stærk, robust og uafhængig databeskyttelsesmyndighed, placeret under Folketinget og med et stærkere fokus på at være teknisk vejledende og kommunikere anbefalinger til offentligheden. Databeskyttelsesmyndigheden skal sikre, at systemer som det offentlige har ansvaret for, løbende vedligeholdes og sikres i forhold til kendte og forudsigelige sikkerhedsrisici.
- at den nationale databeskyttelsesmyndighed eller en anden myndighed får de fornødne beføjelser til at stille konkrete krav til leverandører af offentlige it-systemer om robust it-sikkerhed, *privacy by design* og gennemførelse af *privacy impact assesments*, til at implementere kontroller hos leverandøren, og føre kontrol med at krav og kontroller fungerer i praksis.
- at regeringen bakker op om EU-kommissionens udkast til persondataforordning, således at der skabes ensartede regler for databeskyttelse i hele Europa.

Baggrund

Regeringen planlægger i efteråret 2014 at lancere en vækstplan med en række konkrete initiativer, som skal fremme den digital vækst i Danmark, baseret blandt andet på anbefalingerne fra Vækstteam for IKT og Digitalvækst fra januar 2014.

Rådet for Digital Sikkerhed vil gerne udtrykke sin fulde støtte til ambitionen om at gøre digital vækst til et centralt fokus, både i forhold til dansk erhvervspolitik og i forhold til det danske samfunds udvikling som helhed. Rådet vil i særlig grad gerne støtte Vækstteamets anbefaling #10: *Digital sikkerhed skal understøtte den digitale vækst.*

Store uudnyttede muligheder

Danmark har aktuelt meget store – og i stort omfang stadig også uudnyttede – muligheder for at drage fordel af og være med til at forme den globale digitale vækst. En indsats på dette område vil kunne:

- Skabe gode vækstvilkår for virksomheder som tilbyder teknologi og services baseret på *big data (data mining)*, bl.a. fordi virksomheder med privatlivsbeskyttende teknologier i mange tilfælde kan gøre deres data offentligt tilgængelige, uden at deres underliggende data og vidensbase kan replikeres af konkurrenter.
- Tiltrække nye kompetencer til Danmark, både forskere og virksomheder, og skabe nye vidensintensive arbejdspladser.
- Sikre borgernes tillid og tryghed til at staten beskytter deres privatlivsoplysninger - og dermed skabe tryg digitalisering med Danmark i rollen som en af de globale frontløbere.

Vi er midt i en digital transformation, der skaber ny kultur. I det globale perspektiv er Danmark med helt i front, når det gælder digitalisering, både i den private og i den offentlige sektor. Vi danner skole for, hvad der kommer til at ske i andre lande, og vi påtager os dermed også et stort ansvar. Derfor er det vigtigt, at vi udvikler eksempler til efterfølgelse, hvor digitale løsninger etableres med tillid som en afgørende del af fundamentet. Det kan ske ved, at vi fremover integrerer både it-sikkerhed og individets ret til privatlivsbeskyttelse i alle nye it-projekter.

Mere digital vækst og mere fokus på de tryghedsskabende faktorer

Desværre ser vi fortsat alt for mange eksempler på, at netop de tillidsskabende elementer fravælges ud fra snævre økonomiske vurderinger, og fordi der, når det gælder it-sikkerhed og privatlivsbeskyttelse, ikke fra offentlig side i tilstrækkelig grad sættes rammer og stilles krav for at sikre et tilstrækkeligt niveau.

Denne form for kortsigtet prioritering vil, når det gælder digitalisering, blive meget dyr på langt sigt af to grunde. Den ene er, at netop tillid er et af de meste værdifulde – men ofte også oversete – elementer i dansk kultur, forretningsliv og national tradition. Den anden er, at al erfaring viser, at det bliver både dyrere og dårligere, når man efterfølgende skal til at reparere og forbedre et dårligt digitalt fundament.

Rådet for Digital Sikkerhed ser det i denne sammenhæng som afgørende vigtigt, at dansk politik på dette område fremover etableres ud fra en tilgang, hvor fuldt integrerede tillids- og tryghedskabende faktorer ses som fundamentale forudsætninger for sund, stabil og langsigtet digital vækst.

En sådan tilgang kan sikre, at både den danske befolkning og erhvervslivets aktører bliver medskabere af en sund digital vækstkultur. Derved kan både det offentlige, virksomhederne og den enkelte borger drage fordel af de store muligheder og fordele, som nye digitale løsninger tilbyder, samtidig med at vi som samfund respekterer individets krav på fortsat at have en beskyttet privatsfære.

I dette perspektiv er it-sikkerhed og privatlivsbeskyttelse to elementer, som komplementerer hinanden. Med en helhedsorienteret tilgang som den her beskrevne kan de to begreber begge rummes under samlebegrebet *informationssikkerhed*, der dermed bør være centralt i forhold udviklingen af nye digitale systemer.

Danske globale styrkepositioner skal bindes sammen

Som det fremgår af Vækstteamets rapport, har Danmark et overordentligt godt udgangspunkt for at udnytte potentialet i data og høste de erhvervsmæssige og samfundsøkonomiske gevinster, som disse rummer. Den danske offentlige sektor ligger inde med store mængder af informationer om fx geografi, klima, trafik, boligforhold, selskabsregistreringer og regnskaber[1], og hertil kommer en internationalt set unik registrering af sundhedsdata, som er et vigtigt grundlag for Danmarks førende position inden for sundhedsforskning[2]. Der er allerede på mange områder skabt øget adgang til offentlige danske data, fx med Virk Data Dag-initiativet[3].

Samtidig er Danmark international førende, når det gælder forskning inden for digitalisering og informationssikkerhed. Dansk IKT-forskning udmærker sig således internationalt ved at placere sig som nr. 1 ift. de fem førende lande inden for forskningsområderne ”Big data” og "Security & Monitoring"[4]. Forskningen er koncentreret på nogle få danske universiteter, der er forbundet med de bedste internationale forskningsmiljøer. Dog sker dette på nuværende tidspunkt kun med spredt deltagelse fra danske og internationale erhvervsvirksomheder. Den nuværende situation kan således danne grundlag for en satsning, hvor der i Danmark skabes et mere ambitiøst og globalt førende forskningsmiljø med invitation til deltagelse til både danske og internationale erhvervsvirksomheder.

De to danske styrkepositioner inden for digitalisering – den store mængde offentligt genererede data og de forskningsmæssige spidskompetencer inden for *big data* og informationssikkerhed – skal efter Rådets mening bindes meget bedre sammen. Det er her, der ligger store muligheder og venter.

Et dansk cluster med fokus på sund digital vækst

Rådet mener, at der bør gøres en målrettet indsats for i Danmark at skabe et cluster af virksomheder og forskningsenheder, der kan nå op på verdensniveau ift. udnyttelse af og forskning i *big data* på basis af maksimal privatlivsbeskyttelse, herunder videreudvikling af de såkaldte privatlivsbeskyttende teknologier (*PET, privacy enhancing technologies*). Dette skal fra lovgivers side følges op med krav og

[1] Vækstteam for IKT og digital vækst, ANBEFALINGER, januar 2014, http://www.evm.dk/~/media/oem/pdf/2014/2014-publikationer/anbefalinger-vaekstteamet-for-ikt-og-digital-vaekst-24-01-14.ashx

[2] Dansk Sundhedsforskning — Status og Perspektiver, 2008, http://www.regioner.dk/~/media/Dansk_sundhedsforskning_Status_og_perspektiver_Hovedrapport.ashx

[3] https://data.virk.dk/events/virk-data-dag-fra-data-til-forretning

[4] Damvad: ”Danske og Internationale styrkepositioner på IKT-området”, 2013, http://erhvervsstyrelsen.dk/file/359359/danske-styrkepositioner-pa-ikt-omradet-V2-pdf.pdf

nye gennemarbejdede og fremtidsorienterede rammebetingelser for it-sikkerhed og privatlivsbeskyttelse.

På den måde vil en fremsynet statslig politik kunne medvirke til at skabe særlig national kompetence, når det gælder sund digital vækst – med mulighed for at gentage de danske globale succeser inden for fx høreapparatindustrien (igangsat af bl.a. fremsynet lovgivning om indsats inden for den danske høreforsorg) og vindmølleindustrien (igangsat af bl.a. gunstige rammebetingelser ift. vedvarende energi).

Det offentlige har i denne sammenhæng en afgørende rolle på flere forskellige punkter:

- Offentligt igangsatte systemer, fx CPR og det danske eID-system (NemID), udgør en vigtig del af den basale infrastruktur for digitaliseringen.
- Det offentlige kan fastsætte de nødvendige rammebetingelser, som er nødvendige for at den digitale vækst kommer til at ske med fokus på informationssikkerhed og på et sundt og tillidsbaseret fundament.
- Det offentlige kan ved sine udbudskrav støtte brugen af de nye værktøjer, som skal tages i brug for at skabe sikre og tillidsskabende digitale systemer.

De ældre it-systemer giver udfordringer

Danske virksomheder, borgere og myndigheder bliver stadig bedre til at udnytte teknologiens mange muligheder. På en lang række områder er digitale transaktioner og forvaltning blevet det normale, fordi det skaber fordele for alle involverede.

Mange af de nye digitale tjenester er imidlertid etableret på basis eksisterende ældre it-systemer. Ofte er der tale ældre mainframe-løsninger, men der bygges også videre på systemer baseret på tidlige versioner af decentrale platforme. I disse sammenhænge er sikkerhed og privatlivsbeskyttelse etableret på grundlag at den viden, der var, da systemerne oprindeligt blev udformet, og i de fleste sammenhænge uden at den nødvendige vedligeholdelse og sikkerhedsmæssige opgradering af systemerne siden er blevet prioriteret. Det har afstedkommet en lang række eksempler på, at borgeres og virksomheders data utilsigtet og med meget alvorlige konsekvenser er blevet eksponeret, og også at offentlige it-systemer er blevet hacket eller misbrugt med meget store økonomiske tab til følge.

Rådet vil i denne sammenhæng påpege, at det er afgørende at eksisterende systemer vedligeholdes og opdateres på basis af en løbende sikkerhedsmæssig risikovurdering. Risikobilledet ændre sig med stor hast, og vedvarende vedligeholdelse af eksisterende løsninger er i dag en nødvendighed for at sikrer systemerne mod nutidige og fremtidige angreb, der kan kompromittere både fortrolighed og integritet.

Sundhedsoplysninger og forskning

Dansk sundhedsforskning er i verdensklasse, og der er opnået imponerende resultater. Et af fundamenterne for denne succes er det danske CPR-system, som har gjort det muligt at lave detaljeret forskning, hvor enkeltpersoner kan følges over lange forløb.

Som systemet fungerer nu, er den enkelte persons oplysninger kun maskeret i det omfang det implementeres af den enkelte forsker. På tilsvarende vis er der for ansatte i sundhedssektoren i stort omfang fri adgang til persondata. Der er i de systemer der benyttes ikke fokuseret på at minimere

adgangen til det, som faktisk er nødvendigt, selv om denne teknologi er kendt og kan implementeres via retningslinjer for *privacy by design*.

En lang række eksempler har vist, at den nuværende danske praksis på området jævnligt fører til datalækager, og det er Rådets vurdering, at det stadig større fokus på beskyttelse af privatlivets fred og databeskyttelse generelt vil sætte de aktuelt benyttede metoder under pres.

Noget tilsvarende gælder de nyligt vedtagne danske regler om lægers indberetningspligt af patientdata, som betyder, at læger på nuværende tidspunkt ikke med sikkerhed kan overholde deres tavshedspligt[5].

Der er derfor behov for nye metoder, som gør det muligt også fremadrettet at indsamle værdifulde sundhedsoplysninger, samtidig med at individets ret til beskyttelse af persondata bliver respekteret. Dette er muligt rent teknologisk, og det vil kræve, at det samlede juridisk/teknologiske-system ændres og optimeres.

Der udvikles vedvarende nye teknikker til avanceret pseudonymisering[6] og anonymisering[7]. Det er Rådets opfattelse, at kendskab til disse metoder, for ikke at tale om brugen af dem, er meget lidt udbredt både blandt danske forskere og i sundhedssektoren generelt. Derfor bør en satsning på styrkelse af netop disse forskningsområder, som del et stærkt "sund digital vækst"-cluster, følges op med en omfattende formidlings- og dokumentationsindsats. På et sådant grundlag vil det være muligt også fremadrettet at indsamle værdifulde sundhedsdata i Danmark, samtidig med at danske borgeres ret til privatliv respekteres.

Det er i denne sammenhæng værd at pointere, at det ikke længere er tilstrækkeligt at pseudonymisere data, hvis man vil forhindre, at enkeltindivider kan genidentificeres. Det er således veldokumenteret, at individer, der i åbne data optræder under pseudonymer, kan genidentificeres ud fra kombination med andre tilgængelige datakilder og brug af mønstergenkendelse[8].

Tillid som et afgørende fundament for digital vækst

Sund vækst i den private sektor er afhængig af, at borgerne bevarer tilliden til digitaliseringen af den offentlige sektor. På samme vis er den offentlige sektor afhængig af, at der generelt er tillid til privat udbudte digitale løsninger.

Mens tillidsniveauet danskere imellem internationalt set er meget højt, er det i denne sammenhæng måske værd at bemærke, at danskernes tillid til den danske stat aktuelt kun ligger på niveau med

[5] "Sundhedsministeren fjerner vores tavshedspligt", debatindlæg skrevet af fire praktiserende læger – http://politiken.dk/debat/debatindlaeg/ECE2356355/sundhedsministeren-fjerner-vores-tavshedspligt/

[6] Pseudonymisering betyder, at individets identitet holdes skjult men vil kunne genfindes af den, som har nøglen til at gøre det. Oplysningerne vil i lovgivningens forstand stadig være persondata og skal behandles jf. gældende EU- og national lovgivning

[7] Anonymisering betyder, at individets identitet ikke kan genetableres, og sådanne data er derfor ikke længere persondata i lovgivningsmæssige forstand. En mellemløsning er pseudonymisering, hvor det kun er den person som har afgivet personoplysninger, der kan har nøglen til at genetablere identiteten.

[8] Nye teknikker på området omfatter blandt andet brug af *differential privacy*, som tilføjer usikkerhed til data (svarende til det som kendes med kunstigt indlejret usikkerhed i det civile GPS-system) og etablering af syntetiske data (hvor der byttes om på data på individniveau, uden at det overordnede billede ændres). Problematikkerne omkring anonymisering og måden hvorpå dette kan løses er beskrevet i Artikel 29 Gruppens "Udtalelse nr 05-2014 om anonymiseringsteknikker" fra april 2014 - http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_da.pdf

OECD-gennemsnittet[9] og langt efter for eksempel Sverige. Det seneste år er netop it-sikkerhed og privatlivsbeskyttelse blevet centrale temaer i den offentlige danske debat – og det må antages, at digitalisering af kommunikationen mellem myndigheder, borgere og virksomheder i de kommende år vil få stigende indflydelse på borgernes generelle tillid til det offentlige og til staten som sådan.

En væsentlig del af borgernes tillid til den offentlige digitaliseringsindsats er fokuseret omkring CPR og det danske eID-system (NemID). Som Rådet for Digital Sikkerhed i andre sammenhænge har peget på[10], vil det derfor være hensigtsmæssigt, at der uden yderligere udsættelse gennemføres en grundig revision af CPR-systemet, og Rådet mener, at denne revision bør planlægges i sammenhæng med udformningen af afløseren for det nuværende NemID-system.

Kun adgang til de data som faktisk er nødvendige

Når målet er at skabe tillid og sikre privatlivsbeskyttelse, er et godt princip kun at give adgang til netop de data, som en bruger har behov for i forhold til en konkret transaktion eller et konkret formål.

Dette princip findes til dels allerede beskrevet i den gældende lovgivning, herunder den danske persondatalov, som har en lang række bestemmelser vedrørende god databehandlingsskik og videregivelse af data. Selv om princippet for formålsbestemthed og nødvendighed gælder for både private aktører og offentlige myndigheder, er der ved anden lovgivning skabt vid adgang for at offentlige myndigheder kan behandle og videregiver personfølsomme data.

Set i sammenhæng med den fortsatte teknologiske udvikling medfører offentligt ansattes meget vide adgang til borgernes persondata en øget generel sikkerhedsrisiko. Offentlige it-systemer, herunder sundhedssektorens systemer, bør derfor omlægges, således at offentligt ansatte kun kan tilgå det minimum af persondata som er nødvendige i den konkrete situation, og således at al tilgang konsekvent logges. En sådan tilgang er i dag gældende bedste praksis for etablering af nye it-systemer, og det bør også være den fremtidige standard for offentlige danske it-systemer.

For at gennemføre et sådant skift, bør alle nye offentlige it-systemer fremover etableres efter principperne for *privacy by design*, og de eksisterende systemer bør, indtil de fornyes, opgraderes så de i størst muligt omfang lever op til tilsvarende krav.

På det tekniske niveau lever kombinationen af CPR-systemet og NemID på nuværende tidspunkt ikke op til princippet om at offentlige myndigheder kun kan tilgå persondata, som er relevante i forhold til en aktuel eller specifik situation.

Problemstillingen kan illustreres ved at der i en virtuel kontekst er brug for at vide, om en bestemt borger er berettiget til en bestemt ydelse eller befinder sig i et bestemt aldersinterval. Det kan for eksempel være relevant i forhold til anonyme rådgivningstilbud omkring sygdom, misbrug, eller

[9] OECD Better Life Index 2013 - http://www.oecdbetterlifeindex.org/topics/civic-engagement/. Resultater vedr. Danmark - http://www.oecdbetterlifeindex.org/countries/denmark/

[10] Rådet har tidligere beskrevet en mulig 4-trinsmodel for revision af CPR-systemet, se http://digitalsikkerhed.dk/nyheder/nyhederfraraadet/nyhed/article/220/. I høringssvar vedr. NemID har Rådet beskrevet hvorledes eID kan afløse det nuværence CPR-system, se http://digitalsikkerhed.dk/nyheder/nyhederfraraadet/nyhed/article/336/. Se også Rådets oplæg om digital tryghed til Retsudvalget: http://digitalsikkerhed.dk/nyheder/nyhederfraraadet/nyhed/article/357/

særlige sociale forhold – og det kan også være relevant i forhold til for eksempel donation af sæd/æg eller andet organisk materiale.

Aktuelt er der via NemID ikke mulighed for at besvare sådanne spørgsmål, uden at den som forespørger modtager flere oplysninger, end der er brug for i den givne situation. Hvis CPR-nummeret bliver involveret, kan spørgsmålene ikke besvares, uden at borgerens identitet bliver afdækket, herunder også borgerens præcise alder, køn og en mulig indikation af, om en person indvandret eller adopteret til Danmark[11].

Endvidere har myndigheder ifølge den nuværende lovgivning altid mulighed for at koble en NemID-forespørgsel sammen med CPR (selv om den teknisk godt kan gennemføres uden inddragelse af CPR-nummer)[12].

I erkendelse af at den digitale teknologi åbner for hidtil usete muligheder for at offentlige og private databehandlere unødigt kan få bred indsigt borgeres private forhold, er man i denne sammenhæng begyndt at tale om udvikling af nye digitale sikkerhedsmodeller. Sådanne nye modeller vil være centrale for den videre udvikling af digitalisering baseret på et fundament af tillid.

Et eksempel er, at en borger vil kunne acceptere at afgive sundhedsoplysninger til forskningsmæssige formål under forudsætning af, at disse oplysninger pseudonymiseres, og at det kun er borgeren selv, der har nøglen til at genetablere forbindelsen til sin identitet. I et sådant scenarie vil en forsker for eksempel kunne meddele – uden at vide til hvem – at der er fundet oplysninger om bestemte sygdomsrisici. Det vil så være op til borgeren selv at beslutte, om vedkommende ønsker disse oplysninger, og dermed via sin læge tilkendegive sin identitet.

Der blev i den nu nedlagte IT- og Telestyrelse taget hul på, hvorledes sådanne nye former for sikkerhedsløsninger kan etableres[13]. Dette arbejde bør videreføres, og indgå i udformningen af efterfølgeren til den nuværende NemID-løsning.

Behov for en stærk og robust national databeskyttelsesmyndighed

For at sikre grundlaget for sund digital vækst er det nødvendigt, at Danmark har en stærk og robust databeskyttelsesmyndighed. I takt med at de digitale teknologier udvikles, er der behov for at styrke beføjelser og kompetencer hos det nationale tilsyn[14].

For at sikre en solid basis for den foreslåede ambitiøse satsning på sund digital vækst, bør Danmark efter Rådets mening i fremtiden have en national databeskyttelsesmyndighed, som kan leve op til og også være med til at udforme fremtidens *best practice*, når det gælder national databeskyttelse.

---

[11] Oplysning om alder og køn er indlejret i CPR-nummeret. Cifrene 7-9 i CPR-nummeret fungerer som et løbenummer, der tildeles fortløbende, hvilket betyder at indvandrede og adopterede som hovedregel vil have højere løbenumre end børn født i Danmark. Kilde: Rådets kommunikation med IT og CPR under Økonomi- og Indenrigsministeriet samt "Besvarelse af de af Folketingets Kommunaludvalg den 29. februar 1996 stillede spørgsmål 16 og 17 (Alm.del – bilag 67)".

[12] En privat virksomhed som e-Boks laver også rutinemæssigt kobling mellem NemID og CPR, idet alle brugere ved hver login bliver anmodet om tilladelse til en sådan sammenkobling. Som bruger kan man ikke få adgang tjenesten, med mindre man accepterer dette.

[13] http://digitaliser.dk/resource/781482 og http://digitaliser.dk/resource/781482/artefact/Nye+digitale+sikkerhedsmodeller.pdf

[14] Jf. artikel 8 i EU's charter for grundlæggende rettigheder fra år 2000, som fastsætter at regler vedrørende personoplysninger skal underlægges en uafhængig myndigheds kontrol - http://www.europarl.europa.eu/charter/pdf/text_da.pdf

På nogle punkter lever den nuværende danske databeskyttelsesmyndighed, Datatilsynet, op til, hvad der kan betegnes som gældende bedste praksis inden for EU[15]. På andre punkter er der muligheder for forbedringer, og på et afgørende punkt – kravet om at databeskyttelsesmyndigheden skal være uafhængig – lever Danmark ikke op til gældende bedste praksis og dermed heller ikke til artikel 8 i EU's charter for grundlæggende rettigheder. Det skyldes, at Datatilsynet er placeret under det danske justitsministerium.

Rådet for Digital Sikkerhed mener, at Danmark snarest muligt bør have en opgraderet national databeskyttelsesmyndighed, og at den bør etableres efter gældende bedste praksis, således at den kan blive en af EU's bedst fungerende. Den skal være selvstændig og placeres under Folketinget, således at den uden tvivl lever op til EU's nationale charter for grundlæggende rettigheder. En sådan stærk og robust databeskyttelsesmyndighed skal være del af det samlede eksempel til efterfølgelse på, hvorledes en nation kan skabe gode rammebetingelser for sund digital vækst.

Danmarks fremtidige databeskyttelsesmyndighed bør ikke være begrænset til at udføre tilsyn men også bidrage til at vurdere, hvilke teknologier, designs og metoder, som kan anbefales til at understøtte god informationssikkerhed. Databeskyttelsesmyndigheden bør således både have et juridisk fokus, et betydeligt teknisk fokus, og det bør være en myndighed, som kan agere selvstændigt og have en aktiv rolle i forhold til at sikre en sund digital vækst og udvikling i Danmark inden for både den offentlige og private sektor.

Gældende bedste praksis for nationale databeskyttelsesmyndigheder findes allerede kortlagt inden for EU[16] og kan tjene som inspiration for en opgradering af den danske indsats på området. Derudover vil Rådet pege på, at der kan indhentes værdifulde erfaringer og viden fra det norske Datatilsynet[17] og fra Canadas *Office of the Privacy Commissioner*[18], to myndigheder som internationalt set er blandt de førende på området.

Leverandørkrav om informationssikkerhed og kontrol

Som nævnt har der de senere år været betydelige og alvorlige datatab fra den offentlige sektor, og der har også været brist i offentlige it-systemer, som har ført til meget store økonomiske tab. Der har dels været tale om fejl, der er blevet udnyttet, dels er eksisterende sikkerhedsløsninger blev angrebet og kompromitteret. Der er tale om en generel problematik for hele den danske offentlige sektor, hvilket blandt kan ses ud af den dokumentation, som Rigsrevisionen har fremlagt vedrørende, hvad der må betegnes som mangelfulde grundlæggende it-sikkerhedsmæssige foranstaltninger hos de myndigheder, som er blevet undersøgt[19].

På baggrund af de forløb vi allerede har set, er det Rådets vurdering, at en fremadrettet udvikling af sund digital vækst i Danmark kræver, at det politisk prioriteres, at der i et helt andet omfang end hidtil sættes ind med krav og kontroller i forhold til leverandører af it-løsninger til det offentlige. Disse krav bør omfatte konkrete krav til informationssikkerhed, der dels omfatter robust it-

[15] Data Protection in the European Union: the role of National Data Protection Authorities (EU's Agentur for Grundlæggende Rettigheder, 2010) - http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf
[16] Ibid.
[17] http://www.datatilsynet.no/
[18] https://www.priv.gc.ca/index_e.asp
[19] Beretning til Statsrevisorerne om revisionen af statsregnskabet for 2012 (udg. November 2013) - http://www.rigsrevisionen.dk/media/1943109/rs-2012.pdf

sikkerhed,[20] dels effektiv privatlivsbeskyttelse, herunder brug af *privacy by design*-løsninger og gennemførelse af *privacy impact assessments* (PIA)[21] af løsninger før og efter ibrugtagning.

Den nationale databeskyttelsesmyndighed eller en anden myndighed skal have de fornødne ressourcer til at kontrollere, at kravene om informationssikkerhed faktisk efterleves.

Delelementer som understøtter Rådets anbefalinger

I forhold til anbefalingerne, som fremgår i starten af dette dokument, peger Rådet for Digital Sikkerhed yderligere på følgende delelementer, som værende nødvendige:

- Anvendelse af sikkerhedsstandarden ISO27000 over alt i den offentlige sektor.
- Obligatorisk brug af PIA (*privacy impact analysis*) ved alle offentlige it-projekter[22].
- Videreførelse af det arbejde med etablering af nye digitale sikkerhedsmodeller, som blev påbegyndt i den nu nedlagte IT- og Telestyrelse.
- Fastsættelse af retningslinjer og krav i forhold til PbD (*privacy by design*), og PET (*privacy enhancing technologies,* herunder *privacy by default*) i alle offentlige it-projekter.
- Ændring af CPR-systemet, så det element der benyttes til identifikation (aktuelt det 10-cifrede nummer) ikke indeholder personfølsomme oplysninger.
- Opgradering af den nuværende NemID-løsning på en måde som inddrager og imødekommer de indkomne høringssvar vedr. udformning af den danske eID-løsnings næste generation, herunder specielt at det sikres, at digitale transaktioner kan gennemføres, så kun de faktisk relevante data videregives.
- Fastsættelse af krav og normer for brug af *big data*, herunder aktiv og bred formidling af viden om hvilke værktøjer der kan benyttes til at pseudonymisere og anonymisere data for at sikre individer mod uønsket identifikation.
- Integrering af informationsbeskyttelse (it-sikkerhed og privatlivsbeskyttelse) på alle niveauer i uddannelsessystemet.

Om Rådet for Digital Sikkerhed

Med mere end 45 private og offentlige medlemsorganisationer arbejder Rådet for Digital Sikkerhed for at skabe fokus på tryg digitalisering. Vi bidrager med viden og analyser, som kan være med til at sætte retningen for fremtidens digitale velfærdssamfund. Rådet arbejder for at it-sikkerhed og privatlivsbeskyttelse bliver naturligt integreret i systemer og samfund. Rådet vil understøtte læring og sund adfærd i den digitale verden samt innovativ udnyttelse af teknologiens muligheder.

Yderligere information: www.digitalsikkerhed.dk

[20] Se IT Branchens forslag til Sikkerhed i Balance, november 2014, der kan anvendes til foranalyse af sikkerhedsbehovet før anvendelse af ISO 27001.

[21] Digitaliseringsstyrelsen har udarbejdet en vejledning til PIA i Danmark. Denne eller tilsvarende bør gøres obligatorisk, fremfor som nu blot at være en anbefaling, der i mange tilfælde ikke bliver fulgt - http://arkitekturguiden.digitaliser.dk/principper/best-practice/beskyt-privatlivet. Se også DI ITEKs anbefaling om brug af PIA, oktober 2014, http://di.dk/Virksomhed/Produktion/IT/Informations-sikkerhed%20og%20Privacy/Trusler%20og%20loesninger/Pages/DIsskabelonforPrivacyImpactAssessment.aspx

[22] Digitaliseringsstyrelsen har udarbejdet en vejledning til PIA i Danmark. Denne eller tilsvarende bør gøres obligatorisk, fremfor som nu blot at være en anbefaling, der i mange tilfælde ikke bliver fulgt - http://arkitekturguiden.digitaliser.dk/principper/best-practice/beskyt-privatlivet