Redegørelse om sundhedswearables og big data

DET ETISKE RÅD

Indhold

Redegørelse om sundhedswearables og big data

ISBN: 978-87-92915-21-4

Grafisk tilrettelægning og illustrationer:
Peter Waldorph

DET ETISKE RÅD

Forord

Denne redegørelse er udarbejdet af en arbejdsgruppe nedsat af Det Etiske Råd i juni 2017.

Rådet vil gerne takke følgende eksperter for at have stillet deres viden til rådighed i arbejdsgruppen:
Hanne Marie Motzfeldt, lektor ved JUR, Center for informations- og innovationsret, Københavns Universitet,
Lars Kai Hansen, Professor, sektionsleder ved Institut for Matematik og Computer Science, DTU,
Thomas Sonne Olesen, Partner, Lakeside A/S og
Thomas Hildebrandt, professor, datalogisk institut, Københavns Universitet

Fra Det Etiske Råd har følgende medlemmer deltaget i arbejdsgruppen: Poul Jaszczak, Henrik Gade Jensen, Bolette Marie Kjær Jørgensen, Henrik Nannestad Jørgensen og Jacob Giehm Mikkelsen. Gorm Greisen (indtil 31. december 2018) og Lise von Seelen var formænd for arbejdsgruppen.

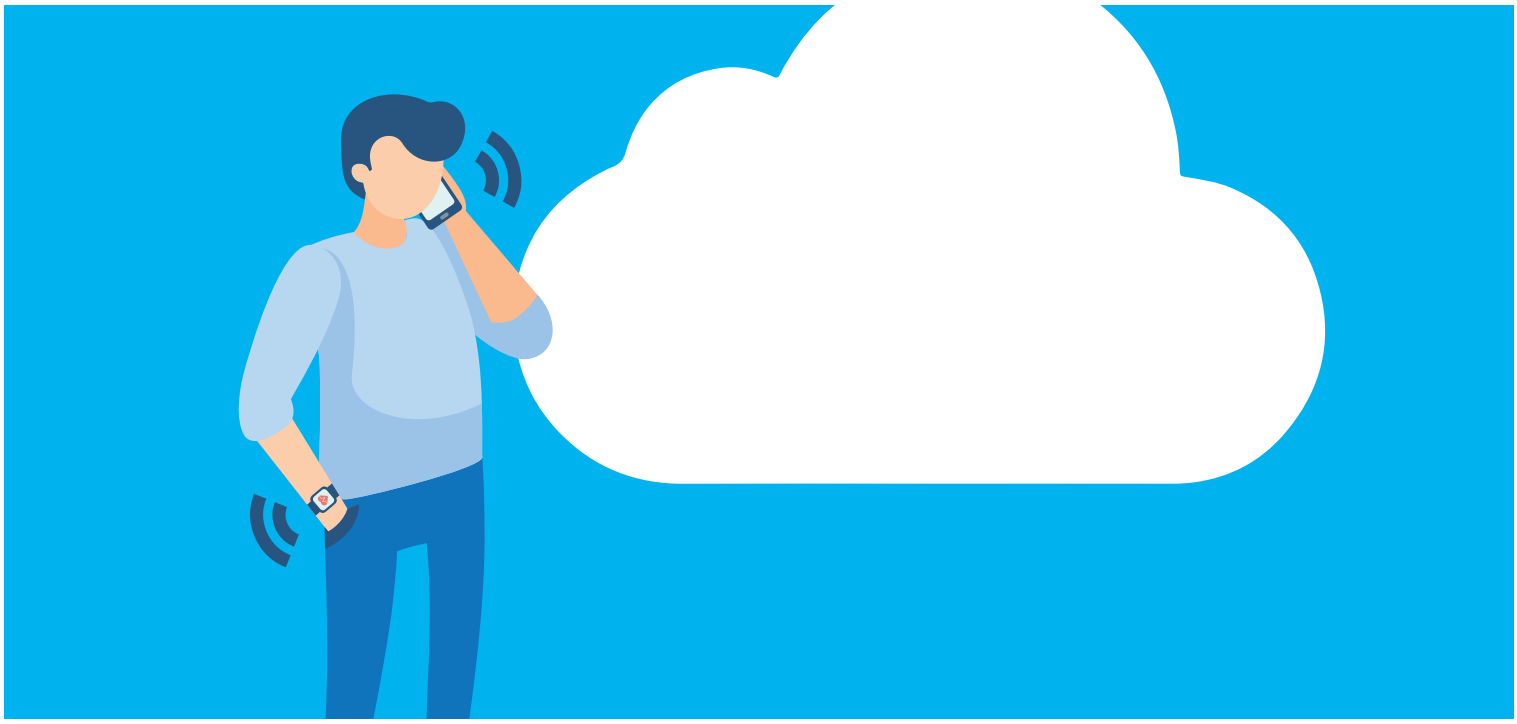
Rådet vil desuden takke følgende personer for at have bidraget med oplæg og viden undervejs i processen:
Stephan Engberg, ejer af Open Business Innovation, Sofie Green, stud.mag., Kaj Grønbæk, professor ved Institut for datalogi, Aarhus Universitet, Christian Damsgaard Jensen, lektor ved sektionen System Security ved DTU Informatik, Jens Winther Jensen, direktør for Regionernes Kliniske Kvalitetsudviklingsprogram, Klemens Kappel, professor i filosofi, Københavns Universitet, Gitte Kjeldsen og Marianne Jørgensen fra projekt Tværspor i Horsens, Jørgen Schøler Kristensen, Lægefaglig direktør, Hospitalsenheden Horsens, Johannes Kruse, stud. polyt., Henning Langberg, professor på KU og direktør for Copenhagen Health Tech Cluster, Henriette Langstrup, Lektor ved Afdeling for Sundhedstjenesteforskning, Københavns Universitet, Lisbeth Nielsen, direktør i Sundhedsdatastyrelsen, Carsten Obel, professor ved Århus Universitet, Kjeld Møller Pedersen, professor ved Institut for Virksomhedsledelse og Økonomi, Thomas Ploug, professor i anvendt etik ved Aalborg Universitet, Nanna Skovgaard, kontorchef i Sundheds- og Ældreministeriet, Tore Tennøe, direktør for Teknologirådet, Norge, Christoph Thuemmler, Professor of health, Edinburgh Napier University, Casper Wichmann, ThinkChina.dk Coordinator, Københavns Universitet.

Anne Lykkeskov har udarbejdet udtalelsen i rådets sekretariat, Ulla Hybel har udarbejdet kapitel 4 om de retlige rammer.

Udtalelsen er vedtaget på rådets møde august 2019.

Anne-Marie Gerdes
Formand for Det Etiske Råd

Christa Kjøller
Sekretariatschef



1. Hvorfor arbejde med wearables?

Wearables er redskaber til at opsamle de data, som er en væsentlig del af råstoffet i den *omstilling af sundhedsvæsenet*, som centrale aktører såvel i Danmark som internationalt er i gang med at iværksætte.

Overalt i den vestlige verden taler man i disse år om, at den nuværende model for sundhedsvæsenet ikke vil kunne finansieres om 20 år.[1] Fra 2000 til 2017 er de offentlige sundhedsudgifter i Danmark steget med 69% i faste priser, så de i 2016 udgjorde 9,8% af BNP.[2] Fremover vil vi leve længere, så befolkningerne bliver ældre. I Danmark vil andelen af ældre over 75 år fordobles de kommende 30 år, og selvom sundhedstilstanden hos de ældre er for opadgående, er der alligevel flere, som vil leve med de mest udbredte kroniske sygdomme.[3] Med uændret behandlingsregime vil dette betyde et øget pres mod sundhedsvæsenet.

Wearables er redskaber til indsamling af data om såvel brugerens adfærd (fx motion, søvn, spisevaner og psykisk velbefindende) som fysiologi (blodtryk, puls, stofskifte mm).
I det følgende bruges betegnelsen Wearables om alle devices, vi bærer på os, og som registrerer data om os. Mobiltelefoner, skridttællere og smartwatches er således eksempler på wearables.

---

1 Thuemmler, Christoph. 2017. The case for health 4.0. In Thuemmler, Christoph and Chunzue Bai eds *Health 4.0: How virtualization and big data are revolutionizing healthcare.* Springer.

2 Rasmussen N og L Kristensen. 2019. De offentlige sundhedsudgifter er steget markant mere end de øvrige offentlige udgifter siden 2000. *DST Analyse 2019.1.*

3 Sundheds- og ældreministeriet, Danske Regioner og KL. 2017. *Strategi for digital sundhed 2018 – 2022*. Danske Regioner. 2017. *Sundhed for alle - vision for et bæredygtigt sundhedsvæsen.*

Politisk ses digitaliseringen som en mulighed for at overgå til en mere proaktiv og effektiv organisering af sundhedsvæsenet. Det skal blandt andet muliggøres af udnyttelsen af de mange, detaljerede data om hver enkelt, det er blevet muligt at indsamle.

Disse data skal gøre det muligt at udvikle bedre behandlinger og decentralisere sundhedsvæsenet.

Der er mange definitioner af Big Data, og de fleste lægger vægt på den voksende teknologiske evne til at opsamle, opbevare og behandle den stadigt voksende mængde, hastighed og variation i data. Data er altså "Big" i to henseender: For det første mængden og variationen af tilgængelige data. For det andet omfanget af analyser (analytics), man kan anvende til at udlede informationer om fx personer, fra den samlede datamængde.

Mange taler om *et paradigmeskift i sundhedsvæsenet*, som baserer sig på Big Data. Betegnelsen bruges bredt om den overflod af data, det er blevet muligt at registrere og lagre fra en mængde kilder såsom sensorer og wearables, men også fra internet-aktivitet, sociale medier, GPS-sporing, e-mails og alle de ting, som er koblet op på nettet, og som indsamler data.

Når alle disse ustrukturerede data kan få værdi, er det bla fordi, man er i gang med at udvikle kunstigt intelligente systemer, som kan behandle mængder af data og finde mønstre, som kan generere en mængde ny viden. I sundhedsvæsenet er forhåbningen, at de digitale data kan kombineres med registerdata, herunder genetiske data, og være med til at give et mere samlet billede af sygdomme og generere kvalitativt nye behandlinger. Mangefacetterede data om hver enkelt skal gøre det muligt at individualisere behandlingen og vælge den, som vil virke bedst på den enkelte patient. Nytten af data stiger med mængden, for når genetiske data kan kobles med som minimum andre sundhedsdata, men også gerne data om adfærd og sociale forhold, bliver det muligt at få detaljeret viden om hver enkelt, som gør, at man muligvis vil kunne behandle sygdomme bedre og mere effektivt.[4]

Når man ligefrem taler om et paradigmeskift i sundhedsvæsenet, skyldes det, at man forventer, at den nye viden vil muliggøre en omstilling fra at behandle sygdomme, når de er opstået, til at holde os raske længere ved at opdage tegn på sygdomme tidligt og forebygge dem, før de opstår. Bliver borgerne alligevel syge, kan de i højere grad behandles i eget hjem med hjælp fra praksissektoren, kommunerne og private aktører.[5] De kan selv tage aktivt del i behandlingen, og også her skal data fra de mange sundhedswearables, som også danskerne anvender, spille en væsentlig rolle.

4 Højgaard, B. og J. Kjellberg. 2017. *Fem megatrends der udfordrer fremtidens sundhedsvæsen*. KORA.

5 Ibid.

De vil gøre det muligt for borgeren at registrere forskellige data af betydning for vedkommendes sygdom og sende dem digitalt til behandlerne, som kan tage kontakt, hvis tallene udvikler sig i forkert retning. Mange behandlinger vil også kunne foretages vha telemedicin.[6]

Dilemmaet

Wearables og de data, de indsamler, ser altså ud til at komme til at spille en positiv og nødvendig rolle, såvel i forhold en påkrævet omstilling af sundhedsvæsenet, som i bedre forebyggelse og behandling af den enkelte patient. Målet er altså at opnå større livskvalitet for borgerne samtidig med en bedre samfundsøkonomi.

De store mængder personfølsomme data, som genereres, vil dog også kunne anvendes på måder, som vil kunne begrænse borgernes grundlæggende frihed og selvbestemmelse. Det er altså vigtigt at sikre transparens om brugen af data allerede i den indledende fase, og at lovgiverne forholder sig til, hvordan området skal reguleres, så der tages højde for de omfattende etiske problemer, udviklingen også kan føre til. Dette dilemma er emnet for den følgende rapport.

1.1 Fordele ved brug af data fra wearables i sundhedsvæsenet

1.1.1 Udvikle ny forståelse af sygdom og nye behandlinger

Som nævnt kan de mange data anvendes til forskning i sygdomme og udvikling af nye behandlinger, som vil komme alle patienter til gode. Her er tale om brug af data på populationsniveau, hvor formålet med databehandlingen er at finde generelle tendenser og mønstre, som kan forklare, hvordan sygdomme opstår, og hvad der får dem til at udvikle sig mhp at designe mere effektive behandlinger. Her indgår data om enkeltpersoner i en samlet vidensbase, men fokus er ikke på den enkelte person. Man arbejder derfor på at designe systemer, som kan sikre de enkelte deltageres anonymitet og nedbringe risikoen for de-anonymisering af deltagerne i databaserne. Forskningsprojekter skal følge gældende regler for registerforskning.

1.1.2 Udvikling af persontilrettede behandlinger

Den bedre forståelse af sygdomme på det overordnede niveau følges af en øget forståelse for betydningen af den enkelte patients individuelle biologi og fysiologi i forhold til at udvikle sygdomme. Der forskes meget i genetikkens betydning for sygdomsudvikling, og hvorfor fx forskellige genvarianter kan føre til brystkræft for nogle, mens de samme genvarianter ikke nødvendigvis udvikler sig til brystkræft hos andre.[7]

Men genetikken giver kun en del af forklaringen på, hvorfor en person bliver syg, og hvilken medicin der vil virke bedst på netop den person. Man ved stadig kun lidt om sammenhængene, men blandt mange andre faktorer har det fysiske og sociale

6 Sundheds- og ældreministeriet et al. 2017.

7 Sundheds- og ældreministeriet og Danske regioner. 2017. *Personlig Medicin til gavn for patienterne – Klar diagnose, Målrettet behandling, Styrket forskning.*

miljø, personen lever i, stor betydning, og det samme har personens adfærd: hvor meget man motionerer, hvilke fødevarer man spiser – og hvor mange – hvor meget man sidder stille, hvor meget og hvor godt man sover osv Mange af disse faktorer kan måles med wearables, ligesom nogle wearables også måler fysiologiske data som puls, hjerne- eller hjerteaktivitet, stoffer i blodet osv. Desuden anvender nogle brugere apps til at indtaste data, som kan betegnes som ekstra følsomme, såsom psykisk velbefindende. Når alle disse data kombineres med traditionelle sundhedsdata, kan de bidrage med væsentlige brikker i et detaljeret billede af patienten, og dermed være med til at muliggøre en personrettet behandling af hver enkelt.

Her er altså tale om data, som ikke skal anonymiseres, fordi det har betydning, at man kan koble dem til den enkelte person. Det er derfor særdeles vigtigt, at data behandles fortroligt, og sundhedsvæsenet har opbygget omfattende systemer til at sikre mod, at uvedkommende får adgang til patienternes data. I det omfang, sundhedsvæsenet selv får udviklet de apps, de opfordrer patienterne til at anvende til at opsamle data til brug for deres behandling, vil de være forpligtet til at sikre disse data på samme måde.

Her er dog en udfordring, for ofte vil det offentlige sundhedssystem hverken have kompetencer eller ressourcer til at udvikle en relevant app til alle de målinger, de har behov for i forhold til at behandle en patient. Det kan derfor være oplagt for en behandler at anbefale sin patient at anvende en kommercielt udviklet app, som vedkommende ved, kan måle de ønskede data. I det tilfælde vil de data, patienten registrerer, altså blive lagret – ikke på sundhedsvæsenets sikrede platform (hvor der også sker fejl, men hvor intentionen er at give patienten mest mulig kontrol over sine data), men derimod på app-udbyderens server. Som oftest vil patienten ved download af app'en blive afkrævet et samtykke til, at udbyderen kan anvende vedkommendes data til viderebearbejdning, samkøring og salg. Det vil altså sige, at disse data ikke er beskyttet i henhold til sundhedsvæsenet standarder. Dette vil vi komme tilbage til.

1.1.3 Målrettet tidlig opsporing og den forebyggende indsats

Et vigtigt element i gentænkningen af sundhedssektoren er som nævnt satsning på forebyggelse og tidlig opsporing af tegn på sygdom.[8] Potentielt giver anvendelsen af data mulighed for mere effektiv forebyggelse, end man hidtil har været i stand til.

For personer, som allerede er i kontakt med sundhedsvæsenet, kan løbende dataindsamling og monitorering vise tidlige tegn på sygdomsudbrud, og muliggøre tidlig indgriben ved tegn på forværring af tilstanden. Der arbejdes fx en del på at frembringe algoritmer, som kan forudse, hvilke patienter som efter afsluttet behandling er i risiko for forværring og akut genindlæggelse.

8 For en yderligere behandling af dilemmaet om henvendelser vedr forebyggelse af sygdom, se Det Etiske Råds udtalelse om Tidlig opsporing af sygdom fra 2019: http://www.etiskraad.dk/~/media/Etisk-Raad/Etiske-Temaer/Forebyggelse/Publikationer/DER_udtalelse_Tidlig_opsporing_af_sygdom_2019.pdf

Nogle er dog skeptiske overfor bestræbelserne, fordi meget tyder på, at årsagerne til genindlæggelse ikke så meget skyldes medicinske forhold, som de skyldes patienternes sociale vilkår.[9] Et amerikansk studie fandt, at patienter, som boede i meget fattige områder, havde 24% højere risiko for at blive genindlagt end andre sammenlignelige patienter.[10] Andre studier peger på, at faktorer som alder, køn og race også har betydning for genindlæggelse. Desuden har gifte patienter i alle studier en reduceret risiko for at blive akut genindlagt.[11]

Med Big Data er det muligt at fremstille programmer, som kan tage højde for de mange – også ikke-medicinske – faktorer, som spiller ind i forhold til en persons helbredstilstand. Det kan man gøre ved at inddrage data fra flere forskellige myndigheder og dermed få et mere omfattende billede af personen.

Således kører der på Hospitalsenheden Horsens et forskningsprojekt, "Tværspor", som skal undersøge, om dataanalyse kan bruges til at forudsige, hvilke patienter der vil blive indlagt akut inden for det næste år. Her indsamles data om de enkelte borgere på tværs af de fire kommuner i Horsens-klyngen, områdets praktiserende læger og hospital. Man håber, at projektet vil resulterer i en afprøvet model for vurdering af den enkelte patients risikoprofil og for tilbud om en tværsektoriel indsats, der kan udbredes til flere klynger.[12]

Man ser også på andre områder bestræbelser på at anvende data til at forudsige hændelser. Eksempler er såkaldt *predictive policing* , hvor politiet anvender algoritmer til at forudse, hvor det er sandsynligt, at forbrydelser vil blive begået, og hvem der kunne tænkes at ville begå dem.[13] På det sociale område har Gladsaxe kommune herhjemme foreslået en model til at finde frem til udsatte børn ved at sammenkøre data fra bla sundhedsplejen, tandplejen, dagtilbud og Jobcentret.[14] I begge tilfældet er målet, at myndighederne skal kunne henvende sig til de borgere, som identificeres som værende i risikogruppen, mhp at forebygge hhv kriminalitet og svigt af børn.

Men i princippet vil data fra endnu flere områder kunne øge muligheden for at lave præcise forudsigelser. En række private firmaer opsamler privatpersoners sundhedsdata fra fx motionsapps, og kombinerer dem med data fra en lang række andre digitale kilder. Det kan de gøre, fordi de kan følge enkeltpersoner på tværs af forskellige tjenester, platforme og devices på nettet ud fra vedkommendes identiteter

---

9 Chen et al. 2017. Machine learning and prediction in medicine, beyond the peak of inflated expectations. *New England jounal of medicine*. 376;26.

10 Hu et al. 2014. Socioeconomic status and readmissions: Evidence from an urban teaching hospital. *Health Affairs* vol. 33, no. 5: 778–785.

11 Nagpal, M. and R. Samavi. 2016. *Using big data & analytics to predict hospital re-admissions*. Working Paper # 56. Hamilton: McMaster eBusiness Research Centre.

12 Region Midt news. 2017. *Ny viden om patientadfærd skal gøre sundhedsvæsenet mere proaktivt* http://www.rm.dk/om-os/aktuelt/nyheder/nyheder-2017/april-17/ny-viden-om-patientadfard-skal-gore-sundhedsvasenet-mere-proaktivt/ (tilgået 1. juli 2019).

13 Se fx Shapiro, Aaron. 2017. Reform predictive policing. Comment. *Nature* Vol. 541, 26 January.

14 Gladsaxe commune. UÅ. *Strategi for Tidlig indsats 2016-19. Familier der lykkes.*

fra email-adresser, telefonnumre, ID'er fra smartphones, computere og brugerkonti.[15] Montgomery et al (2018) beskriver, hvordan amerikanske firmaer fx anvender store datamængder om individer fra en lang række online og offline kilder til at udlede, om de har bestemte sygdomme eller er i risiko for at udvikle dem. Det kan de fx gøre ved at sammenligne de opsamlede data fra en person med adfærden hos mennesker med bestemte sygdomme. Hvis de finder ligheder, vil de udlede, at personen også er i risiko for at udvikle disse sygdomme.[16]

1.2 Udfordringer ved brug af wearables

De store fordele, som kan høstes ved brug af Big data på sundhedsområdet, følges imidlertid af nogle ulemper, som ikke umiddelbart er synlige, fordi de langt hen ad vejen foregår uden vores vidende. Men de fleste er enige om, at problemerne med beskyttelse af de omfattende mængder personfølsomme data er store og til dels uløste. Det skyldes ikke mindst, at en stor del af sundhedsdata opsamles af apps udviklet af private firmaer, som har et andet formål med opsamlingen, end sundhedsvæsenet, nemlig at opsamle data om personen, som kan sælges for at dække firmaets udgifter til at fremstille app'en. Dette har betydning for, hvilke spilleregler der gælder for omgangen med og anvendelse af data.

Der arbejdes fra mange sider på at designe systemer, som kan sikre privatpersoner ejerskab over deres egne data og kontrol over, hvem der anvender dem. Det er dog ikke i dag muligt at sikre dette i alle situationer, som det fremgår af bilag 2 til denne redegørelse: "På nuværende tidspunkt har vi ikke kendskab til et system eller et teknisk redskab, der kan forhindre, at privatpersoners data opsamles, identificeres og kombineres med henblik på profilering, hvis ikke servicen selv har implementeret det i deres system. Privatpersoners privacy kan ikke sikres, når først en service har dine data. Det er derfor vigtigt at brugeren undersøger og gør sig overvejelser om, hvilken sikkerhedsgaranti og tekniske redskaber en elektronisk service tilbyder."[17]

1.2.1 Personprofilering og handel med personfølsomme data

Som allerede nævnt lagres de sundhedsrelaterede data om fx motions-, kost- og søvnvaner, man fx opsamler med sin mobiltelefon eller en anden wearable, ikke på mobil, fitness-ur osv. I stedet bliver de indsamlet og gemt på serveren hos den producent, som har solgt eller fremstillet ens device. Man kan sige, at man ejer mobilen men ikke de data, som ligger på den, dem kontrollerer ejeren af serveren, og ofte har firmaet sikret sig vidtgående ret til at bearbejde data og sælge dem videre.[18]

---

15 Christl, Wolfie. 2017. *Corporate Surveillance in everyday life - How Companies Collect, Combine, Analyze, Trade, and Use Personal Data on Billions*. Vienna: Cracked Labs, p 9.

16 Montgomery, K. Chester J and Kopp, K. 2018. Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment. *Journal of Information Policy*, Vol. 8:. 34-77.

17 Se bilag 2: Kruse, Johannes & Lars Kai Hansen. 2018. *Privacy-by-Design - Teknisk Notat.*

18 Piwek et al. 2016. The Rise of Consumer Health Wearables: Promises and Barriers. *PLoS Med* 13(2), 4.

Hvor og hvordan opsamles data?

Firmaer får deres betaling gennem salg af data som opsamles fra wearables, mobiltelefon-apps (som enten selv registrerer – eller brugeren indtaster – data om kost, motion, søvn, tanker, bevægelser (gps)), computere (sociale media posts, søgninger, browserhistorie, mails, internethandel, hastighed af tastning, ordvalg), dankortkøb, elforbrug, data fra the internet of things (biler, tv, køleskabe osv) mmm.

Vi trykker accept, accept, accept...

Firmaer lokaliserer personers identiteter via e-mailadresser, telefonnumre, ID'er fra smartphones, computere og brugerkonti, og følger dem på tværs af forskellige tjenester, platforme og devices.

Når det kan lade sig gøre, skyldes det systemet med elektroniske ***tilsagn***, som de fleste brugere rutinemæssigt afgiver, når de fx downloader en motionsapp. Persondataforordningen opstiller ganske vist beskyttelser i form af krav til udformningen af de betingelser, som accepteres, men reelt er det en forsvindende lille del af forbrugerne, som overhovedet læser betingelserne, før de giver deres tilsagn. En årsag til, at alle rutinemæssigt giver tilsagn, angives ofte at være de lange, juridiske tekster, som er svære at forstå og tidskrævende at læse. I USA, som ikke er omfattet af forordningen, har forskere beregnet, at hvis en typisk amerikansk internetbruger faktisk ville læse alle de aftaler ord for ord, som de indgår ved at trykke accept, skulle de bruge 244 timer om året eller 40 minutter om dagen på det.[19]

Men selvom teksterne gøres kortere og mere pædagogiske, tilbagestår det forhold, at de færreste gør sig klart, hvor omfattende tilsagn de afgiver, og hvad deres data faktisk kan anvendes til. Man kan sige, at belønningen ved at acceptere er meget håndgribelig og øjeblikkelig – man får adgang til en app eller et program, som man står og mangler her og nu. Ulempen ligger ude i fremtiden og er for de færreste konkret nok til, at de kan forholde sig til den.

Det er for de fleste uklart, hvor omfattende tilsagn de afgiver, fordi de ikke har indsigt i, hvordan forskellige firmaer anvender deres umiddelbart set uskyldige data. Men det er kombinationen af mange i sig selv ubetydelige data, som giver mulighed for at udlede omfattende personlige oplysninger om personer. Fx angiver konsulentfirmaet McKinsey, at de arbejder med at forudse akutte indlæggelser ved at analysere data om personer på denne måde:

> *I et projekt udført for en stor, amerikansk kunde anvendte vi data om demografi, familie struktur, forbrug (fx indkøbsvaner, bil-ejerskab osv) til at konstruere et social isolations-index (en variabel konstrueret for at måle hvert individs grad af sociale forbindelser) for en målgruppe. Når dette blev kombineret med data om skadesanmeldelser, kunne index'et anvendes til mere præcist at forudse, hvilke personer indenfor grupper med kroniske sygdomme som mest sandsynligt ville opsøge omkostningstunge akut-modtagelser eller blive indlagt på hospital.*[20]

Når man køber en bil eller en vare på nettet, så er det formentlig uklart for de fleste, at man samtidig har givet samtykke til, at ens personlige oplysninger kan samkøres med det formål at forudse ens risiko for akut indlæggelse. Eksemplet er fra USA, i Europa ville nogle af disse data ikke kunne bruges i de nye sammenhænge uden fornyet samtykke fra de registrerede, men det viser teknologiens mulighed for at sammenkøre personlige data, fremstille personprofiler og konstant monitorere enkeltpersoners færden på en måde, der nærmer sig egentlig overvågning.

---

19 McDonald et al. 2008. The Cost of Reading Privacy Policies. *A Journal of Law and Policy for the Information Society*. Vol. 4, no 3, p 560.

20 McKinsey's Healthcare Systems and Services Practice. 2012. Changing patient behavior: the next frontier in healthcare value, p 68. Tilgængelig på: http://healthcare.mckinsey.com/sites/default/files/791750_Changing_Patient_Behavior_the_Next_Frontier_in_Healthcare_Value.pdf (egen oversættelse). Tilgået 260919.

Når en app eller et internetprogram stilles gratis til rådighed, skyldes det, at udbyderen får sin betaling ved at få adgang til ens data. Disse data har en værdi for udbyderen, som vedkommende kan realisere på anden vis. Men præcis hvordan køb og salg af data foregår, og hvad det kan betyde på langt sigt, er nok meget uklart for de fleste.

Der er tale om en udvikling, som startede i internettets ungdom i 1990'erne. Her opstod den norm, at tjenester på nettet i reglen var gratis, og udbyderne af internettjenester fik i stedet deres indtjening ved at sælge annoncer. For at tiltrække annoncører, anvendte udbyderne de digitale data, de fik adgang til om deres brugere, til at kategorisere brugerne og opdele dem i livsstilsgrupper, så de kunne tilbyde annoncørerne at målrette deres markedsføring til præcis de forbrugere, som kunne være interesserede i deres produkt. Derved fik data om brugeren værdi for udbyderen, og brugeren kunne betale for tjenesten ved at give tilsagn om, at udbyderen til gengæld fik lov at bruge disse data kommercielt.

Brugen af data til at skræddersy annoncer til forbrugeren er et eksempel på en anvendelse af big data, som synes uproblematisk og endda som en fordel for forbrugeren. Med årene er indsamlingen og bearbejdningen af data om hver enkelt imidlertid vokset, og i dag foregår der en meget omfattende overvågning af vores digitale adfærd mhp at kunne lave meget omfattende personprofilering af hver enkelt bruger. For jo mere omfattende viden, udbydere har om en person, jo større værdi har den ved videresalg. Data får de fra de forskellige devices, websider og elektroniske apparater, som indsamler data om os. Alt det vi gør, både offline og online, sætter digitale spor – alle køb vi foretager med kreditkort, hver søgning vi foretager med søgemaskiner, alle bevægelser vi gør med telefonen i lommen, alle 'likes' vi giver.[21] Med digitaliseringen og det, man har kaldt *The Internet of Things* (IoT), er der kommet endnu flere datamaskiner, såsom ure, biler osv, som også registrerer og lagrer oplysninger om vores færden.[22]

Ved at lokalisere personers identiteter fra e-mailadresser, telefonnumre, ID'er fra smartphones, computere og brugerkonti, er det muligt at følge dem på tværs af forskellige tjenester, platforme og devices. Dermed kan de samle data om personen fra mange kilder, såsom fra sociale medier, wearables, sensorer, internet køb, e-mails, videoer, åbne offentlige registre,[23] forskellige selskabers kunderegistre mm. Informationerne samkøres og analyseres.[24]

1.2.2 Fra opsamling til profilering

De data, som opsamles på sundheds-wearables, kombineres altså, hos fx marketing-firmaer eller store internationale firmaer som Google, Facebook eller Amazon, med

21 Grassegger et al. 2017. The data that turned the world upside down. *Motherboard* 28. Januar.

22 Teknologirådet og Datatilsynet i Norge. 2017. *Personvern 2017: Persontilpasning og kunstig intelligens*, 10.

23 Datatilsynet nævner Statstidende, CVR, Bilbogen, Motorregistret o. lign. som eksempler på offentligt tilgængelige registre (se: https://www.datatilsynet.dk/emner/internet-og-apps/behandling-af-oplysninger-fra-offentligt-tilgaengelige-registre/). Tilgået 260919.

24 Executive Office of the President. 2014. *Big Data And Privacy: A Technological Perspective*, 28.

personlige informationer fra alle de andre digitale kilder.[25] I dag er der utroligt mange aktører, som køber og sælger data om personer, helt overvejende uden at personen selv er klar over, at deres data handles og behandles.[26]

Når data indsamlet om en person fra mange forskellige kilder kombineres, kan der udledes mønstre vha algoritmer, som analyserer sig frem til meget private data ud fra informationer, som, da de blev indsamlet, forekom at være ret trivielle. En videnskabelig komité nedsat af tidligere præsident Obama giver som eksempler, at en persons seksuelle præferencer kan udledes af deres indkøbsmønster, og at hastigheden af klik med computermusen kan afsløre, at en person er ved at udvikle Alzheimer's sygdom, før personen selv er klar over det.[27]

Man kan udlede disse private og personfølsomme oplysninger af data, fordi det har vist sig, at der skal forbavsende få informationer om en person til, før man kan give et vældigt præcist billede af personen. En meget anvendt model til at måle personlighed er den såkaldte fem-faktor model.[28] Ved at bedømme kun fem egenskaber: åbenhed, samvittighedsfuldhed, extroversion, samarbejdsvilje og følelsesmæssig stabilitet, kan modellen udlede, hvor personen er placeret på de fleste kendte karaktertræk.[29] Forskere har vist, at disse egenskaber kan udledes af vores digitale adfærd på mange måder. Fx har forskere fra Stanford University vist, hvordan ret basale digitale registreringer kan bruges til at lave en psykologisk profil og udlede en mængde personlige egenskaber, som folk vil betragte som private. De har fx lavet en model, som ud fra en persons Facebook-likes med ret stor sikkerhed kunne udlede personens seksuelle orientering, etnicitet, politiske synspunkter, religion, personlighed, intelligens, køn, alder, hvor mange venner personen har mm. Forskerne angiver desuden, at samme type oplysninger kan udledes af andre data som web-søgninger, browser-historie, kreditkortkøb mm.

De siger endda, at oplysninger, som folk vælger at holde for sig selv, som fx deres seksuelle orientering, kan afsløres ud fra de aspekter af deres liv, som de gerne afslører, fordi de virker uskyldige og ukontroversielle – som fx at de motionerer, hvad de spiser osv.[30] Sådanne bedømmelser af karaktertræk indgår også i personprofilerne.

---

25 Montgomery, K. Chester J and Kopp, K. 2018. Health Wearables: Ensuring Fairness, Preventing Discrimination, and Promoting Equity in an Emerging Internet-of-Things Environment. *Journal of Information Policy*, Vol. 8: 34-77.

26 Federal Trade Commission. 2014. *Data Brokers - A Call for Transparency and Accountability.*

27 Ibid.

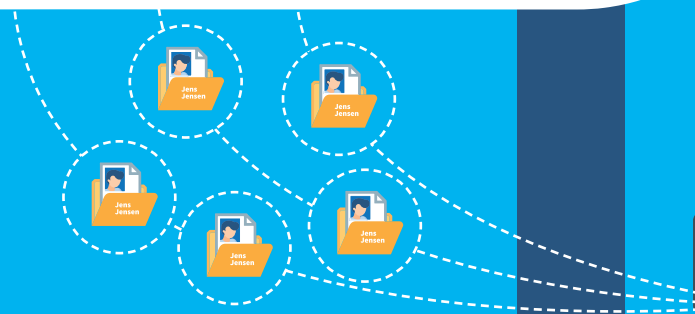
28 Goldberg, L. 1993. The structure of phenotypic personality traits. *American Psychology*, vol. 48, no. 1: 26–34.

29 Lambiotte BR, Kosinski M. 2014. Tracking the Digital Footprints of Personality. *Proceedings of the IEEE*. Vol. 102: 1934–1939.

30 Kosinski M, Stillwell D, Graepel T. 2013. Private traits and attributes are predictable from digital records of human behavior. *PNAS*: 110(15):5802–5).

PROFILERING INC.

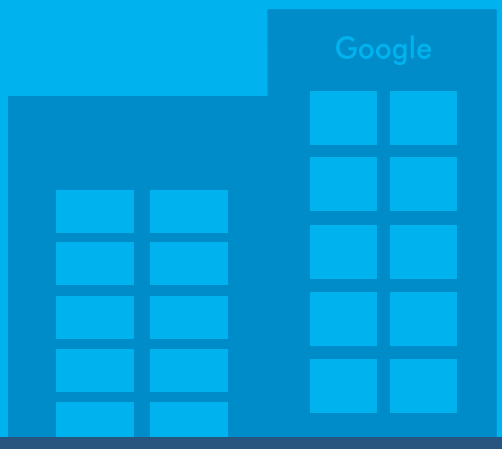
Der skal forbavsende få informationer til, før man kan give et vældigt præcist billede af en person. Kun fem egenskaber kan udlede, hvor personen er placeret på de fleste kendte karaktertræk (Fem-faktor modellen). Disse egenskaber kan udledes ud fra Facebook-likes, men også fra andre tilgængelige data som web-søgninger, browserhistorie, kreditkortkøb mm.



Ved hjælp af algoritmer udleder aktører personfølsomme oplysninger som:

- **Sygdomsdispositioner**
- **Seksuel orientering**
- **Etnicitet**
- **Politiske synspunkter**
- **Religion**
- **Personlighed**
- **Intelligens**
- **Køn**
- **Alder**
- **Antal venner**

mmm.



Mange aktører køber og sælger data om personer, helt overvejende uden at personen selv er klar over, at deres data handles og behandles.

Hvordan laves person-profiler og hvordan videregives og sælges de?

Der er allerede firmaer, som sælger data om folk, de har analyseret sig frem til har – eller er i risiko for at få – sygdomme.

Jens Jensen

Køn: Mand
Alder: 37 år
Status: Gift
Børn: 2
Uddannelse: Mellemlang
Beskæftigelse: Mekaniker
Etnicitet: Nordisk
Religion: Protestant (ikke udøvende)
Sexualpreference: Bisexuel
Interesser: Fodbold, bøger, biler
Sygdomme: Astma, tinitus, disposition for diabetes, depression.

1.2.2.1 Opsamlede data og fremanalyserede personinformationer
Man skal altså gøre sig klart, at de data, som florerer om en person på markedet, ikke bare er dem, vedkommende har registreret i sin fitness-app eller afgivet ved at søge på nettet. For disse førstehånds-data bearbejdes og bruges til at udlede andenhånds-'data' om vedkommende, som herefter sælges videre. I profileringen indgår altså data som er:

- Oplyste data: som er afgivet direkte af personen
- Observerede data: som er registreret ved at følge personens aktiviteter
- Udledte data: fremkommet ved at analysere forskellige data om personen og nå frem til antagelser eller forudsigelser om vedkommende.[31]

Kvaliteten af de data, som firmaer udleder fra andre data, afhænger naturligvis af mange forhold, herunder troværdigheden af de oprindelige data og kvaliteten af de algoritmer, som anvendes til at nå frem til de afledte data. Dette kommer vi tilbage til herunder.

1.2.2.2 Hvor havner data?
Oplysninger fra sundhedswearables spiller en vigtig rolle i fremstillingen af personprofiler, og sundhedstilstande og mulige sygdomsdispositioner er blandt de faktorer, mange firmaer analyserer sig frem til. Dette sker især i USA, hvor det er tilladt at annoncere for medicinske produkter.[32]

Firmaerne bruger altså algoritmer til at analysere data om personer, så de kan lave detaljerede profiler af dem. Nogle store firmaer angiver selv at have profileret hundreder af millioner af personer.[33] De kan så gruppere personerne i kategorier – det kunne fx være personer i risiko for at udvikle alzheimers – og sælge deres adresser til firmaer eller andre, der ønsker at henvende sig meget målrettet til denne gruppe.

Montgomery nævner, hvordan et marketingfirma, AdRx Media, tilbyder sine kunder at målrette deres annoncer mod kunder, som de har analyseret sig frem til har – eller er i risiko for at få – sygdomme som: *allergier, astma og luftvejssygdomme, kræft, influenza, diabetes, fordøjelsesproblemer, hjertesygdomme, mentale sygdomme, osteoporose, alvorlige hovedpiner og migræne, seksuelle sygdomme, søvnforstyrrelser, vægtproblemer og mere.*[34]

Det vil sige, at de samme redskaber, som folk bruger til at registrere deres motion, kost og kropsfunktioner, også vil gøre dem til mål for meget personrettede henvendelser fra kommercielle firmaer.[35] Men udover firmaer, som ønsker at anvende personprofilerne til markedsføring, kan en række andre aktører være interesserede i at få adgang til data om en persons sygdomme eller sygdomsdispositioner. I nogle

31 Christl 2017, 15.

32 Montgomery 2018.

33 Executive office of the president. 2014. *Big data, seizing opportunities, preserving values*, 44.

34 Montgomery 2018.

35 Ibid.

hænder vil data kunne anvendes til skade for ophavsmanden; det kunne fx være tilfældet, hvis arbejdsgivere, forsikringsselskaber, banker, realkreditinstitutioner osv fik adgang til data:

Forsikringsselskaberne er allerede igang med at overveje, hvordan data fra wearables kan indgå i beregning af individuelle kunders forsikringspræmier. Flere forsikringsselskaber, også i Skandinavien, giver allerede rabatter til kunder, som indvilger i at dele oplysninger om deres adfærd med selskabet. Herhjemme har Alka indtil april 2019 givet 25% rabat på bilforsikringer, hvis man installerede en boks, som bla måler, om man kører for hurtigt.[36] I Sverige giver forsikringsselskabet Moderna Forsäkring rabat til kunder, som indvilger i at anvende en app, der måler deres skridt. De kan få op til 15% rabat afhængigt af, hvor mange skridt de går dagligt.[37] I USA har forsikringsselskabet John Hancock annonceret, at det vil ophøre med at oprette traditionelle livsforsikringer og kun sælge interaktive policer, som måler den forsikredes fitness og helbred vha wearables og smartphones og giver belønninger til dem, der når bestemte fitness-mål.[38]

Forsikringsselskaber har historisk anvendt data om kunderne til at differentiere deres vilkår. Yngre mænd, som lige har fået kørekort, betaler således højere præmier end andre forsikringstagere, fordi de statistisk set har flere ulykker og derfor er dyrere for selskabet at forsikre. Folk, som bor i kvarterer med flere indbrud, betaler højere forsikringspræmier end dem, der statistisk set har en lavere risiko for indbrud. Kvinder får lavere pensionsudbetalinger end mænd, fordi tidligere generationer af kvinder statistisk set har levet længere end mænd osv.

Hvis man differentierer yderligere ned til individniveau, vil nogle kunder kunne få fordele af at dele deres adfærdsdata med forsikringsselskaberne. Mange vil også se det som en fordel at kunne gøre noget selv for at få mulighed for at kunne nedbringe sin præmie. Herhjemme rapporterede fagbladet 3F dog for nylig, hvordan forsikringsselskabet AP blandt andet anvendte data, de uden kundens vidende havde fået adgang til fra hendes løbeapp. Disse data anvendte de til delvis at frakende hendes pension.[39] Her bliver kunden stillet dårligere, fordi forsikringsselskabet fik disse data, men nogle vil argumentere for, at problemet her alene er, at selskabet har skaffet sig adgang til kundens data uden samtykke. Grundlæggende er det retfærdigt, at man belønnes for at gøre en indsats for at holde sig sund længst muligt – men at man samtidig også har frihed til at vælge ikke at leve maximalt sundt, og til gengæld accepterer at betale en højere forsikringspræmie for sit valg.

---

36 Se nærmere på Alkas hjemmeside: https://www.alka.dk/forsikringer/lp/farvel-boks

37 Moderna Försäkring. 2016. Nu kan vardagsmotion ge dig rabatt på din sjuk- och olycksfallsförsäkring. Pressemeddelelse udsendt 11. februar.

38 Barlyn, Suzanne. 2018. Strap on the Fitbit: John Hancock to sell only interactive life insurance. *Reuters news service* 19. September (https://www.reuters.com/article/us-manulife-financi-john-hancock-lifeins/strap-on-the-fitbit-john-hancock-to-sell-only-interactive-life-insurance-idUSKCN1LZ1WL). Tilgået 260919.

39 Overgaard, N. 2018. Pensionsselskab overvågede kvindes løbe-app. Fagbladet 3F. https://fagbladet3f.dk/artikel/pensionsselskab-overvaagede-kvindes-loebe-app (tilgået 130618).

Andre vil være skeptiske overfor muligheden for at bruge adfærdsdata til at opnå et godt helbred, fordi så mange faktorer spiller ind udover motion, og fordi mange, fx miljøfaktorer, ikke er nogle, individer bare kan ændre. Ud fra denne tankegang er det desuden uretfærdigt, hvis de, der i forvejen er stillet ringere pga et dårligt helbred, skal 'straffes' yderligere ved også at skulle betale en højere forsikringspræmie. Derfor bør man tilstræbe en model for forsikring, som er mere solidarisk og mindre baseret på opdeling af kunder efter detaljerede, individuelle risikoprofiler.

Uanset om man er positiv overfor muligheden for at bruge data til at leve sundere, så man kan forebygge sygdomme, og man ligeledes er positiv overfor at lade sund levevis påvirke forsikringspræmien, vil det være et problem, hvis de individuelle sundhedsprofiler, algoritmerne regner sig frem til, er behæftet med store usikkerheder. Grundlaget for at kunne påvirke ens helbred må naturligvis være solidt, for at det giver mening. På nuværende tidspunkt er der sjældent solide, videnskabelige data, som underbygger de datagenererede sygdomsfremskrivninger, og erfaringsgrundlaget er særdeles kort.

Hvor det gælder forsikringsselskabernes brug af genetiske tests til at forudsige arvelige sygdomme, er dette ikke tilladt i dag. Men såfremt big data også anvendes til at prædiktere, om kunder har øget risiko for at udvikle sygdom, vil forsikrings-selskaberne i princippet kunne anvende sådanne usikre datagenererede forudsigelser som grundlag for at differentiere præmierne.

Mange forsikringsselskaber undersøger altså muligheden for at kunne anvende Big data om deres kunder til at forudsige disses fremtidige sygdomme. Det sker dog, ifølge Wall Street Journal, med forsigtighed, fordi forsikringsområdet er underlagt mere striks regulering end marketingområdet. Herhjemme udviser Forsikring og Pension en forsigtig tilgang og afventer signaler fra brugerne.[40] Men Wall Street Journal beretter om adskillige firmaers forsøg med at anvende såkaldte "predictive modelling" systemer, som delvis baserer sig på data fra marketingfirmaer, og som har vist lovende resultater.[41] I Storbritanien tilbyder firmaet HelthyHealth at forudsige personers risiko for at udvikle over 800 sygdomme ud fra deres aktivitetsdata opsamlet af telefoner og wearables. De tilbyder også forsikringsselskaber og arbejdsgivere at lave helbredsvurderinger af deres kunder baseret på deres digitale data.[42]

Arbejdsgivere eller potentielle arbejdsgivere kan være interesserede i, om deres ansatte eller potentielle ansatte er sunde og raske, fysisk og mentalt. For arbejdstager kan det desuden være en fordel at undgå jobs, som vil medføre helbredsproblemer, fx vil det være uhensigtsmæssigt, hvis en bager har forhøjet risiko for melallergi. En

40 Forsikring og Pension hjemmeside. 2018. Vi vil gerne bruge jeres data – men ikke uden jeres accept. Se: https://www.forsikringogpension.dk/nyheder/fp-forsikringsbranchen-til-danskerne-vi-vil-gerne-bruge-jeres-data-men-ikke-uden-jeres-accept/. Tilgået 260919.

41 Scism, Leslie and Mark Maremont. 2010. Insurers Test Data Profiles to Identify Risky Clients. *Wall Street Journal*. Updated Nov. 19, 2010.

42 Se firmaets hjemmeside: https://www.healthyhealth.uk/ (tilgået 2. juli 2019).

fordel ved at reducere sygdomsrisiko for arbejdstager er bedre muligheder for at fastholde kompetente medarbejdere.

Nogle arbejdsgivere går aktivt ind i at monitorere medarbejderne, fx tilbyder *Falck Healthcare* programmer til at hjælpe arbejdsgivere til at lette adgangen til sundhed på arbejdspladsen og forebygge tab af erhvervsevne hos medarbejderne. De tilbyder at forsyne medarbejderne med appen Howdy, som registrerer sundhedsdata for at forebygge stress. Medarbejderen skal hver anden uge svare på fem spørgsmål, der kan afgøre, om vedkommende er på vej til at havne i stress eller mistrivsel. Er det tilfældet, kontaktes medarbejderen over telefonen af Falck Healthcares team af psykologer.[43] De data, som opsamles på app'en, opbevares på app-firmaets server.[44]

Personer som fx viser sig at leve usundt eller på anden måde risikobetonet, motionere for lidt eller stresse for meget, vil alt andet lige kunne opfattes som mindre attraktive ansatte end dem, der lever mere fornuftigt. Teknisk vil det også være muligt at anvende data om levevis; motion, kost og bredere sundhedsrelateret adfærd for at nå frem til forudsigelser om, hvem der har en forøget risiko for at blive syg i fremtiden. Den type forudsigelser vil kunne spille ind i forhold til, hvem af flere ansøgere som ansættes eller forfremmes, og hvem der står yderst ved en fyringsrunde

1.2.3 Kvaliteten af data og forudsigelser

Som nævnt indsamles big data på en række forskellige devices og fra en mængde kilder, lige fra systematiske indsamlinger i sundhedsvæsenet til mere tilfældige data opsamlet fra internetsøgninger eller digitale medier. Og ud fra algoritmer udledes yderligere data fra de første data. Det giver selvsagt en lang række fejlmuligheder på flere områder:

I sundhedsvæsenet kan der være en risiko i forhold til kvaliteten af data fra apps, især i det omfang, det offentlige ikke selv har mulighed for at fremstille dem. De fleste forestiller sig, at sundhedsvæsenet langt hen ad vejen må basere sig på apps udviklet af private firmaer. Her støder man dog på den udfordring, at hovedparten af dem ikke er godkendt til medicinsk brug; de er ikke standardiserede og der er store problemer med sikkerheden. Som SIRI kommissionen angiver, kan hvem som helst lave en app, og det er "svært for forbrugerne at gennemskue, hvem der har programmeret/finansieret app'en og hvilken viden om fx kost og motion, som app'en er baseret på."[45] Derfor foreslår de, at der udarbejdes en app-guide, som kan gøre det nemmere for både borgere og sundhedspersonale at finde frem til gode sundhedsapps. Dette i erkendelse af, at det vil være uoverskueligt for Danmark at udforme en egentlig certificering af apps, og at dette må foregå internationalt.

Andre har ligeledes peget på, at de fleste wearables i dag befinder sig i en gråzone i forhold til brugersikkerhed. De forskellige devices markedsføres med løfter om at

43 Falck Health care pressemeddelelse 18. marts 2018. Falck Healthcare siger howdy til stress-app.

44 Baagø, Helle. 2016. Selvmonitorering vinder frem på arbejdspladsen. *DJØF-bladet* no 13, august.

45 SIRI kommissionen. 2018. *Samlede anbefalinger.*

kunne forbedre brugens helbred eller fitness, men i hovedparten af tilfældene opgives ingen empiriske undersøgelser til at underbygge disse løfter.[46] Spørgsmål der kan stilles er, hvem der i sidste ende står inde for, at kvaliteten af de sundhedsdata, som borgeren selv medbringer, er tilstrækkelig høj, og hvem der har ansvaret i forbindelse med anvendelse af eksterne data?[47] En rapport fra EU-kommissionen peger på, at der kan være risici for patienten fra flere kilder; en defekt device, en forkert diagnose stillet af en sundhedsprofessionel på baggrund af unøjagtige data, en fejl fra en IT specialist eller en patient som ikke anvendte sit device korrekt eller sendte de forkerte data til sin læge osv.[48] Samlet set er der for en stor del af wearables mangel på evidens for intervention og problemer med såvel kvaliteten som validiteten af data.

Inddrager man brug af andenhånds-data, som ikke er opfanget direkte af sundhedsapps, men som er genereret vha algoritmer, så stiger usikkerhederne naturligvis betydeligt.

Bruger man data til at forudse fremtidige hændelser, fx en persons risiko for at blive syg, er de i sagens natur behæftet med store usikkerheder. De oprindelige indsamlede data kan være fejlagtige eller mangelfulde. Hvor det drejer sig om observerede data er en kilde til unøjagtighed, at man ikke har en kontekst med; fx kunne en ung mand lave mange søgninger på fitness, men deraf kan man ikke udlede, at han motionere – det kunne være at han blot lavede en skoleopgave om emnet. Men selv hvis de anvendte data er korrekte, vil forudsigelserne naturligvis ikke blive bedre, end de algoritmer, som blev anvendt til at nå frem til dem, og de berørte har sjældent indblik i, hvordan algoritmerne er udformet.

Der er altså stor risiko for at nå frem til et forkert eller mangelfuldt billede af personen, når det genereres på denne måde. Kosinski viser, hvordan en model baseret på facebook-likes kan forudse forskellige egenskaber ved en person med mellem 60% og 95% sikkerhed. Etnicitet kan således forudses med 95% sikkerhed, mens modellen kun rammer rigtigt i 67% af tilfældene, når den forudser, om personen tager stoffer.[49] Det vil altså sige, at selv hvor det drejer sig om at forudse etnicitet, vil modellen tage fejl i 5% af tilfældene. Skulle man lægge disse data til grund for behandling eller for at udregne forsikringspræmier, kan konsekvenserne for de 5% - 33%, hvor data forudsiges forkert, blive alvorlige. Hvis indsamlingen – og især samkøringen - af data sker uden personens viden, har vedkommende ikke mulighed for at opdage eventuelle fejl. Det norske Teknologirådet skriver om dette: *Hvis vi ikke vet hvem som samler inn opplysninger om oss kan vi heller ikke be om innsyn i hvilke opplysninger som samles inn. Vi får da heller ikke mulighet til å be om at opplysningene slettes, eller at uriktige opplysninger korrigeres.*[50]

---

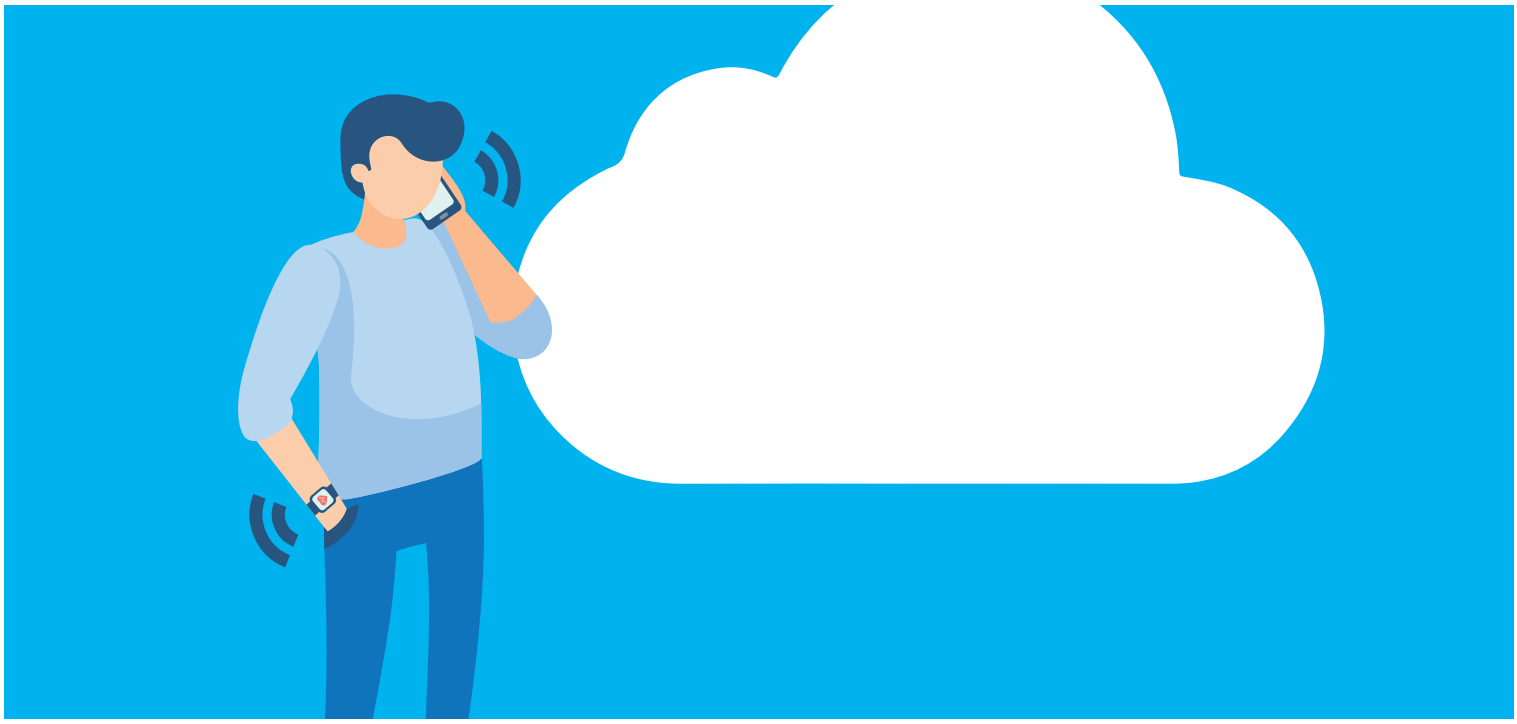
46 Piwek et al. 2016. The Rise of Consumer Health Wearables: Promises and Barriers. *PLoS Med* 13(2), Thuemmler 2017.

47 Mandag Morgen. 2017. *Sundhed i Skyen - Et kig ind i den digitale fremtid på sundhedsområdet.* Udarbejdet for Danske Regioner.

48 European Commission. 2014. *Green Paper on mobile Health ("mHealth").* COM(2014) 219.

49 Kosinski et al. 2013.

50 Teknologirådet og Datatilsynet i Norge. 2016, 53.



2. Etik: beskyttelse af privatliv og frihed

Som beskrevet ovenfor betyder disse års digitale udvikling, at store mængder af personfølsomme informationer opsamles eller udledes om hver enkelt borger. Og at disse data cirkulerer til en mængde forskellige aktører på måder, som i større eller mindre grad er udenfor den enkelte borgers vidende og kontrol.

Det har fået mange debattører til at hævde, at det, vi kender som 'privathed', ikke længere er muligt at opretholde. Den digitale udvikling gør, at vi er overvågede og gennemsigtige, og vi kan lige så godt vænne os til, at vi ikke længere har kontrol over, hvem der har adgang til personfølsomme oplysninger om os.

I det omfang, dette er rigtigt, kan det siges at være et opgør med noget, der normalt opfattes som et grundvilkår ved menneskelivet; at alle mennesker har en privat sfære, hvor de kan være sig selv på en anden måde, end de kan i den offentlige sfære. Der er nogle ting, de kan vælge at holde væk fra den offentlige sfære og kun dele med nogle få.

Men selvom det er den måde, vi er vant til, at tingene er, er det jo ikke sikkert, det vil være et etisk problem, hvis vi må opgive ideen om at have et privatliv? Om – og i givet fald hvorfor – det ville være et etisk problem at miste muligheden for privatliv, er temaet for dette afsnit. Vi diskuterer også, om det at have et privatliv har værdi i sig selv, eller om det især er værdifuldt som beskyttelse af noget mere grundlæggende: frihed til at leve det liv, vi ønsker at leve.

2.1 En ret til privatliv

I flere internationale traktater optræder beskyttelse af privatlivet som en grund-

læggende ret. Således nævner FNs menneskerettighedserklæring fra 1948 retten til ikke at udsættes for "vilkårlig indblanding i private forhold, familie, hjem eller korrespondance"[51], og EU's charter for grundlæggende rettigheder fra 2010 angiver at "Enhver har ret til respekt for sit privatliv og familieliv, sit hjem og sin kommunikation."[52]

Alligevel er det faktisk ikke spor klart, hvad en sådan ret præcis omfatter, eller hvordan den er begrundet. Antropologer har påvist, at mens alle kulturer har noget, der anses for at være privat, så varierer det mellem forskellige kulturer, *hvad* der præcis anses for at være privat.[53] Ser vi på vores kultur, er det ved nærmere eftertanke heller ikke entydigt, hvad der egentlig skal opfattes som privat og som noget, man kan holde ude af det offentlige rum. Hvis retten omfatter for lidt, kan fx alle vores sundhedsoplysninger lægges offentligt tilgængeligt på nettet. Men hvis retten omfatter for meget, kan den bruges til at retfærdiggøre vold og undertrykkelse indenfor hjemmets vægge, og nogens 'ret' til privatliv kan bruges til at undertrykke andres frihed til at leve deres liv, som de ønsker.

Så retten til privatliv er ikke absolut, og der foregår en livlig debat om, hvad den egentlig dækker, og hvordan man kan begrunde sådan en ret. På det seneste diskuteres det også, om det overhovedet – givet den teknologiske udvikling i disse år – fortsat giver mening at tro, at vi kan holde nogle oplysninger om os selv private, og om det egentlig ville være et problem, hvis muligheden for at have et privatliv forsvinder.

2.2 Hvorfor skal privatlivet beskyttes?

2.2.1 Frihed og tolerance

Et bud på, hvorfor privatlivet er værdifuldt i liberale demokratier, er, at det beskytter individers frihed og autonomi; deres muligheder for at vælge hvordan de ønsker at leve.[54]

Flere har argumenteret for, at det er en grundpille i samfund som vores, at individer har frihed til privat at kunne vælge at leve efter deres egne værdier og interesser i forhold til fx livsstil, religiøse eller ateistiske spørgsmål, seksuelle præferencer mmm. Den amerikanske filosof, John Rawls, har vundet stor tilslutning til sine teorier om, hvordan borgerne i liberale demokratiske samfund kan leve sammen, selvom de vedvarende er uenige i spørgsmålet om, hvordan og efter hvilke overbevisninger, man lever det gode liv. Hans svar var, at der må gælde forskellige regler på det politiske og på det private område. På det politiske niveau bør den fælles lovgivning kun basere sig på et begrænset sæt af politiske værdier: frihed og lighed sammen med adgang

51 FN. 1948. *Verdenserklæringen om Menneskerettighederne* artikel 12.

52 *Den Europæiske Unions Charter om Grundlæggende Rettigheder*, (2010/C 83/02), artikel 7.

53 Westin, Alan. 1984. The origins of modern claims to privacy. In Schoeman ed, *Philosophical dimensions of privacy: an anthology.*

54 DeCew, Judith. 2002. Privacy. *The Stanford Encyclopedia of Philosophy* (Spring 2015 Edition), Edward N. Zalta (ed.)

til basale fornødenheder. Netop fordi disse værdier er så overordnede, vil mange ideologier kunne acceptere dem og dermed acceptere lovgivning, som baserer sig på dem. Staten må til gengæld være neutral i forhold til forskellige religioner, ideologier og livsvalg, og give plads til, at borgerne privat har frihed til at leve på mange forskellige måder, bare de respekterer disse overordnede værdier.[55]

Den britiske filosof, John Stuart Mill, har ligeledes haft stor indflydelse med sine tanker om værdien af, at borgerne i et demokrati har størst mulig frihed til at leve deres liv på en måde, der er tro mod deres egen karakter. Han mener, denne frihed skal være meget omfattende og kun begrænses der, hvor en persons opførsel skader andre og deres mulighed for at leve, som de ønsker. At en person træffer valg, som er ufornuftige eller forkerte, er ikke i sig selv grund til at forbyde dem – tværtimod påpeger Mill, at samfund kun udvikler sig, hvis nogen udfordrer konventionerne og gør ting, som andre slet ikke kan se perspektivet i. Mange af de vigtigste opfindelser og fremskridt ville aldrig være sket, hvis ikke borgere havde frihed til at gå nye veje og udfordre vanetænkningen.[56]

Men hvis man skal kunne være fri til privat at leve på måder, som mange andre ikke billiger, er det nødvendigt, at man kan holde visse tanker og handlinger private, siger den amerikanske filosof, Thomas Nagel. Vi vil aldrig nå dertil, hvor intet af det, nogen gør, vil frastøde andre, og hvis alle ens tanker og handlinger blev synlige for enhver, ville der opstå evindelige konflikter. I mange år valgte homoseksuelle fx at holde deres seksualitet for sig selv, fordi de blev forfulgt og diskrimineret imod, hvis andre opdagede den, og der er stadig lande, hvor det kan være farligt at være erklæret homoseksuel (det er tankevækkende, at dette er en af de private oplysninger, firmaer som laver personprofiler rutinemæssigt 'afslører'). Nagel mener i det hele taget, at civilisation og samarbejde ville være umulig, hvis alle kunne læse hinandens tanker eller bralrede ud med deres holdning til andres valg eller værdier i alle mulige situationer.[57]

At kunne leve i overensstemmelse med ens egne ønsker til et godt liv forudsætter frihed – under ansvar - men for at kunne udnytte friheden, uden at andre løbende lader én vide, hvad de mener om ens valg og måske viser deres misbilligelse eller afstandtagen, har man brug for privatliv, påpeger den hollandske filosof, Beate Rössler. At blive kritiseret, eller diskrimineret er belastende, og derfor bør vi kunne trække os tilbage til den private sfære og kun indvi dem, vi deler præferencer med eller bare har tillid til vil være tolerante i forhold til, hvordan vi forvalter vores private liv. [58]

2.2.2 Kontrol over egne informationer

Retten til privatliv kan altså siges at have en væsentlig funktion ved, at den beskytter vores mulighed for at holde personlige informationer for os selv – eller til selv at

55 Rawls, John. 2005. *Political Liberalism*. Columbia classics in philosophy.

56 Mill, John Stuart. 1859. *On liberty*. 2012 edition, Simon & Brown.

57 Nagel, Thomas. 1998. Concealment and Exposure. *Philosophy and Public Affairs,* 27(1), 4.

58 Rössler, B. 2001. *The value of privacy.* Polity Press.

vælge, hvem vi vil dele dem med. Det kan være en beskyttelse mod misbilligelse fra dem, der ikke deler vores værdier. Men det kan også være, påpeger Nagel, fordi der er ting, vi ikke ønsker at dele med fremmede, selvom vi ikke frygter deres afstandtagen. Fx kunne en overvægtig person frabede sig at diskutere sin vægt med sine kolleger. Årsagen kunne måske være, at vedkommende satte stor pris på god mad og ønskede frihed til at vælge dette fremfor at tilstræbe et langt og sundt liv, men personen vidste, at nogle kolleger slet ikke ville kunne forstå den prioritering. Årsagen kunne dog også være mere følsom; måske skyldtes overvægten tvangsbetonet overspisning pga nogle barndomstraumer, som var smertefulde for personen at mindes. Her beskytter privathedskonventionerne vedkommendes ret til ikke at indvi sine kolleger i sine traumer, men kun at dele disse med sine nærmeste og måske med sin terapeut.

Dette er i overensstemmelse med den såkaldte *kontrolbaserede tilgang til privathed,* som har mange tilhængere. Som navnet siger, definerer tilgangen privathed som muligheden for at kontrollere, hvem der skal have adgang til hvilke informationer om en person. Det er vigtigt for os som autonome individer at kunne begrænse myndigheders, arbejdsgiveres, forsikringsselskabers m.fl.'s adgang til informationer om os. Der er naturligvis grænser for, hvad man kan erklære for at være private oplysninger: Det kan være problematisk at sige til sin læge, at vedkommende ikke må få at vide, hvordan man har det, eller til politiet eller sin ægtefælle, at man ikke vil fortælle, hvor man befandt sig en given aften. Men det kan man godt sige til en fjernere bekendt eller til sit forsikringsselskab.

Forskellen bunder naturligvis i de forskellige relationer, man har til disse personer eller instanser; en given information om én selv kommer kun andre ved, hvis man har en relation til dem, som berettiger dem til denne viden. Værdien af privathed ligger ifølge denne opfattelse i at kunne vælge (inden for lovens grænser), hvem der må få adgang til hvilke informationer om én selv. Hvor det gælder personlige informationer, vil man ofte vælge kun at dele dem med sine nærmeste; dem man har nære relationer til. Grunden til, at privathed er vigtig, er altså, at uden muligheden for at kunne vælge, hvem der må vide hvad om én selv, ville det slet ikke være muligt at opretholde forskellige relationer til forskellige mennesker og institutioner.[59]

2.2.3 Overvågning

Vi anvender hele tiden smartphones og andre wearables samt en mængde andre apparater, som efterhånden er koblet op på 'the internet of things'. Det, vi foretager os her, registreres – ofte fordi vi giver samtykke til det uden helt at vide, hvad samtykket omfatter. Informationerne bliver potentielt viderebearbejdet og videregivet i et omfang, vi ikke har indsigt i.

Beate Rössler sammenligner det med situationen i det berømte tankeeksperiment, Panopticon, som den britiske filosof, Jeremy Bentham, opstillede sent i det 18. århundrede. Bygningen var et fængsel designet sådan, at en vagt hele tiden var i stand til at overvåge alle indsatte, uden at de vidste præcist, hvornår de blev

59 Rachels, J. 1975. Why privacy is important. *Philosophy & Public Affairs*, Vol. 4, No. 4, 331. Fried, Charles. 1984. Privacy, a moral analysis. In Schoeman ed, *Philosophical dimensions of privacy: an anthology*, 205.

overvåget. Problemet med en sådan diffus mulighed for overvågning er, påpeger Rössler, at den vil få én til at ændre opførsel. Fordi andre muligvis kigger med, vil man begynde at opføre sig som om, man bliver iagttaget. Og man vil ikke længere være fri til at gøre de ting, som man ikke ønsker, at andre skal se. Fx tør man måske ikke google en sygdom, man frygter at have, af frygt for, at oplysningen vil blive brugt i en personprofil, som falder i de forkerte hænder. Tør man give sundhedsvæsenet adgang til ens app, som måler hvad man spiser, hvor meget man sover og om man føler sig deprimeret, hvis der er risiko for, at disse oplysninger deles med fx sociale myndigheder? På længere sigt er der risiko for, at friheden til under ansvar at leve efter sine egne værdier, undergraves.

2.3 Begrænsninger for frie valg

I det ovenstående er vi gået ud fra, at mennesker har frihed til at vælge deres handlinger. Dette er imidlertid ikke en så selvfølgelig antagelse, som man kunne tro, og filosoffer har diskuteret spørgsmålet om fri vilje i årtusinder uden at nå til enighed om andet, end at der er mange begrænsninger for, at mennesker kan vælge helt frit og uafhængigt af de omstændigheder, de er underlagt. Her skal vi ikke komme nærmere ind på disse diskussioner men nøjes med at konstatere, at der på sundhedsområdet er en del evidens for, at folks valg af livsstil og sundhedsrelateret adfærd ikke foregår i et tomrum, hvor de vælger fuldstændigt frit på alle hylder. De er derimod i stor udstrækning formet af personens omgivelser og sociale omstændigheder.

Empirisk kan man iagttage, at det ikke er en tilfældig mængde borgere jævnt fordelt i befolkningen, som vælger at leve efter forskernes og sundhedsmyndighedernes råd om, hvordan man lever sundt. Der er en påviselige social slagside i, hvem der lever sundt, og hvem der ikke gør. Usund levevis ser ud til at være mere udbredt i de mindst ressource- og købestærke socialgrupper, mens omvendt sund levevis er udbredt blandt de veluddannede og ressourcestærke. I begge grupper ser man, at valg af levevis 'går i arv' fra generation til generation.

Det ser altså ikke ud som om, vores adfærd på sundhedsområdet er et udslag af hver enkelts helt frie valg. Vi fødes jo trods alt ind i en familie og en kultur, som lærer os, hvad der er god og attraktiv mad, hvor meget man skal spise, og hvor meget man skal røre sig osv. Hver dag bekræftes man i den opfattelse, når man iagttager, hvad menneskene omkring én gør, hvad der udbydes i butikkerne dér hvor man bor osv. Usund levevis kan ligefrem være knyttet til vigtige fællesskaber, som kan gøre det uønsket at ændre adfærd, eller svært at gøre, selv hvis man ønsker det.

På samme måde opstår der subkulturer i mere ressourcestærke segmenter af befolkningen, som er velorienterede om de seneste kostråd, lægger cigaretterne på hylden og har abonnement i fitnesscenteret. På den måde, vil mange hævde, er man et produkt af sit miljø og ikke en person, som vælger frit blandt alle mulige måder at leve på. Det vil være en hel del lettere for en veluddannet, ressourcestærk person at forstå lægens anvisninger om omlægning af vedkommendes levevis og at rette

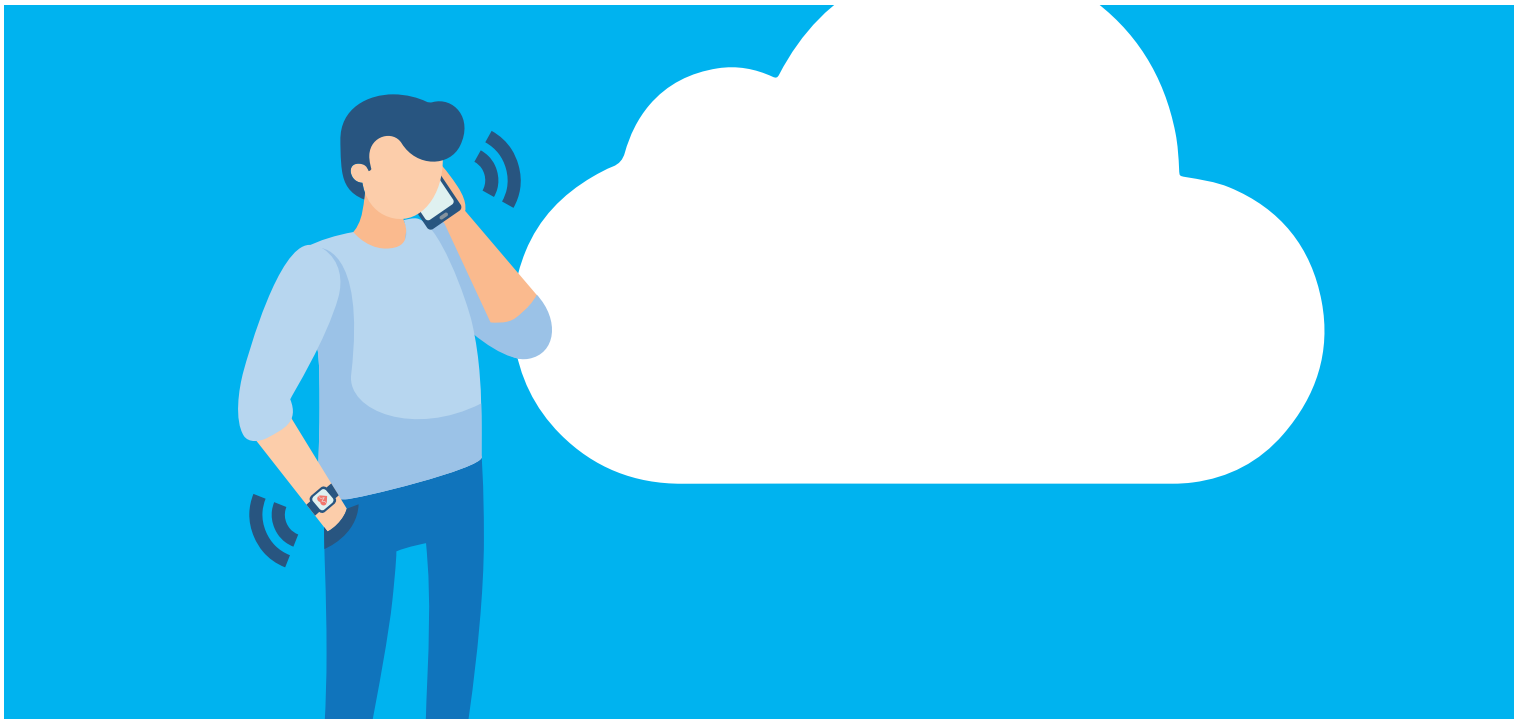
sig efter rådene, end det ville være for en person, som skulle bryde helt med sine egne og familiens kost- og motionsvaner, og måske bruge flere penge på sund mad, vedkommende slet ikke kunne lide. Derfor vil krav om sund levevis ramme socialt skævt.

2.4 Opsamling

Det fremføres stadigt oftere, især af folk i IT industrien, at vi allerede nu ikke har nogen privathed givet den digitale udvikling og massive generering af data. Der er ingen måde, hvorpå vi kan beskytte personlige data længere, så vi kan lige så godt vænne os til den nye realitet og lære at leve med den.

Hvis ovenstående argumenter er sande, vil det være etisk problematisk at anlægge en sådan strategi. Vi har argumenteret for, at respekten for privatlivet beskytter væsentlige værdier og er fundamental for såvel sammenhængen i demokratiske samfund som for relationer mellem personer og myndigheder og mellem personer indbyrdes.

Respekt for privatlivet har en vigtig funktion i at gøre det muligt for os at være fri til at leve efter vores egne ideer om det gode liv – og hvis vi betragter frihed som en væsentlig grundpille i liberale demokratier, er det fortsat vigtigt at værne om privatheden. Samtidig er det også vigtigt at være opmærksom på begrænsningerne for frie valg i forhold til de sociale omstændigheder, personer er underlagt.



3. Hvornår rejser brug af wearables etiske spørgsmål?

De forudgående afsnit lægger op til, at den væsentligste funktion ved privathed og muligheden for at beskytte private, personfølsomme oplysninger er, at man derved sikrer personers frihed. Der opstår etiske problemer, når adgang til private data om personer giver andre, især virksomheder og offentlige organisationer, mulighed for at gribe ind i vores liv efter forgodtbefindende.

I det følgende skal vi se på konkrete situationer, hvor spredning af personfølsomme data kan begrænse personers frihed, føre til uretfærdig forskelsbehandling eller til at svække det fælles sundhedsvæsen.

3.1 Forebyggelse og prioritering *inden for* sundhedsvæsenet

I strategien for et bedre og mere effektivt sundhedsvæsen baseret på digitale data er det et mål, at data skal kunne anvendes til at forebygge sygdom og optimere behandlingen af de allerede syge. Ved hjælp af wearables kan behandlerne løbende få adgang til data og følge med i personers sygdomsudvikling og adfærd. Patienten får også mulighed for at være mere med i behandlingen og blive inddraget i højere grad. Dermed håber man, det vil blive muligt at angive retningslinjer for, hvordan vedkommende kan leve for at mindske risikoen for at få en bestemt sygdom. Eller at øge sandsynligheden for at kunne tilbyde en mere virksom behandling, hvis personen allerede er syg. På længere sigt er visionen at kunne sammenkøre data fra forskellige myndigheder for at give et endnu mere præcist billede af borgerne – og måske kunne henvende sig til folk, som endnu ikke er syge, fordi data viser, at de er i risiko for at blive det.

Denne udvikling gør det nødvendigt på forhånd at diskutere nogle etiske dilemmaer, som kan opstå:

3.1.1 Uopfordrede henvendelser og retten til ikke-viden

For det første opstår spørgsmålet om, hvornår det er legitimt at henvende sig uopfordret til en borger med et budskab om, at vedkommende bør ændre sin levevis for evt at mindske risikoen for at udvikle en sygdom. Her er et dilemma, for der er nogle mennesker, som vil ønske at blive kontaktet, mens andre foretrækker ikke-viden om sådanne risici fremfor at skulle leve med bekymringer på forhånd. Måske foretrækker de at leve på deres måde, selvom det betyder, at de mister nogle leveår i sidste ende.

Dette dilemma vil også gøre sig gældende i situationen, hvor myndighederne vha data fra forskellige kilder opdager sygdomsrisici, som kan forebygges. Særligt hvis der er tale om resultater opnået ved samkørsel af data, som personen var uvidende om foregik, kan det være svært at vide, om personen vil være interesseret i en sådan henvendelse, eller om vedkommende vil anse den for at begrænse personens frihed til at leve, som vedkommende selv ønsker. Omvendt kan andre borgere finde, at en sådan henvendelse vil forøge deres frihed, fordi de får mulighed for at holde sig raske i længere tid, hvis de får en henvendelse med opfordring til forebyggende adfærdsændring. Meget vil derfor afhænge af, om det bliver muligt at finde måder at henvende sig til borgeren på, som tillader dem at vælge ikke at modtage informationen, hvis de ikke ønsker den.

3.1.2 Gode råd eller nedprioritering af de usunde

For det andet opstår spørgsmålet om, hvorvidt et godt råd om ændret levevis, som tilbydes patienten, risikere at gå over til at være et krav om at leve sundt.

De fleste anser sundhed for at være en væsentlig værdi i et godt menneskeliv; en sund person har alt andet lige større velvære, færre begrænsninger og flere leveår, end en syg person. Derfor har vi et sundhedsvæsen til at fremme sundhed, og til at promovere sund levevis. Det er imidlertid værd at huske, at ikke alle har sundhed som den væsentligste værdi for deres idé om det gode liv. Når mange ikke vælger en optimalt sund levevis, er det derfor ikke nødvendigvis fordi, de ikke har forstået de råd og vejledninger, som fx gives om kost, motion, alkoholindtag osv. For mange er der derimod tale om, at de prioriterer den fornøjelse, de har ved fx at spise god mad og hygge med venner og familie, højere end maximal sundhed og længst mulig levetid.

Man kan naturligvis hævde, at i et samfund, hvor man har et fælles sundhedssystem, som skal forvalte de fælles ressourcer bedst muligt, bør brugerne bestræbe sig på at leve sådan, at de belaster sundhedsvæsenet mindst muligt. Dette synspunkt ligger tæt op ad en idé om, at selvforskyldt sygdom enten ikke bør behandles eller bør prioriteres lavere i sundhedssystemet, fordi borgeren burde have undladt at bringe sig i en situation, hvor vedkommende blev syg. Eller med det synspunkt, at det er væsentligt at kunne træffe sine egne valg om sund eller usund levevis,

men at der med valget følger nogle omkostninger, som man skal være villig til at betale (tilhængere af denne position vil typisk gå ind for en højere grad af private sundhedsforsikringer).

Selvforskyldthed er imidlertid ikke et anvendt prioriteringskriterium i Danmark, hvilket formentlig har flere årsager. Dels vil et krav om at leve på bestemte måder for at undgå sygdom være i strid med idealet om størst mulig frihed til alle til at leve efter deres egne værdier. Et krav om at leve, så man ikke fremkalder sygdom, kan potentielt være meget omfattende: kan man bevæge sig ud i trafikken, hvis man skal leve efter det? Og hvor mange glas alkohol kan man helt nøjagtigt drikke om ugen? Det er i det hele taget ikke spor entydigt, hvilke sygdomme, som er selvforskyldte, og hvilke der ikke er. Forskningen viser, at stort set alle sygdomme har mange årsager, herunder det omgivende fysiske og sociale miljø, forurening, arbejdsforhold, gener og adfærd. Det giver derfor ofte ikke mening at tale om, at en sygdom er selvforskyldt, da man i det enkelt tilfælde aldrig kan vide, hvilke af disse faktorer, som har været afgørende. Fx kan man få lungekræft uden at ryge, og de fleste rygere får ikke lungekræft.

Et yderligere argument imod at anvende selvforskyldthed i prioriteringen er overvejelserne om solidaritet og den sociale skævhed i sundhed. Hvis sund levevis bliver et prioriteringskriterium i sundhedsvæsenet, vil det ramme socialt skævt, og det vil kunne forstærke den sociale ulighed i sundhed, som allerede eksisterer.

Det er derfor vigtigt at være opmærksom på, at henvendelser med gode råd om ændret levevis bør gives i respekt for borgerens frihed til at vælge rådet fra, fordi vedkommende prioriterer andre værdier end maximal sundhed højest.

Hertil kan dog indvendes, at selvom alle sygdomme ikke er selvforskyldte, så kan man ikke se bort fra, at usund adfærd spiller en rolle ved udviklingen af sygdom. I nogle tilfælde en markant rolle, som ved valg om at undlade at lade sig vaccinere eller tage sin medicin. I andre tilfælde en medvirkende rolle, som ved usunde spisevaner. Hvis usunde vaner er særligt hyppige i nogle befolkningsgrupper taler det i denne forståelse ikke for helt at undlade at tage selvforskyldthed i betragtning, men snarere for at en særlig indsats rettes mod de udsatte grupper, så deres risiko reduceres eller forsvinder.

I forlængelse af denne tilgang kan man desuden anse, at alle borgere i en velfærdsstat har en forpligtelse til at leve så sundt som muligt, så de belaster det fælles sundhedsvæsen mindst muligt. Det kan ses som uretfærdigt, hvis de, der lever sundt, skal være med til at finansiere behandlingen af dem, der ikke gør det.

3.2 Diskrimination og begrænsning af valgmuligheder *uden for* sundhedsvæsenet

Data har meget forskellig status i sundhedsvæsenet – hvor man traditionelt har været meget opmærksom på at beskytte følsomme oplysninger – og i IT-verdenen, hvor

personlige data er varer, som kan handles og får ekstra værdi ved at samkøres med andre data om os. I det omfang, sundhedsvæsenet vælger at anbefale kommercielle apps til patienterne, for at opsamle nyttige sundhedsdata, sker der imidlertid en sammenblanding af de to 'verdener'. Det skyldes, at patienten, for at få adgang til app'en, må afgive et samtykke til, at udbyderen lagrer deres data og anvender dem i anden sammenhæng.

3.2.1. Forsikring og arbejde

Som allerede nævnt er det almindeligt anerkendt, at de samtykker til brug af data, der afgives som modydelse for at kunne downloade gratis sundhedsapps, er illusoriske på flere punkter:

- Incitamentet til at acceptere afgivelsen af data er stort, fordi belønningen følger øjeblikkeligt, mens ulemperne er uklare for de fleste

- Brugeren er uopmærksom på omfanget af samtykket og på, at deres data vil kunne indgå i udarbejdelsen af personprofiler, som vil udlede meget personfølsomme oplysninger om fx deres generelle sundhedstilstand, seksuelle orientering, personlighed, politiske ståsted mmm. Langt de fleste brugere er endvidere ikke klar over, at tilsagn om, at data fra fx en motionsapp må anvendes af udbyderen, vil kunne resultere i, at disse data i bearbejdet form kan havne hos fx deres forsikringsselskab

Uden at brugeren gør sig klart, at vedkommende har givet tilsagn til det, kan omfattende, personfølsomme data altså være til salg til forskellige aktører, hvor de vil kunne skade ophavsmanden. Det giver anledning til en række problemer på forskellige områder, to af dem er forsikring og ansættelse.

Der er lovgivet mod at anvende prædiktive gentest som bedømmelseskriterium, idet forsikringsselskaber og arbejdsgivere ikke må anvende disse ved bedømmelse af forsikringsvilkår eller ansættelser.[60]

En lignende situation vil imidlertid opstå, hvis firmaerne diskriminerer på grundlag af sundhedsdata fra wearables eller personprofiler. Her vil man dog kunne forskelsbehandle langt mere differentieret, fordi disse test potentilet siger meget mere om personen. Hertil kommer, at hvis man laver meget detaljerede risikoprofiler på hver enkelt, vil man finde, at alle har mere eller mindre forhøjede risici for at udvikle en række sygdomme, så der kan blive tale om en stor opgave med at tilpasse forsikringerne til hver enkelt.

En gentest kan vise en større eller mindre sandsynlighed for, at en person vil udvikle en alvorlig sygdom på et tidspunkt i sit liv. Men gentest giver som nævnt kun en lille del af billedet af personen; generne har betydning for de fleste sygdomme, men mange andre faktorer, som fx miljø og valg af levevis, er afgørende for, om sygdommene faktisk bryder ud.

60 Jf Lov om brug af helbredsoplysninger mv på arbejdsmarkedet, LOV nr 286 af 24/04/1996 og Bekendtgørelse af lov om forsikringsaftaler, LBK nr 1237 af 09/11/2015.

Hvis man kommer dertil, at de genetiske oplysninger kan kombineres med alle de data, wearables kan opsamle om personens adfærd: fx hvor meget vedkommende motionerer, hvad vedkommende spiser – og hvor meget – alkoholvaner, sexuel adfærd, psykisk velbefindende mm, så vil nogle fortolke de usikre data som meget mere tydelige. Hvis firmaerne yderligere får adgang til at anvende personprofiler, som er fremstillet ved at sammenkøre data fra forskellige platforme og udlede antagelser om personlighed og sociale forhold, vil det kunne muliggøre omfattende forskelsbehandling af forsikringstagerne.

Forsikringsselskaberne er allerede meget aktive i forhold til at undersøge mulighederne for at få adgang til kundernes adfærdsdata, så de kan differentiere præmien efter, hvem der lever sundt og hvem der ikke gør. Hvis forsikringsselskaberne får adgang til omfattende data om alle deres kunder, vil præmierne fremover kunne differentieres langt mere end hidtil, i forhold til den enkelte persons profil.

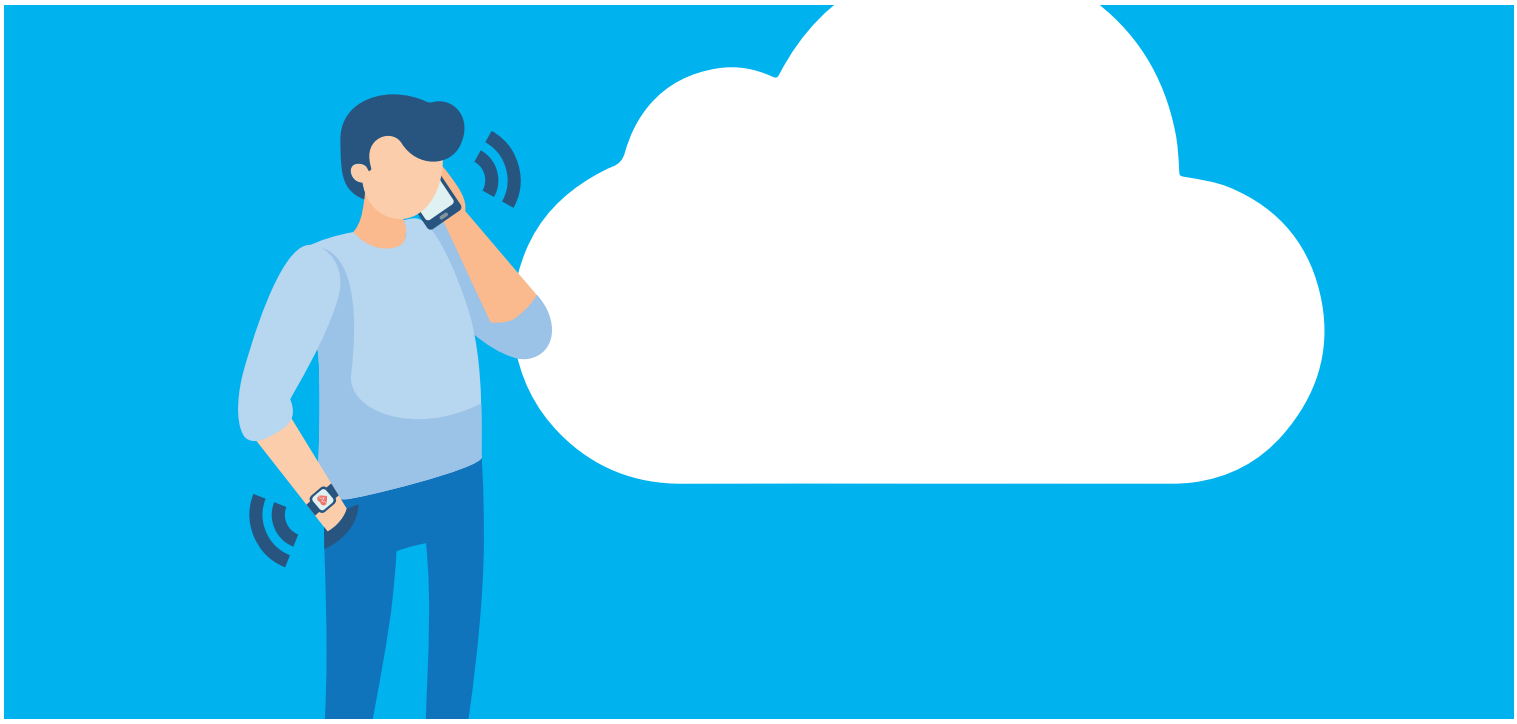
Mange af de oplysninger, wearables opsamler, vil være interessante for en arbejdsgiver at få fingre i. Personer som fx viser sig at leve usundt eller på anden måde risikobetonet, motionere for lidt eller stresse for meget, vil alt andet lige kunne opfattes som mindre attraktive ansatte end dem, der lever mere fornuftigt. Oplysningerne vil derfor kunne spille ind i forhold til, hvem af flere ansøgere som ansættes eller forfremmes, og hvem der står yderst ved en fyringsrunde.

Nogen vil anse diskrimination på baggrund af adfærdsdata for at være forkert, fordi det skader personen ved ikke at tillade personen at leve efter sin egen opfattelse af det gode liv. Vedkommende skal leve efter firmaets definition af, hvad der udgør et sundt liv. Man kan også have den tilgang, at folk skal have frihed til at vælge at leve usundt, men at de så også bør være villige til at betale en højere pris for deres forsikring. Men heraf følger ikke, at firmaer eller arbejdsgivere skal have lov til at indhente sundhedsdata om personer fra databrookere eller andre uden personens samtykke, og anvende disse data til at forringe forsikringstageres vilkår.

3.2.2 Forskelsbehandling af udsatte grupper

Som tidligere nævnt tyder forskning i forskelle i sund levevis på, at hvis man i en given sammenhæng lægger vægt på, hvor sundt folk lever, vil dette i udstrakt grad ramme de i forvejen dårligst stillede hårdest. Det er her, man finder flest med usund levevis, som vil have svært ved bare at træffe et valg om at leve maximalt sundt.

Der vil ligeledes være en risiko for, at i et samfund, som i vidt omfang baserer sig på digitale løsninger, vil grupper som gamle, blinde, kort uddannede og dem, der ikke har den nyeste teknologi eller mulighed for at bruge den, få svært ved at deltage på lige fod.



4. Retlige rammer

4.1 Indledning

Privatlivets fred er forankret i menneskeretten, som beskytter det enkelte menneskes personlige integritet og varetager dennes mulighed for privatliv, selvbestemmelse og selvudfoldelse. Privatlivets fred er dermed en menneskeret. Den retlige beskyttelse af det private er dog ikke ubetinget, men skal ses i en samfundsmæssig sammenhæng. Menneskeretten anerkender, at det i nogle situationer kan være bremsende for en fornuftig samfundsudvikling, hvis der ikke åbnes op for visse muligheder for adgang til privatheden.

Det er blandt andet denne adgang til privatheden, som databeskyttelsesretten retter sig mod. Databeskyttelsesretten bygger således på nogle grundprincipper, der har til formål at beskytte privatlivets fred og skal sikre nødvendigheden og kvaliteten af brug af data.

Teknologien har med tiden givet enorme muligheder for at indsamle data om den enkelte. Hvor fokus tidligere i høj grad var rettet mod retten til privathed, er der i dag sket en glidning, hvor vi må acceptere, at 'havelågen' til vores private gemmer har åbnet sig. Fokus er derfor i dag i højere grad rettet mod *brugen* af alle disse informationer om os. Målet med databeskyttelsesretten er således til stadighed at danne en fleksibel ramme om en hensigtsmæssig udnyttelse af de stadigt større muligheder for at registrere og anvende personoplysninger på en måde, der af borgerne opleves som acceptabel. Det er en balance, som både samfundet, markederne og borgerne har en interesse i.

Præcist hvordan denne balance opretholdes er ikke til enhver tid og på ethvert sted fastlagt på forhånd. Holdningen til privatlivsbeskyttelse og vurderingen af værdien

af det private er både historisk, kulturelt og politisk betinget. I de forskellige lande – og områder i verden – kan der således være store forskelle i synet på det private og statens rolle heri. Tilgang til og anvendelse af data i et land som fx Kina ligger meget langt fra de vestlige landes opfattelse af acceptabel anvendelse af data. I de vestlige lande er der en større grad af konsensus, men stadig med store forskelle fx mellem USA og Europa. EU's databeskyttelsesforordning er en fælles europæisk regulering, med et fælles grundlag i synet på det individuelle menneske og dermed på betydningen af transparens i behandling af data om den enkelte. Uanset der således er en stor grad af fælles forståelse internt i Europa af vigtigheden af at beskytte borgernes data og synet på, hvad der hører til privatlivets fred, kan der dog være forskelle i de forskellige europæiske landes holdning til forskellige værdier og ikke mindst prioritering af forskellige interesser. Forordningen skal derfor ses og anvendes som et kompromis, der rummer sådanne forskelle.

I dette kapitel er sundhedsvæsenets opsamling og anvendelse af data i Danmark i fokus.

I det følgende vil der i hovedtræk blive gjort rede for nogle af de centrale juridiske regler, der kommer i spil, når sundhedsvæsenet anvender data opsamlet gennem wearables. Både EU's databeskyttelsesforordning, den danske databeskyttelseslov samt de danske regler for sundhedsområdet inddrages. For en mere detaljeret gennemgang af databeskyttelsesrettens betydning ved anvendelse af wearables (herunder referencer til de specifikke regler) kan henvises til bilag 1 om Wearables i databeskyttelsesretlig belysning.

I det følgende *afsnit 4.2* ses nærmere på baggrunden for EU's databeskyttelses-forordning. Vurderingen af forordningens betydning for anvendelse af wearables må ses i lyset af de formål og interesser, som forordningen bygger på.

I *afsnit 4.3* præsenteres kortfattet nogle centrale danske love af relevans for anvendelse af wearables samt samspillet mellem EU-retten og national ret. I redegørelsen er konsekvenserne af benyttelse af wearables for borgernes frihed et centralt element. *Afsnit 4.4* i dette kapitel sætter fokus på, i hvilket omfang lovgivningen beskytter individers frihed i forbindelse med anvendelse af wearables.

4.2 EU's databeskyttelsesforordning

I 2000 blev Den Europæiske Unions Charter om Grundlæggende Rettigheder (2000/C 364/01) gjort til en del af traktaterne. Det følger af charterets artikel 8, at enhver har ret til beskyttelse af personoplysninger, der vedrører ham eller hende. Denne ret er tæt forbundet med retten til beskyttelse af privatlivets fred, som er fastslået i charterets artikel 7.

I Traktaten om den Europæiske Unions Funktionsmåde (TEUF) anføres i artikel 16, at "Enhver har ret til beskyttelse af personoplysninger om vedkommende selv".

Med hjemmel i TEUF blev Europa-Parlamentets og Rådets Forordning (EU) 2016/679 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF, vedtaget (i daglig tale kaldet GDPR efter den engelske titel General Data Protection Regulation). Forordningen blev vedtaget i 2016 med virkning i dansk ret fra den 25. maj 2018. Det er en generel forordning om databeskyttelse.

> Om begrundelsen for dette tiltag anføres i præamblen til databeskyttelses-forordningen, at direktiv 95/46/EF er gennemført og anvendt forskelligt i Unionen, hvilket har givet en fragmenteret databeskyttelse og en forskel i beskyttelsesniveauet. Disse forskelle kan forhindre fri udveksling af personoplysninger i Unionen og udgøre en hindring for udøvelsen af en række økonomiske aktiviteter på EU-plan, virke konkurrenceforvridende og hindre myndighederne i at varetage de opgaver, der er pålagt i medfør af EU-retten.

Om baggrunden for databeskyttelsesforordningen anføres i præamblen, at den hastige teknologiske udvikling og globaliseringen har skabt nye udfordringer, hvad angår beskyttelsen af personoplysninger. Omfanget af indsamlingen og delingen af personoplysninger er steget betydeligt. Også det indre markeds funktion har medført en kraftig vækst i bevægelserne af personoplysninger på tværs af landegrænserne. Teknologien giver både private selskaber og offentlige myndigheder mulighed for at udnytte personoplysninger i et hidtil uset omfang, når de udøver deres aktiviteter. Fysiske personer udbreder i stigende grad deres personoplysninger offentligt og globalt. Udvekslingen af personoplysninger mellem offentlige og private aktører, herunder fysiske personer, sammenslutninger og virksomheder i Unionen er steget. For at sikre et ensartet beskyttelsesniveau for fysiske personer i hele Unionen og for at hindre, at forskelle hæmmer den frie udveksling af personoplysninger på det indre marked, er der ifølge medlemslandene behov for en forordning for at skabe retssikkerhed og gennemsigtighed.

Om målene for databeskyttelsesforordningen anføres i præamblen, at det er vigtigt at skabe den tillid, der gør det muligt, at den digitale økonomi kan udvikle sig på det indre marked. Denne udvikling kræver en stærk og mere sammenhængende databeskyttelsesramme i Unionen, som understøttes af effektiv håndhævelse. Det anføres, at for at sikre effektiv beskyttelse af personoplysninger i Unionen er det nødvendigt at styrke og præcisere de registreredes rettigheder og de forpligtelser, der påhviler dem, der behandler og træffer afgørelse om behandling af personoplysninger, samt der gives tilsvarende beføjelser til at føre tilsyn med og sikre overholdelse af reglerne om beskyttelse af personoplysninger og indføres tilsvarende sanktioner ved overtrædelser i medlemsstaterne. Det anføres, *at* fysiske personer bør have kontrol over deres personoplysninger, og *at* sikkerheden både retligt og praktisk bør styrkes for fysiske personer, erhvervsdrivende og offentlige myndigheder. Endelig anføres i præamblen, at behandling af personoplysninger bør have til formål at tjene menneskeheden. Retten til beskyttelse af personoplysninger er ikke en absolut ret; den skal ses i sammenhæng med sin funktion i samfundet

og afvejes i forhold til andre grundlæggende værdier i overensstemmelse med proportionalitetsprincippet.

Databeskyttelsesforordningen er bindende for EU-landene. Som nævnt i afsnit 1 skal forordningen derfor vurderes i lyset af, at den skal rumme alle de europæiske landes ønsker til og syn på, hvordan data kan opsamles, og hvad de kan bruges til. Dette kan selvsagt være en udfordring for forståelsen og anvendelsen af forordningen.

4.3 National ret

Dette kapitel har fokus på samspillet mellem EU-ret og dansk ret ved opsamling og anvendelse af data inden for Danmarks grænser.

Det følger af databeskyttelsesforordningen, at de enkelte medlemsstater inden for nærmere bestemte områder enten skal eller kan fastsætte nationale regler. Medlemsstaterne har bla mulighed for inden for en vis manøvremargin at præcisere forordningens regler, ligesom der i national ret kan fastsættes særlige regler og undtagelser i et ikke-ubetydeligt omfang. I Danmark er disse muligheder generelt udnyttet i databeskyttelsesloven. Loven præsenteres kortfattet herunder i *afsnit 4.3.1*. I dansk ret findes regler for offentlige myndigheders behandling af fortrolige oplysninger. Disse regler er generelle regler gældende for al offentlig virksomhed. Inden for sundhedssektoren har man i sundhedsloven fastsat regler for behandling af fortrolige oplysninger. Disse regler er særligt tilpasset de forhold, der gør sig gældende i patientbehandlingen, og de skal anvendes, når en patient modtager behandling af en sundhedsperson. Når det gælder sundhedsvæsenets anvendelse af data fra wearables til helbredsformål er sundhedslovens regler om tavshedspligt og videregivelse af helbredsoplysninger således helt centrale. Sundhedsloven præsenteres kortfattet i *afsnit 4.3.2*.

4.3.1 Databeskyttelsesloven[61]

Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven) har haft virkning i dansk ret fra 25. maj 2018. Samtidig med databeskyttelsesloven blev konsekvensændringer (konsekvenser for anden lovgivning) som følge af databeskyttelsesloven og databeskyttelsesforordningen vedtaget ved lov[62].

Databeskyttelsesloven supplerer og gennemfører databeskyttelsesforordningen. Loven opretholder og fastsætter supplerende nationale bestemmelser om behandling af personoplysninger inden for det nationale råderum, som forordningen giver mulighed for.

---

61 Lov nr. 502 af 23. maj 2018. Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven).

62 Lov nr. 503 af 23. maj 2018. Lov om ændring af lov om retshåndhævende myndigheders behandling af personoplysninger, lov om massemediers informationsdatabaser og forskellige andre love.

4.3.2 Sundhedsloven[63]

Databeskyttelsesforordningen giver medlemsstaterne et relativt stort nationalt råderum på sundhedsområdet. Det anføres i Betænkning nr. 1565 om *Databeskyttelsesforordningen – de retlige rammer for dansk lovgivning*, at det er Sundheds- og Ældreministeriets vurdering, at de gældende regler i Sundheds- og Ældreministeriets lovgivning om behandling af personoplysninger mv (i det store og hele) kan opretholdes, efter databeskyttelsesforordningen har fået virkning[64]. Sundhedslovens afsnit 9 om tavshedspligt, videregivelse og indhentning af helbredsoplysninger mv bibeholdes således. Der er dog sket enkelte modifikationer som konsekvens af forordningen i forhold til indsigtsret og oplysningspligt, idet sådanne forpligtelser for sundhedsvæsenet fremadrettet vil følge direkte af databeskyttelsesforordningen i relation til elektroniske patientjournaler.

SAMSPILLET MELLEM DATABESKYTTELSESFORORDNINGEN OG NATIONAL RET

Som følge af dels forordningens direkte virkning, dels opretholdelsen af nationale regler på sundhedsområdet, må der ske en afgrænsning mellem de sundhedsretlige og databeskyttelsesretlige regelsæt. I dette kapitel, hvor fokus er på anvendelse af wearables, tages der udgangspunkt i følgende to relationer:

En sundhedsperson behandler data indsamlet gennem wearables til helbredsformål. Dette kan ske med hjemmel i databeskyttelsesforordningen i det omfang, det er nødvendigt i patientbehandlingen (i bred forstand). Opbevaring, indhentning og videregivelse af data reguleres af de sundhedsretlige regelsæt, suppleret af databeskyttelsesretten. Indsigtsret og oplysningspligt reguleres af de databeskyttelsesretlige regelsæt, ligesom fx sikkerhedskravene kan supplere de sundhedsretlige regler. I sådanne tilfælde er den sundhedsmyndighed, hvor sundhedspersonen er ansat, dataansvarlig med de pligter, som følger af forordningen.

En kommerciel udbyder af wearables behandler data indsamlet gennem wearables til helbredsformål. Dette kan ske med hjemmel i databeskyttelsesforordningen med den registreredes samtykke (eller andet hjemmelsgrundlag i forordningen). Den videre behandling reguleres af de databeskyttelsesretlige regelsæt. Den private aktør er dataansvarlig.

De to situationer kan kombineres på forskellig måde. Et eksempel kan være, hvis anvendelse af wearable involverer både en relation til en kommerciel udbyder *og* en relation til en sundhedsperson. Her vil begge de ovenfor beskrevne relationer komme i spil. Eller det kan være den situation, at der er etableret en form for samarbejdsrelation mellem sundhedsmyndigheden og en privat udbyder af wearables. Her kan det undertiden være uklart, hvem der er dataansvarlig og dermed hvilke regelsæt, der skal anvendes. Disse scenarier uddybes nærmere under punkt 4.4.1.

63 LBK nr. 1286 af 2. november 2018.

64 Se Betænkning nr. 1565, Del II, afsnit 11. Sundheds- og Ældreministeriet.

4.4 Databeskyttelsesforordningen og –loven med fokus på beskyttelse af individers frihed i forbindelse med sundhedsvæsenets anvendelse af wearables

Brug af wearables til opsamling af data til helbredsformål vil stort set altid være omfattet af databeskyttelsesforordningen (herefter benævnt GDPR), og der vil ofte tillige være tale om en indgribende behandling i forordningens forstand. Der kan således bla være tale om profilering, hvis oplysningerne anvendes til at analysere eller forudsige den registreredes helbredstilstand, adfærd eller lignende, hvilket betragtes som en særligt indgribende form for behandling. GDPR giver et højere beskyttelsesniveau ved sådanne former for behandling.

I dette afsnit er der fokus på, i hvilket omfang de omtalte regelsæt beskytter individers frihed i forbindelse med anvendelse af wearables. Der ses i hovedtræk nærmere på udvalgte dele af GDPR og relevant national lovgivning, særligt med fokus på en vurdering af, i hvilket omfang individers frihed i forbindelse med sundhedsvæsenets anvendelse af wearables, beskyttes. For en mere detaljeret beskrivelse (herunder en beskrivelse af de undtagelser, som findes i databeskyttelsesforordningen) kan henvises til bilag 1 om Wearables i databeskyttelsesretlig belysning.

I *afsnit 4.4.1* fastlægges det dataansvar, som er grundlæggende for opfyldelsen af GDPR's principper. Der tages udgangspunkt i to mulige scenarier for anvendelse af data fra wearables i sundhedsvæsenet.

I *afsnit 4.4.2* vurderes de retlige rammer for behandling af data opsamlet gennem wearables. Samspillet mellem de relevante regelsæt klarlægges.

Profilering gennem wearables er et centralt tema ved anvendelse af wearables og kan på forskellig måde få konsekvenser for den registrerede. I *afsnit 4.4.3* ses nærmere på de retlige rammer for profilering.

4.4.1 Hvem har det retlige (data)ansvar?

Anvendes data fra wearables i sundhedsvæsenet vil det først og fremmest være relevant at fastlægge, hvem der må anses som dataansvarlig i forhold til opsamling og behandling af disse data. Som udgangspunkt bygger databeskyttelsesretten på den grundtanke, at den dataansvarliges regelrette adfærd sikrer den ønskede beskyttelse af borgerne.

Scenarie 1 *Indsamling af data i sundhedsvæsenet gennem wearables (sundhedsvæsenet får data om patienten direkte fra wearables)*

Når det skal fastlægges, hvem der har dataansvaret under dette scenarie, hvor sundhedsvæsenet er direkte aftager af de data, der genereres via wearable, må man se nærmere på, hvilken forbindelse der er mellem den tekniske (private/kommercielle) udbyder af wearables/apps og sundhedsvæsenet.

Indgår en sundhedsmyndighed en kontrakt om udvikling og drift af en wearable-tjeneste med en privat it-leverandør med henblik på opsamling af data, der skal anvendes ved myndighedens behandling af en konkret patient, er sundhedsmyndigheden at betragte som dataansvarlig. Har leverandøren ikke et selvstændigt formål med at behandle de indsamlede data, men leverer blot den tekniske udførelse, vil denne leverandør være at betragte som databehandler. Sundhedsmyndigheden skal i denne situation sikre reglerne om brug af databehandlere overholdt, herunder indgå en databehandleraftale og føre (aktivt) tilsyn med leverandørens håndtering af oplysningerne. I dette tilfælde gælder den databeskyttelsesretlige tilsynspligt med databehandlere direkte.

Man kan også forestille sig den konstruktion, at sundhedsmyndigheden indgår i et *samarbejde* med en privat udbyder, der fungerer som *et fællesskab*, hvor organisationerne som parter i fællesskab fastlægger formål og midler for behandlingen af personoplysninger. Det kan fx være i tilfælde af, at den kommercielle part udbyder supplerende, men forbundne, sundhedstjenester, og dataene skal anvendes både hertil og til myndighedens patientbehandling. Samarbejdspartnerne vil være at regne som fælles dataansvarlige. GDPR stiller her krav om klare arbejds- og rollefordelinger samt krav om information til de registrerede om fordelingerne. I en sådan konstruktion følger det således direkte af forordningen, at sundhedsvæsenet vil være (med)ansvarlig for behandling af personoplysninger indsamlet gennem wearable. Hertil kommer, at det – uafhængigt af forordningen – til en vis grad må antages, at i det omfang offentlige sundhedsmyndigheder indgår i et samarbejde med private, vil der være en forpligtelse til at sikre sig, at udmøntningen af samarbejdet sker på et lovligt grundlag.

Endelig kan der være tale om en situation, hvor sundhedsmyndigheden *og tillige* en kommerciel udbyder begge er direkte aftagere af data, men med forskellige formål, fra wearable. I forbindelse med brug af wearables i sundhedssektoren kan et eksempel være, at en kommerciel udbyder af wearables selv anvender de indsamlede data til fx at danne markedsføringsprofiler eller til at udvikle nye tekniske løsninger. Denne konstruktion kan indebære *flere selvstændige dataansvarlige*, der hver især er ansvarlige for deres databehandling. I sidstnævnte tilfælde vil der som udgangspunkt ikke efter GDPR være en pligt til at undersøge, om den anden part i forbindelse med dennes behandling af personoplysninger respekterer forordningens regler og de registreredes rettigheder. Det er dog kun et udgangspunkt. Det danske Datatilsyn har nemlig meldt ud, at den hidtidige nationale praksis om god databehandlingsskik i forbindelse med offentlige myndigheders modtagelse af oplysninger fra andre aktører består under GDPR. Offentlige myndigheder kan dermed som udgangspunkt ikke bruge oplysninger, de har modtaget fra en samarbejdsparter, der har indsamlet dem ulovligt. Også EU-domstolens praksis lægger op til, at der kan statueres fælles ansvar under visse omstændigheder (se mere herom i bilag 1 om Wearables i databeskyttelsesretlig belysning). Sundhedsvæsenet har således et reelt ansvar for at beskytte data om patienter, i det omfang at sundhedsvæsenet har været medvirkende til, at sådanne oplysninger opsamles gennem wearable.

Det kan antageligt undertiden være vanskeligt at kategorisere et (vist) samarbejde mellem sundhedsmyndigheden og en privat udbyder som enten et egentligt samarbejde eller en konstruktion med flere selvstændige databehandlere.

Scenarie 2 *Indsamling af data i sundhedsvæsenet fra patienten, men opsamlet gennem kommercielle wearbles/apps (sundhedsvæsenet får data af patienten)*

Dette scenarie er i og for sig helt som vanligt, når en patient giver oplysninger ved sin kontakt med sundhedsvæsenet. Det er ikke ukendt for sundhedsvæsenet, at de oplysninger, som patienten giver, er dannet ved hjælp af teknologi. Et eksempel kan være, at patienten derhjemme tager sit blodtryk ved hjælp af et blodtryksapparat, noterer tallene ned og giver lægen disse informationer under konsultationen. Spørgsmålet her er, om det giver anledning til (andre) retlige overvejelser, når de oplysninger, som patienten giver til sundhedsvæsenet, er opsamlet gennem wearables? Nogle typer af udstyr, fx et simpelt blodtryksapparat, gemmer ikke oplysningerne. I et sådant "lukket rum" vil data derfor ikke gå videre. Andre typer af udstyr er i højere grad computere med muligheden for at gemme og anvende gemte data. Men uanset om det er den ene eller anden type af medicinsk udstyr, så er der krav om, at udstyret gennemgår omfattende godkendelsesprocedurer, fastlagt på EU-niveau, inden de kan tages i brug. Dette adskiller sig fra wearables, som i højere grad udbydes på et "frit marked".

Når det skal fastlægges, hvem der har dataansvaret (eller andre former for ansvar) under dette scenarie, vil den rolle, som sundhedsmyndigheden spiller ved patientens valg af wearable, antagelig være afgørende.

Det første man kan overveje er en situation, hvor en sundhedsperson *anbefaler* en patient at anvende wearables, uden at sundhedspersonen selv får adgang til de indsamlede data eller på anden måde er direkte involveret i den behandling af oplysninger, der sker gennem det pågældende wearable. Den registrerede indsamler her selv oplysningerne via et wearable og afgiver oplysningerne til sundhedsmyndigheden /sundhedspersonen.

> GDPR's bestemmelser om dataportabilitet skal kort nævnes i denne sammenhæng. Er der med brugerens samtykke opsamlet data via wearables, har den registrerede ret til "i et struktureret, almindeligt anvendt og maskinlæsbart format" at modtage personoplysninger om sig selv, som vedkommende har givet til den dataansvarlige. Den registrerede har også ret til at transmittere disse oplysninger direkte til en anden dataansvarlig (her sundhedsvæsenet).

I en sådan situation vil sundhedsmyndigheden/sundhedspersonen næppe databeskyttelsesretligt have noget (med)ansvar for den databehandling, der ligger forud for sundhedspersonens egen modtagelse af data. Forholdet mellem den registrerede og den private udbyder af tjenester forbundet til det pågældende wearable vil være reguleret af de databeskyttelsesretlige regler som en selvstændig relation (privat

relation). Den private virksomhed er dataansvarlig i forhold til den registrerede og er underlagt GDPR's regler.

Sundhedspersonens modtagelse af de genererede oplysninger direkte fra den registrerede må betragtes som en anden databeskyttelsesretlig relation, hvor sundhedsmyndigheden er dataansvarlig. Ved modtagelsen skal sundhedsmyndigheden sikre sig, at der er et tilstrækkeligt behandlingsgrundlag samt sikre overholdelse af de databeskyttelsesretlige principper, som fx at data har en tilstrækkelig kvalitet.

> Anvendelse af data opsamlet gennem wearables kan give særlige udfordringer i forhold til vurdering af kvalitet. Fejlbehæftede oplysninger kan dannes ved svigt i teknologien eller forkert anvendelse af denne. Det kan også være fejlagtige oplysninger, der indgår i fx dannelse af en sundhedsprofil. Dårlig datakvalitet kan selvsagt have store konsekvenser for patienten.

En variant af denne situation er, hvis sundhedspersonen har anbefalet *en bestemt wearable* til sin patient. Dette vil antagelig heller ikke føre til, at sundhedsmyndigheden får et (med)ansvar for den databehandling, der finder sted gennem det pågældende wearable. Man kan i sådanne tilfælde overveje, om sundhedspersonen kan ifalde et fagligt ansvar (omhu og samvittighedsfuldhed), herunder evt et erstatningsansvar for eventuelle skader, som påføres patienten gennem (ulovlig) databehandling. Et beslægtet spørgsmål er, om sundhedspersonen forud for en sådan anbefaling bør undersøge lovligheden af det pågældende wearable. Disse spørgsmål ses ikke afklaret i retspraksis.

> Hvis en sundhedsmyndighed opretter og offentliggør en form for katalog over wearables, som kan anvendes af patienter i forskellige sammenhænge, må ansvarsforholdene, herunder kravene til forvaltningsmyndigheders forsvarlige vejledning, nøje overvejes, da patienter kan få den opfattelse, at disse wearables er "godkendte" af den offentlige myndighed.

Hvis sundhedsmyndigheden/ sundhedspersonen direkte har *anvist en bestemt wearable* – måske endda som en betingelse for videre undersøgelse og behandling - vil ovenstående betragtninger utvivlsomt skulle skærpes. Om der i sådanne situationer kan pålægges en form for (med)ansvar kan næppe udelukkes. Dette gælder både i forhold til behandling af data og i forhold til et fagligt ansvar.

4.4.2 Behandling af oplysninger

Som udgangspunkt må behandling af oplysninger om en persons helbredsforhold, herunder genetiske data, ikke finde sted. Behandling kan dog finde sted i det omfang, behandlingen kan hjemles i et eller flere af de behandlingsgrundlag, som GDPR anviser.

4.4.2.1 Hjemmelsgrundlag for behandling af data
Efter GDPR kan der behandles (nødvendige) oplysninger i sundhedsvæsenet til

behandlingsformål *uden samtykke* fra den registrerede, når behandling foretages af en sundhedsperson. Anvendes wearables ved indsamling af data, kan der opstå et spørgsmål om tilstrækkeligt behandlingsgrundlag, hvis der opsamles data ud over dette. "Ekstra" oplysninger nødvendiggør et selvstændigt behandlingsgrundlag, fx et samtykke fra den registrerede (se om udfordringer ved anvendelse af samtykke som hjemmel til behandling af data i sundhedsvæsenet, i bilag 1 om Wearables i databeskyttelsesretlig belysning).

Behandler en kommerciel udbyder data opsamlet gennem wearable, kan dette efter GDPR lovligt ske med samtykke fra brugeren af wearable. Forordningen skelner mellem behandling af (almindelige) personoplysninger, der kræver *utvetydigt* samtykke, og behandling af følsomme oplysninger, herunder helbredsoplysninger, der forudsætter *udtrykkeligt* samtykke fra brugeren (se om udfordringer ved samtykke, når ydelse af en tjeneste gøres afhængig af afgivet samtykke, i bilag 1 om Wearables i databeskyttelsesretlig belysning).

4.4.2.2 Informationspligt
GDPR lægger vægt på, at det skal være gennemsigtigt for fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles. Forordningen fastsætter derfor en *informationspligt* for den dataansvarlige. Hvad der skal informeres om, er fastlagt i forordningen (en lovpligtig information om hvem der er dataansvarlig, til hvilke formål oplysningerne behandles mm – ikke at forveksle med pligten til at give *indsigt* i de registrerede oplysninger, hvis den registrerede anmoder om det, se senere om indsigt). Denne informationspligt over for den registrerede gælder både ved registrering af oplysninger og ved eventuel videreanvendelse af de indsamlede oplysninger til nye formål. Pligten til at informere gælder både for oplysninger indsamlet hos den registrerede og for oplysninger indsamlet på anden vis. Den registrerede skal således – uanset om behandling af data sker i sundhedsvæsenet eller hos en privat udbyder af wearables – *informeres* om registreringen, hvem der er dataansvarlig mv. Den dataansvarlige har på eget initiativ denne pligt til at informere den registrerede.

4.4.2.3 Videreanvendelse
GDPR forhindrer ikke videreanvendelse af opsamlede data – men opsætter nogle grænser for videreanvendelse. Det følger af både GDPR og databeskyttelsesloven, at personoplysninger skal indsamles til udtrykkeligt angivne og legitime formål og ikke må viderebehandles på en måde, der er *uforenelig* med disse formål.

Ønsker den dataansvarlige at anvende indsamlede personoplysninger til *andre formål* end det formål, som oplysningerne oprindeligt blev indsamlet til, skal den dataansvarlige vurdere, om behandling til dette andet formål er forenelig med det oprindelige formål. Formålsbestemthedsprincippet hindrer ikke viderebehandling af oplysninger, hvis der er tale om forbundne eller beslægtede behandlings-sammenhænge (se om forskellige momenter, som den dataansvarlige myndighed skal inddrage i sin vurdering af, om databehandling til et andet formål er forenelig

med det formål, som personoplysningerne oprindeligt blev indsamlet til, i bilag 1 om Wearables i databeskyttelsesretlig belysning).

a. Videreanvendelse – offentlige myndigheder

GDPR giver forholdsvis vide rammer for offentlige myndigheder – i modsætning til private aktører, hvor rammerne er snævrere – til at viderebehandle personoplysninger til andre formål. Rammerne for tilladeligt formålsskift er dog snævrere, når det handler om følsomme oplysninger, som fx helbredsoplysninger. Viderebehandling af data til et nyt (ikke-uforeneligt) formål kræver, at den dataansvarlige har et gyldigt behandlingsgrundlag. Offentlige myndigheder vil ofte have hjemmel i lov (behandlingsgrundlag) til en sådan viderebehandling, mens private virksomheder ofte (på baggrund af specifikationskravet) må have et (nyt) samtykke fra den registrerede til en sådan viderebehandling til nye formål.

Hvis den dataansvarlige ønsker at anvende de indsamlede oplysninger til nye formål, kræver GDPR, at den registrerede skal have dette oplyst, *inden* den nye behandling sker. Den registrerede vil dermed få lejlighed til at gøre indsigelser mod eventuelle forkerte data mv. Formålet med denne (nye) forpligtelse for den dataansvarlige er at skabe gennemsigtighed og transparens i de store datastrømme, som forordningen åbner op for.

Videregives/overføres oplysninger til en *ny dataansvarlig* påhviler det den nye dataansvarlige at informere den registrerede om, at databehandling finder sted (dvs efterfølgende information, jf ovenfor om informationspligt). Det forudsættes her på samme måde, at den (nye) dataansvarlige har et tilstrækkeligt behandlingsgrundlag (samtykke eller andet hjemmelsgrundlag).

Databeskyttelsesloven indeholder imidlertid en bemyndigelsesbestemmelse til udstedelse af regler om, at personoplysninger må viderebehandles af offentlige myndigheder til andre formål, end de oprindeligt var indsamlet til, uafhængigt af formålenes forenelighed (dvs også til formål der er uforenelige med det oprindelig indsamlingsformål). Den registrerede skal *ikke* informeres om videreanvendelse hjemlet i denne bemyndigelse.

Bestemmelsen indeholder visse begrænsninger. For det første kan den nævnte bemyndigelse ikke anvendes til at fastsætte regler om en viderebehandling af personoplysninger, der vil være i strid med anden lovgivning. Bestemmelsen kan således ikke anvendes til at tilsidesætte fx den enkelte sundhedspersons lovbestemte tavshedspligt. Dette reguleres i sundhedslovens regler om tavshedspligt og videregivelse af oplysninger. For det andet kan bemyndigelsen, hvad angår helbredsoplysninger og genetiske oplysninger, heller ikke anvendes til at fastsætte regler om viderebehandling til formål, der er uforenelige med det oprindelige formål, i det omfang disse følsomme oplysninger er indsamlet i medfør af sundhedslovgivningen og/eller som led i nødvendig behandling af personoplysninger med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje

eller patientbehandling. Omvendt kan bemyndigelsen – som reglerne fremstår – anvendes, når blot videreanvendelsen ikke kan regnes som uforenelig.

Anvendelse af nævnte bemyndigelse har den betydning *inden for sundhedssektoren*, at når der fx af en læge på et hospital er indsamlet helbredsoplysninger (samt andre oplysninger) om en patient til brug for behandling af patienten, kan bemyndigelsen anvendes i forhold til samkøring af data opsamlet i sundhedsvæsenet inden for tavshedspligtens rammer (fastlægges af sundhedsloven), hvor formålet med denne samkøring er patientbehandling (i bred forstand). Det kan fx være inddragelse af data opsamlet i en konkret behandlingssituation (evt gennem wearables), som kan (gen) anvendes og samkøres med andre data til vurdering af fx forebyggelsestiltag over for den enkelte patient. Har sundhedsvæsenet også sociale (eller andre) oplysninger om patienten, fx indsamlet gennem wearables, kan disse oplysninger indgå i samkøringen. Patienten skal i så fald ikke informeres om sådanne tiltag.

Bemyndigelsesbestemmelsen kan af en offentlig myndighed som nævnt anvendes til samkøring af oplysninger, uanset om formålet med denne samkøring er uforeneligt med det oprindelige indsamlingsformål. Er der fx (med hjemmel i sundhedslovgivningen) videregivet helbredsdata fra sundhedsvæsenet til den sociale sektor til ét formål (fx arbejdsprøvning eller pensionssag), vil den modtagende myndighed som udgangspunkt informere den registrerede ved modtagelsen. Herefter kan disse oplysninger indgå i den modtagende myndigheds egen brug af data. Med hjemmel i regler udstedt efter den nævnte bemyndigelse, vil de modtagne data kunne samkøres og anvendes også til uforenelige formål indenfor den modtagende myndigheds administration, da oplysningerne ikke er indsamlet af denne myndighed med henblik på sygdomsbekæmpelse mv. Myndighedsafgrænsningen vil her i stedet være afgørende for, hvilke oplysninger i den sociale sektor, der kan indgå i samkøringen. En kommune vil fx efter forordningen være én myndighed, hvilket betyder, at alle oplysninger (herunder helbredsoplysninger) om en bestemt borger i kommunen vil kunne indgå i en samkøring efter bemyndigelsen. Den registrerede borger skal ikke informeres om sådanne tiltag.

b. Videreanvendelse – private virksomheder

For private dataansvarlige gælder oplysningspligten efter GDPR fuldt ud. Den registrerede skal således have information forud for en eventuel videreanvendelse af de indsamlede data til nye (ikke-uforenelige) formål.

I det omfang viderebehandlingen sker på en måde, der er *uforenelig* med indsamlingsformålet, forudsætter dette, at den registrerede forud for videreanvendelsen har givet samtykke hertil (eller der er andet behandlingsgrundlag). Gyldigheden af et sådant samtykke skal hvile på tilstrækkelig og specifik information herom.

En kommerciel udbyder af wearables kan videregive (evt mod betaling) indsamlede oplysninger til en ny dataansvarlig. Den (nye) dataansvarlige skal have et tilstrækkeligt behandlingsgrundlag og skal informere den registrerede om, at der behandles oplysninger.

Videregives oplysningerne med henblik på anvendelse direkte til *markeds-føringsformål*, kræver dette et udtrykkeligt samtykke fra den registrerede.

> Særligt i forhold til lægemidler gælder der i Danmark snævre regler for lovlig markedsføring. Blandt andet må der ikke over for offentligheden reklameres for receptpligtige lægemidler. Der er tillige fastsat danske regler om markedsføring af sundhedsydelser.
>
> Særligt i forhold til forsikringsselskaber er der ved tegning af forsikring i dansk ret forbud mod at bruge oplysninger, der kan belyse en persons arveanlæg og risiko for at udvikle eller pådrage sig sygdomme. Dette gælder dog ikke oplysninger om den pågældendes nuværende eller tidligere helbredstilstand. Det samme gælder for tegning af pensioner og for arbejdsgivere.

4.4.2.4 Anden behandling
GDPR har regler om berigtigelse og sletning. Forordningen lægger vægt på, at det skal være let for den registrerede at udøve disse rettigheder.

Den registrerede har ret til at få urigtige oplysninger om sig selv *berigtiget* af den dataansvarlige (eller fuldstændiggjort ufuldstændige oplysninger). Det samme gælder i forhold til eventuelle profiler, der er dannet om den registrerede.

GDPR indeholder desuden en ret til – under visse omstændigheder - at få *slettet* korrekte oplysninger (kaldet retten til at blive glemt). Der gælder ifølge forordningen visse undtagelser til denne ret.

Reglerne om berigtigelse og sletning har primært betydning i forhold til en privat udbyder af wearable. For offentlige myndigheder vil det være de offentligretlige regler, der regulerer berigtigelse og sletning. Dette indebærer, at data ikke kan kræves slettet, men at der ved klart faktuelt forkerte oplysninger tilføjes supplerende tekster. Når det gælder data i sundhedsvæsenets journaler reguleres dette af de sundhedsretlige journalføringsregler.

4.4.2.5 Indsigt
En registreret person har efter GDPR ret til indsigt i de data, der er registreret om den pågældende. Denne ret til indsigt gælder både for registrerede data hos en privat virksomhed og for registrerede data i sundhedsvæsenets elektroniske journaler. GDPR giver den registrerede ret til at få udleveret de oplysninger, den dataansvarlige behandler om vedkommende.

Hvis en wearable-tjeneste profilerer de registrerede brugere, har den registrerede krav på både at få udleveret de personoplysninger, der anvendes til at profilere, og information om den dannede profil, herunder de ”kategorier”, den registrerede er blevet placeret i.

4.4.3 Særligt om profilering

Databeskyttelsesretligt betragtes profilering som en særligt indgribende form for behandling. Baggrunden for dette er den store betydning, profilering kan have for en person. Profilering indebærer, at der foregår hel eller delvis automatisk opsamling og behandling af data om vedkommende med det formål at evaluere (analysere eller forudsige) bestemte personlige forhold (karakteristika eller adfærdsmønstre) med henblik på at placere vedkommende i en bestemt kategori eller gruppe.

Profilering kan dermed på forskellig måde indskrænke den registreredes frihed. Det kan være en følelse af overvågning, der medfører, at man (selv) afstår fra visse ting, eller det kan være en konsekvens af profileringen, at de valgmuligheder, der stilles til rådighed for én (fx fra forsikringsselskabers side), er reduceret. Dette er selvsagt især problematisk, hvis profileringen er fejlagtig (fx på baggrund af dårlig datakvalitet). Anvendes data fra wearables til profilering i fx (sygdoms)behandlingssammenhænge, kan det have store konsekvenser for patientsikkerheden, hvis de data, som opsamles gennem wearable, er mangelfulde eller forkerte. Et eksempel kan være, hvis wearable skal registrere patientens aktivitet, men patienten glemmer i perioder at anvende wearable, låner sin wearable ud til andre, eller blot tager det af under den ugentlige svømmetræning. Tilsvarende gælder, hvis profileringen sker ud fra urigtige eller ufuldstændige sundhedsfaglige forudsætninger, dvs der er fejl i de algoritmer, der danner profilen. Et simpelt eksempel kan være en programmeringsfejl, hvor en anbefaling om 4 timer ugentlig motion er blevet til 14 timer.

Det følger direkte af GDPR, at den registrerede skal informeres om profilering i det omfang, dette anvendes i forbindelse med (visse) automatiske afgørelser, se umiddelbart nedenfor. Også i andre situationer (af betydning for den registrerede) vil der antagelig være en oplysningspligt ved profilering begrundet i den dataansvarliges forpligtelser til gennemsigtig databehandling. Den registrerede vil dermed have mulighed for at udøve sine rettigheder efter forordningen (berigtigelse, sletning mv).

Automatiske afgørelser

Hvis profilering anvendes i sammenhæng med afgørelser, der *alene* baseres på automatiske beslutninger, og disse afgørelser har retsvirkning eller på tilsvarende vis betydeligt påvirker den registrerede, skal den registrerede ved indsamling af oplysninger *informeres* om forekomsten af automatiske afgørelser, herunder profilering. Den registrerede skal desuden have oplysninger om logikken heri samt betydningen og de forventede konsekvenser, som profileringen vil have for den registrerede. Anvender en sundhedsmyndighed profiler fra wearables, vil myndigheden som følge af denne oplysningspligt være forpligtet til at sikre sig viden om og indsigt i funktionaliteten af de teknologier, der anvendes.

Som nævnt ovenfor, har den registrerede – efter anmodning – ret til at få indsigt i og at få udleveret oplysninger fra en wearable, der profilerer. Dette gælder både de personoplysninger, der har været input, og information om den dannede profil og de ”kategorier”, den registrerede er blevet placeret i. Retten til at få berigtiget

urigtige oplysninger gælder både i forhold til de indsamlede data og de dannede profiler.

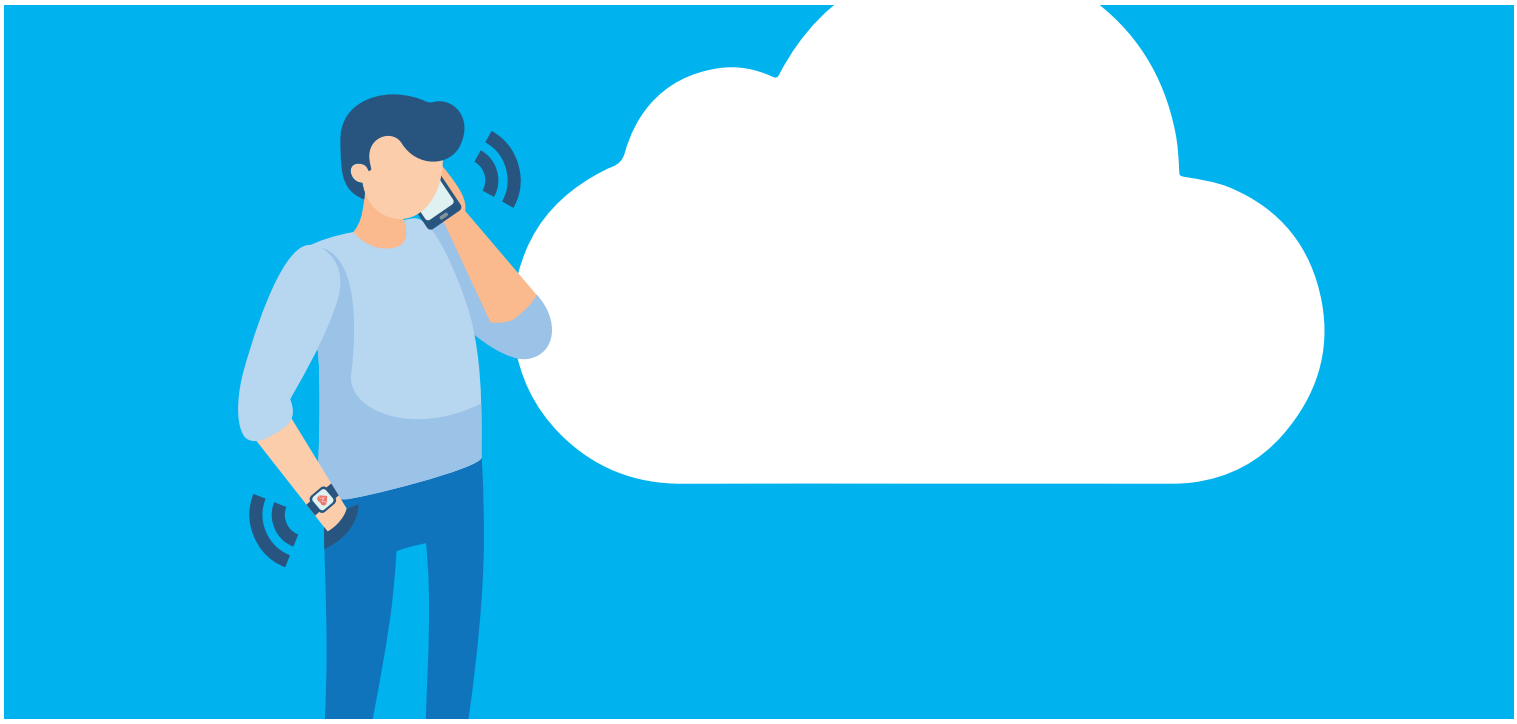
Ret til indsigelse

Det følger af GDPR, at en registreret har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk behandling, herunder profilering, hvis dette har retsvirkning for den registrerede eller på tilsvarende måde betydeligt påvirker den pågældende. Indgår der en menneskelig vurdering af beslutningsgrundlag eller udfald, vil det ikke være en automatisk afgørelse i forordningens forstand.

En beslutning om, at en patient kan tilbydes behandling eller lignende, kan efter omstændighederne være en afgørelse i GDPR's forstand. Retten til indsigelse gælder dog ikke i forhold til det offentlige sundhedsvæsen, da lægelige afgørelser i forordningens forstand er hjemlet i national ret. Denne undtagelse gælder imidlertid kun i det omfang, oplysningerne behandles med patientens samtykke. Er oplysningerne behandlet med hjemmel i forordningen uden samtykke, har patienten ret til indsigelse mod automatiske afgørelser (med mindre andet er fastsat i national ret).

I forhold til en privat udbyder af tjenester forbundet til wearables, vil den registrerede have ret til at gøre indsigelse. Følgen af berettiget indsigelse er, at profileringen og beslutningstagningen skal indstilles.

Uanset om der er mulighed for at gøre indsigelser eller ej, er det et krav, at der er indført passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser.



5. Hvordan kan personers data beskyttes

Data om personer opsamles på et utal af måder, hvoraf nogle giver anledning til visse udfordringer for privatheden, mens andre giver anledning til meget store problemer og kan føre til omfattende privatlivskrænkelser. Det har hidtil ikke nødvendigvis været de situationer, hvor privathedskrænkelserne er størst, som har givet anledning til mest debat, hvilket måske især skyldes, at de mest indgribende privathedskrænkelser foregår på måder, som de fleste ikke kan gennemskue og ikke har indblik i.

GDPR udgør i manges øjne verdens mest ambitiøse forsøg på at dæmme op for disse risici, men det står endnu tilbage at se, om det reelt vil være muligt at sikre overholdelsen af reglerne om kommercielle aktørers indsamling og videregivelse af data, som foregår i et stort omfang og på tværs af lande og jurisdiktioner. I det følgende beskrives nogle af disse udfordringer, og det leder frem til spørgsmålet, om reguleringen af brug af data hovedsageligt bør rette sig mod visse problematiske *anvendelser* af sundhedsdata fremfor mod *opsamling*, bearbejdning og videregivelse af dem.

Sundhedsdata opsamles i en meget bred vifte af situationer:

- direkte i sundhedsvæsenet eller hos behandlere,
- på wearables og andre devices enten i sundhedsvæsenets regi eller af private udbydere, og endelig
- data som opsamles ved at fx registrere personers besøg på webtjenester eller sociale medier, deres indkøb, motionsvaner, søgehistorik, omgangskreds, medlemskab af foreninger osv, som indirekte og sammenholdt med andre oplysninger kan sige noget om personens sundhedstilstand

Disse situationer svarer formentlig til en glidende skala i forhold til dataafgiverens indsigt i, og accept af, at hun/han afgiver sine data til bestemte formål. Fra sundhedsvæsenet, hvor data afgives bevidst, der orienteres om, hvad data vil blive anvendt til, og der er relativt snævre grænser for, hvad data kan bruges til efterfølgende. Over sundhedsapps og andre digitale tjenester, hvor data ofte afgives med et samtykke som betingelse for adgang til app eller tjeneste, og der gives en mere eller mindre udtømmende orientering om, hvad data videre vil blive anvendt til. Til visse digitale tjenester, som ulovligt opsamler data om borgeren uden tilladelse eller information.

Den sidste type dataopsamling er som nævnt ofte ulovlig, men formentlig vanskelig helt at forhindre. Der findes i dag ikke tekniske løsninger, som effektivt kan beskytte personer mod, at de digitale 'spor', de afsætter i cyberspace, kan registreres og bearbejdes mod deres vilje.

Data opsamlet i wearables eller andre digitale tjenester, vil hyppigt blive sammenstillet og anvendt til at udlede yderligere data, fx om personens sundhedstilstand. Det sker som nævnt ved, at firmaet anvender algoritmer til at sammenkøre data om personen fra mange kilder og udarbejde en personprofil. De fremanalyserede data må anses for særdeles personfølsomme, og så er de endda usikre pga tilblivelsesformen.

Predictive medicine indebærer ligeledes kombination af data om personer fra mange kilder, som bearbejdes mhp at kunne forudse risiko for fremtidig sygdom og angive forebyggelsestiltag.

Det er et problem, hvis indsamlingen foregår 'bagom ryggen' på personen, som derved ikke har kendskab til eventuelle personprofilers eksistens, og ikke har mulighed for at rette fejl i dem. Da kvaliteten af de anvendte data og de anvendte algoritmer ret oplagt må være svingende, er der rig mulighed for, at der vil være fejl i profilerne, som ikke opdages.

Men selv hvis der på baggrund af disse data vil kunne udledes korrekte forudsigelser om fremtidig sygdom, vil der være problemer forbundet med, at data er sammenkørt og bearbejdet uden borgerens vidende.

5.1 Grænser for privatlivsbeskyttelse

Som nævnt er det meget uigennemskueligt for de fleste mennesker, hvordan deres sundhedsdata opsamles og anvendes, fordi en stor del af opsamlingen foregår 'i cyberspace' og er usynlig for ikke-fagfolk. Derfor kan der være en tendens til, at opmærksomheden om indsamlingen populært sagt koncentrerer sig om de situationer, som er mest åbne og synlige, nemlig opsamlingen i sundhedsvæsenet. Her bekymrer mange sig – med rette – om, hvor mange data de afgiver, og hvad de bliver brugt til. Men der synes her at være et paradoks. Man kunne lidt provokerende

hævde, at vi samtidig meget ubekymret afgiver store mængder data til web-udbydere og tech-firmaer, oftest på baggrund af et meget tvivlsomt samtykke, og at denne afgivelse kan få langt mere vidtgående konsekvenser for vores frihed i et lidt større perspektiv.

I det følgende vil vi se på, hvor 'udsatte' danskernes sundhedsdata er for uønskede anvendelser i tre forskellige sammenhænge.

5.1.1 Sundhedsvæsenet opsamler og anvender data til bestemte formål

Når patienten kontakter sundhedsvæsenet, afgiver patienten data. I patientens undersøgelses- og behandlingsforløb indsamles yderligere data. Når sundheds-personer behandler alle disse data om patienten, kan det ske uden dennes samtykke, men patienten skal informeres om databehandlingen. Stort set alle data, der indsamles om patienten vedrørende dennes helbredssituation, betragtes og behandles som følsomme oplysninger.

Alle data om patienten samles i den elektroniske journal. De elektroniske systemer skal sikres, så der ikke sker uautoriseret adgang. Patienten har ret til indsigt i de data, der findes om den pågældende i den elektroniske patientjournal. Patienten har mulighed for at få tilført manglende oplysninger i journalen, eller evt at få det anført i journalen, hvis en oplysning er urigtig. I nogle systemer vil patienten desuden have adgang til logningsdata, og dermed mulighed for at følge med i, hvordan data anvendes.

5.1.2 Data opsamlet i sundhedsvæsenet til bestemte formål, men anvendt til andre formål

Sundhedsvæsenet kan have et ønske om at anvende indsamlede data til andre formål (end indsamlingsformålet). Man må her vurdere, om det nye formål er uforeneligt med det oprindelige formål med indsamlingen.

Sundhedsvæsenet kan frit anvende indsamlede data fra patientbehandlingen til andre (ikke uforenelige) formål. Hvad der er ikke-uforeneligt fortolkes bredt. En bremse vil dog være de barrierer, man lovgivningsmæssigt opsætter specifikt for sundhedsvæsenet. Det afgørende spørgsmål vil her være, hvor bredt – eller hvor snævert – man tolker sundhedspersonens tavshedspligt. Tavshedspligten har hidtil været tolket relativt restriktivt, idet man retligt har karakteriseret det som en videregivelse af data (og altså ikke en intern anvendelse), hvis data går fra fx en sygehusafdeling til den praktiserende læge. Med oprettelse af en digital infrastruktur på tværs af sundhedsvæsenet har man anlagt en mere bred fortolkning af tavshedspligten. Den retlige regulering har nu fokus på, hvornår det er berettiget at en sundhedsperson (på tværs af sundhedsvæsenet) indhenter oplysninger fra infrastrukturen, og man kan hævde, at patienten herved i højere grad får et fortrolighedsforhold til et "væsen" end til en konkret sundhedsperson. Efter GDPRs regler skal der som udgangspunkt informeres om nye formål inden for samme myndighed. Udgangspunktet kan dog være fraveget via en af

undtagelsesbestemmelserne i GDPR eller den danske databeskyttelseslov, herunder en bekendtgørelse udstedt i henhold til loven

Andre offentlige myndigheder kan have en interesse i at anvende sundhedsdata opsamlet i sundhedsvæsenet. Der er i forbindelse med forebyggelse ønske om at kunne sammenkøre data om personer fra forskellige myndigheder, fx sundhedsvæsenet, socialforvaltningen, politiet, forsyningstjenester mm for at forudsige hændelser, fx fremtidig sygdom eller (gen)indlæggelse, udpegning af familier med behov for støtte, risikogrupper ved kriminalitet, mm.

I hvilket omfang data kan overgå til anden offentlig myndighed, fx en kommunes socialforvaltning, afhænger af lovgivning om videregivelse af data indsamlet i patientbehandlingen. Det er således først og fremmest op til lovgiver, i hvilket omfang dette kan ske. Patienten skal som udgangspunkt orienteres efter GDPRs regler af de myndigheder, der modtager oplysningerne (den nye dataansvarlige). I det nævnte tilfælde vil kommunen være den nye dataansvarlige og dermed have pligt til at oplyse patienten om, at kommunen behandler data om patienten. Data kan anvendes på tværs af forskellige sektorer i kommunen, da en kommune vil blive anset som én myndighed. Data, som oprindeligt blev opsamlet i sundhedsvæsenet i patientbehandlingen, vil således kunne bruges til andre (ikke-uforenelige) formål i andre dele af den offentlige forvaltning. Ved bekendtgørelse (som nævnt ovenfor) kan data endvidere behandles også til uforenelige formål – og uden at den registrerede orienteres herom. Den registrerede har ret til indsigt i de oplysninger, der behandles om den pågældende, men dette forudsætter selvsagt viden om, at der behandles oplysninger.

Offentlige myndigheder er begrænset i deres handlinger af de offentligretlige principper for god forvaltningsudøvelse. Her kan nævnes specialitetsprincippet og forbuddet mod magtfordrejning, der sætter grænser for, hvilke formål en offentlig myndighed kan forfølge, pligten til at vurdere i hvert enkelt tilfælde, krav til forvaltningsmyndigheders forsvarlige vejledning mm.

5.1.3 Data opsamlet og anvendt af private firmaer

Data opsamles i vid udstrækning gennem forskellige former for devices, som er udviklet og udbudt af kommercielle firmaer. Det kan være opsamling af sundhedsdata fx via wearables, mobiltelefon eller via webtjenester eller sociale medier (se ovenfor). I modsætning til opsamling af data i sundhedsvæsenet vil en del adfærdsdata opsamlet af kommercielle firmaer ikke blive betragtet som følsomme oplysninger. Hvis data fx ”blot” er oplysninger om adfærd, spise- eller bevægemønstre eller lignende, vil det ikke blive betragtet som følsomme oplysninger, da de ikke opsamles med det formål at yde patientbehandling. Kobler man imidlertid alle disse enkeltinformationer sammen, kan det give et yderst følsomt billede af det enkelte menneske.

I Europa har man med GDPR søgt at opsætte beskyttelser mod, at personers data kan opsamles og anvendes til formål, de ikke ønsker. Som nævnt indledningsvist vil den

registrerede i nogle situationer være vidende om, at der opsamles information om den pågældende – mens det i andre situationer foregår "bagom ryggen" på personen.

5.1.3.1 Personen er vidende om opsamling og samtykker hertil
Hvis man ønsker at anvende en bestemt wearable, vil det typisk kræve, at man først accepterer at stille sine data til rådighed for den kommercielle udbyder. En betingelse for at anvende den pågældende wearable vil som regel være, at man giver sit samtykke til, at de data, der opsamles gennem denne wearable, må behandles af udbyder. Typisk vil dette samtykke række ud over behandling af de data, der er nødvendige for udbyder i forbindelse med aftalens indgåelse og drift af wearable for den enkelte bruger. Mange af disse samtykkebetingelser går således videre end det strengt nødvendige, fordi udbyderen dermed kan få en større værdi "frigivet" i form af data.

Der er flere problemer forbundet med afgivelse af samtykke som betingelse ved ibrugtagning af net-baserede services (wearables, apps mv). For det første er afgivelse af samtykke tidskrævende. De færreste læser vilkårene for brugen af apps, og hvad deres samtykke nærmere omfatter. Samtykke afgives i stedet rutinemæssigt. Anvendelse af samtykke som behandlingsgrundlag ved wearables kan for det andet være problematisk i de tilfælde, hvor anvendelsen af det pågældende wearable ikke opleves som (helt) frivilligt af den pågældende. Dertil kommer, at man i mange tilfælde først præsenteres for betingelserne for at anvende den pågældende wearable, når man har købt produktet. Man kan således ikke anvende det købte produkt, hvis man ikke accepterer de opstillede vilkår.

GDPR stiller krav til gyldigheden af et afgivet samtykke. Informationen skal være relativt kortfattet og forståelig, og det skal være tilstrækkeligt konkret beskrevet, hvad et samtykke omfatter. Det er tvivlsomt, om disse krav reelt overholdes og skaber den tilstræbte bevidsthed hos brugeren. Det kan være både vanskeligt, en langvarig proces og dyrt at få domstolene mv til at drage grænserne på dette område gennem sanktioner.

5.1.3.2. Personen er ikke vidende om opsamling
Det følger af GDPR, at i det omfang, der behandles data om en person, har den dataansvarlige en informationspligt over for den pågældende. Denne informationspligt over for den registrerede gælder både ved registrering af oplysninger og ved eventuel videreanvendelse af de indsamlede oplysninger til nye formål. Et samtykke fra den registrerede på baggrund af et (meget) bredt formuleret formål, vil kun i de færreste tilfælde kunne betragtes som et gyldigt samtykke til, at data anvendes til andre formål. Det samme gælder, når data videregives til en ny dataansvarlig. Det synes meget tvivlsomt, om denne informationspligt overholdes i den ånd, som synes at være tiltænkt. Der er næppe nogen tvivl om, at opsamling af data har et uendeligt meget større omfang, end den enkelte kan forestille sig.

GDPR stiller også krav om, at udbyder skal kunne aflevere alle registrerede data om en person på maskin-læsbar form. Dette kræver dog naturligvis, at personen er

klar over, at udbyderen ligger inde med data om personen, hvilket ofte ikke vil være tilfældet. Det ville dog formentlig være positivt for debatten, hvis flere gjorde brug af denne mulighed og dermed fik indblik i, hvad tech-firmaerne ligger inde med af data om dem.

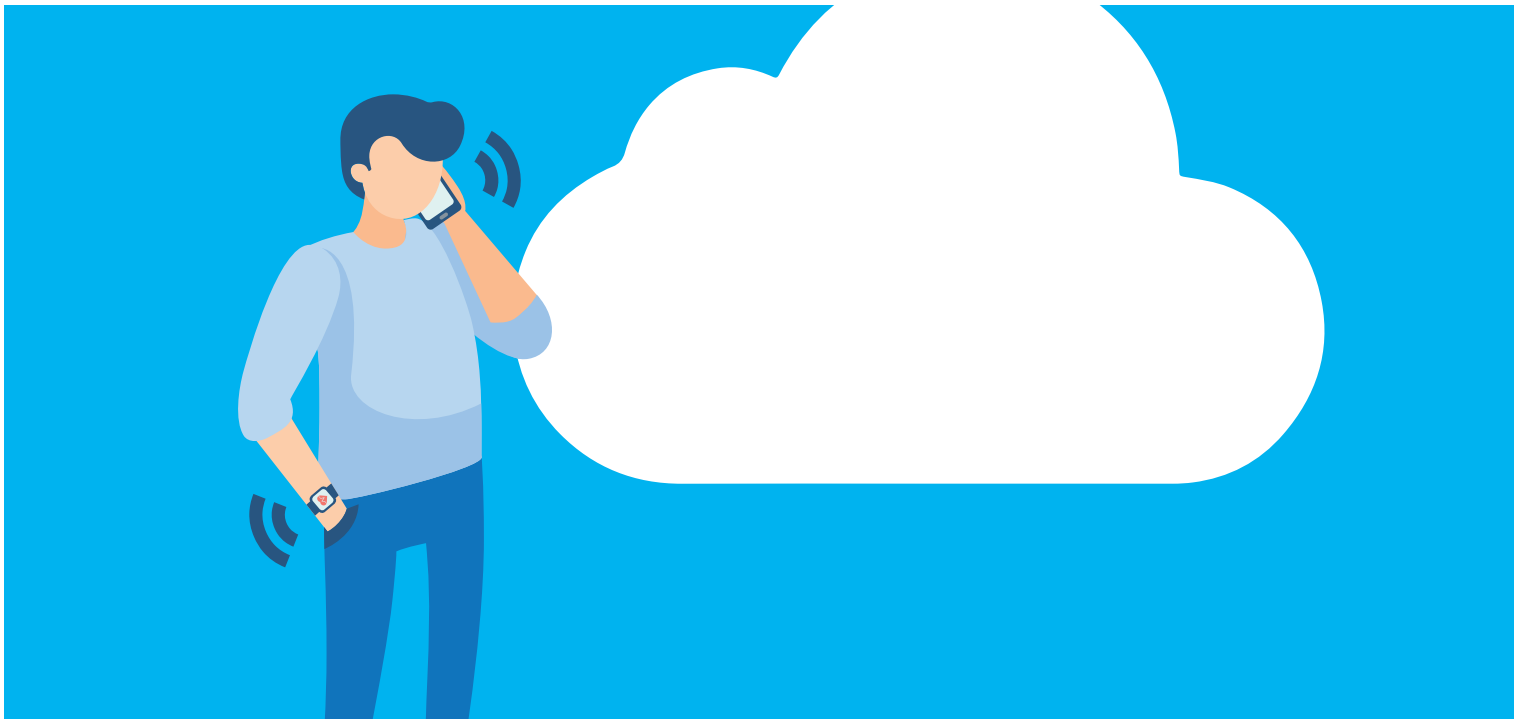
Men som nævnt lagres og anvendes megen data, uden at den registrerede er klar over det. Dermed har man næppe reelt mulighed for indsigt i disse data og dermed ikke mulighed for at berigtige eller supplere data, ej heller for at få slettet urigtige data. Der er dermed stor risiko for, at der dannes forkerte profiler, og at disse (urigtige) profiler kan give store ulemper for – og nogle tilfælde skade – den registrerede.

Som følge af GDPR og den opmærksomhed, forordningen har fået i forbindelse med dens ikrafttræden, popper der i højere grad end tidligere samtykkeerklæringer op, når man søger på websider og anvender forskellige devices. Det er selvfølgelig positivt, men man kan også frygte, at den stadigt øgende mængde af samtykkeerklæringer, man dagligt skal forholde sig til, yderligere vil trivialisere samtykket, fordi det ikke er muligt i hvert enkelt tilfælde at sætte sig ind i, hvad man samtykker til og hvordan ens data vil blive brugt.

5.2 Konklusion

Ovenstående tegner et billede af, at selv med de juridiske og tekniske sikkerheds-foranstaltninger, som findes, er der mange situationer, hvor personers sundhedsdata ikke er tilstrækkeligt beskyttede – og at disse situationer paradoksalt nok hoved-sageligt ligger uden for selve sundhedsvæsenet.

Hovedproblemet er her, at der af mange aktører indsamles data om alle borgere såvel med som uden samtykke, og at disse data sammenkøres med andre data for at skabe personprofiler ved hjælpe af algoritmer. De udledte, personfølsomme data videregives og sælges i et omfang, der som oftest er helt ukendt for borgeren. Disse processer sker meget ofte, uden at den registrerede reelt har viden om det, og det kan forekomme at være nærmest umuligt at håndhæve de begrænsninger, som sættes af GDPR for at modgå problemet. Hertil kommer risikoen for fejlkilder undervejs, og uden reel viden om, hvordan de indsamlede data anvendes, har den profilerede person heller ikke mulighed for at opdage, hvis fejlagtige informationer om personen cirkulerer.



6. Stillingtagen til anvendelse af datagenererede sundhedsdata

Med de følgende anbefalinger ønsker Rådet at brede debatten om anvendelse af sundhedsdata, som er opsamlet via wearables, ud, så den adresserer flere situationer, hvor der kan være krænkelser af personers kontrol over egne sundhedsdata. Rådet finder, at det er væsentligt at adressere, at personfølsomme sundhedsoplysninger ikke kun genereres og anvendes i sundhedsvæsenet. Den digitale udvikling giver mulighed for, at mange aktører kan opsamle data om personer og ud fra dem analysere sig frem til mere eller mindre pålidelige oplysninger om deres sundhed og levevis. Og disse informationer kan anvendes på måder, som giver anledning til store etiske problemer. Det ville nok være naivt at forestille sig, at denne *opsamling* helt kan forhindres, selvom der kan gøres meget via lovgivning for at begrænse den. Rådet anbefaler derfor også, at der ses på muligheden for at begrænse visse *anvendelser* af de indsamlede og fremanalyserede data.

Sundhedsoplysninger er særdeles personfølsomme, og der er som nævnt stor international enighed om, at sådanne oplysninger bør være beskyttede som private. Men som ovenfor nævnt ses personers sundhedsdata i en række sammenhænge ikke at være tilstrækkeligt beskyttede – og disse situationer ligger paradoksalt nok hovedsageligt uden for selve sundhedsvæsenet. Trods de skærpede krav til samtykkets omfang, som fremgår af GDPR, er der stadig reelt tale om, at alle personer dagligt giver tilsagn om, at firmaer kan anvende deres data, uden at gøre sig klart, i hvor høj grad disse anvendes til at udlede personfølsomme oplysninger, såsom sundhedsoplysninger, om dem. Disse oplysninger bliver allerede videregivet og solgt, og de vil fremover potentielt kunne anvendes til formål, personen, de stammer fra, ikke ønsker, eller som direkte kan skade personen.

Som beskrevet er det væsentligste etiske problem ved, at private, personfølsomme data bliver tilgængelige for andre end dem, personen ønsker skal have adgang til dem, at det reducerer vedkommendes frihed til at leve efter personens egne værdier og ønsker til et godt liv. Andre får adgang til at misbillige og søge at påvirke personens valg.

Men først og fremmest opstår der etiske problemer, hvis adgang til private data om personer giver virksomheder og offentlige myndigheder mulighed for at gribe ind i personernes liv på kontrollerende vis. Det kunne være ved, at data om en persons levevis blev anvendt til at forsøge at presse vedkommende til at leve efter et ideal om sundhed i alle situationer, også hvor en sådan levevis kommer i konflikt med personens egen opfattelse af det gode liv. Såvel sundhedsvæsenet som andre myndigheder, samt forsikringsselskaber, arbejdsgivere, kreditinstitutter m.fl. kunne potentielt være interesserede i at støtte borgerne i, at de skal leve maximalt sundt.

Frihedskrænkelsen bliver mere alvorlig, hvis de gode råd om at ændre levevis i sundere retning skulle ende med at blive til krav i den forstand, at manglende efterlevelse kunne føre til, at vedkommende nedprioriteres i forhold til visse ydelser i sundhedsvæsenet. Eller hvis fremanalyserede data om disposition for fremtidig sygdom bruges til at fratage eller forringe personens adgang til fx forsikringer eller jobs. Det er væsentligt at være opmærksom på disse farer, når wearables og big data gør deres indtog i sundhedsvæsenet og i andre områder af vores liv.

Sundhedsdata kan sige meget om det enkelte menneske, og i de forkerte hænder vil de kunne anvendes til diskrimination og dermed til at begrænse personers grundlæggende friheder. I det følgende vil rådet derfor komme med anbefalinger på 4 områder, hvor brugen af wearables og opsamling af big data bør reguleres. Det er områderne: *Behandling, opsamling, forebyggelse* og *anvendelse*. Også indenfor *forskningen* kan data fra wearables få stor betydning, men dette område har rådet valgt at vente med at tage op til den kommende redegørelse om brug af kunstig intelligens i sundhedsvæsenet.

6.1 Opsamling og anvendelse af data (herunder data genereret fra kommercielle apps)

Wearables og de data, de indsamler, har store positive potentialer. De vil spille en væsentlig rolle i den omstilling af sundhedsvæsenet, vi står overfor. De adfærdsdata, som kan indsamles vha wearables, vil være væsentlige for udvikling af både person-tilpassede behandlinger og af kvalitativt nye behandlinger, og de vil åbne for, at flere behandlinger kan ske udenfor sygehusene, fordi patienten løbende kan opsamle og indsende data til behandlerne. Derudover ser data fra wearables, evt kombineret med andre data om patienten, ud til at komme til at spille en positiv rolle i forebyggelsen, hvor de kan være en hjælp til patienter, som ønsker at undgå fremtidig sygdom.

Samtidig er udfordringerne for anvendelse af persondata i sundhedsvæsenet velkendte, og de har været debatteret en del i de senere år. Sundhedsoplysninger

er personfølsomme, og i erkendelse af dette er der i sundhedsvæsenet udviklet omfattende sikkerhedssystemer, som har til formål at sikre en høj grad af beskyttelse af de data, der opbevares i sundhedsvæsenet. Med data fra wearables og fra andre digitale kilder vokser mængden af personfølsomme data på en måde, som giver anledning til nye dilemmaer.

6.1.1. Anbefaling 1. Behandling: Bør sundhedsvæsenet anvende apps udviklet af kommercielle udbydere?

Adfærdsdata fra wearables, fx motions- og sundhedsapps, som måler motion, søvn, kost- og medicinindtag, stressniveau, psykiske tilstande mmm, vil kunne udgøre væsentlige supplementer til de data, sundhedsvæsenet allerede ligger inde med. Dermed kan de komme til at udgøre en væsentlig forudsætning for vellykket behandling. Imidlertid kan apps være kostbare at udvikle, og behandlere vil i mange tilfælde med fordel kunne anbefale eller foreslå patienten at anvende en egnet app, som er udviklet af kommercielle udbydere.

Hvis der er tale om en gratis app, som downloades mod, at patienten samtykker i, at udbyderen må anvende personens data til videre bearbejdning og salg, opstår imidlertid et problem. Behandleren vil da i realiteten opfordre patienten til at afgive sine data til en udbyder, som kan anvende vedkommendes data til at udlede og videregive personfølsomme oplysninger om personen. I hvilket omfang, behandleren pådrager sig et ansvar for app-udbyderens videre anvendelse af data, afhænger dels af karakteren af relationen mellem behandler og den private udbyder (eller den manglende relation), og dels udviklingen i retspraksis (afgørelser ved domstolene). På nuværende tidspunkt er det vanskeligt at afgrænse et sådant eventuelt (med)ansvar mere præcist.

I nogle tilfælde vil patienten måske på eget initiativ have registreret data på en wearable og tilbyde at dele disse data med behandleren. Her kan opstå spørgsmål om app'ens kvalitet, idet en meget stor del af apps ikke er godkendt til medicinsk brug; de er ikke standardiserede og kvalitetstestede, det kan være vanskeligt for behandleren at vurdere, om forskellige apps leverer data af tilstrækkelig kvalitet, da der er mange apps på markedet. Under alle omstændigheder er det vigtigt, at kvaliteten af data er kendt – og at kvaliteten er gemt sammen med data, så andre efterfølgende ved, hvilken kvalitet målingen er foregået med.[65]

Det har været foreslået at udvikle en certificeringsordning for sundhedsapps, som dels oplyser brugeren om kvaliteten af app'en og hvem der har udviklet den, dels om hvorvidt den opsamler informationer om personen og giver dem videre til 3. part. Dette kunne være en stor hjælp for såvel forbrugere som sundhedsvæsen.

Endelig er der problemet med ejerskab til de data, wearables udviklet af tredjeparter genererer. Hvis patienten samtykker i, at data må lagres og anvendes af udbyderen, har vedkommende i princippet frasagt sig den fulde kontrol over disse data.

65 Det skal tilføjes, at hvis patienten selv måler fx motion eller kost med ikke-digitale instrumenter, vil der naturligvis også være risiko for fejl i data.

Medlemmerne af etisk råd er delt i deres anbefalinger til brug af wearables i sundhedsvæsenet:

Nogle medlemmer (Poul Jaszczak, Lise von Seelen, Karen Stæhr og Signild Vallgårda) anbefaler, at sundhedsvæsenet kun bør anvende egne apps, dvs apps udviklet i sundhedsvæsenet, til opsamling af sundhedsdata om patienterne. De indsamlede data bør overføres til sundhedsvæsenets beskyttede platforme og behandles fortroligt på linje med andre former for journaldata**.**

Begrundelsen for anbefalingen er, at man hermed både sikrer kvaliteten af de anvendte apps og forhindrer, at patientens data havner på kommercielle udbyderes platforme. Her vil disse data kunne anvendes på måder, patienten ikke ønsker, eller som direkte skader vedkommende.

Sundhedsvæsenet bør dog kunne indgå partnerskaber med kommercielle udbydere om at udvikle apps, som de kan udlevere til patienterne. Derved sikres, at disse apps lever op til behandlernes krav til kvalitet, men nok så vigtigt bør partnerskabet indebære, at de registrerede data ikke må lagres på udbyderens server, men overføres til sundhedsvæsenets beskyttede platforme.

Andre medlemmer (Morten Bangsgaard, Anne-Marie Axø Gerdes, Herdis Hansen, Mia Amalie Holstein, Henrik Gade Jensen, Bolette Marie Kjær Jørgensen, Henrik Nannestad Jørgensen, Rune Engelbreth Larsen, Eva Secher Mathiasen, Rico Mathiesen, Jacob Giehm Mikkelsen og Leif Vestergaard Pedersen) anbefaler, at sundhedsvæsenet også bør tage imod data, som patienten selv indsamler på en wearable leveret af kommercielle udbydere.

Det er dog en forudsætning, at behandleren har mulighed for at sikre kvaliteten af de data, som genereres af den pågældende wearable. Derfor anbefaler disse medlemmer, at alle apps og enheder, der anvendes i sundhedsvæsenet, som minimum bør sikkerhedsgodkendes efter standarder svarende til det amerikanske FDA, men det ville være ønskeligt at udvikle en europæisk certificeringsordning. Denne bør, foruden den nævnte kvalitetsgodkendelse, omfatte information om, hvorvidt udbyderen opsamler flere informationer om personen end nødvendigt. Samt om de sletter oplysningerne efter brug, eller om de tværtimod giver dem videre til 3. part. Desuden bør det være et krav, at det er muligt at lagre de indsamlede data på sundhedsvæsenet platforme udover på udbyderens platform. Sundhedsvæsenet bør være opmærksomme på, i hvilket omfang sundhedspersoners anbefaling af at anvende bestemte kommercielle apps kan give et medansvar for den videre brug af patienternes data**.**

I en ideel verden ville det være ønskeligt, at sundhedsvæsenet selv havde mulighed for at udvikle tilstrækkeligt mange, specialiserede apps, men det er urealistisk. Udviklingen taget i betragtning anerkender rådet, at dette ikke er muligt grundet manglende ressourcer og kompetencer i det offentlige. Hvis der findes kommercielt

udviklede apps, som forsvarligt vil kunne opsamle de nødvendige data, bør de anvendes på de angivne betingelser, fordi man herved vil kunne opnå store fordele for behandling både af den enkelte patient og af fremtidige patienter.

Anbefalingen kan siges at være pragmatisk i den forstand, at den også baseres på den vurdering, at de data om patienten, som kommer fra den pågældende wearable, kun udgør en meget lille del af de data, som under alle omstændigheder opsamles om vedkommende og bearbejdes hver dag. At forsøge at forhindre denne *opsamling* er formentlig under alle omstændigheder illusorisk, hvorfor kræfterne bør koncentreres om at forhindre, at data senere *anvendes* til skade for patienten. Dette bør gøres ved at forbyde visse anvendelser af personprofiler mm, hvilket behandles i anbefaling 2 og 4.

6.1.2 Anbefaling 2. Opsamling: Bør der eksistere et alternativ til at betale med sine data?

Data opsamlet fra wearables eller andre digitale tjenester er i en række sammenhænge ikke tilstrækkeligt beskyttede. Disse data sammenkøres vha algoritmer med data fra andre kilder til personprofiler, som bla indeholder oplysninger om personens sundhedstilstand. Disse fremanalyserede sundhedsdata må anses for særdeles personfølsomme, og de er endvidere usikre pga tilblivelsesformen.

En stor del af problemet er her traditionen for, at sundhedsapps og digitale tjenester stilles gratis til rådighed mod, at brugeren giver sit samtykke til, at udbyderen må anvende vedkommendes data til forskellige formål. Trods de skærpede krav til samtykkets omfang, som fremgår af GDPR, er der stadig reelt tale om, at alle personer dagligt giver sådanne samtykker uden at gøre sig klart, i hvor høj grad disse fører til, at der udledes personfølsomme oplysninger, såsom sundhedsoplysninger, om dem.

De fleste erkender, at der er store problemer forbundet med disse elektroniske samtykker. Som nævnt viser forskning, at en typisk amerikansk internetbruger skulle bruge 40 min om dagen på faktisk at læse alle de betingelser, de samtykker til, og det er nok de færreste, som gør det. GDPRs indførelse har betydet en stor vækst i antallet af situationer, hvor den almindelige borger giver samtykke, hvilket, trods den gode intention, formentlig bidrager til, at aftalerne reelt ikke læses. Som systemet fungerer, er belønningen ved at afgive samtykket håndgribelig; det giver direkte adgang til app eller webtjeneste. Derimod er skaden i form af, at personfølsomme data genereres og havner i de forkerte hænder, uklar og ligger ude i fremtiden. De fleste oplever, at de giver samtykke til brug af en tilsyneladende triviel oplysning, som fx hvor langt og hvor hurtigt de løber. At deres løbedata samkøres med andre oplysninger om dem og bruges til at udlede meget personfølsomme data, fx om sygdomsdispositioner, er meget vanskeligt at gennemskue eller forstå.

Af disse grunde finder rådet ikke, der ligger et reelt, informeret samtykke til grund for de algoritmegenererede sundhedsoplysninger om enkeltpersoner, som videregives og sælges.

Nogle medlemmer (Morten Bangsgaard, Anne-Marie Axø Gerdes, Herdis Hansen, Mia Amalie Holstein, Poul Jaszczak, Bolette Marie Kjær Jørgensen, Henrik Nannestad Jørgensen, Rune Engelbreth Larsen, Eva Secher Mathiasen, Rico Mathiesen, Jacob Giehm Mikkelsen, Leif Vestergaard Pedersen, Lise von Seelen, Karen Stæhr og Signild Vallgårda) anbefaler på den baggrund, at der bør tages et opgør med det gratis-princip, som betyder, at apps og andre tjenester stilles gratis til rådighed mod, at udbyderen får adgang til borgeres data. Det bør som minimum altid være muligt for borgeren at vælge at betale et beløb for at få adgang til app'en mod, at udbyderen ikke får ret til at anvende vedkommendes data til andre formål.

Medlemmerne anbefaler derfor**,** at det aldrig må være en betingelse for at få adgang til en app eller webtjeneste, at man accepterer, at udbyderen opsamler og anvender ens data. Man må ikke nægtes adgang til en app eller en hjemmeside pga manglende samtykke, og brugeren skal oplyses om, at samtykke ikke er en betingelse for at få adgang. I stedet bør det være muligt at betale et beløb fremfor at betale ved at stille sine data til rådighed for videre bearbejdning. Samtidig bør der sættes massivt ind på at informere befolkningen om den omfattende profilering, som foregår, og om de reelle omkostninger ved at afgive samtykker til opsamling af personlige data.

Begrundelsen er, at medlemmerne finder, at den nuværende opsamling og profilering af identificerbare personer, som bla anvendes til at fremanalysere mere eller mindre korrekte data om vedkommendes helbred og sygdomsdispositioner, udgør et meget alvorligt problem. Som nævnt hører privatlivets fred til blandt menneskerettighederne, og respekten for privatlivet beskytter væsentlige værdier og er fundamental for såvel personlig frihed som for relationer mellem personer og myndigheder og mellem personer indbyrdes. At væsentlige personfølsomme informationer fremanalyseres og sættes til salg uden vores vidende, udgør et meget væsentligt anslag mod retten til privatliv.

Andre medlemmer (Henrik Gade Jensen) anbefaler ikke tiltag rettet mod opsamling af data, da de ikke finder, opsamlingen i sig selv er et problem. Opsamlingen vedrører ofte ganske trivielle informationer, som fx motionsvaner eller andet, og de anvendes hovedsagligt til at markedsføre relaterede produkter som fx løbeudstyr. Her er ikke tale om personfølsomme oplysninger, og der er ikke noget galt i, at personer samtykker til den type brug af deres data. GDPR giver nogle sikringer i forhold til brede samtykker og videregivelse af data, som naturligvis skal have tid til at virke, men medlemmerne finder ikke, der er behov for yderligere lovgivning i forhold til samtykke.

Begrundelsen for anbefalingen er til dels pragmatisk, idet medlemmet konstaterer, at der allerede er indsamlet og genereret så mange persondata om os alle, at det vil være naivt at forestille sig, at denne udvikling kan rulles tilbage. En del af databearbejdningen sker i andre lande, og er vanskelig at adressere med europæisk regulering. Det er derfor nødvendigt at tilpasse sig denne nye virkelighed og gennemtænke, hvornår der faktisk er tale om, at brug af data begrænser personers frihed og handlemuligheder.

Medlemmerne finder her, at det ikke er opsamlingen af data eller profileringen i sig selv, som begrænser personers frihed. En del anvendelser af persondata, fx når data anvendes til at målrette reklamer eller indhold på hjemmesider til den specifikke person, begrænser ikke personens valgmuligheder og frihed. Kræfterne bør derfor anvendes på at regulere de *anvendelser* af personprofiler, som faktisk kan medføre en frihedsbegrænsning, fordi adgang til de private data tillader virksomheder, offentlige myndigheder eller andre at gribe ind i personernes liv på kontrollerende vis. Denne type anvendelser bør derfor reguleres, jf nedenfor.

6.1.3 Anbefaling 3. Forebyggelse: Bør sundhedsvæsenet samkøre borgernes data, opsamlet med wearables, med data fra forskellige forvaltninger mhp forebyggende tiltag?

Data opsamlet med wearables kan, sammen med andre data om personer, indgå i såkaldt *predictive medicine,* hvor målet er at holde borgerne sunde længst muligt. Man forsker i at udvikle intelligente systemer, som kan forebygge sygdomme og akut-indlæggelser ved at samkøre data om borgere på tværs af offentlige sektorer såsom sundhedsvæsen, socialforvaltning, politi, skat, forsyningsvirksomheder m.fl. Her kunne også indgå data om borgernes daglige liv fra wearables som fx registrerede motion, kost, søvn, socialt liv mm.

Her er altså ikke tale om samkøring af anonymiserede data fra grupper af personer for at forudsige tegn på fremtidige sygdomsmønstre i befolkningen. Der er derimod tale om samkøring af data om identificerbare borgere i håb om, at sådanne data vil kunne give et mere fuldstændigt billede af personen og vedkommendes risici for fremtidig sygdom.

Disse datakørsler kan potentielt ske uden patientens/borgerens samtykke eller vidende, og hvis de peger på uheldige udviklinger, vil de kunne resultere i henvendelse til borgeren. Det kunne være med tilbud om hjælp til livsstilsændringer – forudsat at man har viden om effektive metoder til at opnå sådanne – mhp at forebygge opståen eller forværring af sygdom. Det kunne også være med tilbud om videre undersøgelser. Det kunne også handle om at undersøge arbejdsmiljøet eller andre forhold i personens omgivelser, som kunne ændres i mere sundhedsgavnlig retning.

Det Etiske Råd anbefaler, at data fra wearables kun bør kunne samkøres med data fra andre myndigheder mhp sygdomsforebyggelse, hvis følgende forhold sikres:

Sikkerhed: Man bør alene kombinere data fra forskellige myndigheder med sygdomsforebyggelse – i bred forstand – for øje, og det bør være en forudsætning, at der er tale om effektiv sygdomsforebyggelse. Data bør kun deles mellem relevante myndigheder, og der bør være vandtætte skotter til andre formål.

Borgerne bør orienteres om, hvor de fremanalyserede data vil blive opbevaret; det kunne fx være i det planlagte nationale patientoverblik, som efter planen kan tilgås af patienten via sundhed.dk.

Information og samtykke: Inden der sker samkørsel af data fra wearables og andre data fra sundhedsvæsenet med data fra andre sektorer mhp forebyggelse, bør den relevante myndighed orientere alle involverede borgerne om deres planer. Her bør alle borgere have mulighed for at fravælge at deltage.

Nogle af medlemmerne (Mia Amalie Holstein, Bolette Marie Kjær Jørgensen, Lise von Seelen og Karen Stæhr) finder dog, at det ikke er tilstrækkeligt, at borgeren gives mulighed for aktivt at fravælge at deltage i programmet (opt-out). Disse medlemmer finder ikke, at samkørslen kan fortsætte uden et udtrykkeligt samtykke fra borgeren.

Retten til at vide eller til ikke-viden om fremtidig sygdom: Rådet anerkender, at der i forhold til datasamkørsler, som potentielt kan forudse fremtidige sygdomme, vil gøre sig et dilemma gældende i forhold til, om fundet skal videregives til personen. Det skyldes, at nogle mennesker foretrækker at leve i uvidenhed om fremtidige sygdomsdispositioner, mens andre vil ønske at få oplysningen, især hvis den giver mulighed for at forebygge, at sygdommen opstår.[66]

For at imødekomme såvel de, der ønsker at kende til risici for fremtidig sygdom, som de, der vil anse en sådan viden for belastende, bør borgerne på forhånd have mulighed for at til- eller framelde sig at modtage henvendelser, hvis dataanalyser viser en risiko for en fremtidig sygdom. Der bør også være mulighed for at vælge kun at modtage henvendelser, hvis der påvises betydelig risiko for, at borgeren udvikler en sygdom, som kan forebygges, eller hvor der er betydelig effekt på levetid eller livskvalitet ved at starte behandling tidligt.

Respekt for borgerens frihed til valg af livsstil: Såfremt borgeren vælger at modtage henvendelser med råd om ændring af levevis, som kan have en gavnlig helbredsmæssige effekt, mener Det Etiske Råd, at det er væsentligt, at rådene udelukkende bør have karakter af tilbud.

Som tidligere nævnt kan der være mange grunde til, at en person vælger at leve usundt på nogle områder. Henvendelser baserede på data fra wearables samkørt med data fra andre kilder vil næsten uvægerligt have karakter af forsøg på påvirkning af personers adfærd, hvilket er med til at forstærke forestillingen om, at adfærden er den vigtigste årsag til sygdom og dermed, at sygdom er den enkeltes ansvar/skyld.

Henvendelsen bør ikke have karakter af pres mod borgeren for at leve efter bestemte sundhedsråd og dermed begrænse personens frihed. Borgeren bør tværtimod have sin frihed til at vælge ikke at følge dem, og dette bør ikke være forbundet med sanktioner i form af nedprioritering af dem i behandlingskøen eller andet.

66 Såvel retten til at kende alle oplysninger, som er indsamlet om personens helbred, som retten til respekt for enkeltpersoners ønske om ikke at få kendskab til sådanne oplysninger fremgår af Europarådets konvention af 4. april 1997 om menneskerettigheder og biomedicin, artikel 10 stk 2.

6.1.4 Anbefaling 4. Anvendelse af udledte sundhedsdata som del af beslutningsgrundlaget eksempelvis hos forsikringsselskaber og arbejdsgivere

Blandt de områder, hvor nogle vil mene, at videregivelse af personfølsomme sundhedsdata fra wearables eller personprofiler vil kunne skade den, oplysningerne vedrører, er forsikringer og ansættelser. Hvis data fra wearables samkøres med andre digitale data, som er afgivet eller opsamlet om en person, er det muligt at anvende algoritmer til at profilere personer, herunder at fremkomme med mere eller mindre pålidelige antagelser om nuværende eller fremtidig sygdom hos personen. Hvis forsikringsselskaber eller arbejdsgivere på den baggrund vælger at forringe personens forsikringsvilkår eller forbigå vedkommende på arbejdsmarkedet, vil sådanne sundhedsdata kunne anvendes til skade for personen.

Nogle vil mene, det er en fordel for individer at kunne vælge at dele nogle af deres sundhedsdata med disse selskaber og dermed kunne påvirke opfattelsen af deres sundhedsstatus mhp at blive ansat eller optaget i forsikringsselskabet trods deres eventuelle sygdom, eller påvirke størrelsen på deres præmie ud fra, hvad de koster selskabet.

Uanset om man mener, forsikringsselskaber bør kunne differentiere forsikringsbetingelser i forhold til risici for fremtidig sygdom, er det centralt, at man kun baserer sig på sikre og pålidelige data: for at data skal kunne danne grundlag for fastlæggelse af forsikringsvilkår eller ansættelser, er det væsentligt, at der er tale om pålidelige data med minimal usikkerhed. Ellers kan disse for hver enkelt meget vigtige beslutninger blive taget på et forkert grundlag.

Hvis en sygdomsforudsigelse er fremkommet ved, at en algoritme har beregnet den ud fra forskellige data opsamlet fra såvel wearables som mange andre digitale kilder, vil disse kunne være behæftet med stor usikkerhed. Den nuværende erfaring med algoritmegenererede sundhedsdata og forudsigelser om fremtidig sygdom er kort, og ofte er de ikke udført efter videnskabelige standarder eller i videnskabeligt regi. Derfor er det problematisk, at der ikke er åbenhed om, hvordan forudsigelserne bliver fremanalyseret og hvilken evidens, de evt baserer sig på.

Der er allerede mange eksempler på, at fx forsikringsselskaber ønsker at anvende digitale sundhedsdata til at udvælge de bedste liv og give dem fordele fremfor de kunder, som har mindre attraktive motions- eller sundhedsdata. Arbejdsgivere kan abonnere på Falck Healthcares programmer, som udstyrer medarbejderne med appen Howdy, der registrerer sundhedsdata for at forebygge stress og sygdom.

Nogle medlemmer (Morten Bangsgaard, Anne-Marie Axø Gerdes, Herdis Hansen, Poul Jaszczak, Henrik Gade Jensen, Bolette Marie Kjær Jørgensen, Henrik Nannestad Jørgensen, Rune Engelbreth Larsen, Eva Secher Mathiasen, Rico Mathiesen, Jacob Giehm Mikkelse, Leif Vestergaard Pedersen, Lise von Seelen, Karen Stæhr og Signild Vallgårda) anbefaler**,** at lovgiver forpligter sig til at sikre, at der laves forpligtende rammesætning og regler for anvendelse af de indsamlede data.

Disse medlemmer anbefaler, at hverken forsikringsselskaber eller arbejdsgivere bør kunne anvende wearables-opsamlede eller algoritmegenererede sundheds-oplysninger til at fastlægge individers forsikringsvilkår, eller som grundlag for at ansætte eller afskedige. Medlemmerne lægger vægt på følgende argumenter:

Usikre data: Forudsigelser om fremtidig sygdom vil altid være behæftet med stor usikkerhed; der er under alle omstændigheder tale om sandsynligheder, ikke om vished for fremtidig sygdom. Hverken oplyste data om motion og kost, eller udledte data i personprofiler, siger noget sikkert om, hvorvidt en person vil udvikle sygdom i fremtiden. Sund levevis er ingen garanti for ikke at udvikle sygdom, og fremanalyserede sygdomsdispositioner angiver heller ikke sikkerhed for at udvikle sygdomme. En person vil altså kunne få forringede forsikringsvilkår eller blive forbigået jobmæssigt, på basis af risiko for sygdom, som aldrig kommer til at bryde ud, og som ikke vil udløse forsikringsydelser eller udgøre en konkret forhindring for at udøve et job.

I tilfældet fremanalyserede digitale sundhedsdata er der endda tale om endnu en usikkerhedsfaktor, for som tidligere nævnt kan der både være usikkerhed om kvaliteten af de data, som opsamles, og om de algoritmer, som anvendes til at generere forudsigelser om sygdomme på baggrund af disse data.

Rammer de svagest stillede: En person, som i forvejen er stillet ringere pga dårlige helbredsperspektiver, bør ikke straffes yderligere ved derudover at blive diskrimineret på vigtige områder som forsikring og arbejde. Såvel forsikrings- som arbejdsområdet bør i videst muligt omfang baseres på et solidarisk princip, hvor alle så at sige yder efter evne og nyder efter behov, og hvor det er vigtigt at tage hånd om de svagest stillede. At lægge risiko for fremtidig sygdom til grund kan desuden forekomme uhensigtsmæssigt, for ingen er uden en risiko for sygdom. Hvis vi undersøges tilstrækkelig grundigt ved fx genomundersøgelse, vil vi alle have genvarianter, som potentielt kan medføre sygdom, således at vi alle kan opfattes som at være præ-patienter med risiko for sygeliggørelse og diskrimination.

Man kan anføre, at de sygdomsdispositioner, som kan udledes på baggrund af digitale data, reflekterer personens adfærd, som vedkommende selv har indflydelse på. Men den antagelse anser medlemmerne for forsimplet. Som nævnt kan der være mange grunde til, at en person ikke lever optimalt sundt, men en årsag kan være, at det er vanskeligt at bryde med de normer, man er vokset op med. Der er en påviselig social slagside i, hvem der lever sundt, og hvem der ikke gør. At lægge sund levevis til grund for udmåling af forsikringspræmier, ansættelser mm vil derfor ende med at blive en straf af de dårligst stillede, og vil derfor i dette perspektiv være uretfærdigt.

Frihed til at leve efter egne værdier: Medlemmerne finder desuden, at det ville udgøre en uacceptabel indblanding i folks frihed til at vælge, hvordan de vil leve, hvis der blev indført økonomiske incitamenter til at vælge en bestemt levevis.

Uden anbefaling

Et medlem (Mia Amalie Holstein) ønsker at udtrykke sin bekymring over visse forsikringsselskaber eller arbejdsgiveres anvendelse af fremanalyserede sundhedsdata i visse situationer. Medlemmet finder det dog ikke principielt problematisk, hvis forsikringsselskaber og arbejdsgivere med borgerens tilladelse anvender data fra wearables såvel som algoritmegenererede sundhedsdata, så længe denne type data anvendes til den enkeltes fordel. Fx kan det være en fordel for en kroniker at redegøre for sundhedsstatus og livsstil med henblik på at øge sandsynligheden for at blive ansat eller forsikret.

Usikre data: Medlemmet deler dog bekymringen for, at algoritmegenererede sundhedsprofiler på basis af data fra wearables sammenkørt med data fra mange andre kilder, på nuværende tidspunkt må anses for at være eksperimentelle og ikke baserer sig på forskning, som viser deres pålidelighed. Der kan være mange fejlkilder; fx anvender app's, som opsamler motionsdata, mange forskellige metoder, heriblandt særdeles upålidelige lokationsmålinger fra GPS og mobil-master. Der kan også være tale om bevidst snyd, hvor man fx lader en anden person eller hunden bevæge app'en rundt. Hvor det drejer sig om app's, som måler psykisk velbefindende, indebærer de selvrapporterede data et subjektivt element, og hertil kommer, at mange app's ikke er udarbejdet af fagpersoner med indsigt i de tilstande, som måles.

Endelig er der tale om store usikkerheder hvor det drejer sig om forudsigelser pba af data fra mange forskelligartede kilder fremanalyseret vha algoritmer, som ikke er udarbejdet efter videnskabelige metoder eller bare efter ensartede metoder. Så hvis data, som meget tyder på, ofte er mangelfulde eller forkerte, eller ikke opfanger alle de facetter, som spiller ind i forhold til en persons sundhed, vil vedkommende blive bedømt på et uretfærdigt grundlag.

Det kan derfor give anledning til bekymring, hvis wearablesopsamlede eller algoritmegenererede sundhedsdata anvendes af forsikringsselskaber og arbejdsgivere, førend der er sket en større vidensopsamling, og der er langt bedre evidens for, at disse redskaber kan anvendes til at generere valide resultater.

Bilag 1
Wearables i databeskyttelsesretlig belysning

Af ph.d. jur. Hanne Marie Motzfeldt

DEL I: INTRODUKTION TIL DATABESKYTTELSESFORORDNINGEN OG DATABESKYTTELSESLOVEN

1. De centrale regelsæt

Databeskyttelse er en grundlæggende rettighed i henhold til artikel 8 i EU's Charter om grundlæggende rettigheder. I EU-Domstolens praksis er retten til beskyttelse af personoplysninger tæt forbundet med retten til beskyttelse af privatlivets fred, som denne er fastslået i Charterets artikel 7 og Den Europæiske Menneskerettighedskonvention artikel 8.

Af præamblen til forordning nr. 2016/679 om beskyttelse af personoplysninger (databeskyttelsesforordningen) fremgår, at den hastige teknologiske udvikling og globaliseringen har skabt nye udfordringer, hvad angår beskyttelse af personoplysninger. Derfor kræves en stærk og sammenhængende databeskyttelsesretlig ramme i EU. Databeskyttelsesforordningen er desuden et af de tiltag, der er opregnet i Kommissionens program om realiseringen af Det Digitale Indre Marked.[67]

Forordningen blev vedtaget i 2016, fik virkning i dansk ret fra den 25. maj 2018, og henviser til artikel 16 i Traktaten om Den Europæiske Unions Funktionsmåde (TEUF) om fastsættelse af regler for beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger.

67 Se om Det Digitale Indre Marked fx http://www.consilium.europa.eu/da/policies/digital-single-market/

En forordning er almengyldig og bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat. Dette indebærer, at en forordning gælder i den form, hvori den er vedtaget. En forordning må således som udgangspunkt ikke gennemføres med national lovgivning. Findes der nationale regler, der regulerer de samme forhold som en forordning, vil en forordnings regler som udgangspunkt fortrænge de nationale regler.

Databeskyttelsesforordningen har ikke fuldt ud en forordnings karakteristika. Det skyldes, at medlemsstaterne inden for nærmere bestemte områder enten skal eller kan fastsætte nationale regler. Der skal fx nationale regler til for at opfylde pligten til at etablere et uafhængigt tilsyn, og medlemsstaterne har mulighed for inden for en vis manøvremargin at præcisere forordningens regler, ligesom der i et ikke-ubetydeligt omfang i national ret kan fastsættes særlige regler, der fraviger/ undtager fra forordningens regler.

Lov om supplerende bestemmelser til forordning om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (databeskyttelsesloven)

Databeskyttelsesloven (lov nr. 502 af 23. maj 2018) supplerer og gennemfører visse regler i databeskyttelsesforordningen. Loven indeholder en række præciseringer, en del undtagelser, regulering af behandling af oplysninger uden for forordningens område samt regler om tilsyn, sanktioner mv.

Databeskyttelsesforordningens og databeskyttelseslovens regler gælder som udgangspunkt både for den private sektors og for den offentlige forvaltnings behandling af personoplysninger. Det offentlige sundhedsvæsen, private sælgere og udbydere af forskellige wearables og tilhørende tjenester vil dermed være omfattet af de samme regler, se herom neden for del I, afsnit 2. Dette er dog kun et udgangspunkt. For det første er enkelte regler i selve forordningen sektorspecifikke. For det andet indebærer udformningen af forordningens regler, at effekten vil være meget forskellig. Et eksempel er, at databehandlingsgrundlaget ofte vil være forskelligt (behandlingsbetingelserne). Et andet eksempel er, at retten til at blive glemt er stort set uden betydning i den offentlige sundhedssektor, men har stor betydning, når private virksomheder udbyder tjenester forbundet til wearables. For det tredje åbner databeskyttelsesforordningen i vidt omfang for, at der på nationalt plan fastsættes særlige regler. Disse muligheder er primært benyttet i relation til den offentlige sektor, herunder på sundhedsområdet.

2. Hvornår gælder reglerne?

Udgangspunktet er, at databeskyttelsesforordningen og databeskyttelsesloven gælder for behandling af personoplysninger, der foretages som led i aktiviteter, der udføres for en dataansvarlig eller en databehandler, der er etableret i Danmark, uanset om behandlingen finder sted i EU, jf forordningens artikel 3, stk. 1, og lovens § 4, stk. 1. Reguleringen vil således gælde for danske myndigheder, der behandler personoplysninger. Den vil også gælde for kommercielle udbydere af tjenester knyttet til wearables, når disse er etableret i EU.

Uanset den dataansvarliges eller databehandlerens etableringssted gælder forordningens regler også for behandling af personoplysninger om registrerede, der befinder sig i Unionen, hvis behandlingen vedrører en tjeneste udbudt til registrerede i Unionen eller indebærer overvågning af en fysisk persons adfærd, når denne finder sted i Unionen, jf forordningens artikel 3, stk. 2. Databeskyttelsesloven finder tilsvarende anvendelse for så vidt angår registrerede, der befinder sig i Danmark, jf lovens § 4, stk. 3. Den praktiske betydning af disse bestemmelser er, at reglerne vil gælde, når en borger bruger et wearable inden for EU henholdsvis Danmark.

De databeskyttelsesretlige regler finder (materielt) anvendelse, når personoplysninger behandles elektronisk, jf databeskyttelsesforordningens artikel 2, stk. 1, og databeskyttelseslovens § 1, stk. 2. Det vil være tilfældet, når der indsamles oplysninger om en borger via et wearable – men også når disse oplysninger fx overføres til en cloud eller en e-journal.

BEHANDLING
Hvad en behandling er, defineres i forordningens artikel 4, nr. 2, som "enhver aktivitet eller række af aktiviteter — med eller uden brug af automatisk behandling — som personoplysninger eller en samling af personoplysninger gøres til genstand for". Behandling eksemplificeres i bestemmelsen som "indsamling, registrering, organisering, systematisering, opbevaring, tilpasning eller ændring, genfinding, søgning, brug, videregivelse ved transmission, formidling eller enhver anden form for overladelse, sammenstilling eller samkøring, begrænsning, sletning eller tilintetgørelse". Som det fremgår, vil stort set alle aktiviteter, hvor personoplysninger håndteres, være at regne som en behandling i databeskyttelsesforordningens forstand.
Når man beskæftiger sig med forhold inden for sundhedssektoren, er der et uheldigt sammenfald i det danske sprog. Udtrykket behandling af personoplysninger (det engelske processing) kan føre til, at en læser skal fokusere unødigt på ikke at forveksle behandling af personoplysninger med sundhedsfaglig behandling af patienter. Lidt utraditionelt er det derfor i det følgende valgt at bruge udtryk som "databehandling eller "behandling af personoplysninger" overfor "sygdomsbehandling" eller "patientbehandling".

Regelsættet vil normalt også gælde, selvom oplysningerne printes, journaliseres eller videregives i papirbåret form. Det skyldes, at forordningen og loven også gælder, hvis oplysningerne hentes fra eller er bestemt til at indgå i et register. Herudover følger det af forvaltningslovens § 28, stk. 1, at dele af regelsættet finder anvendelse ved manuel videregivelse mellem forvaltningsmyndigheder. Hvilke organisationer, der regnes som forvaltningsmyndigheder efter databeskyttelseslovens forstand, afgrænses på samme måde som i den danske forvaltningslov.[68]

PERSONOPLYSNINGER
Ved personoplysninger forstås enhver form for information om en identificeret eller identificerbar fysisk person, jf forordningens artikel 4, nr. 1. Der er således tale om en meget bred definition, som omfatter alle oplysninger, der direkte eller indirekte kan henføres til en fysisk person. Det er ikke afgørende, om personen er nævnt ved navn. Omfattet af begrebet personoplysninger er også oplysninger, som kun kan kobles til en fysisk person gennem kendskab til et registreringsnummer, medlemsnummer, journal¬nummer eller lignende. På tilsvarende måde vil oplysninger, som foreligger i form af et billede, en persons stemme, fingeraftryk eller genetiske kendetegn, ofte have karakter af personoplysninger, således at behandlingen reguleres af databeskyttelsesforordningen. Det er i den forbindelse uden betydning, om den pågældende identifikationsoplysning er alment kendt eller umiddelbar tilgængelig. Også oplysninger, hvor det kun for den indviede vil være muligt at forstå, hvem informationen vedrører, er omfattet af begrebet personoplysninger. Dog er oplysninger, som er gjort anonyme på en sådan måde, at den registrerede ikke længere kan identificeres, ikke omfattet af definitionen.

Behandling af personoplysninger er dog ikke ”bare” behandling og personoplysninger ikke ”bare” personoplysninger. Forordningens regler skal læses i lyset af deres formål; at beskytte privatlivets fred og retten til beskyttelse af personoplysninger i den digitale tidsalder. Visse oplysninger anses som mere følsomme end andre, ligesom visse former for databehandling betragtes som mere indgribende end andre. Til de mere risikofyldte databehandlinger stilles højere krav til fx nødvendighed af behandlingen, sikkerhed, foranstaltninger til dataminimering mv, end tilfældet er for de mindre indgribende databehandlinger. Et eksempel på en meget indgribende behandling er offentliggørelse på internettet. Et eksempel på en ikke videre indgribende behandling er opbevaring internt hos en myndighed, fx i en journal.

68 Datatilsynets vejledning om databeskyttelsesrådgivere, pkt. 4.2.

PROFILERING

Profilering defineres i forordningens artikel 4, nr. 4, som enhver form for automatisk behandling af personoplysninger, der består i at anvende oplysningerne til at evaluere bestemte personlige forhold vedrørende en fysisk person, navnlig for at analysere eller forudsige forhold vedrørende den fysiske person, som fx helbred. Det nævnes i forordningens præambelbetragtning nr. 30, at fysiske personer kan tilknyttes online identifikatorer, som tilvejebringes af deres enheder, applikationer mv, og dette kan efterlade spor, der kan bruges til at oprette profiler om fysiske personer og identificere dem.

Udtrykket 'evaluering af personlige forhold' betyder ifølge Datatilsynets vejledning om registreredes rettigheder, at profileringen skal indebære en kategorisering efter det, der i vejledningen kaldes bløde værdier. Dette kan eksempelvis være interesser. Derimod er der ikke tale om profilering, hvis løsningen kun evaluerer hårde værdier. Eksemplet på hårde værdier er et indestående beløb på en bankkonto (Datatilsynets vejledning om registreredes rettigheder pkt. 10.1).

Det Europæiske Databeskyttelsesråd har præciseret, at der indgår tre hovedelementer i profilering. For det første skal der være tale om i hvert fald delvis automatisk behandling, for det andet skal det være personoplysninger, der behandles, og for det tredje skal formålet være at evaluere bestemte personlige forhold om en fysisk person, primært en form for vurdering eller bedømmelse. Rådet har i samme udtalelse "omskrevet" definitionen til mere dagligdags sprogbrug ved at betegne profilering som det at samle oplysninger ind om en person og evaluere vedkommendes karakteristika eller adfærdsmønster for at placere vedkommende i en bestemt kategori eller gruppe – især for at forudsige eller analysere vedkommendes evne til at udføre en opgave, interesser eller forventelige adfærd (Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 5 f).

Profilering er en af de behandlinger, der betragtes som en indgribende og risikofyldt form for databehandling. Grunden til denne tilgang til profilering er beskrevet af Det Europæiske Databeskyttelsesråd i en udtalelse fra 2018: "Profilering og automatiske afgørelser kan imidlertid udgøre en betydelig risiko for den enkeltes rettigheder og frihedsrettigheder, og der skal således indføres de fornødne garantier. Disse processer kan være uigennemsigtige. Den enkelte ved måske ikke, at vedkommende er ved at blive profileret, eller forstår måske ikke, hvad dette betyder (..) Profilering kan fastholde eksisterende stereotyper og social adskillelse. Den kan også fastlåse personer i en bestemt kategori og begrænse dem til deres foreslåede præferencer. Dette kan underminere deres frihed til at vælge fx bestemte produkter eller tjenesteydelser såsom bøger, musik eller nyhedsfeeds. I visse tilfælde kan profilering

føre til unøjagtige forudsigelser. I andre tilfælde kan den føre til, at de nægtes adgang til tjenesteydelser og varer, og urimelig forskelsbehandling."[69]

Denne tilgang indebærer bla, at profilering kan udløse krav om såkaldt konsekvensvurdering (Data Protection Impact Assessment) efter forordningens artikel 35, se herom neden for del II, afsnit 4. Hertil kommer, at profilering som behandlingsform bør give anledning til særlige overvejelser i forbindelse med en række af forordningens regler, se herom i del II.

Som det fremgår, vil både offentlige myndigheders og kommercielle aktørers brug af wearables stort set altid være omfattet af databeskyttelsesforordningen, og der vil ofte tillige være tale om en indgribende databehandling, idet der behandles mange oplysninger, og disse kan have følsom karakter. Herudover kan der være tale om profilering efter artikel 4, nr. 4, hvis de indsamlede data anvendes til at analysere eller forudsige den registreredes helbredstilstand, adfærd eller lignende.

3. Databeskyttelsesrettens reguleringsmodel og centrale definitioner af aktører

Som udgangspunkt bygger databeskyttelsesforordningen på den samme grundtanke som den tidligere regulering; nemlig at den dataansvarliges overholdelse af reglerne sikrer den ønskede beskyttelse af borgerne (de registrerede). Den dataansvarlige kan imidlertid samarbejde med andre end den registrerede. Det kan skabe tvivl om – eller der kan være manglende opmærksomhed i forhold til – hvem der i givet fald er ansvarlig for at sikre overholdelse af reglerne om beskyttelse af personoplysninger. Sådan uklarhed indebærer risiko for at svække beskyttelsen af borgerne.

DATAANSVARLIG
Den dataansvarlige er den, der bestemmer en databehandlings formål og de hjælpemidler, der benyttes til behandlingen, jf forordningens definition i artikel 4, nr. 7. Det er muligt at fastsætte i lovgivningen, hvem der er dataansvarlig. En registeret kan ikke være dataansvarlig for oplysninger om sig selv.

Forordningen indeholder på den baggrund både en række definitioner af "aktørerne" i en databehandling og en tættere regulering af visse samarbejdskonstruktioner. Dette fører til, at man i relation til sundhedsvæsenets brug af data fra wearables groft sagt kan operere med fire konstruktioner:

- Samarbejde mellem flere selvstændige dataansvarlige, der udveksler oplysninger (flere selvstændige dataansvarlige).

69 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 5-6.

- Samarbejde mellem dataansvarlige og disses databehandlere (databehandler-konstruktionen).
- Samarbejde mellem dataansvarlige, hvor der statueres fælles dataansvar (fælles dataansvar).
- Flere dataansvarlige behandler samme oplysninger uden at samarbejde eller udveksle oplysninger (mellemledskonstruktionen).

Samarbejder to eller *flere selvstændige dataansvarlige*, er de hver især ansvarlige for den databehandling, de foretager. Udveksler de to dataansvarlige personoplysninger, er de fx hver især ansvarlige for henholdsvis den videregivelse og den indhentning, de foretager. Et typisk eksempel vil være, at nogle af de oplysninger, der er indsamlet på et plejehjem i forbindelse med omsorgsopgaver, senere videregives til en præst eller en bedemand, der bruger oplysningerne til at udføre deres egne opgaver. I forbindelse med brug af wearables i sundhedssektoren kan et eksempel være, at en kommerciel udbyder af wearables selv anvender de indsamlede data til at stille dem til rådighed for de registrerede, til at danne markedsføringsprofiler og/eller til at udvikle nye tekniske løsninger, fx nudgings- eller diagnosticeringsredskaber. Uden at dette var tilsigtet på indsamlingstidspunktet, indvilger den kommercielle udbyder imidlertid senere i (også) at videregive dataene til den registreredes sundhedsperson, der anvender oplysningerne i forbindelse med sygdomsbehandling. Sundhedspersonens organisation er selvstændig dataansvarlig for databehandlingen efter modtagelsen af dataene. Se om Sag C 210/16 - Wirtschaftsakademie Schleswig-Holstein senere i nærværende afsnit.

I denne samarbejdskonstruktion har aktørerne som udgangspunkt ikke pligt til at undersøge, om samarbejdsparten i forbindelse med dennes behandling af personoplysninger respekterer forordningens regler og de registreredes rettigheder. Det er dog kun et udgangspunkt. Det danske datatilsyn har nemlig meldt ud, at den hidtidige nationale praksis om god databehandlingskik i forbindelse med offentlige myndigheders modtagelse af oplysninger fra andre aktører består under forordningen. Offentlige myndigheder kan dermed som udgangspunkt ikke bruge oplysninger, de har modtaget fra samarbejdspartnere, der har indsamlet dem ulovligt.[70]

Anvendes derimod en *databehandlerkonstruktion*, er den dataansvarlige fortsat ansvarlig for den håndtering af personoplysninger, der sker hos databehandleren. Samtidig påtager den dataansvarlige sig en række forpligtelser, herunder at sikre indgåelse af en såkaldt databehandleraftale og at udforme en instruks om, hvorledes persondatabehandlingen skal foregå hos databehandleren, jf forordningens artikel 28.

Et eksempel på en databehandlerkonstruktion vil være, at en sundhedsmyndighed indgår en kontrakt om udvikling og drift af en wearable-tjeneste med en privat it-leverandør. Hvis denne it-leverandør blot leverer "den tekniske ramme" og ikke selv bruger oplysningerne til egne formål (fx til at danne markedsføringsprofiler og sælge disse), vil leverandøren ofte være en databehandler. I denne situation skal myndigheden som dataansvarlig overholde databeskyttelsesforordningens regler om

70 Datatilsynets j.nr. 2018-32-0065, Skats brug af ulovligt fremskaffede oplysninger.

brug af databehandlere (herunder indgå en databehandleraftale og føre (aktivt) tilsyn med leverandørens håndtering af oplysningerne).

Den tredje databeskyttelsesretlige konstruktion er de *fælles dataansvarlige*. Heri ligger, at to eller flere parter i fællesskab fastlægger formål og midler for behandlingen af personoplysninger – dvs bestemmer, hvorfor der skal behandles personoplysninger (formålet), og hvordan der skal behandles personoplysninger (hjælpemidlerne). En sådan konstruktion kan – afhængig af de konkrete forhold – opstå, hvis en offentlig sundhedsmyndighed og en privat udbyder af sundheds-tjenester samarbejder om at (sundheds-)behandle patienten og i den forbindelse etablerer en ordning, hvor de begge har adgang til data fra patientens wearable.

DATABEHANDLER
En databehandler defineres som den, der "behandler personoplysninger på den dataansvarlige vegne", jf forordningens artikel 4 nr. 8. En registeret kan ikke regnes som databehandler for oplysninger om vedkommende selv.

Er der fælles dataansvar, skal der sikres klare arbejds- og rollefordelinger og information til de registrerede om fordelingerne, jf databeskyttelsesforordningens artikel 26.

Praksis om fælles dataansvar er under udvikling. Nyere praksis synes – uden at dette endnu er sikkert – at bygge på, at forordningens behandlingsdefinition kan dele en behandlingskæde op i forskellige "operationer". Der kan være flere stadier af en databehandling, der har forskellige formål og hjælpemidler, såsom indsamling, registrering, systematisering, opbevaring, tilpasning eller ændring, selektion, søgning, brug, videregivelse ved transmission, formidling, anden overladelse, sammenstilling eller samkøring, analyse samt blokering, slettelse eller tilintetgørelse. De forskellige involverede, fx et sygehus og en kommerciel udbyder af wearables, kan være fælles dataansvarlige for operationer (stadier), hvor de deler formål eller sammen bestemmer hjælpemidlerne. De kan samtidig være selvstændige dataansvarlige for de tidligere eller senere stadier i den samlede kæde af behandlinger, hvor de hver især alene har bestemt formål eller hjælpemidler. EU-Domstolen har dog endnu ikke forholdt sig til det forslag til afgørelse fra generaladvokat Bobek af 9. december 2018 i sag C-40/17, Fashion ID GmbH & Co. KG, præmis 96-108 vedrørende tredjepartsplug-ins på hjemmesider, hvor dette er beskrevet.

Databeskyttelsesforordningen tager ikke direkte højde for den situation, der her kaldes *mellemledskonstruktionen*. Et eksempel på denne situation er, at en offentlig ansat sundhedsperson anbefaler en borger at anvende et wearable, der udbydes af en kommerciel aktør – men uden at hverken sundhedspersonen eller myndigheden får direkte adgang til de indsamlede data eller på anden måde involveres i den behandling af oplysninger, der sker via det pågældende wearable.

SAG C-210/16 - WIRTSCHAFTSAKADEMIE SCHLESWIG-HOLSTEIN
EU-Domstolen udtalte sig den 5. juni 2018 om ansvarsforholdene, når organisationer (myndigheder eller virksomheder) opretter en såkaldt fanside på Facebook. Baggrunden for sagen var en afgørelse fra datatilsynet i Schleswig-Holstein. Tilsynet krævede, at en uddannelsesinstitution skulle lukke sin side på Facebook. Dette begrundede tilsynet med, at hverken uddannelsesinstitutionen eller Facebook informerede brugerne om den behandling af personoplysninger, som skete, når brugerne gik ind på fansiden.
På tidspunktet for sagen kunne alle, der ønskede en fanside, oprette en sådan gratis ved at registrere sig hos Facebook (blive administrator af en fanside). Administratoren skulle i den forbindelse acceptere Facebooks vilkår, herunder om brug af cookies. Disse (som udgangspunkt to år aktive) cookies ville blive placeret på de besøgendes devices. Facebook modtog, gemte og behandlede herefter personoplysninger, når de forskellige brugere besøgte Facebook, brugte tjenester leveret af andre facebookvirksomheder, og når brugerne brugte andre tjenester, der leveres af andre virksomheder, der brugte Facebook. Et led i aftalen, når administratoren af fansiden registrerede sig, var, at Facebook stillede værktøjet Facebook-Insights gratis til rådighed for administratoren (levering af statstikker). Administratoren af fansiden kunne tilpasse, hvilke statistikker vedkommende ønskede fra Insight ved at indstille bla målgruppen for indhold og reklamer. Administratorens valg af indstilling fik derefter indflydelse på indsamlingen og brugen af persondata til statistikkerne. Anderledes udtrykt kunne administratoren ved hjælp af de filtre, som Facebook stillede til rådighed, definere kriterierne for statistikkerne, og angive de kategorier af personer, som Facebook skulle indsamle personoplysninger om. Formålet med indsamling og brug af personoplysningerne i sagen var således for det første at gøre det muligt for Facebook at forbedre sit reklamesystem. For det andet var formålet at give administratoren af fansiden mulighed for at reklamere og tilpasse aktiviteterne via de statistikker, som Facebook udarbejdede.
EU-Domstolen bemærkede indledningsvis, at Facebook var dataansvarlig for behandling af oplysninger om de besøgendes adfærd. Derefter fastslog domstolen, at en administrator af de beskrevne fansider på Facebook skulle anses som fælles dataansvarlig med Facebook i relation til denne behandling. I forbindelse hermed lagde domstolen særlig vægt på brug af "Facebook Insights" og på, at en administrator ved at indstille filtrene var med til at afgøre formål og hjælpemidler for databehandlingen (præmis 39). Domstolen lagde desuden vægt på, at fansiderne kunne besøges af personer, som ikke havde en Facebook-konto – men hvor deres blotte besøg på siden udløste behandling af deres personoplysninger (præmis 41).

Den registrerede indgår her først i *en* relation til en privat virksomhed, der udbyder en tjeneste, hvor der kan anvendes et wearable. Virksomheden er dataansvarlig i forhold til den registrerede og er underlagt databeskyttelsesforordningens regler. Sundhedspersonen (og myndigheden) har databeskyttelsesretligt ingen rolle i denne relation.

Derefter giver den registrerede selv de opsamlede oplysninger til sundhedspersonen – og indgår i en anden databeskyttelsesretlig relation, hvor sundhedsmyndigheden er dataansvarlig. Omvendt har den kommercielle udbyder ikke som sådan nogen rolle i forbindelse med borgerens afgivelse af oplysningerne og myndighedens modtagelse af oplysningerne. Dette svarer i grove træk til det forhold, at en arbejdsgiver fra en ansøger modtager en udskrift af vedkommendes straffeattest, som ansøgeren selv har indhentet – en situation der adskiller sig fra visse offentlige arbejdsgiveres direkte indhentelse af oplysninger i Det Centrale Kriminalregister.

De databeskyttelsesretlige regler vil i en sådan situation regulere sundheds-myndighedernes brug af personoplysninger *under* og *efter* deres modtagelse som enhver anden behandling af personoplysninger inden for den offentlige sundheds-sektor. Ved modtagelsen skal myndigheden fx sikre sig behandlingsgrundlag og overholdelse af principper såsom datakvalitet. Det er derimod yderst tvivlsomt, om sundhedsmyndigheden i denne sammenhæng databeskyttelsesretligt bærer nogen form for ansvar for den behandling af oplysningerne, der sker *forudgående* via det pågældende wearable, se dog Datatilsynets j.nr. 2018-32-0065 om Skats brug af ulovligt fremskaffede oplysninger. Har sundhedspersonalet anbefalet en patient brug af et bestemt wearable, kan denne anbefaling derimod være reguleret af de sundhedsretlige og forvaltningsretlige regler.

De ovenstående konstruktioner kan over tid blive justeret og tilpasset ændrede forhold. Databeskyttelsesrettens regler er bevidst udformet på en måde, der skal sikre, at de kan tilpasse sig ændrede teknologiske og samfundsmæssige forhold. EU-Domstolen er den autoritative fortolker af de unionsretlige databeskyttelsesregler – og denne domstol anvender en dynamisk fortolkningsstil.

4. De grundlæggende databeskyttelsesretlige principper

Databeskyttelsesforordningens artikel 5, stk. 2, er et af de tydelige udslag af princip-pet om ansvarlighed (accountability), se også artikel 24. Af forordningens artikel 5, stk. 2, fremgår, at en dataansvarlig til enhver tid skal kunne påvise sin overholdelse af de grundlæggende databeskyttelsesretlige principper, der er fastlagt i artikel 5, stk. 1. En behandling af personoplysninger må ikke ske uden et behandlingsgrundlag i (hovedsagelig) forordningens artikel 6 eller 9 samt databeskyttelseslovens §§ 6-7. Det er dog ikke tilstrækkeligt at opfylde en af disse behandlingsbetingelser. Enhver behandling skal samtidig respektere de databeskyttelsesretlige principper i artikel 5, stk. 1:

- Ifølge litra a, skal personoplysninger behandles lovligt, rimeligt og på en gennemsigtig måde i forhold til den registrerede (lovlighed, rimelighed og gennemsigtighed).
- Ifølge litra b, skal personoplysninger indsamles til udtrykkeligt angivne og legitime formål og må ikke viderebehandles på en måde, der er uforenelig med disse formål. Viderebehandling til bla videnskabelige formål anses dog ikke som uforenelig med de oprindelige formål (formålsbegrænsning).
- Ifølge litra c, skal de behandlede oplysninger være tilstrækkelige, relevante og begrænsede til, hvad der er nødvendigt i forhold til databehandlingsformålet (dataminimering).
- Ifølge litra d, skal de behandlede oplysninger være korrekte og om nødvendigt ajourførte, og der skal tages ethvert rimeligt skridt for at sikre, at oplysninger, der er urigtige i forhold til databehandlingsformålet, straks slettes eller berigtiges (rigtighed).
- Ifølge litra e, skal oplysninger opbevares på en sådan måde, at det ikke er muligt at identificere de registrerede i et længere tidsrum end det, der er nødvendigt til de formål, hvortil de behandles, medmindre dette alene sker til fx videnskabelige formål (opbevaringsbegrænsning).
- Ifølge litra f, skal oplysninger behandles på en måde, der sikrer tilstrækkelig sikkerhed herunder beskyttelse mod uautoriseret eller ulovlig databehandling og mod hændeligt tab, tilintetgørelse eller beskadigelse, under anvendelse af passende tekniske eller organisatoriske foranstaltninger (integritet og fortrolighed).

Udgangspunktet er, at enhver brug af wearables til indsamling af data og den senere anvendelse af oplysningerne skal indrettes til at respektere disse principper. Dette gælder både for offentlige myndigheder og private udbydere af tjenester forbundet til wearables. Dette skal indtænkes ved valg af såvel det tekniske design som i forbindelse med tilrettelæggelse af arbejdsgange og organisatoriske forhold ved behandlingen af personoplysninger, jf herved også databeskyttelsesforordningens artikel 25 om databeskyttelse gennem design og via indstillinger og om konsekvensvurderinger i artikel 35. Se herom neden for, del II, afsnit 3.2. og 4.

5. Kategorier af personoplysninger

I databeskyttelsesforordningen og databeskyttelsesloven skelnes bla mellem almindelige personoplysninger og følsomme personoplysninger. Hertil kommer fx oplysninger om strafbare forhold og CPR-numre, der dog formentlig kun sjældent får betydning i forbindelse med brug af wearables.

Helbredsoplysninger og oplysninger om genetiske data er som følsomme personoplysninger omfattet af databeskyttelsesforordningens artikel 9. Biometriske data kan være følsomme oplysninger, hvis de bruges i identifikationsøjemed.

KATEGORISERING AF OPLYSNINGER

Det afgørende for databeskyttelsesforordningens opdeling af oplysninger i kategorier er den information, der afgives om den registrerede i den konkrete behandlingskontekst.

Det klassiske lærebogseksempel er, at adresseoplysninger normalt regnes som almindelige, ikke-følsomme personoplysninger. Er adressen imidlertid en lukket psykiatrisk afdeling, afgives følsom information – og oplysningerne er dermed omfattet af databeskyttelsesforordningens artikel 9. Eksemplet viser, hvordan en simpel samstilling af to oplysninger kan resultere i en tredje oplysning.

Det kan virke mindre enkelt, men samme tilgang skal anvendes, når avancerede modeller mv anvendes til at samstille store mængder almindelige oplysninger om enkeltpersoner for derved at udlede informationer om fx sygdomsrisiko.

HELBREDSOPLYSNINGER, GENETISKE OG BIOMETRISKE DATA

***Helbredsoplysninger* er i databeskyttelsesforordningen defineret som personoplysninger, der vedrører en fysisk persons fysiske eller mentale helbred, herunder levering af sundhedsydelser, og som giver information om vedkommendes helbredstilstand, jf artikel 4, nr. 15. *Genetiske data* er defineret som oplysninger vedrørende en fysisk persons arvede eller erhvervede genetiske karakteristika, som giver entydig information om denne fysiske persons fysiologi eller helbred, og som navnlig foreligger efter en analyse af en biologisk prøve fra den pågældende, jf artikel 4, nr. 13. *Biometriske data* regnes som personoplysninger, der som følge af specifik teknisk databehandling vedrørende en fysisk persons fysiske, fysiologiske eller adfærdsmæssige karakteristika muliggør eller bekræfter en entydig identifikation af vedkommende, fx ansigtsbillede eller fingeraftryksoplysninger, jf artikel 4, nr. 14.**

Ved fastlæggelsen af, hvad der nærmere skal forstås ved helbredsoplysninger, indeholder databeskyttelsesforordningens præambelbetragtning nr. 35 fortolkningbidrag. Herefter omfatter begrebet helbredsoplysninger alle informationer om den registrerede, som giver viden om vedkommendes tidligere, nuværende eller fremtidige fysiske eller mentale helbredstilstand. Også et nummer, symbol eller særligt mærke, der tildeles en fysisk person for entydigt at identificere den pågældende til sundhedsformål, er ifølge betragtning nr. 35 omfattet, ligesom enhver oplysning om fx en sygdom, et handicap, en sygdomsrisiko, en sygehistorie, en sundhedsfaglig behandling eller den registreredes fysiologiske eller biomedicinske tilstand uafhængigt af kilden hertil. I forbindelse med sidstnævnte nævnes direkte, at det er uden betydning, at kilden til oplysningerne er medicinsk udstyr. Endelig

fremgår det af betragtning nr. 35, at alle oplysninger indsamlet med henblik på eller under levering af sundhedsydelser er at betragte som helbredsoplysninger. Idet informationer om nuværende eller fremtidige helbredstilstand og om sundhedsrisiko, der indsamles med henblik på eller under levering af sundhedsydelser, er omfattet af definitionen af helbredsoplysninger, må det antages, at langt størstedelen af de oplysninger, der stammer fra brug af wearables i sundhedssektoren, falder ind under definitionen.

Vurderingen er mere kompleks i forhold til kommercielle udbydere af wearables og tilknyttede tjenester. Indsamles der blot almindelige data som fx lokalisation eller spisetider med henblik på at præsentere disse for den registrerede, er der som den ene yderpol næppe tale om helbredsoplysninger. Knyttes der til det pågældende wearable en tjeneste, der kobler de forskellige data og foretager en vurdering af den registreredes fysiske eller mentale tilstand, er der som den anden yderpol utvivlsomt tale om helbredsoplysninger. Mellem disse yderpoler må det bero på en konkret vurdering, om den samlede datamængde afgiver, eller indenfor rimelighedens grænse kan antages at afgive, information om brugerens tidligere, nuværende eller fremtidige fysiske eller mentale helbredstilstand. Ved vurderingen skal der formentlig lægges vægt på, om formålet med dataindsamlingen er at give indblik i eller påvirke (nudge) den registreredes adfærd med henblik på vurdering og påvirkning af sundhedstilstand, sygdomsrisiko mv.

Det synes umiddelbart at være sådan, at de fleste kommercielle udbydere af wearables kombinerer dataopsamlingen med tjenester, der foretager vurderinger af de registreredes tilstand, fx om vedkommende bevæger sig tilstrækkeligt eller søvnrytmen er tilfredsstillende. På den baggrund må det antages, at den centrale regel om adgang til at indsamle og bruge oplysninger i nærværende sammenhæng er databeskyttelsesforordningens artikel 9, selvom enkelte ordninger kan være relateret til artikel 6, se nærmere herom nedenfor.

6. Databehandlingsgrundlag

Behandling af følsomme personoplysninger, såsom helbredsoplysninger og genetiske data, er som teoretisk udgangspunkt ikke tilladt efter databeskyttelsesforordningens artikel 9, stk. 1. Generelle undtagelser til dette udgangspunkt er ifølge artikel 9, stk. 2, bla:

- Ifølge litra a, kan behandling af følsomme oplysninger ske, hvis den registrerede har givet udtrykkeligt samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål (se nærmere om samtykke neden for i del II, afsnit 1).
- Ifølge litra f, kan behandling af følsomme oplysninger ske, hvis databehandlingen er nødvendig for, at et retskrav kan fastlægges, gøres gældende eller forsvares.
- Ifølge litra g, kan behandling af følsomme oplysninger ske, hvis databehandlingen er nødvendig af hensyn til væsentlige samfundsinteresser på grundlag af [EU-retten eller] medlemsstaternes nationale ret. Dette forudsætter, at databehandlingen

står i rimeligt forhold til det mål, der forfølges, respekterer det væsentligste indhold af retten til databeskyttelse, og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser.
- Ifølge litra h, kan behandling af følsomme oplysninger ske, hvis databehandling foretages af en person underlagt (fagpersoners) tavshedspligt og er nødvendig med henblik på forebyggende medicin eller arbejdsmedicin til (..) medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester på grundlag af EU-retten eller medlemsstaternes nationale ret eller i henhold til en kontrakt med en sundhedsperson.

De muligheder for behandling af helbredsoplysninger via wearables i sundhedssektoren, som de ovenfor nævnte bestemmelser åbner for, har forskellig karakter. Artikel 9, stk. 2, litra a og f kan anvendes direkte af de dataansvarlige som grundlag for behandling af personoplysninger. Artikel 9, stk. 2, litra g og h, skal ifølge forarbejderne til databeskyttelsesloven "aktiveres" i lovgivningen.[71]

AKTIVERING
Nogle af de bestemmelser i databeskyttelsesforordningen, som giver grundlag for at behandle personoplysninger, kan uden videre anvendes af en dataansvarlig i Danmark. Artikel 9, stk. 2, litra a, om samtykke er en af disse bestemmelser. Artikel 9, stk. 2, litra f, om retskrav er en anden. Andre bestemmelser forudsætter en national, implementerende lovgivning om selve den konkrete behandling eller en anden form for "aktivering" (lovforslag nr. 68 af 25. oktober 2017 om databeskyttelsesloven, pkt. 2.3.3.2). Artikel 9, stk. 2, litra g og h, regnes som nogle af de bestemmelser, der skal "aktiveres" i national ret (eller unionsretten).
Artikel 9, stk. 2, litra g, om behandling på grundlag af national ret (eller unionsret), der varetager væsentlige samfundsinteresser, kan aktiveres generelt eller i særlovgivningen, herunder bekendtgørelser. Artikel 9, stk. 2, litra h, om behandling af oplysninger med henblik på levering af sundhedsydelser mv kan aktiveres på to måder. Den ene er en kontrakt med en sundhedsperson. Den anden er via lovgivningen. Også for artikel 9, stk. 2, litra h, gælder det, at bestemmelsen kan aktiveres generelt eller i særlovgivningen.

Artikel 9, stk. 2, litra f, om retskrav vil kunne fungere som databeskyttelsesretligt behandlingsgrundlag, når det er nødvendigt at behandle helbredsoplysninger for at vurdere, om enten en patient, en anden borger eller en myndighed har et retskrav henholdsvis nærmere at fastlægge eller realisere dette retskrav. Anderledes udtrykt kan bestemmelsen udgøre det databeskyttelsesretlige grundlag for, at følsomme oplysninger kan indgå i patientbehandlingstilbud. I det offentlige sundhedsvæsen.

71 Lovforslag nr. 68 af 25. oktober 2017 om databeskyttelsesloven, pkt. 2.3. og 2.3.3.2.

Bestemmelsen vil i så fald ofte udgøre en del af et dobbelt eller tredobbelt grundlag sammen med fx artikel 9, stk. 2, litra h.

I den danske databeskyttelseslov er hele *artikel 9, stk. 2, litra g, om databehandling af hensyn til væsentlige samfundsinteresser* på grundlag af national ret generelt "aktiveret", jf lovens § 7, stk. 4. Derudover kan bestemmelsen aktiveres via særregler. Det antages i forarbejderne til databeskyttelsesloven, at dette kan ske ved, at sådan særlovgivning forudsætter brug af oplysningerne. Det er ikke nødvendigt, at særlovgivningen indeholder en udtrykkelig regel, der tillader eller pålægger brugen af de følsomme personoplysninger. "Aktivering" kan ifølge forarbejderne ske ved, at der er pålagt myndighederne en opgave, til hvis løsning behandling af oplysningerne er nødvendig.[72]

Bestemmelsen synes i et vist omfang at kunne fungere som databehandlingsgrundlag, hvis der fx tilbydes anvendelse af wearables i forbindelse med oplysningskampagner eller arbejdes med "nudging" (hvor det ikke nødvendigvis er en person inden for sundhedssektoren, der foretager behandlingen af personoplysningerne). Dette skyldes, at forordningens præambelbetragtning nr. 52 nævner, at medlemsstaterne skal kunne fravige forbuddet mod at behandle følsomme kategorier af data på områder som fx folkesundhed og social sikring.

En sundhedsmyndighed skal i modsætning til en kommerciel leverandør af wearables ikke have forudgående tilladelse fra Datatilsynet for at anvende forordningens artikel 9, stk. 2, litra g, som behandlingsgrundlag. Gives en kommerciel aktør tilladelse til behandling efter bestemmelsen, vil Datatilsynet dog formentlig fastsætte vilkår i forbindelse med tilladelsen, se til sammenligning Datatilsynets nyhed af 19. maj 2019 om Brøndbyernes I.F. Fodbold A/S.

Den danske databeskyttelseslov aktiverer derimod kun generelt dele af *artikel 9, stk. 2 litra h, om sundheds- og socialsektoren* i databeskyttelseslovens § 7, stk. 3. Herefter kan behandling af helbredsoplysninger ske, hvis databehandlingen er nødvendig med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

Anvendelse af den generelt aktiverende regel i lovens § 7, stk. 3, jf forordningens artikel 9, stk. 2, litra h, som grundlag for at indsamle og bruge helbredsoplysninger vil herefter forudsætte, at to krav er opfyldt. Det ene er, at behandlingen af oplysningerne fortages af en sundhedsperson underlagt tavshedspligt. Det andet krav er, at behandlingen af (alle) oplysningerne er nødvendig for den pågældende forebyggelse, patientbehandling, administration mv.

72 Ibid.

Bestemmelsen i artikel 9, stk. 2, litra h, kan dog også her ifølge forarbejderne til databeskyttelsesloven "aktiveres" i særlovgivningen, fx den sociale lovgivning. Her gælder det formentlig ikke som forudsætning, at databehandling foretages af en sundhedsperson. Dette skyldes, at kun databeskyttelsesloven begrænser til sundhedspersoner, mens databeskyttelsesforordningen blot kræver en fagpersons tavshedspligt, jf herved artikel 9, stk. 3, og præambelbetragtning nr. 53. Alle offentligt ansatte *og* ansatte i de virksomheder, der får adgang til fortrolige oplysninger som led i deres opgaver for myndighederne, er underlagt tavshedspligt ved behandling af helbredsoplysninger, jf straffelovens § 152 ff. og forvaltningslovens § 27 – og må vel for manges vedkommende regnes som fagpersoner indenfor deres respektive hverv. Brug af en helbredsoplysning kan, som nævnt ovenfor, have mere end et behandlingsgrundlag (dobbelt eller tredobbelt mv). Anderledes udtrykt kan en sundhedsmyndighed eller en kommerciel udbyder af wearables-tjenester udmærket henvise til flere af de ovennævnte bestemmelser som grundlag for databehandling. Dette kan for sundhedsmyndighederne især få betydning, hvis brugen af wearables kobles med udvikling af forskellige former for Machine Learning-baserede modeller eller kunstig intelligens med henblik på at træffe beslutning om behandling, prioriteringer mv, se om automatiske afgørelser nedenfor afsnit 7.5.

Anvendelsen af andre bestemmelser end samtykke som behandlingsgrundlag forudsætter dog i alle tilfælde, at (alle dele af) behandlingen af (alle) oplysningerne er nødvendig for den pågældende forebyggelse, patientbehandling, samfundsinteresse, vurdering af det pågældende retskrav mv. Man skal holde sig til de behandlinger, der er knyttet til at opnå formålet. Se om kravene, når samtykke er behandlingsgrundlag nedenfor del II, afsnit 1.

NØDVENDIGHEDSKRAVET

Det er et fælles træk ved de fleste af de bestemmelser i forordningen, der giver grundlag for at behandle personoplysninger, at de indeholder en nødvendighedsbetingelse. Denne betingelse skal være opfyldt for hver oplysning og hver databehandling. I almindelighed gælder, at jo mere følsom oplysningen er, og jo mere indgribende form for databehandling, der er tale om, jo strengere er nødvendighedsbedømmelsen. Behandlingens intensitet kan således ses som en skala, hvor samkøring i kontroløjemed, profilering og videregivelse (særligt offentliggørelse) er de mest indgribende behandlingsformer. Derimod anses opbevaring og intern brug for at være mindre indgribende. Det har også stor betydning, om oplysningernes behandling kan få konsekvenser for de registrerede – så som foranstaltninger i form af ringere behandlingstilbud mv.

Som det er nævnt ovenfor, kan der være tale om en relation, hvor borgeren selv indgår en aftale med en kommerciel udbyder og selv anvender det pågældende

wearable – for derefter at "trække oplysninger ud" og give dem til en sundhedsperson (mellemledskonstruktionen). I disse tilfælde sker behandlingen hos den kommercielle udbyder ikke nødvendigvis med henblik på levering af sundhedsydelser.

Dette rejser for det første spørgsmålet, om der er tale om helbredsoplysninger, se om vurderingen heraf oven for del I, afsnit 5. Det andet – og i nærværende afsnit relevante – spørgsmål er, hvilket behandlingsgrundlag, der er relevant i den kommercielle relation.

Er der tale om helbredsoplysninger (eller andre følsomme oplysninger) synes navnlig samtykkebestemmelsen eller behandling med forudgående tilladelse efter databeskyttelsesforordningens § 7, stk. 4, jf forordningens artikel 9, stk. 2, litra g, om væsentlige samfundsinteresser at være relevant for en kommerciel udbyder af wearables som dataansvarlig. Se neden for i del II, afsnit 1, om overordnede forskelle på samtykke som behandlingsgrundlag i den offentlige forvaltning og i den private sektor. Er der derimod tale om almindelige personoplysninger, kan også forordningens artikel 6, jf databeskyttelseslovens § 6 fungere som databehandlingsgrundlag.

Databehandling af (almindelige) personoplysninger må – forudsat overholdelse af de øvrige bestemmelser i forordningen – finde sted i nærmere beskrevne tilfælde, som er nævnt i forordningens artikel 6, stk. 1, litra a - e. De bestemmelser, der synes mest relevante for kommercielle udbydere af wearables og tilknyttede tjenester, er:

- Ifølge litra a, må behandling af almindelige personoplysninger ske, hvis den registrerede har givet (utvetydigt) samtykke til behandling af sine personoplysninger til et eller flere specifikke formål.
- Ifølge litra b, må behandling af almindelige personoplysninger ske, hvis databehandlingen er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt.
- Ifølge litra c, må behandling af almindelige personoplysninger ske, hvis databehandlingen er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige.
- Ifølge litra e, må behandling af almindelige personoplysninger ske, når dette er nødvendigt af hensyn til udførelse af en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt.
- Ifølge litra f, kan den private udbyder af tjenesterne – i modsætning til en offentlig myndighed – behandle almindelige personoplysninger, hvis databehandlingen er nødvendig for, at den dataansvarlige eller en tredjemand kan forfølge en legitim interesse, medmindre den registreredes interesser eller grundlæggende rettigheder og frihedsrettigheder, der kræver beskyttelse af personoplysninger, går forud herfor, navnlig hvis den registrerede er et barn.

Særligt artikel 6, stk. 1, litra a og b, kan være relevante databehandlingsgrundlag, når en kommerciel udbyders databehandling sker helt løsrevet fra den senere anvendelse af oplysningerne i sundhedsvæsenet (mellemledskonstruktionen). Interesseafvejningsreglen i artikel 6, stk. 1, litra f, er en yderligere mulighed, men der bør formentlig udvises tilbageholdenhed med at anvende reglen som eneste behandlingsgrundlag, hvis den kommercielle udbyder foretager profilering.[73] I en databehandlerkonstruktion vil grundlaget knytte sig til den dataansvarlige sundhedsmyndigheds aktiviteter, hvorfor artikel 6 ikke er relevant, se ovenfor del I, afsnit 5 om kategorisering af personoplysninger og definitionen af helbredsoplysninger.

Når der etableres fælles dataansvar eller faste samarbejder mellem kommercielle aktører og sundhedsmyndigheder som selvstændige dataansvarlige, kan der teoretisk skelnes mellem den kommercielle udbyders og sundhedsmyndighedernes indsamling og brug af (samme) data. Meget taler dog for, at tilsynsmyndighederne vil søge at nedskalere den retlige kompleksitet i et sådan scenarie. En oplagt mulighed er at betragte alle de indsamlede personoplysninger som følsomme, hvorefter artikel 6 ikke er relevant. Det kan dog ikke udelukkes, at dataene vil kunne betragtes som almindelige under en kommerciel udbyders brug og som følsomme under en sundhedsmyndigheds brug. Den kommercielle udbyder kan i så fald muligvis komme i en situation, hvor også artikel 6, stk. 1, litra c, kan være relevant som behandlingsgrundlag.

Der synes under alle omstændigheder at være en bred vifte af bestemmelser, der kan give grundlag for databehandling af almindelige oplysninger, når private udbyder wearables i de formentlig mangfoldige scenarier, hvor de indsamlede oplysninger senere helt eller delvis vil indgå i det offentlige sundhedsvæsens arbejde.

7. De registreredes rettigheder

Fysiske personer er i databeskyttelsesforordningen givet en række rettigheder, når der behandles oplysninger om dem (inden for forordningens anvendelsesområde, se del I, afsnit 2). Rettighederne er dog ikke ubetingede.

Databeskyttelsesforordningen indeholder en række almindeligt gældende undtagelser til rettighederne. Dertil kommer, at forordningens artikel 23 inden for visse rammer giver mulighed for at begrænse de registreredes rettigheder yderligere.

Denne mulighed er udnyttet i databeskyttelsesloven, der indeholder en række undtagelser. Det er imidlertid ikke et krav efter forordningen, at undtagelserne skal være at finde i databeskyttelsesloven. Der kan derfor findes yderligere undtagelser til rettighederne i særlovgivningen, fx i den sociale lovgivning.

---

73 Tilsvarende Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 13 f.

Det følger af databeskyttelsesforordningens artikel 23, at medlemsstaterne i lov eller ved lov (fx bekendtgørelser) kan begrænse rækkevidden af de forpligtelser og rettigheder, der følger af reglerne om de registreredes rettigheder.
Det er et krav efter forordningen, at begrænsningerne skal respektere det væsentligste indhold af de grundlæggende rettigheder og friheds-rettigheder, og være en nødvendig og forholdsmæssig foranstaltning i et demokratisk samfund af hensyn til en række nærmere oplistede hensyn. Det kan fx være en medlemsstats væsentlige økonomiske interesser.
I forordningens artikel 23, stk. 2, er det uddybet, at sådan lovgivning som minimum – hvor det er relevant – skal indeholde specifikke bestemmelser om formålet med behandlingerne, kategorierne af oplysninger, rækkevidden af begrænsningerne, garantierne for at undgå misbrug, opbevaringsperioder og gældende garantier under hensyntagen til behandlingens karakter, omfang, formål og kategorier af behandling, risikoen for de registrerede og deres rettigheder og de registreredes ret til at blive underrettet om begrænsningen (medmindre sådan underretning kan skade formålet med begrænsningen).
Den danske opfattelse er, at vurderingen af, hvornår det er relevant at fastsætte specifikke bestemmelser efter artikel 23, stk. 2, i forbindelse med fravigelse af de registreredes rettigheder, er national og foretages i forbindelse med udarbejdelsen af loven eller bekendtgørelsen (Betænkning nr. 1565, s. 399-404). Dertil kommer, at Justitsministeriet i forarbejderne til databeskyttelsesloven har givet udtryk for, at forordningens artikel 23, stk. 2, ikke indeholder noget absolut krav om, at der i regler, der begrænser rettighederne efter artikel 23, stk. 1, skal være specifikke bestemmelser vedrørende de hensyn, der er nævnt i artikel 23, stk. 2 (Justitsministerens svar på spørgsmål 63 fra Retsudvalget vedrørende lovforslag nr. 68 om databeskyttelsesloven).

Databeskyttelsesforordningens artikel 12 fastslår overordnet visse pligter for den dataansvarlige i forbindelse med de registreredes udøvelse af deres rettigheder. Den dataansvarlige skal bla tilrettelægge sine digitale og analoge arbejdsgange, så de registrerede let kan udøve deres rettigheder. Der skal anvendes en gennemsigtig, letforståelig og lettilgængelig form og et klart og enkelt sprog. Sidste vil især være relevant, når det – af hensyn til den anvendte teknologis kompleksitet – er vanskeligt for den registrerede at vide og forstå, om, af hvem og til hvilket formål der indsamles personoplysninger om vedkommende.

I det følgende er kun beskrevet informationspligten, indsigtsretten, reglerne om berigtigelse og sletning samt den almindelige indsigelsesret og reglen om auto-

matiserede afgørelser og profilering. Det skyldes, at disse rettigheder vurderes at være de mest relevante, når der anvendes wearables og data indhentet via wearables i sundhedssektoren. For så vidt angår dataportabilitet er retten primært relevant i relationen mellem kommercielle udbydere og registrerede, hvorfor der henvises til gennemgangen i den danske betænkning om databeskyttelse og Datatilsynets vejledning om registreredes rettigheder.[74]

7.1 Informationspligt ved indsamling af oplysninger

Det bør være *gennemsigtigt* for fysiske personer, at personoplysninger, der vedrører dem, indsamles, anvendes, tilgås eller på anden vis behandles, og i hvilket omfang personoplysningerne behandles eller vil blive behandlet, jf databeskyttelsesforordningens artikel 5, stk. 1, litra a, og præambelbetragtning nr. 60. Forordningen fastsætter derfor i artikel 13, stk. 1- 2, og artikel 14, stk. 1- 2, at en dataansvarlig har pligt til at informere den registrerede om en række forhold allerede ved indsamling af personoplysninger.

7.1.1 Information ved indsamling hos den registrerede selv

Artikel 13 gælder, når den dataansvarlige indsamler oplysningerne direkte hos den registrerede. Af bestemmelsen i artikel 13, stk. 1, fremgår, at den dataansvarlige på det tidspunkt, hvor personoplysningerne indsamles, og medmindre den registrerede allerede er bekendt med oplysningerne, skal give den registrerede borger følgende informationer:

a) Identitet på, og kontaktoplysninger for, den dataansvarlige.
b) Kontaktoplysninger for en eventuel databeskyttelsesrådgiver.
c) Formålene med den databehandling, som personoplysningerne skal bruges til og retsgrundlaget for databehandlingen.
d) De legitime interesser, der forfølges af den dataansvarlige eller tredjemand, når behandlingen er baseret på artikel 6, stk. 1, litra f.
e) Eventuelle modtagere eller kategorier af modtagere af personoplysningerne.
f) Hvor det er relevant, at den dataansvarlige agter at overføre personoplysninger til et tredjeland eller en international organisation og visse oplysninger i forbindelse hermed.

Information om de legitime interesser, der forfølges, vil primært være relevant for de kommercielle udbydere af wearables og wearables-tjenester, fordi interesseafvejningsbestemmelsen ikke kan udgøre grundlaget for offentlige myndigheders behandling af personoplysninger, jf artikel 6, stk. 1, sidste punktum og databeskyttelseslovens § 6, stk. 1 – og selv da, kun i de tilfælde, hvor det er almindelige oplysninger, der behandles.

Artikel 13, stk. 2, opregner ikke-udtømmende, hvilke informationer der i øvrigt kan være relevante at give de registrerede for at sikre, at databehandlingen sker på

74 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, s. 347 og Datatilsynets vejledning om registreredes rettigheder.

rimelig og gennemsigtig måde. Er sådanne andre informationer relevante, *skal* de gives ved indsamlingen.[75] Der opregnes følgende eksempler:

a) Det tidsrum hvor personoplysningerne vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier der anvendes til at fastlægge dette tidsrum.
b) Retten til at anmode den dataansvarlige om indsigt i, og berigtigelse eller sletning af, personoplysninger eller begrænsning af databehandling vedrørende den registrerede eller til at gøre indsigelse mod databehandling samt retten til dataportabilitet.
c) Når databehandling er baseret på den registreredes samtykke, retten til at trække samtykke tilbage på ethvert tidspunkt (uden at dette berører lovligheden af databehandling, der er baseret på samtykke inden tilbagetrækning heraf).
d) Retten til at indgive en klage til en tilsynsmyndighed.
e) Om meddelelse af personoplysninger er lovpligtigt eller et krav i henhold til en kontrakt eller et krav, der skal være opfyldt for at indgå en kontrakt, samt om den registrerede har pligt til at give personoplysningerne og de eventuelle konsekvenser af ikke at give sådanne oplysninger.
f) Forekomsten af automatiske afgørelser og i givet fald oplysninger om logikken heri samt om betydningen og de forventede konsekvenser af en sådan databehandling for den registrerede.

Når der bruges wearables – uanset om den dataansvarlige er en kommerciel udbyder eller en sundhedsmyndighed – er det af særlig betydning for åbenhed og gennemsigtighed (transparens), hvordan artikel 13, stk. 2, litra f, fortolkes.

Det Europæiske Databeskyttelsesråd har i vejledningen om profilering og automatiske afgørelser skrevet følgende: "I betragtning af det centrale princip om gennemsigtighed, der ligger til grund for databeskyttelsesforordningen, skal de dataansvarlige sikre, at de tydeligt og klart forklarer de registrerede, hvad automatiske afgørelser og profilering indebærer. Hvis behandlingen omfatter afgørelser baseret på profilering (uanset om de er omfattet af artikel 22), skal det forhold, at behandlingen sker både med henblik på a) profilering og b) for at træffe en afgørelse baseret på den genererede profil, gøres klart over for den registrerede (..) I betragtning 60 anføres det, at afgivelse af oplysninger om profilering er en del af den dataansvarliges gennemsigtighedsforpligtelser i henhold til artikel 5, stk. 1, litra a). Den registrerede har *ret til at blive informeret* af den dataansvarlige, og under visse omstændigheder *ret til at gøre indsigelse* mod 'profilering', *uanset* om der er tale om individuelle afgørelser, der alene er baseret på automatisk behandling, herunder profilering."[76]

Dette synes umiddelbart at skulle forstås sådan, at det er Databeskyttelsesrådets opfattelse, at pligten til at give information efter artikel 13, stk. 2, litra f, udløses *både* ved profilering, hvor der efterfølgende træffes automatiske beslutninger på

75 Retningslinjer for gennemsigtighed i henhold til forordning 2016/679, WP 260, s. 12.

76 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 16-17. Fremhævelserne er rådets egne.

baggrund af den pågældende profil – og hvor der efterfølgende sker en manuel behandling på baggrund af profilen. Anderledes udtrykt: at der skal informeres om logikken, der anvendes til at profilere, betydningen heraf og eventuelle konsekvenser, uanset om der træffes automatiske afgørelser eller ej. Slår denne forståelse igennem i dansk tilsyns- og domstolspraksis, vil informationsforpligtelsen fx blive udløst, hvis et wearable eller en tilknyttet tjeneste anvender en algoritme til at behandle de indsamlede data til at evaluere brugerens adfærd med henblik på fx at beslutte en af flere behandlingsplaner.

I forbindelse med brug af wearables, hvor der sker profilering, bør informationen efter artikel 13, stk. 2, litra f, udformes efter retningslinjerne i forordningens artikel 12 om forståelig sprogbrug. Ifølge den danske betænkning om databeskyttelsesforordningen indebærer oplysning om "logikken" ikke en detaljeret beskrivelse af den "tekniske" programmering, der ligger bag løsningen. Det centrale er, at den registrerede kan forstå de overvejelser, der ligger til grund for behandlingen af oplysninger, og hvordan "systemet" kommer frem til de forskellige afgørelser.[77]

Det danske datatilsyns vejledning om registreredes rettigheder er ganske kortfattet på dette punkt, men Det Europæiske Databeskyttelsesråds vejledning[78] anbefaler, at der informeres om:

- Kategorierne af data, der anvendes i forbindelse med profileringen.
- Hvorfor disse data er vurderet at skulle inddrages.
- Hvordan profilerne opbygges (herunder statistik anvendt i forbindelse med profilerne).
- Hvorfor netop de anvendte profiler er fundet relevante.
- Hvordan profilerne eventuelt anvendes i en automatiseret beslutningsproces.

Opsummerende gælder der som udgangspunkt en pligt for både kommercielle udbydere af wearables-tjenester og for sundhedsmyndigheder til at give ret omfattende information om, hvorfor og hvordan borgerens data bliver behandlet. Informationen skal sikre gennemsigtighed – og dermed skabe tryghed hos de registrerede.

7.1.2 Informationspligt ved videreanvendelse af oplysninger indsamlet hos den registrerede

Hvis den dataansvarlige senere vil bruge de indsamlede oplysninger til et andet formål, skal den registrerede desuden efter databeskyttelsesforordningens regler informeres herom, *inden* den nye databehandling sker, jf artikel 13, stk. 3, smh. med stk. 2. Dette er en ny forpligtelse i forhold til den tidligere regulering, og formålet er at skabe gennemsigtighed og transparens i de store datastrømme i den digitale tidsalder.

77 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1, s. 293.

78 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 30.

Baseret på Justitsministeriets svar til Folketingets Retsudvalg fortolkes bestemmelsen formentlig nationalt indskrænkende til kun at omfatte den dataansvarliges egen videre*anvendelse* til nye formål.[79] Reglen finder derimod ikke anvendelse, hvis den dataansvarlige videre*giver* oplysningerne til en anden dataansvarlig, som ønsker at behandle oplysningerne til et nyt formål. Her er det den nye dataansvarlige, der skal informere efter artikel 14. Der kan dog være fastsat særlige regler om pligt til forudgående information, dvs information inden videregivelsen.

Medmindre der er tale om samkøring i kontroløjemed, følger det af databeskyttelseslovens § 23, at denne (nye) informationspligt ved videreanvendelse ikke gælder, når offentlige myndigheder viderebehandler personoplysninger til nye formål, og viderebehandlingen af oplysningerne sker på baggrund af regler fastsat efter lovens § 5, stk. 3, som efter den tilknyttede politiske aftale skal i høring i Datatilsynet, og godkendes af det relevante folketingsudvalg samt Folketingets Retsudvalg.[80]

Ovenstående betyder, at der ikke skal informeres, når det i bekendtgørelsesform er bestemt, at en bestemt videre brug af de indsamlede personoplysninger lovligt skal kunne finde sted i den offentlige forvaltning. Netop for helbredsoplysninger og genetiske oplysningers vedkommende kan sådanne bekendtgørelser dog kun udstedes, hvis den nye anvendelse er forenelig med den oprindelige, jf lovens § 5, stk. 3, 3. punkt, eller en lovbestemt tavshedspligt ikke gennembrydes. Sidstnævnte kan være sundhedslovens § 40 om sundhedspersoners tavshedspligt.

Informationspligten efter artikel 13, stk. 3, gælder ifølge databeskyttelsesloven heller ikke, hvis den registreredes interesse i oplysningerne findes at burde vige for afgørende hensyn til private interesser, herunder hensynet til den pågældende selv, jf databeskyttelseslovens § 22, stk. 1. Undtagelse kan også gøres efter de supplerende danske regler, hvis den registreredes interesse i at få kendskab til oplysningerne findes at burde vige for afgørende hensyn til offentlige interesser (hvor en række eksempler på sådanne offentlige interesser er opregnet i bestemmelsens nr. 1 - 10), jf databeskyttelseslovens § 22, stk. 2. Der skal foretages en konkret vurdering af, om der er nærliggende fare for, at de pågældende interesser lider skade af væsentlig betydning. I modsætning til undtagelse efter databeskyttelseslovens § 23, må der efter § 22 dog kun undtages i det omfang, at de modstående hensyn kan begrunde undtagelsen. De øvrige informationer, fx om den dataansvarliges identitet og databeskyttelsesrådgiver, skal stadig gives til den registrerede.[81]

Opsummerende vil en privat udbyder af tjenester i forbindelse med brug af wearables meget ofte være underlagt den ovenfor beskrevne informationspligt både ved indsamling *og* ved videreanvendelse til nye formål. Der vil være begrænset mulighed

79 Antagelsen er baseret på, at ministeriet på intet tidspunkt nævner en sådan underretningspligt, men udelukkende har besvaret spørgsmålene med henvisning til intern videreanvendelse. Antagelsen er dog ikke utvivlsom.

80 Gengivet i Betænkning afgivet af Retsudvalget den 9. maj 2018, https://www.retsinformation.dk/Forms/R0710.aspx?id=201193. Se også Svar på spørgsmål 115 og 126.

81 Datatilsynets vejledning om registreredes rettigheder, pkt. 3.4.3.

for at undtage helt, men i et vist omfang kan der undtages delvist, når dette fx er nødvendigt af hensyn til ophavsretlig beskyttelse af software. Det vil derimod bero på omfanget af fremtidige bekendtgørelser og øvrige særregler, hvor omfattende en informationsforpligtelse der vil påhvile wearables-aktører ved videreanvendelse af de modtagne personoplysninger til nye formål.

7.1.3 Informationspligt når indsamling ikke sker hos den registrerede selv
Databeskyttelsesforordningens artikel 14 ligner artikel 13 ganske meget, men regulerer den situation, at personoplysningerne indsamles hos andre end den registrerede; enten fra tredjemand eller anden indirekte indsamling. De informationer, den dataansvarlige skal give til den registrerede, er grundlæggende de samme som efter artikel 13. Der skal dog også informeres om kategorier af personoplysninger, fra hvilken kilde personoplysningerne hidrører, samt i påkommende tilfælde om de stammer fra offentligt tilgængelige kilder, jf artikel 14, stk. 1, litra e, og stk. 2, litra f.

Hvor oplysningerne indsamles indirekte, det vil sige ikke udleveres af den registrerede selv, skal den dataansvarlige efterfølgende meddele de nævnte oplysninger inden for en rimelig frist efter indsamlingen af personoplysningerne, men senest inden for en måned, jf artikel 14, stk. 3, litra a. Hvis personoplysningerne skal bruges til at kommunikere med den registrerede, skal underretningen dog ske senest på tidspunktet for den første kommunikation med den registrerede, jf artikel 14, stk. 3, litra b. Er oplysningerne bestemt til videregivelse til en anden modtager, skal informationspligten iagttages senest, når personoplysningerne videregives første gang, jf artikel 13, stk. 3, litra c.

Når den registrerede selv samler dataene og udleverer dem til den dataansvarlige sundhedsmyndighed (mellemledsituationen), er der ikke tvivl om, at sundheds-myndighedernes modtagelse af oplysningerne falder ind under artikel 13, jf herom ovenfor. Der kan derimod være usikkerhed i forhold til, om selve indsamlingen via de forskellige former for wearables og profilering via tilknyttede tjenester skal regnes som direkte indsamling hos den registrerede efter artikel 13, eller kan kategoriseres som indsamling omfattet af databeskyttelsesforordningens artikel 14. Kategoriseringen vil, som det fremgår af ovenstående, bla have betydning for tidspunktet for informationen.

Dette vil dog formentlig primært være af akademisk interesse, da det må antages, at information om dataindsamling via wearables i videst muligt omfang skal ske forudgående, hvilket vil sige inden det pågældende wearable tages i brug. Om ikke andet vil dette formentlig følge af databeskyttelsesforordningens generalklausul om lovlighed, rimelighed og gennemsigtighed i artikel 5, stk. 1, litra a. Der kan her sammenlignes med, at der tidligere med hjemmel i persondatalovens § 5, stk. 1, litra a, om god databehandlingsskik blev krævet forhåndsinformation til registrerede i en række atypiske indsamlingssituationer. Dette var bla tilfældet, når der ville ske

en indgribende behandling af (potentielt) fortrolige eller følsomme oplysninger.[82] Eksempler er arbejdsgiveres kontrol af ansattes internetforbrug og mails samt brug af overvågning i lokaler mv, samkøringer i kontroløjemed, formentlig videregivelse af lønoplysninger til bredere kreds samt kreditvurderinger baseret på samkøringer. Wearables med tilknyttede profileringstjenester synes at ligge i naturlig forlængelse heraf.

7.1.4 Informationspligt ved videreanvendelse af oplysninger, der ikke er indsamlet hos den registrerede

Også artikel 14 indeholder den nye regel om information om viderebehandling til nye formål, jf artikel 14, stk. 4. Heller ikke her indtræder denne informationspligt i Danmark, når offentlige myndigheder viderebehandler personoplysningerne til et andet formål end det, hvortil de er indsamlet, og viderebehandlingen desuden sker på baggrund af regler fastsat efter lovens § 5, stk. 3, jf loven § 23, se del I, afsnit 7.1.2.

Forordningen indeholder en række undtagelser til informationspligten i artikel 14, stk. 1. For det første kan information undlades, hvis og i det omfang den registrerede allerede er bekendt med oplysningerne, jf artikel 14, stk. 5, litra a. Informationspligten indtræder heller ikke, hvis gennemførelsen viser sig umulig eller vil kræve en uforholdsmæssigt stor indsats, jf artikel 14, stk. 5, litra b. Det samme gælder efter litra b, i det omfang videregivelsen af de pågældende oplysninger til den registrerede sandsynligvis vil gøre det umuligt eller i alvorlig grad vil hindre opfyldelse af formålene med den pågældende databehandling. Der er endvidere ingen informationspligt, hvis indsamling eller videregivelse udtrykkelig er fastsat i EU-ret eller i dansk ret, og denne lovgivning fastsætter passende foranstaltninger til beskyttelse af den registreredes legitime interesser, jf artikel 14, stk. 2, litra c. Endelig gælder informationspligten ikke, såfremt de pågældende personoplysninger skal forblive fortrolige som følge af tavshedspligt i henhold til EU-retten eller dansk ret, jf databeskyttelsesforordningens artikel 14, stk. 5, litra d. Disse undtagelser kan anvendes både af en privat udbyder af tjenester forbundet til wearables og inden for den offentlige sundhedssektor.

7.2 Indsigtsret

Efter forordningens artikel 15 har en registreret ret til at få den dataansvarliges bekræftelse på, om der behandles personoplysninger om den pågældende. Hvis det er tilfældet, har den registrerede også ret til at få adgang til personoplysningerne og følgende information:

a) Formålene med databehandlingen,
b) De berørte kategorier af personoplysninger,
c) De modtagere eller kategorier af modtagere, som personoplysningerne er eller vil blive videregivet til, og
d) Om muligt det påtænkte tidsrum, hvor personoplysningerne vil blive opbevaret, eller, hvis dette ikke er muligt, de kriterier der anvendes til fastlæggelse af dette tidsrum.

82 Motzfeldt, Hanne Marie. God databehandlingsskik – udvalgte problemstillinger ved forvaltningsmyndigheders videregivelse af personoplysninger, DJØF 2009, s. 217 ff.

Den dataansvarlige skal også – hvor det er relevant – give den registrerede information om:

e) Retten til at anmode om berigtigelse eller sletning af personoplysninger eller begrænsning af databehandling af personoplysninger vedrørende den registrerede eller til at gøre indsigelse mod en sådan databehandling,
f) Retten til at indgive en klage til en tilsynsmyndighed,
g) Enhver tilgængelig information om, hvorfra personoplysningerne stammer, hvis de ikke indsamles hos den registrerede, og
h) Forekomsten af automatiske afgørelser, herunder profilering, og som minimum meningsfulde oplysninger om logikken heri samt betydningen og de forventede konsekvenser af en sådan databehandling for den registrerede.

Som det fremgår, er der to særlige aspekter relateret til wearables, når der dannes profiler af de registrerede.

For det første giver bestemmelsen den registrerede ret til at få udleveret de oplysninger, den dataansvarlige behandler om vedkommende. Når en wearable-tjeneste profilerer de registrerede brugere, behandles ikke kun de oplysninger, som algoritmerne så at sige fodres med – men også de oplysninger der udgør resultatet. Anderledes udtrykt skal den registrerede både have udleveret de personoplysninger, der anvendes til at profilere (input), og information om den dannede profil og de "kategorier", den registrerede er blevet placeret i (output).[83] *Se i øvrigt ovenfor, del I, afsnit 7.1.1. om information om logikken bag profilering.*

For det andet er bestemmelsen i artikel 15, stk. 4, formentlig mere relevant i forbindelse med brug af wearables end ved mere traditionelle former for databehandling. Efter artikel 15, stk. 4, må retten til indsigt ikke krænke andres rettigheder eller frihedsrettigheder herunder forretningshemmeligheder eller intellektuel ejendomsret; navnlig den ophavsret som programmerne er beskyttet af. Dette kan fx have betydning, hvis en registreret ønsker viden om, *hvordan* en wearable fungerer eller danner vedkommendes profil, da sådan software kan være ophavsretligt beskyttet, jf også præambelbetragtning nr. 63.

Undtagelserne til indsigtsretten er derudover at finde i databeskyttelseslovens § 22, se herom ovenfor, del I, afsnit 7.1.2. Herudover kan der undtages fra indsigt i samme omfang som efter reglerne i §§ 19 - 29 og 35 i lov om offentlighed i forvaltningen, jf databeskyttelseslovens § 22, stk. 3.

Det kan samlet vurderes, at patienter vil have en ret vidtgående adgang til indsigt i de personoplysninger, der er indsamlet om dem, deres eventuelle profiler, samt de øvrige informationer nævnt i artikel 15. Det bemærkes, at Det Europæiske Databeskyttelsesråd anser det som god praksis – ikke et egentligt krav – at

83 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 17.

give de registrerede adgang til selv at undersøge deres profil og detaljer om databehandlingen, jf også præambelbetragtning nr. 63.[84]

7.3 Berigtigelse og sletning

Der er stor opmærksomhed omkring reglerne om berigtigelse og sletning i databeskyttelsesforordningens artikel 16 og 17. Betydningen af reglerne om berigtigelse og sletning er dog meget forskellig for en kommerciel udbyder af wearables-tjenester henholdsvis for en sundhedsmyndigheds brug af tilsvarende til patientbehandling eller forebyggende indsatser.

Det fremgår af databeskyttelsesforordningens artikel 16, at den registrerede har ret til at få *urigtige* personoplysninger om sig selv berigtiget af den dataansvarlige uden unødig forsinkelse. Den registrerede har under hensyntagen til formålene med databehandlingen også ret til at få fuldstændiggjort ufuldstændige personoplysninger bla ved at fremlægge en supplerende erklæring. Sker sådan berigtigelse, skal den dataansvarlige som udgangspunkt yderligere underrette dem, som oplysningerne er videregivet til, jf forordningens artikel 19. Dette vil således give de registrerede mulighed for at få korrigeret i alle led af de "kæder", som er beskrevet i del I, afsnit 3. Også her gælder det, at behandlede personoplysninger ikke kun er de oplysninger, der indsamles via et wearable. Dannes der profiler, er også de vurderinger mv, der er dannet, omfattet af begrebet personoplysninger – hvorfor der er ret til sletning eller korrektion af både indsamlede og dannede profiler.[85] Det Europæiske Databeskyttelsesråd anvender i sin udtalelse om automatiske beslutninger og profilering følgende eksempel:

"I en lokal kirurgisk kliniks computersystem placeres en person i en gruppe af personer, som højst sandsynligt vil få en hjertesygdom. Denne "profil" er ikke nødvendigvis ukorrekt, selv om den pågældende aldrig vil få en hjertesygdom. Det anføres blot i profilen, at det er mere sandsynligt, at vedkommende får denne sygdom. Dette kan være faktuelt korrekt rent statistisk. Den registrerede har imidlertid under hensyntagen til formålet med behandlingen ret til at fremlægge en supplerende erklæring. I ovennævnte scenarie kunne denne fx baseres på et mere avanceret medicinsk computersystem (og statistisk model), hvor der tages højde for yderligere oplysninger og foretages mere detaljerede undersøgelser end på den lokale kirurgiske klinik, hvor mulighederne er mere begrænsede."[86]

Anderledes udtrykt vil de registrerede som udgangspunkt have ret til at få deres profiler berigtiget ved at få tilføjet en erklæring, uanset om der kan føres bevis for disses rigtighed eller ej. Denne ret vil gælde både i forhold til sundhedsmyndigheder og i forhold til kommercielle udbydere af wearables-tjenester.

---

84 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 31.

85 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 16.

86 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 19.

For så vidt angår den offentlige sektor, antages det i den danske betænkning om databeskyttelsesforordningen, at bestemmelsen ikke indebærer ændringer i forhold til nugældende ret i den offentlige sektor, hvorefter der ved klart faktuelt forkerte oplysninger tilføjes supplerende tekster i journaler, og der ikke sker sletning.[87] Hertil kommer, som beskrevet i del I, afsnit 1, at fravigelser kan følge af særlovgivningen, herunder den sundhedsretlige regulering. Det må derfor antages, at bestemmelsen i artikel 16 får begrænset betydning i den offentlige sundhedssektor, idet det vil være journalføringsreglerne, der regulerer området.

Databeskyttelsesforordningens artikel 17, der også kaldes retten til at blive glemt, indeholder retten til *sletning af korrekte oplysninger*. Udgangspunktet efter bestemmelsens første stykke er, at registrerede har ret til at få slettet deres personoplysninger, hvis forsat behandling af oplysningerne ikke længere er nødvendig for at opfylde et databehandlingsformål, eller der ikke eksisterer et andet databehandlingsgrundlag, efter at den registrerede har trukket et samtykke tilbage, jf artikel 17, stk. 1, litra a - b. Herudover er der ret til at få slettet oplysninger, hvis den registrerede berettiget gør indsigelse af særlige grunde, der vedrører den pågældendes særlige situation, jf artikel 17, stk. 1, litra c. Tilsvarende gælder, hvis databehandlingen er ulovlig, at den dataansvarlige er retligt forpligtet i lovgivningen til at slette oplysningerne, eller hvis indsamlingen skete i forbindelse med udbud af informationssamfundstjenester, mens den registrerede var barn, jf artikel 17, stk. 1, litra d - f.

Ingen af disse opregnede grunde giver dog adgang til at få slettet personoplysninger, hvis forsat databehandling er nødvendig for at *"overholde en retlig forpligtelse, der kræver behandling i henhold til EU-retten eller medlemsstaternes nationale ret, og som den dataansvarlige er underlagt, eller for at udføre en opgave i samfundets interesse, eller som henhører under offentlig myndighedsudøvelse, som den dataansvarlige har fået pålagt"*. Retten til at blive glemt viger også, hvis databehandlingen er nødvendig for at forfølge hensyn til samfundsinteresser på folkesundhedsområdet i overensstemmelse med artikel 9, stk. 2, litra h eller i, samt artikel 9, stk. 3. Endelig viger retten, hvis forsat databehandling er nødvendig for at forfølge interesser, der er nødvendige for at forfølge arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål, og sletning sandsynligvis vil gøre det umuligt eller i alvorlig grad hindre dette, eller databehandling er nødvendig for, at retskrav kan fastlægges, gøres gældende eller forsvares.

Ovenstående følger af databeskyttelsesforordningens artikel 17, stk. 3, litra b – e, og indebærer i grove træk, at artikel 17 næppe vil få nogen videre betydning for det offentlige sundhedsvæsen. Bestemmelsen kan derimod få betydning for forholdet mellem den registrerede og en kommerciel udbyder af tjenester forbundet til wearables i de tilfælde, hvor sundhedsmyndigheden ikke er direkte involveret i et samarbejde med udbyderen, hvor denne er databehandler, se del I, afsnit 3 og databeskyttelsesforordningens artikel 17, stk. 2, litra b-d og i sjældnere tilfælde e.

87 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1 s. 330 og s. 338.

Anderledes udtrykt vil det i realiteten være de sundhedsretlige journalregler og arkivlovgivningen, der er afgørende for, om en registeret har en ret til at få slettet oplysninger inden for sundhedssektoren – ikke databeskyttelsesforordningens regler om berigtigelse og sletning. Reglerne vil derimod give borgeren mulighed for at sikre sig, at kommercielle udbydere overholder principperne om rigtighed (datakvalitet) og opbevaringsbegrænsning (tidsbegrænsning) i forordningens artikel 5, stk. 1, litra e og d, samt tilbagetrækning af samtykke efter artikel 7.

7.4. Indsigelse

I databeskyttelsesforordningens artikel 21 er indsat en almindelig, bred indsigelsesret. Retten er imidlertid begrænset til at gælde, når der behandles almindelige personoplysninger på baggrund af forordningens artikel 6, stk. 1, litra e og f. Da helbredsoplysninger er følsomme oplysninger, jf oven for del I, afsnit 5, vil retten få begrænset betydning i forbindelse med brug af wearables i sundhedssektoren. For så vidt angår relationen mellem registrerede og kommercielle udbydere, kan der dog, som tidligere beskrevet være tilfælde, hvor oplysningerne må regnes som almindelige – men her vil grundlaget for behandling af oplysninger oftest være artikel 6, stk. 1, litra a, om samtykke eller litra b, om kontrakter, hvorfor bestemmelsen heller ikke her kan antages at få videre betydning for beskyttelsen af borgerne.

7.5. Automatiske afgørelser

Af artikel 22, stk. 1, følger, at en registreret har ret til ikke at være genstand for en afgørelse, der alene er baseret på automatisk databehandling, herunder profilering, som har retsvirkning eller på tilsvarende vis betydeligt påvirker den pågældende.[88]

Formålet med bestemmelsen i databeskyttelsesforordningens artikel 22, stk. 1 er at beskytte mod såvel data som programmering af dårlig kvalitet. Ringe data- og programmeringskvalitet kan føre til urigtige beslutninger, som ikke desto mindre bliver accepterede pga for megen tiltro til teknologien, hvorfor grundtanken er at give mulighed for en menneskelig vurdering (kontrol).

Til trods for, at artikel 22, stk. 1 er formuleret som en rettighed, betragtes den af Det Europæiske Databeskyttelsesråd som et forbud. Dette forbud er dog langt fra undtagelsesfrit. Artikel 22, stk. 2, litra b, undtager, når afgørelsen er hjemlet i lovgivningen – forudsat at der indføres passende foranstaltninger til beskyttelse af den registreredes rettigheder og frihedsrettigheder samt legitime interesser. En sådan garanti kan ifølge de danske forarbejder fx være en adgang til at klage over den trufne afgørelse (fx en beslutning om behandlingsform).[89] Hertil gælder imidlertid det, man kalder en undtagelse til undtagelsen. Er der – som ved brug af wearables – tale om følsomme oplysninger, gælder undtagelsen ikke, medmindre behandlingen

88 Af forordningens præambelbetragtning nr. 71, første afsnit, sidste punktum fremgår yderligere, at automatiske afgørelser ikke bør omfatte børn. Dette antages dog af det danske datatilsyn kun at gælde i forbindelse med myndighedsudøvelse, hvis barnet interagerer direkte med myndigheden – men ikke hvis interaktionen med myndigheden foretages på vegne af barnet af dets forældre eller værge, se Datatilsynets vejledning om de registreredes rettigheder, 2018, pkt. 10.2.

89 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1, s. 380.

af oplysningerne hviler på enten artikel 9, stk. 2, litra a, om databeskyttelsesretligt samtykke eller artikel 9, stk. 2, litra g, om væsentlige samfundsinteresser.

Anderledes udtrykt vil automatiske beslutninger truffet af det offentlige sundhedsvæsen på grundlag af oplysninger indsamlet fra wearables være omfattet af hovedreglen om retten til indsigelse i artikel 22, stk. 1, medmindre behandlingen (også) hviler på forordningens artikel 9, stk. 2. litra g, om væsentlige samfundsinteresser (dobbelt hjemmelsgrundlag). Det vil dog formentlig ofte være tilfældet, hvorfor man returnerer til undtagelsen i artikel 22, stk. 2, litra b. Artikel 22 hindrer således ikke brug af automatiske beslutningssystemer i den offentlige sektor, når beslutningerne har hjemmel i lovgivningen, og der er fastsat passende garantier.

For så vidt angår kommercielle udbydere af tjenester forbundet til wearables, vil artikel 22, stk. 1, næppe heller have nogen videre betydning. Idet behandlingen oftest vil hvile på den registreredes samtykke eller en tilladelse efter databeskyttelseslovens § 7, stk. 4, vil indsigelsesretten ikke finde anvendelse, jf artikel 22, stk. 4, jf artikel 22, stk. 2, litra c.

Opsummerende har bestemmelsen om ret til indsigelse mod automatiske beslutninger næppe nogen større selvstændig betydning i forbindelse med brug af wearables i sundhedssektoren.

AUTOMATISKE AFGØRELSER
Afgørelser i databeskyttelsesforordningens forstand må ikke forveksles med det danske, forvaltningsretlige afgørelsesbegreb. Efter databeskyttelsesforordningen er det centrale, at beslutningen påvirker den registrerede betydeligt. Det Europæiske Databeskyttelsesråd skriver herom: "Selv om en beslutningsproces ikke påvirker den enkeltes juridiske rettigheder, kan den stadig være omfattet af artikel 22, hvis den på tilsvarende vis betydeligt påvirker den pågældende. Selv om der ikke er sket ændringer i den registreredes juridiske rettigheder eller forpligtelser, vil den pågældende med andre ord stadig kunne blive påvirket i tilstrækkelig grad til at kræve beskyttelse i henhold til denne bestemmelse. I databeskyttelsesforordningen indsættes ordene "på tilsvarende vis" (findes ikke i artikel 15 i direktiv 95/46/EF) foran "betydeligt påvirker". Tærsklen for betydning skal derfor være den samme som for en afgørelse, der har retsvirkning. I betragtning 71 anføres følgende typiske eksempel: "automatisk afslag på en onlineansøgning om kredit eller e-rekrutteringsprocedurer uden nogen menneskelig indgriben". Hvis databehandlingen skal kunne anses for betydeligt at påvirke en person, skal virkningerne af behandlingen være tilstrækkeligt betydelige eller vigtige for at blive taget i betragtning. Med andre ord skal afgørelsen potentielt (…) betydeligt påvirke den pågældendes situation, adfærd eller valg, have langvarig eller permanent indvirkning på den registrerede eller medføre udelukkelse eller forskelsbehandling af enkeltpersoner i de

mest ekstreme tilfælde. Det er vanskeligt at præcisere, hvad der vil blive anset for at være tilstrækkelig betydeligt til at opfylde tærsklen, selv om følgende afgørelser kunne falde ind under denne kategori: Afgørelser, der påvirker en persons økonomiske situation, fx vedkommendes adgang til kredit, afgørelser, der påvirker en persons adgang til sundhedsydelser, afgørelser, hvorved en person udelukkes fra en beskæftigelsesmulighed eller står betydeligt svagere og afgørelser, der påvirker en persons adgang til uddannelse, fx optagelse på universitetet" (Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 22-23). Det betyder, at fx en beslutning om, hvilken af flere behandlinger en patient tilbydes, formentlig vil være en afgørelse omfattet af artikel 22.

En afgørelse efter artikel 22 skal "alene" være baseret på automatisk behandling. Det afgørende er her, om der i realiteten sker en menneskelig vurdering af beslutningsgrundlag og udfald. Om dette skriver Det Europæiske Databeskyttelsesråd: "Den dataansvarlige kan ikke omgå bestemmelserne i artikel 22 ved at opdigte menneskelig indgriben. Hvis en person fx rutinemæssigt anvender automatisk genererede personprofiler uden reel indflydelse på resultatet, vil det stadig være en afgørelse, der alene er baseret på automatisk behandling. For at kunne betragtes som menneskelig indgriben skal den dataansvarlige sikre, at et tilsyn med afgørelsen er meningsfuldt og ikke blot en tom gestus. Det bør foretages af en person, der har den fornødne kompetence og mulighed for at ændre afgørelsen. Der bør som led i analysen tages hensyn til alle relevante oplysninger. Som led i konsekvensanalysen vedrørende databeskyttelse bør den dataansvarlige identificere og registrere omfanget af enhver menneskelig indgriben i beslutningsprocessen og i hvilken fase heraf" (Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 21-22).

Inden for en given type af automatiserede beslutningsprocesser vil der formentlig ofte opstå den situation, at nogle beslutninger træffes automatisk, mens der sker en reel menneskelig vurdering i forhold til andre beslutninger. Billeder fra mammografi kan fx sorteres af Machine Learning algoritmer i tre kategorier. For det første billeder, hvor softwaren vurderer, at der ikke er grund til at iværksætte tiltag (ikke kræft). For det andet billeder, der er uafklarede og derfor henvises til lægelig vurdering (tvivl). For det tredje billeder, hvor softwaren vurderer, at der skal iværksættes behandling (kræft). Hvis kun de to sidstnævnte kategorier overgår til en konkret lægelig vurdering, vil der være truffet rent automatiske afgørelser i den første kategori, idet softwarens vurdering lægges til grund for beslutningen om, at der ikke skal følges op på billedet.

DEL II. CENTRALE ASPEKTER VED BRUG AF WEARABLES

1. Samtykke som databehandlingsgrundlag

Samtykke regnes som en ganske integreret bestanddel af den danske offentligretlige retskultur. Det er imidlertid væsentligt at være opmærksom på, at denne kultur hviler på en i forhold til databeskyttelsesretten anderledes opfattelse af, hvornår et samtykke er frivilligt i retlig forstand, se herom nedenfor. Samtidig er det databeskyttelsesretlige samtykke af stor betydning, da samtykke er det mest relevante retsgrundlag for kommercielle udbydere af tjenester knyttet til wearables, hvis disse ikke er databehandlere for en sundhedsmyndighed og dermed behandler efter sundhedsmyndighedens databehandlingsgrundlag.

SAMTYKKE TIL BEHANDLING AF OPLYSNINGER ER IKKE DET SAMME SOM SAMTYKKE TIL SYGDOMSBEHANDLING
Det er væsentligt at skelne mellem det samtykke, der gives til sygdomsbehandling (patientbehandling) og det samtykke, der gives til elektronisk behandling af personoplysninger (databehandling).
De to "samtykker" skal betragtes som adskilte. Et samtykke til fx operation er ikke et samtykke til elektronisk behandling af de oplysninger, der indsamles i forbindelse med operationen. Tilsvarende gælder, at et samtykke til at indgå i en given forebyggende indsats ikke samtidig er et samtykke til behandling af helbredsoplysninger via et wearable.

Behandling af almindelige personoplysninger er lovlig efter databeskyttelses-forordningen, når den registrerede har givet *utvetydigt* samtykke til behandling af sine personoplysninger til et eller flere specifikke formål, jf forordningens artikel 6, stk. 1, litra a. Behandling af følsomme personoplysninger, herunder helbredsoplysninger, er lovlig, når den registrerede har givet *udtrykkeligt* samtykke til behandling af sådanne personoplysninger til et eller flere specifikke formål, jf artikel 9, stk. 2, litra a.

SAMTYKKE
Samtykke fra den registrerede defineres i forordningen som "enhver frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved den registrerede ved erklæring eller klar bekræftelse indvilliger i, at personoplysninger, der vedrører den pågældende, gøres til genstand for behandling", jf artikel 4, nr. 11.

Hvad der nærmere ligger i samtykke, uddybes dels i definitionen af samtykke i forordningens artikel 4, nr. 11, dels i databeskyttelsesforordningens præambelbetragtning nr. 32, hvorefter: "samtykke bør gives i form af en klar bekræftelse, der indebærer en frivillig, specifik, informeret og utvetydig viljestilkendegivelse fra den registrerede, hvorved vedkommende accepterer, at personoplysninger om vedkommende behandles. Tavshed, forud afkrydsede felter eller inaktivitet bør ikke udgøre samtykke. Samtykke bør dække alle behandlingsaktiviteter, der udføres til det eller de samme formål. Når behandling tjener flere formål, bør der gives samtykke til dem alle. Hvis den registreredes samtykke skal gives efter en elektronisk anmodning, skal anmodningen være klar, kortfattet og ikke unødigt forstyrre brugen af den tjeneste, som samtykke gives til".

Hertil kommer, at der i databeskyttelsesforordningens artikel 7 stilles en række betingelser til samtykket. Er betingelserne ikke opfyldt, er samtykket ikke gyldigt – og kan ikke anvendes som grundlag for behandling af personoplysninger.

De forskellige krav til det databeskyttelsesretlige samtykke er tæt forbundne og til dels overlappende.

I kravet om, at et samtykke skal være *specifikt*, ligger, at samtykket skal være konkretiseret, således at det klart og utvetydigt fremgår, hvad der meddeles samtykke til, herunder hvilke oplysninger der må behandles på baggrund af samtykket, af hvem og til hvilke formål, jf fx Datatilsynets journalnummer 2007-321-0047.

Af kravet om, at samtykket skal være *informeret*, følger, at den samtykkende skal være klar over, hvad det er, vedkommende meddeler samtykke til – dvs kan vurdere, om vedkommende vil give samtykke. Af databeskyttelsesforordningens præambelbetragtning nr. 42 fremgår om information, at den registrerede som minimum skal gøres bekendt med den dataansvarliges identitet og formålene med den behandling, som personoplysningerne skal bruges til. Forordningens artikel 7, stk. 2, supplerer her ved at stille krav til den måde, der informeres på. Fx skal der anvendes et egnet sprog, så de registrerede forstår, hvad de samtykker til – herunder til hvilke formål oplysningerne kan bruges. Anvendelse af en kompliceret retlig eller teknisk jargon lever ikke op til kravene. Dertil kommer, at de informationer, der gives til de registrerede, skal være adskilt fra andre tekster og være klare og tilstrækkeligt synlige, så de registrerede ikke overser dem.

I kravet om *utvetydighed* ligger, at den registrerede skal give et aktivt signal, som er tilstrækkeligt klart til, at det markerer vedkommendes vilje og er forståeligt for den dataansvarlige. Et eksempel herpå kan være, at der forudgående gives information, hvorefter ibrugtagelse af en teknologi betragtes som samtykke, saml. fx Datatilsynets journalnummer 2007-212-0042 (FDB og Coop) om ibrugtagelse af medlemskort. En sådan konstruktion vil dog sjældent kunne anvendes ved brug af wearables, idet behandling af helbredsoplysninger kræver et udtrykkeligt, ikke blot utvetydigt, samtykke, jf artikel 9, stk. 2, litra a – og der vil oftest være tale

om helbredsoplysninger, se del I, afsnit 5. Et *udtrykkeligt* samtykke forudsætter i modsætning til det utvetydige samtykke et aktivt svar – mundtligt eller skriftligt – hvorved den pågældende udtrykker ønske om, at hans/hendes oplysninger behandles med henblik på bestemte formål.

Databeskyttelsesforordningen indeholder flere fortolkningsbidrag til forståelsen af *frivillighed*. Af præambelbetragtning nr. 42 fremgår, at "samtykke bør ikke anses for at være givet frivilligt, hvis den registrerede ikke har et reelt eller frit valg eller ikke kan afvise eller tilbagetrække sit samtykke, uden at det er til skade for den pågældende". I den efterfølgende betragtning nr. 43 står følgende: "med henblik på at sikre, at der frivilligt er givet samtykke, bør samtykke ikke udgøre et gyldigt retsgrundlag for behandling af personoplysninger i et specifikt tilfælde, hvis der er en klar skævhed mellem den registrerede og den dataansvarlige, navnlig hvis den dataansvarlige er en offentlig myndighed, og det derfor er usandsynligt, at samtykket er givet frivilligt under hensyntagen til alle de omstændigheder, der kendetegner den specifikke situation. Samtykke formodes ikke at være givet frivilligt, hvis det ikke er muligt at give særskilt samtykke til forskellige behandlingsaktiviteter vedrørende personoplysninger, selv om det er hensigtsmæssigt i det enkelte tilfælde, eller hvis opfyldelsen af en kontrakt, herunder ydelsen af en tjeneste, gøres afhængig af samtykke, selv om et sådant samtykke ikke er nødvendigt for dennes opfyldelse".

Datatilsynet har sammen med en række andre myndigheder udsendt en vejledning om databeskyttelsesforordningens samtykkekrav i november 2017. Også denne vejledning kommer ind på skævheden mellem den dataansvarlige og den registrerede som en faktor, der kan udfordre samtykkets gyldighed som databehandlingsgrundlag. Under pkt. 3.3.1 står bla: "Det kan fx være tilfældet, hvis den dataansvarlige er en offentlig myndighed og den registrerede ansøger om en offentlig ydelse hos myndigheden. Den registrerede vil i dette tilfælde oftest ikke have andre alternativer end at give samtykke til behandlingen, hvis borgeren vil have ydelsen. Offentlige myndigheder bør derfor overveje anvendelsen af samtykke som behandlingshjemmel".

Det Europæiske databeskyttelsesråd kobler i den europæiske vejledning om samtykke efter databeskyttelsesforordningen frivillighed og ulighed i magtbalancer sæt sammen. I vejledningen står bla: "Elementet "frit" indebærer, at de registrerede har et reelt valg og kontrol. Generelt fastslås det i databeskyttelsesforordningen, at et samtykke er ugyldigt, hvis ikke den registrerede er i stand til at foretage et reelt valg, hvis han/hun føler sig tvunget til at give sit samtykke, eller hvis det vil få negative konsekvenser, hvis han/hun ikke samtykker. Hvis samtykke er knyttet til betingelser og vilkår og ikke kan forhandles, er det ikke givet frivilligt. Tilsvarende vil et samtykke ikke være frit, hvis ikke den registrerede kan sige nej til eller trække sit samtykke tilbage, uden at det er til skade for den registrerede. I databeskyttelsesforordningen tages der desuden hensyn til begrebet skævhed mellem den dataansvarlige og den registrerede."

Videre står der i vejledningen – selvom det ikke fuldkommen udelukkes, at offentlige myndigheder kan anvende samtykke som behandlingsgrundlag, at: ”Af betragtning 43 fremgår det klart, at det er usandsynligt, at offentlige myndigheder kan basere deres behandling på samtykke, for når den dataansvarlige er en offentlig myndighed, er der ofte en klar magtubalance i forholdet mellem den dataansvarlige og den registrerede. Det er endvidere klart, at den registrerede i de fleste tilfælde ikke har noget realistisk alternativ til at acceptere den dataansvarliges behandling(svilkår). Gruppen mener, at der er andre retsgrundlag, som i princippet er bedre egnede til de offentlige myndigheders aktiviteter.”[90]

Vejledningen om samtykke efter databeskyttelsesforordningen henviser til Artikel 29 gruppens tidligere udtalelser om samtykke under persondatadirektivet – og bemærker, at disse stadig kan regnes som gyldige.[91] Gruppen udtalte sig flere gange under persondatadirektivet om, hvornår der opstår udfordringer med at sikre, at samtykke er reelt frivilligt. I en udtalelse om samtykke står fx at ”for at et samtykke er gyldigt, skal det være frivilligt. Det betyder, at der ikke må være nogen risiko for vildledning, intimidering eller væsentlige negative konsekvenser for den registrerede, hvis han/hun ikke samtykker. Databehandling i en ansættelsessammenhæng, hvor der er et underordningsforhold, og i forbindelse med offentlige tjenester, fx inden for sundhedsområdet, kan kræve en nøje vurdering af, om der er tale om et frivilligt samtykke fra de ansattes/borgernes side.”[92]

Også i en række andre udtalelser om mere specifikke temaer forholdt denne gruppe sig til samtykkets tilsvarende begrænsninger i forhold til persondatadirektivet, herunder i udtalelsen om elektroniske patientjournaler (WP 131), i udtalelsen om behandling af personoplysninger ved ansættelsesforhold (WP 48) og i udtalelsen om Det Internationale Antidopingagenturs behandling af oplysninger (WP 162). Gruppen anførte i udtalelsen om elektroniske patientjournaler[93], at ”ved frivilligt samtykke menes en viljesbeslutning, som en person, der er ved sine evners fulde brug, har truffet uden nogen form for tvang af social, økonomisk, psykologisk eller anden art. Ethvert samtykke til databehandling, der er afgivet under trussel om, at den pågældende ikke vil blive sygdomsbehandlet eller få en dårligere sygdomsbehandling, kan ikke anses for at være frivilligt”. Gruppen anførte videre, ”at det er vildledende, hvis en erhvervsudøvende i sundhedssektoren, der er nødt til at behandle personoplysninger i et EPJ-system (..) forsøger at begrunde dette under henvisning til patientens samtykke. Anvendelsen af samtykke skal begrænses til de tilfælde, hvor patienten har et reelt valg og som følge heraf uden at lide skade kan trække sit samtykke tilbage.”

Opsummerende indikerer et særdeles overbevisende kildemateriale, at samtykke kun sjældent kan anvendes som sundhedsmyndighedernes databeskyttelsesretlige grundlag for behandling af personoplysninger i patientbehandlingssammenhænge.

---

90 Henvisninger fjernet her. WP 259, Retningslinjer vedrørende samtykke i henhold til forordning 2016/679, s. 6-7.

91 Ibid, s. 3.

92 WP 187 om samtykke, s. 38 ff.

93 WP 131 vedrørende behandling af personlige sundhedsoplysninger i elektroniske patientjournaler (EPJ), s. 9.

At sundhedsmyndigheder ikke kan bruge samtykke på grund af frivillighedsbetingelsen, udelukker imidlertid ifølge den danske betænkning om databeskyttelsesforordningen ikke, at der i sundhedsloven forsat stilles krav om indhentelse af samtykke til fx videregivelse fra borgere, der modtager en ydelse fra det offentlige.[94] Samtykket skal dog i så fald databeskyttelsesretligt betragtes som en yderligere foranstaltning, der indføres af hensyn til de registrerede, men *ikke* som det databeskyttelsesretlige behandlingsgrundlag.

Anderledes udtrykt skal det reelle databehandlingsgrundlag for sundhedsmyndighedernes behandling af helbredsoplysninger ofte findes i forordningens artikel 9, stk. 2, litra f, om retskrav, i artikel 9, litra g, om væsentlige samfundsinteresser og/eller artikel 9, stk. 2, litra h, jf databeskyttelseslovens § 7, stk. 3, om databehandling med henblik på forebyggende sygdomsbekæmpelse, diagnose, sygepleje eller patientbehandling, eller forvaltning af læge- og sundhedstjenester mv.

EU-Domstolen har vurderet spørgsmålet om frivillighed i Michael Schwartz, Sag C 291/12, om afgivelse af fingeraftryk til pas. Præmis 31-32 lyder som følger: ”31. Det fremgår af chartrets artikel 8, stk. 2, at personoplysninger kun kan behandles på grundlag af den berørte persons samtykke eller på et andet berettiget ved lov fastsat grundlag.” og ”32. Hvad for det første angår betingelsen om pasansøgeres samtykke til optagelse af deres fingeraftryk bemærkes, at det generelt er nødvendigt for EU-borgere at besidde et pas, bla for at kunne rejse til tredjelande, og at dette dokument skal indeholde fingeraftryk, jf artikel 1, stk. 2, i forordning nr. 2252/2004. EU-borgere, der ønsker at foretage sådanne rejser, kan derfor ikke frit modsætte sig behandlingen af deres fingeraftryk. Under disse omstændigheder kan pasansøgere ikke anses for at have samtykket til en sådan behandling.”

Som det er beskrevet indledningsvis i del I, afsnit 3, kan den dataansvarlige imidlertid også være (en af flere) kommercielle udbydere af wearables-tjenester. Her består det ovenfor beskrevne, ulige forhold ikke nødvendigvis – hvorfor det i højere grad er muligt at opfylde alle kravene til et gyldigt samtykke.

Udover de ovenfor beskrevne krav gælder det, at hvis samtykke anvendes som databehandlingsgrundlag, skal det samtidig sikres, at den registrerede kan trække dette tilbage – og at tilbagetrækning kan ske lige så let som afgivelse, jf databeskyttelsesforordningens artikel 7, stk. 3. Den dataansvarlige skal desuden sikre sig at kunne påvise, at den registrerede har givet samtykke til databehandling af sine personoplysninger, jf artikel 7, stk. 1. Herudover følger det af databeskyttelsesforordningens artikel 7, stk. 4, at der ved vurdering af, om samtykke er givet frit, tages størst muligt hensyn til bla om opfyldelse af en kontrakt, herunder om en tjenesteydelse, er gjort betinget af samtykke til behandling af personoplysninger, som ikke er nødvendig for opfyldelse af denne kontrakt.

94 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1, s. 152 ff.

For så vidt angår betydningen af den sidstnævnte betingelse, skaber denne en vis usikkerhed. I den danske betænkning om databeskyttelsesforordningen kobles artikel 7, stk. 4, sammen med frivillighed og præambelbetragtning nr. 42 og nr. 43. I betænkningen står herudover: "Netop det faktum, at artikel 7, stk. 4, indeholder ordet bla vil bevirke, at bestemmelsen i praksis vil kunne få betydning i en række forskellige situationer, hvor der kan siges at være en klar skævhed mellem den registrerede og den dataansvarlige. Det er vanskeligt at fastlægge rækkevidden af denne bestemmelse på forhånd, og bestemmelsen vil utvivlsomt blive udviklet gennem praksis i de kommende år Bestemmelsen må fastlægge et fortolkningsprincip om størst mulig hensyntagen til "skævheder" ved vurderingen af samtykkets gyldighed."[95] Når der opsamles data via wearables, vil der utvivlsomt også udenfor databehandlerkonstruktionen være situationer, hvor alle aktører er vidende om, at de indsamlede data skal anvendes af en sundhedsmyndighed i forbindelse med patientbehandling, se del I, afsnit 3 om forskellige samarbejdskonstruktioner. I sådanne tilfælde kan det ikke udelukkes, at den ulige relation mellem sundheds-myndighed og patient muligvis så-at-sige smitter af på relationen mellem den kommercielle udbyder og den registrerede. Afsmitningen vil i så fald formentlig være stærkere, når der er tale om data til patientbehandling end data til forebyggelse, da den registrerede som udgangspunkt må antages at stå svagest i sygdomsbehandlingssituationen.

Opsummerende er udgangspunktet, at samtykke til elektronisk behandling af helbredsoplysninger ikke bør bruges til at behandle helbredsoplysninger i forbindelse med sundhedsmyndighedernes patientbehandling – heller ikke når oplysningerne er indsamlet ved hjælp af et wearable. I stedet bør mulighederne for databehandling og udveksling af helbredsoplysninger ske med grundlag i databeskyttelseslovens artikel 9, stk. 2, litra f, g, h eller i, idet betingelserne i en eller flere af disse bestemmelser oftest vil være opfyldt, hvis sundhedsmyndighederne har brug for oplysninger til at udføre deres lovbestemte opgaver. I overensstemmelse med Datatilsynets vejledning om samtykke bør dette udgangspunkt kun fraviges, hvis det i sjældne tilfælde sker, at der ikke er et andet behandlingsgrundlag end samtykke, og oplysningerne er nødvendige for, at sundhedspersonen kan udføre sine opgaver.[96]

Kommercielle udbydere af wearables-services vil derimod sjældent samtidig tilbyde sygdomsbehandling – og selv i sådanne tilfælde vil udbyderen næppe have den samme styrkeposition som det offentlige sundhedsvæsen. Disse kommercielle udbydere vil derfor hyppigt kunne anvende samtykke til indsamling og videre behandling af helbredsoplysninger i forbindelse med brug af wearables. I de tilfælde, hvor der etableres en samarbejdsrelation med sundhedsmyndighederne, er der dog grund til at være opmærksom på, om databeskyttelsesforordningens artikel 7, stk. 4, kan indebære en skærpet vurdering af, om der indhentes flere oplysninger end nødvendigt for at opfylde formålet.

---

95 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1, s. 180 f.

96 Se samme, men i forhold til alle former for offentlige ydelser, Datatilsynets vejledning om samtykke, 2017, pkt. 3.3.1.

2. De databeskyttelsesretlige principper

I det følgende uddybes de databeskyttelsesretlige principper, der må anses som de mest relevante, når sundhedsmyndigheder behandler helbredsoplysninger om borgerne. Som beskrevet i del I, afsnit 4, har tidsbegrænsningsprincippet i databeskyttelsesforordningens artikel 5, stk. 1, litra e, ikke nogen videre betydning i sundhedssektoren, som er det centrale tema for Etisk Råd. Kravene til sikkerhed har derimod ganske stor betydning. De generelle betragtninger fremgår imidlertid af del II, afsnit 3 om databeskyttelse via design og indstillinger og sikkerhedsspørgsmål er samtidig beskrevet i andre af de underliggende notater udarbejdet i arbejdsgruppen. Heller ikke databeskyttelsesforordningens artikel 5, stk. 1, litra f, er dermed uddybet i det følgende.

2.1. Lovlighed, rimelighed og transparens

Kravet i databeskyttelsesforordningens artikel 5, stk. 1, litra a, antages i den danske betænkning om databeskyttelsesforordningen at svare til kravet om god databehandlingsskik i persondatalovens § 5, stk. 1.[97] I praksis har denne tidligere regel om god databehandlingsskik været anvendt til at sikre forudgående information i en række særlige databehandlingssammenhænge samt til at stille krav om, at de dataansvarlige skulle begrænse skadevirkningerne for de registrerede ved sikkerhedsbrud.

Forordningen bringer dog visse nye aspekter med sig. Der er sket en ændring af ordlyden, idet kravet om gennemsigtighed (transparens) nu er udtrykkeligt nævnt. Der er samtidig tale om en fælleseuropæisk standard, hvor det Europæiske Databeskyttelsesråd formentlig vil spille en større rolle for udviklingen af standarden end hidtil.

Den øgede harmonisering ses allerede ved, at der er givet en række konkrete anbefalinger om bedste praksis i de tæt forbundne vejledninger om henholdsvis transparens og om automatiske afgørelser og profilering. Anbefalingerne om bedste praksis er baseret på de forskellige tilsynsmyndigheders hidtidige erfaringer inden for området. De må antages at få betydning for, hvordan kravene til rimelighed og gennemsigtighed vil udvikle sig de kommende årtier.[98]

Sammenholdes de to vejledningers anbefalinger, kan det bla udledes, at data-ansvarlige, der foretager profilering i forbindelse med wearables-tjenester, bør overveje at etablere mekanismer, der giver de registrerede mulighed for selv at tilgå både deres personoplysninger og de profiler, der dannes om dem. Videre anbefales det, at de registrerede gives mulighed for selv at opdatere eller tilføje informationer til såvel de anvendte data som de profiler, der dannes af dem. Det synes endelig at være rådets opfattelse, at dette bør samles for alle behandlinger, der foretages af den dataansvarlige – dvs en samlet indgang; et databeskyttelsesretligt dashboard.

---

97 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1, s. 92 f.

98 Retningslinjer for gennemsigtighed i henhold til forordning 2016/679, WP 260 og Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251.

2.2. Udtrykkelighed, saglighed og formålsbestemthed

Af databeskyttelsesforordningens artikel 5, stk. 1, litra b, jf databeskyttelseslovens § 5 følger for det første et krav om, at indsamling af personoplysninger skal ske til *udtrykkeligt angivne og legitime formål*. Som gengivet i den danske betænkning om databeskyttelsesforordningen, blev det tilsvarende udtrykkelighedskrav i persondataloven og persondatadirektivet antaget at indebære, at[99]:

- Formålet skal være så åbenbart og udtrykkeligt, at alle involverede har den samme utvetydige forståelse af formålene uden hensyn til kultur eller sproglige forskelligheder.
- Meget vage og generelle beskrivelser af formålet med behandlingen af oplysninger opfylder ikke kravet. De dataansvarlige kan ikke fx angive til "administration" som formål, mens "til brug for udbud af sundhedsydelser" vil opfylde kravet.
- Der må ikke indsamles oplysninger, som den dataansvarlige ikke aktuelt har brug for, men som den dataansvarlige håber, at der senere viser sig at være behov for.

For så vidt angår kravet om legitime (saglige) formål, vil dette være opfyldt for sundhedsmyndighederne, hvis indsamlingen sker til formål, som det ligger inden for myndighedens område at varetage efter lovgivningen (i bred forstand). Kommercielle virksomheders indsamling af oplysninger, der ligger inden for den lovlige virksomhed, som de udøver, vil tilsvarende være til legitime (saglige) formål.

Efter databeskyttelsesforordningens artikel 5, stk. 1, litra b, og databeskyttelsesloven § 5 må indsamlede oplysninger – i mangel af samtykke fra den registrerede eller særskilt hjemmel herfor – desuden ikke senere bruges til formål, der er uforenelige med det oprindelige indsamlingsformål. Dette *formålsbestemthedsprincip* skal overholdes både ved intern databehandling og ved videregivelse af oplysninger.

Formålsbestemthed vurderes fra den registreredes afgivelse af oplysningerne – og er således ikke relevant for en sundhedsmyndigheds indsamling af oplysninger i de tilfælde, hvor den registrerede selv har anvendt en kommerciel aktørs wearable og via fx en digital kopi af en dannet profil eller en udskrift af samtlige data udleverer disse oplysninger til en sundhedsperson. Princippet regulerer dog sundhedsmyndighedens videre behandling af oplysningerne (efter den registreredes udlevering af oplysningerne).

99 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1, s. 83 med henvisninger til WP 203 om formålsbegrænsning s. 38 f.

FORMÅLSFORENELIGHED OG BEHANDLINGSGRUNDLAG ER TO FORSKELLIGE TING
Som det er beskrevet ovenfor i afsnit 6, skal alle databehandlinger både opfylde en behandlingsbetingelse og være i overensstemmelse med principperne i artikel 5, herunder princippet om formålsbestemthed. Det betyder, at en behandling kan være i overensstemmelse med formålsbestemthedsprincippet, men være udelukket som følge af, at der ikke er et behandlingsgrundlag. Omvendt kan der være et behandlingsgrundlag, men behandling være udelukket som følge af formålsbestemthedsprincippet.
Et fiktivt eksempel kan være en ældre borger med hoftebrud, der står til udskrivelse fra et hospital. Fra et databeskyttelsesretligt perspektiv, er det oplagt formålsforeneligt at videregive en række af de indsamlede personoplysninger til hjemmeplejen og genoptræningscentrene i borgerens kommune. Det skyldes den naturlige sammenhæng mellem sygdomsbehandlingen og den efterfølgende sociale omsorg. At princippet i artikel 5, stk. 1, litra b, er opfyldt, er imidlertid ikke ensbetydende med, at en behandlingsbetingelse er opfyldt.

Databeskyttelsesforordningens artikel 6, stk. 4, præambelbetragtning nr. 50 og databeskyttelsesloven § 5, stk. 2, indeholder en liste over forskellige momenter, som den dataansvarlige myndighed skal inddrage i sin vurdering af, om databehandling til et andet formål er forenelig med det formål, som personoplysningerne oprindelig blev indsamlet til.

Der skal for det første lægges vægt på enhver forbindelse mellem det oprindelige indsamlingsformål og formålet med den nu påtænkte viderebehandling. Heri ligger, at der ikke vil opstå problemer i form af formålsuforenelighed, hvis det nye formål ikke adskiller sig grundlæggende fra det oprindelige indsamlingsformål. Formålsbestemthedsprincippet vil således ikke hindre viderebehandling af oplysninger, hvis der er tale om forbundne eller beslægtede databehandlings-sammenhænge, hvor videregivelsen hviler på det samme databehandlingsgrundlag som den oprindelige indsamling.

For det andet skal der tages hensyn til den sammenhæng, hvori personoplysningerne er blevet indsamlet, navnlig med hensyn til forholdet mellem den registrerede og den dataansvarlige. Dette kan tale for en vis skærpelse i nærværende fremstillings kontekst, se om ulige forhold del II, afsnit 1.

For det tredje skal personoplysningernes art indgå i vurderingen. Det fremgår af bestemmelserne, at der navnlig skal lægges vægt på, om oplysningerne er omfattet af forordningens artikel 9 eller artikel 10 om følsomme personoplysninger. I så fald

er rammerne for tilladeligt formålsskift snævrere, end tilfældet er for almindelige personoplysninger.

For det fjerde skal der tages hensyn til den påtænkte viderebehandlings mulige konsekvenser for de registrerede, og for det femte kan myndigheden lægge vægt på tilstedeværelsen (eller manglen på samme) af fornødne garantier, som kan omfatte bla pseudonymisering, jf forordningens artikel 6, stk. 4, litra d - e, og databeskyttelseslovens § 5, stk. 2, nr. 4 og 5. Det kan således indgå, om videregivelse sker til en afgrænset gruppe, der ikke umiddelbart på egen hånd kan identificere de registrerede på grund af pseudonymisering. Det kan også i øvrigt have betydning, om der i øvrigt gælder videregivelsesbegrænsninger efter den nye anvendelse, eller om videregivelsen indebærer, at oplysningerne vil blive tilgængelige for enhver. Der vil derfor være en videre adgang inden for den offentlige sektor, idet lovgivningen begrænser spredning af oplysninger fra den offentlige sektor (og fra leverandører til det offentlige), jf straffelovens § 152 f, jf forvaltningslovens § 27.

Der er forholdsvist vide rammer for offentlige myndigheder – i modsætning til private aktører, hvor rammerne i praksis er snævrere – til at viderebehandle personoplysninger til andre formål.[100] For sundhedssektorens vedkommende kan fx nævnes, at nogle af Justitsministeriets svar på Retsudvalgets spørgsmål til lovforslaget kan forstås sådan, at videregivelse til eksempelvis sociale sager eller beskæftigelsessager ikke kan regnes som uforenelig med det oprindelige indsamlingsformål (patientbehandling).[101] Dette synes da også at stemme med, at forordningen åbner for en vis selvstændig national tilpasning af princippets anvendelse i den offentlige sektor i præambelbetragtning nr. 10 sammenholdt med forordningens artikel 6, stk. 3-4, og at de danske lovbemærkninger fremhæver et politisk ønske om, at "det offentlige kan videreanvende og genbruge data på en effektiv, åben og transparent måde, der stadig lever op til kravene om databeskyttelse", og at der skal "skabes rammer for en effektiv datadeling, så borgerne og virksomhederne kan få en mere effektiv sagsbehandling og mere målrettede, sammenhængende indsatser, der virker bedre for den enkelte".

For så vidt angår kommercielle udbydere af tjenester knyttet til wearables, vil formålsbestemthedsprincippet fx efter indsamlingen udgøre en grænse for videreanvendelse og videregivelse uden samtykke til forsikringsselskaber, arbejdsgivere mv.

Samtidig gælder det, at formålsbestemthedsprincippet gennembrydes af samtykke. Det betyder, at en sundhedsmyndighed eller en kommerciel udbyder af tjenester forbundet til wearables kan behandle til et uforeneligt formål, hvis den registrerede giver sit (gyldige) samtykke hertil, jf databeskyttelsesforordningens artikel 6, stk. 4. Opsummerende vil formålsbestemthedsprincippet kun sjældent hindre videreanvendelse af personoplysninger til et andet formål end det oprindelige

100 Justitsministerens svar på Retsudvalgets spørgsmål nr. 4 vedrørende L 68 og 69.

101 Justitsministerens svar på Retsudvalgets spørgsmål nr. 55 vedrørende L 68 og 69.

indsamlingsformål indenfor den offentlige sektor. Herudover gælder, som beskrevet i del I, afsnit 4, at det med hjemmel i databeskyttelseslovens § 5, stk. 3, kan fastsættes, at der kan ske videreanvendelse til uforenelige formål. Princippet begrænser i højere grad den videre brug af data i den private sektor – men en kommerciel udbyder af wearables-tjenester kan bede om den registreredes samtykke til at behandle med det nye formål – hvorefter formålsbestemthedsprincippet er uden betydning.

2.3. Proportionalitet (dataminimering)

Som det er beskrevet i del 1, afsnit 4, kræves det i forordningens artikel 5, stk. 1, litra c, at personoplysninger skal være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til de formål, hvortil de behandles. Bestemmelsen antages i den danske betænkning i det store hele at svare til persondatalovens § 5, stk. 3.[102] I tilknytning hertil fremgår af præambelbetragtning nr. 39, at personoplysningerne bør være tilstrækkelige, relevante og begrænset til, hvad der er nødvendigt i forhold til formålene med deres databehandling. Personoplysninger bør kun behandles, hvis formålet med databehandlingen ikke med rimelighed kan opfyldes på anden måde. Dataminimeringsprincippet (proportionalitetsprincippet) er nært forbundet til kravet om angivelse af, og oplysning om, formålet med en given indsamling og behandling af personoplysninger. Det skyldes, at målestokken er det angivne formål. Dette formuleres populært sådan, at der ikke kan indhentes, bruges og opbevares oplysninger, der er "nice to have". Man skal holde sig til at behandle de oplysninger, der er "need to have" for at opfylde det specificerede formål. Dette vil hindre både sundhedsmyndigheder og kommercielle aktører i at "benytte lejligheden" til at indsamle oplysninger, der ikke er relateret til det eller de formål, der er oplyst til den registrerede.

Dataminimeringsprincippet er dog ikke nødvendigvis kun relateret til spørgsmålet om, hvorvidt indsamling henholdsvis videre databehandling må ske. Det Europæiske Databeskyttelsesråd fremhæver fx, at dataansvarlige skal kunne forklare og retfærdiggøre behovet for at indsamle og opbevare data *og* overveje at anvende aggregerede, anonymiserede eller pseudonymiserede data (hvis dette giver tilstrækkelig beskyttelse), når der sker profilering.[103] Dette synes at være særlig relevant for wearables, især i de tilfælde hvor der angives flere formål med behandling af de indsamlede oplysninger.

2.4. Datakvalitet

Det fremgår af forordningens artikel 5, stk. 1, litra d, at personoplysninger skal være korrekte og om nødvendigt ajourførte; der skal tages ethvert rimeligt skridt for at sikre, at personoplysninger, der er urigtige i forhold til de formål, hvortil de behandles, straks slettes eller berigtiges. Det fremgår af præambelbetragtning nr. 39, at der bør træffes enhver rimelig foranstaltning for at sikre, at personoplysninger, som er urigtige, berigtiges eller slettes.

---

102 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1, s. 97.

103 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 11.

I den danske betænkning vurderes forordningens regler at svare til den tidligere gældende regel om datakvalitet i persondatalovens § 5, stk. 4 – bortset fra, at sletning efter forordningen skal ske straks og dermed formentlig hurtigere, end hvad der fulgte af persondatalovens regler.[104]

Hvad der ikke er omtalt i betænkningen er, at princippet om datakvalitet må antages at omfatte alle databehandlinger, herunder de forskellige led i en vurderingsproces forbundet med en wearable-tjeneste. Dette fremgår særlig klart for så vidt angår profilering. Princippet om datakvalitet skal samtidig læses i lyset af forordningens artikel 16, 2. pkt., hvorefter den registrerede under hensyntagen til formålene med behandlingen har ret til få fuldstændiggjort ufuldstændige personoplysninger, bla ved at fremlægge en supplerende erklæring.

Det vil sige, at alle personoplysninger skal være korrekte ved indsamlingen, analysen og opbygningen af brugerens profil, samt når der træffes en beslutning på baggrund af en dannet profil. Dette skyldes ikke mindst de særlige forhold, som bla er fremhævet af Det Europæiske Databeskyttelsesråd i følgende, om at såfremt de anvendte data er: "ukorrekte, vil afgørelserne eller profilerne være fejlbehæftede. Afgørelserne er muligvis truffet på grundlag af forældede data eller en forkert fortolkning af eksterne oplysninger. Unøjagtigheder kan føre til uhensigtsmæssige forudsigelser eller erklæringer, fx om en persons helbreds- kredit- eller forsikringsrisiko. Selv om rådata registreres korrekt, er datasættet muligvis ikke fuldt repræsentativt, eller analysen kan indeholde skjulte skævheder. Dataansvarlige skal indføre robuste foranstaltninger for løbende at kontrollere og sikre, at oplysninger, der genanvendes eller indhentes indirekte, er korrekte og ajourførte. Dette styrker betydningen af at informere klart om de personoplysninger, der behandles, således at den registrerede kan rette eventuelle unøjagtige oplysninger og forbedre datakvaliteten."[105]

Databeskyttelsesrådet har videre anbefalet som bedste praksis, at dataansvarlige giver de registrerede mulighed for selv at få adgang til og kontrollere såvel de profiler, der er dannet om dem, som de data profilerne er dannet på baggrund af. Yderligere anbefales det at give de registrerede mulighed for at opdatere eller ændre ukorrekte data: "Dette giver de registrerede mulighed for at styre, hvad der sker med deres oplysninger på tværs af en række forskellige tjenester, og således mulighed for at ændre indstillinger, ajourføre deres personoplysninger og gennemse eller ændre deres profil for at rette eventuelle unøjagtige oplysninger", se om databeskyttelsesretligt dashboard oven for del II, afsnit 2.1. [106]

---

104 Betænkning nr. 1565 om Databeskyttelsesforordningen – og de retlige rammer for dansk lovgivning, del 1, bind 1, nr. 1565 s. 99.

105 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 12.

106 Retningslinjer om automatiske individuelle afgørelser og profilering i henhold til forordning 2016/679, WP 251, s. 31 f.

3. Databeskyttelse via design og indstillinger

Databeskyttelsesforordningens artikel 25 fastsætter principperne om databeskyttelse gennem design og databeskyttelse gennem standardindstillinger; principper der må antages at få stor betydning for både kommercielle udbydere af wearable-tjenester og sundhedsmyndigheders indkøb og brug af wearables.

Artikel 25 er tæt forbundet med de persondataretlige principper, se herom oven for del I, afsnit 4, og med kravet om konsekvensanalyse i artikel 35, se neden for del II, afsnit 4. Bestemmelsens formål er at rette fokus mod, hvordan den dataansvarlige indretter sig både teknisk og organisatorisk og dermed styrke den effektive overholdelse af forordningens regler: Hele databehandlingsmiljøet, kravene til et beskyttelsesvenligt design og til fornuftige standardindstillinger retter sig fx mod midlet til databehandling; det anvendte wearable og den tilhørendes software, de digitale kommunikationsveje, de løsninger der opsamler dataene mv. Kravene retter sig dog også mod den måde, den dataansvarliges organisation og arbejdsgange indrettes på mv.

Af bestemmelsen i artikel 25, stk. 1, om design fremgår, at databeskyttelsesretlige overvejelser skal foretages og gennemføres både på "tidspunktet for fastlæggelse af midlerne til databehandling" (forberedelsesfasen) og på "tidspunktet for selve databehandlingen." Heraf følger, at kravene i artikel 25, stk. 1, påvirker andre end den dataansvarlige sundhedsmyndighed; også udviklere, forhandlere, enhedsproducenter og tredjeparter skal tage højde for principperne.[107]

Der er ikke tale om et sikkerhedskrav, men med det danske Datatilsyns ord indebærer bestemmelsen for det første "en generel overvejelses- og håndteringsforpligtelse", som forpligter "til at håndtere og overveje, hvordan alle forordningens bestemmelser kan efterleves gennem konkrete tekniske og organisatoriske tiltag." For det andet skal der anvendes foranstaltninger, der sikrer en effektiv implementering af de øvrige krav i forordningen, herunder principperne og behandlingsbetingelserne, se del I, afsnit 4 og 5 og del II, afsnit 2. For det tredje indebærer henvisningen til de registreredes interesser, at hele forordningens kapitel III, om de registreredes rettigheder skal tages i betragtning og sikres gennem designet. For det fjerde skal den – til den konkrete situation passende – sikkerhed, være indbygget i hele opsætningen og effektueringen af behandlingen af personoplysningerne.[108]

Hvilke konkrete tiltag, der skal tages efter artikel 25, stk. 1, om databeskyttelse gennem design, beror på en konkret vurdering af det aktuelle tekniske niveau, implementeringsomkostningerne og den pågældende databehandlings karakter, omfang, sammenhæng og formål samt risicienes varierende sandsynlighed og alvor for fysiske personers rettigheder og frihedsrettigheder.[109]

---

107 Se også fx Artikel 29-gruppens udtalelse udtalelse nr. 02/2013 om apps i intelligente enheder, WP 202.

108 Datatilsynets vejledning om datasikkerhed og databeskyttelse gennem design og indstillinger, s. 25 og 27.

109 Ibid, s. 26.

Denne risikobaserede tilgang til databeskyttelse skal være dokumenteret, fx i form af førelse af en logbog fra det tidligste udviklingsstadie, og der vil formentlig blive stillet ganske strenge krav til grundigheden af overvejelserne (og iværksættelse af foranstaltninger) ved brug af wearables i den offentlige sundhedssektor.[110] Dette vil indebære, at det overvejes at sikre:

- Minimering af databehandlingen af personoplysninger, jf artikel 5, stk. 1, litra c, og præambelbetragtning nr. 78.
- Hvis muligt, hurtig pseudonymisering, jf artikel 4, nr. 5, jf artikel 5, stk. 1, litra e, og præambelbetragtning nr. 78.
- Gennemsigtighed for så vidt angår personoplysningers funktion og behandling, således at den registrerede kan overvåge databehandlingen, se artikel 5, stk. 1, litra a og om privacy dashboard ovenfor del II, afsnit 2.1.
- Gennemsigtighed med henblik på, at den dataansvarlige skal overvåge databehandlingen og tilvejebringe og forbedre sikkerhedselementer, jf præambelbetragtning nr. 78
- Ved udbud eller indkøb stilles krav om indarbejdede Privacy Enhancing Technologies (PET's).
- Ved udbud eller indkøb stilles krav om funktioner, der letter adgang til de registreredes indsigt mv, se om privacy dashboard oven for del II, afsnit 2.1.
- Foranstaltninger vedr. autorisation, adgangsbegrænsninger (herunder effektive organisatoriske kontroller til autorisation og styring af adgangsrettigheder), logning, tilvejebringelse af medarbejderinstrukser og sikring af infrastrukturen mod uautoriseret indtrængen, kryptering af data i transit eller hvile og undladelse af visning af oplysninger i brugergrænseflader, når disse ikke er nødvendige for en given behandling, jf artikel 5, stk.1, litra f, og artikel 32, stk. 1, litra b.

Det danske Datatilsyns vejledning nævner endvidere, at der kan hentes inspiration til både mulige it-designprincipper og privatlivsfremmende foranstaltninger fx i ENISAs rapport fra 2014 om "privacy and dataprotection by design", ISO 29151:2017 kodeks for beskyttelse af personhenførbar information eller designstrategier. [111]

SIKKERHED OG HELBREDSOPLYSNINGER
At der stilles strenge krav ved håndtering af helbredsoplysninger er ikke nyt. Datatilsynet har tidligere udtalt sig om en hjemmeside, hvor brugerne havde mulighed for at oprette en personlig helbredsboks med adgang til bla helbredsoplysninger fra læger. Tilsynet udtalte, at login baseret på brugernavn og adgangskode ikke i tilstrækkelig grad levede op til den sikkerhed, som må kræves, når en hjemmeside som den i sagen omhandlede gav adgang til følsomme personoplysninger på sundhedsområdet. (Datatilsynets j.nr. 2015-631-0108)

110 Ibid, s. 26-27.

111 Ibid, s. 26.

Et tiltag, der synes oplagt for wearables, kan være, at de indsamlede data helt eller delvis opbevares på det pågældende device eller anden lagringsfacilitet, som kun den registrerede har kontrol over – fremfor hos leverandøren eller dennes cloudleverandør (databehandler).

Forordningens artikel 25, stk. 2, fastsætter princippet om databeskyttelse gennem standardindstillinger. Det fremgår direkte af bestemmelsen, at den dataansvarlige skal sikre, at det kun er de personoplysninger, der er nødvendige til hvert specifikt formål med databehandlingen, der bliver behandlet. Det skal derudover sikres, at personoplysninger ikke uden den pågældende fysiske persons indgriben stilles til rådighed for et ubegrænset antal personer.

Også her skal bestemmelsen forstås bredt; både tekniske og organisatoriske foranstaltninger. Standardindstillinger kan derfor forstås som både it-tekniske indstillinger og indretningen af sagsgange og organisation. Et klassisk eksempel er, at adgang til personoplysninger – analoge såvel som digitale – skal være arbejdsbetingede og derfor ikke tildeles alle i den dataansvarliges organisation. Hvor artikel 25, stk. 1, vedrører selve designfasen, indeholder 25, stk. 2, en pligt for den dataansvarlige til at sikre, at de teknologiske løsningers muligheder indstilles på en måde, der understøtter bestemmelsens krav om bla formålsspecifik behandling af personoplysninger. Er der designet flere muligheder ind i en given teknologi, skal standardindstillingen altså være at behandle færrest mulig personoplysninger (dataminimering) og sprede de indsamlede oplysninger mindst muligt (begrænsning af databehandlingsintensiteten) mv.

Et af de eksempler, der er er nævnt i den danske betænkning om databeskyttelses-forordningen, er ganske illustrativt for wearables. I betænkningen nævnes, at forordningens artikel 25, stk. 2, 1. pkt., kan betyde, at når en fysisk person eksempelvis downloader en app på en smartphone, et smartwatch eller en fitness tracker, skal den dataansvarlige gennem standardindstillinger sikre, at der ikke bliver indsamlet flere oplysninger end nødvendigt for at opnå formålet med app'en. Derudover nævnes i betænkningen, at en sådan app og tilknyttet tjeneste – i det omfang forholdet er regulerbart gennem standardindstillinger – ikke må have standardindstillinger, der gør, at der deles oplysninger om, hvorvidt en person har været på en bestemt beværtning, løbet en tur eller hvem vedkommende har været sammen med, medmindre denne deling er selve formålet med app'en. Det tilføjes yderligere, at såfremt deling af personoplysninger ikke kan styres gennem standardindstillinger i app'en, kan det være tegn på manglende efterlevelse af artikel 25, stk. 1 (dvs den dataansvarlige ikke har sikret databeskyttelse gennem design i app'en).

De nye regler om databeskyttelse via design og indstillinger vil påvirke beskyttelsen af borgerne fra flere vinkler, når der anvendes wearables som led i sygdomsbehandling og forebyggelse i sundhedssektoren. Er sundhedspersoner direkte involveret som dataansvarlige, jf herom oven for del I, afsnit 3, vil sundhedsmyndigheden

være forpligtet til at undersøge, om det pågældende wearable og håndteringen af personoplysninger er indrettet til at respektere databeskyttelsesforordningens artikel 25, jf herved også forordningens artikel 24. Også kommercielle udbydere af de tjenester, der er forbundet til et wearable, vil være forpligtet til at indtænke principperne, når det pågældende wearable og tilhørende tjeneste designes og indstilles, og de organisatoriske rammer fastlægges. Principperne har derfor også betydning i den situation, at den registrerede selv bruger det pågældende wearable uden sundhedsmyndighedens direkte indblanding.

4. Kravet om konsekvensvurderinger ved risikofyldt databehandling

Databeskyttelsesforordningens artikel 35 indeholder et krav om, at der gennemføres konsekvensanalyser før behandling af personoplysninger, "hvis en type behandling, navnlig ved brug af nye teknologier og i medfør af sin karakter, omfang, sammenhæng og formål, sandsynligvis vil indebære en høj risiko for fysiske personers rettigheder og frihedsrettigheder", jf forordningens artikel 35, stk. 1. Det er uddybet i artikel 35, stk. 3, at konsekvensanalyse især er nødvendig, når der sker:

a) En systematisk og omfattende vurdering af personlige forhold vedrørende fysiske personer, der er baseret på automatisk databehandling, herunder profilering, og som er grundlag for afgørelser, der har retsvirkning for den fysiske person eller på tilsvarende vis betydeligt påvirker den fysiske person,
b) Behandling i stort omfang af særlige kategorier af følsomme oplysninger eller af personoplysninger vedrørende straffedomme og lovovertrædelser, eller
c) Systematisk overvågning af et offentligt tilgængeligt område i stort omfang.

Det Europæiske Databeskyttelsesråd har (også) adopteret den tidligere Artikel 29-gruppes vejledning om konsekvensanalyse.[112] I vejledningen opstilles ni kriterier, der kan inddrages i vurderingen af, om en behandling indebærer en høj risiko for de registrerede.[113] De ni kriterier er:

1) Om der sker evaluering eller analyse, herunder profilering og forudsigelse, især på baggrund af forhold vedrørende den registreredes arbejdsindsats, økonomiske situation, helbred, personlige præferencer eller interesser, pålidelighed eller adfærd eller geografiske position eller bevægelser.
2) Om der indgår automatiseret beslutningstagning med juridisk eller tilsvarende betydelig virkning for de registrerede.
3) Om der sker systematisk overvågning, dvs behandlingsaktiviteter, der anvendes til at observere, overvåge eller kontrollere registrerede, herunder data indsamlet gennem netværk, eller systematisk overvågning af et offentligt tilgængeligt område.
4) Om der behandles følsomme oplysninger eller oplysninger af meget personlig karakter. I vejledningen nævnes som eksempel et sygehus, der fører journal over

112 Retningslinjer for konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, WP 248.

113 Ibid s. 10 ff.

patienterne. Til kategorien af følsomme oplysninger regnes i denne sammenhæng også oplysninger om aktiviteter, der henhører under privatlivets fred. Under beskrivelsen af dette nævnes "personlige oplysninger i applikationer til registrering af kropsfunktioner."

5) Om de indsamlede oplysninger gøres til genstand for omfattende behandling ud fra antallet af registrerede. Dette angives at være enten som et specifikt antal af registrerede eller som en andel af den relevante population. Relevante momenter beskrives som mængden af data og/eller de forskellige data, der behandles, behandlingsaktivitetens varighed eller regelmæssighed og databehandlingsaktivitetens geografiske omfang.
6) Om der sker matching eller kombination af datasæt, fx hidrørende fra to eller flere behandlinger af oplysninger med forskellige formål og/eller foretaget af forskellige dataansvarlige på en måde, som ville overstige den registreredes rimelige forventninger.
7) Om der behandles oplysninger om sårbare registrerede, jf databeskyttelsesforordningens præambelbetragtning 75. Dette angives at skyldes den øgede skævhed i magtfordelingen mellem den registrerede og den dataansvarlige, der kan føre til, at en registreret kan være ude af stand til på en nem måde at give deres samtykke til eller modsætte sig behandlingen af oplysningerne eller i øvrigt udøve vedkommendes rettigheder. Som eksempler på sårbare personer nævnes bla psykisk syge personer, ældre og patienter.
8) Om der iværksættes innovativ brug eller anvendelse af ny teknologi eller nye organisatoriske løsninger.
9) Når behandlingen i sig selv hindrer registrerede i at udøve en rettighed eller gøre brug af en tjeneste eller en kontrakt.

Datatilsynet har på baggrund heraf offentliggjort en ikke-udtømmende liste over behandlinger, der med sikkerhed udløser krav om udarbejdelse af en konsekvensanalyse.[114] Det er meget tydeligt fremhævet af tilsynet, at der også ud over de otte opregnede kategorier kan være krav om konsekvensanalyse. Den danske liste opregner:

1) Behandling af biometriske data med det formål entydigt at identificere en fysisk person i sammenhæng med mindst et yderligere kriterium fra Artikel 29-gruppens retningslinjer.
2) Behandling af genetiske data i sammenhæng med mindst et yderligere kriterium fra Artikel 29-gruppens retningslinjer.
3) Behandling af lokationsdata i sammenhæng med mindst et yderligere kriterium fra Artikel 29-gruppens retningslinjer.
4) Behandling ved brug af nye teknologier i sammenhæng med mindst et yderligere kriterium fra Artikel 29-gruppens retningslinjer.
5) Behandling der fører til afgørelser om en fysisk persons rettigheder til et produkt, en service, en potentiel mulighed eller begunstigelse, der er baseret på en hvilken som helst form for automatiseret afgørelse (herunder profilering).

114 Datatilsynets liste over de typer af behandlingsaktiviteter, der er underlagt kravet om en konsekvensanalyse vedrørende databeskyttelse jf databeskyttelsesforordningens artikel 35, stk. 4.

6) Behandling der omfatter profilering af fysiske personer i stor skala, sådan som dette er defineret i Artikel 29-gruppens retningslinjer.
7) Behandling af personoplysninger om sårbare personer eller hvor der er tale om behandling af følsomme oplysninger (særlige kategorier) og hvor, der benyttes profilering eller andre former for automatiserede afgørelser.
8) Behandlinger hvor et brud på persondatasikkerheden kan have en direkte effekt på en persons fysiske helbred eller på sikkerheden for en fysisk person.

Kravet om konsekvensanalyser har til formål at sikre, at betydningen for beskyttelse af personoplysninger kortlægges og overvejes, inden databehandlinger iværksættes, og nye teknologier tages i anvendelse.[115] Som afledt formål skal konsekvensanalysen også sikre, at det på et tidligt tidspunkt overvejes, om indretning af teknologier og organisationer kan afbøde eventuelle negative indvirkninger på beskyttelsen af personoplysninger og privatlivets fred. Det skal også overvejes, om der kan indføres foranstaltninger til at sikre fx dataminimering, eller om pseudonymisering kan bidrage til en bedre beskyttelse. Anderledes udtrykt bidrager konsekvensanalysen for de mere risikofyldte databehandlingers vedkommende til at sikre, at artikel 25 om databeskyttelse via design og indstillinger indarbejdes i teknologier, organisation og arbejdsgange. Artikel 35 og 25 er således nært forbundne regler.

Viser det sig under konsekvensanalysen, at det ikke er muligt at afbøde de negative virkninger for beskyttelse af personoplysninger og privatlivets fred, og der forsat vil være høj risiko ved at starte behandlingen af oplysninger, skal den dataansvarlige henvende sig til Datatilsynet, jf databeskyttelsesforordningens artikel 36. Tilsynet skal rådgive den dataansvarlige, ligesom tilsynet kan vælge at anvende sine beføjelser, herunder forbyde den pågældende databehandling.

Kravet om konsekvensanalyser forudsætter klarhed over de databeskyttelsesretlige roller, se herom del I, afsnit 3. Efter databeskyttelsesforordningen er det nemlig den aktør, der har ansvaret for behandlingen af personoplysninger, der skal sikre konsekvensanalysen gennemført. Dette øger behovet for klarlæggelse af de retlige rammer og ansvarsforholdene i de forskellige situationer, der er omtalt i del I, afsnit 2.

115 WP 248 om konsekvensanalyse vedrørende databeskyttelse (DPIA) og bestemmelse af, om behandlingen "sandsynligvis indebærer en høj risiko" i henhold til forordning (EU) 2016/679, s. 4.

Bilag 2
Privacy-by-Design – Teknisk Notat

Privacy-by-Design – Teknisk Notat
Dette notat er udarbejdet af:
Johannes Kruse

Vejleder:
Lars Kai Hansen, Professor, Head of Section Cognitive Systems Technical University of Denmark

1. Introduktion

Det er de færreste, der er klar over mængden af personlig data, vi tillader firmaer at indsamle om os (Camenisch 2012). Der opstår en vis forundring over mængden af personlig data du skal afgive, når du benytter dig af en online service – hvorfor skal ens telefon nummer angives for at købe en tog billet? Mange daglige processer i et moderne liv kræver, at vi genererer yderligere information, som overvåges, opbevares og analyseres (Camenisch et al. 2005), og vi er i en tid, hvor personlige data er blevet en ny *valuta* på internettet (Camenisch 2012).

Et eksempel, hvor opbevaring og brug af personfølsom data skaber særlig bekymring, er de nye muligheder for individuel brug af sundhedsteknologi, blandt andet i form af wearables. Teknologier du kan tage på, såsom skridttællere, intelligente smykker og smartwatches (Højgaard et al. 2017). Disse teknologier kræver ofte, at der deles potentiel følsom sundhedsdata med systemet, men hvordan sikres det, at individer, der bruger teknologien, ikke på et senere tidspunkt får krænket deres privatliv (Househ et al. 2018)?

Problematikken kan løses gennem Privacy-by-Design (privacy gennem design). Privacy-by-Design blev defineret i 1990'erne af den canadiske *Information and Privacy Commissioner* Ann Cavoukian udfra syv principper (Cavoukian 2010).

- Proaktivitet - forudse privatlivsproblemer før de sker
- Privacy er 'default'
- Privacy er integreret i design struktur af et IT-system
- Fuld funktionalitet – Privacy-by-Design handler ikke om at reducere funktionalitet, men om at sikre privatlivet
- End-to-End sikkerhed – hele værdikæden skal være sikker
- Gennemsigtighed – åbenhed skal sikre, at privacy løsninger kan checkes af en kritisk offentlighed
- Respekt for brugerens privatliv – design skal have brugeren i centrum

Hvis et system fra begyndelsen er designet efter Privacy-by-Design principperne, har enkeltpersoner ejerskab over alle deres data i systemet, og på den måde tillader det brugeren at styre og bestemme, hvem der må få adgang til dem (Cavoukian 2010). Privacy-by-Design handler således ikke om, hvordan vi beskytter data, men hvordan vi designer systemet således, at data ikke behøver beskyttelse. Det er altså et krav for et system at have tænkt principperne ind fra begyndelsen (The National IT and Telecom Agency 2011).

Et udbredt system, der tillader samarbejder mellem databaser, er brugen af en global identifikationsmarkør, svarende til det danske civil registreringsnummer (CPR-nummer). Her tildeles alle danske statsborgere et unikt personnummer, som muliggør, at alle enheder, der opererer i systemet, kan arbejde sammen (Camenisch

og Lehmann 2015). Når du logger på SKAT, e-boks eller pension, genkender alle systemer dig på baggrund af dit CPR-nummer. I Danmark benytter vi NemID som et ekstra sikkerhedslag, for at kunne bevise, at du rent faktisk er den person, du udgiver dig for at være.

Der opstår dog flere privacy problemer ved systemer, der understøtter brugen af én global identifikations markør: (1) data, der går tabt eller hackes, kan uden vanskeligheder kobles, så al information om det enkelte individ i systemet, på tværs af enhederne, er tilgængelige, (2) udvekslinger mellem enheder i systemet er lette at spore, (3) selvom vi lovgiver om, at borgeren gennem samtykke skal kunne bestemme om hans/hendes data må indgå i et bestemt dataudtræk, kan dataejerne i teorien ignorere et manglende samtykke og bruge en persons data alligevel. Dette er nogle af problematikkerne ved at have én global identifikations markør (Camenisch og Lehmann 2015), men hvad er muligheden for, at borgeren kan sikres ejerskab til sin data ad teknisk vej?

Notatet udspringer af denne denne problemstilling, og vil give et svar på spørgsmålet:

- *Hvad er muligheden for at sikre privacy gennem design: at udvikle systemer, som kan sikre borgeren kontrol over sine egne data? Kan det lade sig gøre at designe sådanne systemer? Hvad er i dag de bedste bud på sådanne systemer, og hvad er styrker og svagheder ved dem?*

Notatet beskriver styrker og svagheder ved de mest lovende systemer/tekniske redskaber og giver desuden et bud på lovende løsninger, som kan forventes i fremtiden. De fire udvalgte tekniske redskaber, der beskrives i notatet, er:

1. *k* -anonymitet
2. Differential Privacy
3. Multiparty Computation
4. Ukoblet Pseudonymitet

De udvalgte systemer er tekniske redskaber, som kan bidrage til tekniske løsninger, der skal beskytte privacy gennem design, så brugeren uden at dele alle sine private oplysninger, eller i hvert fald selv styre hvor stort et tab af privatliv en bestemt service eller sundhedsteknologi vil indebære. Brugeren kan undersøge og bør gøre sig overvejelser om, hvilken sikkerhedsgaranti og tekniske redskaber en elektronisk service tilbyder. Hvis først en service har opsamlet privat data, har brugeren potentielt ikke længere kontrol over sin data. Det er således vigtigt at sikre, at data modtageren eller servicen håndterer data på en sådan måde, at brugerens privacy ikke på et senere tidspunkt bliver krænket.

Notatets systemer omhandler ikke situationerne, hvor servicer tracker brugerens almindelig færden på internettet med henblik på profilering og skræddersyet reklamering. Internettets nuværende opbygning tillader at firmaer, såsom Google, Facebook og Microsoft, kan monitorere deres brugere (Chester 2012), dette kan blandt andet gøres ved hjælp af IP adresser, JavaScripts og cookies (McKinley 2008).
Det tekniske værktøj cookies er en hjælp, når brugeren ønsker at gemme oplysninger som brugernavn og kodeord eller sin online indkøbskurv, men det også muligt at få cookies til at indsamle og gemme data vedrørende brugens adfærd og præferencer fra et bestemt domæne (Mao et al. 2009). Hvilke oplysninger der indsamles, lagres og videregives, afhænger af hjemmesiden, og dem der har lavet den (Eckersley 2010).
Den nuværende situation er, at hvis du ønsker at bruge en service, der benytter tracking tools, herunder cookies og JavaScripts, er det meget svært at undgå tracking, selv med de eksisterende anti-tracking tools (Castelluccia 2012). Problematikken kommer af, at flere domæner og apps ikke tillader brugeren at benytte deres service hvis ikke vedkommende accepterer servicens betingelser. Betingelser som kan involvere, at servicen må benytte tracking tools. Privacy problematikken, når en service tracker sine brugere med henblik på at lave online adfærdsmæssig profilering, kan ikke løses alene ad teknisk vej (Castelluccia 2012). Situationen, hvor der indsamles data om brugeren uden nogen form for samtykke, er situationer hvor services ikke lever op til EU-lovgivningen om databeskyttelse og privacy, General Data Protection Regulation (GDPR) (European Commission 2018), eller anden ulovlighed (virus, "hacking"etc).

Baggrund for de tekniske redskaber: Brugeren sættes i et tilsyneladende svært dilemma: På den ene side vil man gerne benytte services, og på den anden side vil man beskytte sit privatliv. Så spørgsmålet er: kan man få adgang til services uden at dele alle sine private oplysninger, eller i hver fald selv styre hvor stort et tab af privatliv en bestemt service vil indebære?

Der er flere dimensioner, der skal tages højde for, når man skal sikre privacy gennem design:

1. Sikre borgenens kontrol over egne data
2. Muligheden for at kunne indgå i og offentliggøre statisktiske databaser
3. Mulighed for at arbejde på tværs af databaser

Ukoblet pseudonymitet er et teknisk redskab, som kan være en del af en løsning som sikrer borgerens kontrol over egen data. Ideen bag ukoblet pseudonymitet er, at brugeren i forskellige sammenhænge er kendt under forskellige pseudonymer.

Pseudonymerne er tilfældigt valgt, og kan derfor ikke knytte data til en bestemt person. Det er således ikke muligt samkører data fra forskellige databaser. En bruger kan få udstedt et certifikat, en form for krypteringsnøgle, så brugeren kan transformeres til et givet pseudonym. Ukoblet pseudonymitet giver dog ikke en løsning på to meget vigtige problemer:

1. Gennemsigtighed: Det kan være svært at forstå hvilket tab af privatliv det vil indebære, hvis man giver en service adgang til givne oplysninger
2. Sociale netværk: Hvordan håndteres data, der ejes af flere i fællesskab, fx en samtale, en gruppechat eller en families sundhed (genetik).

Disse problemer kan til gengæld løses med to metoder, der slører henholdsvis data og modelberegninger, nemlig *k* -anonymitet og *differential privacy*. Dette er nødvendigt, da data om samfund, befolkningsgrupper og personspecifik information er en værdifuld ressource for organisationer, forskning og kommercielle virksomheder. De to metoder giver denne mulighed, og det er selvsagt vigtigt, at man som borger trygt, med samtykke, kan dele data til denne brug.

Beregninger i sundhedssystemer er typisk baseret på statistik og machine learning algoritmer. I visse tilfælde er det nyttigt, at en given beregning kan foretages under garanti for gensidig beskyttelse af data og algoritme. Multiparty Computation (MPC) giver denne mulighed. Ved anvendelse af MPC kan man garantere, at både dataejer og algoritmeejer bliver beskyttet, og efter den fælles beregning har begge kendskab til resultatet, men har ikke lært noget om den anden part (dvs data eller algoritme).

1 Det engelske ord attributes bliver brugt om egenskaberne i tabellernes kolonner (Holohan m.fl. 2017), her oversat simpelt til det danske 'attributter'.

2. *k*-anonymitet

Når person-specifik information deles i form af tabeller eller lignende, fjernes eller krypteres eksplicitte identifikationsmarkører; navn, adresse og telefonnummer, men dataen kan stadig indeholde oplysninger som; køn, fødselsdato og postnummer. Informationen virker anonym, men er det i realiteten ikke, da persondata kan blive koblet til ekstern data og være med til at re-identificere individer og deres sensitive data (Ciriani et al. 2007).

Tabel 1: Ikke Identificerbar privat tabel (medicinsk data)

CPR-nummer	Navn	Fødselsdato	Køn	Postnummer	Civilstatus	Sygdom
		.....	.....	.....	.....	.....
		13/09/65	K	3712	Gift	Diabetes
		16/01/64	**K**	**3700**	**Single**	**Cancer**
		02/11/64	M	3730	Skilt	Cancer
		.....	.....	.....	.....	.....

Tabel 2: Identificerbar offentligt tilgængelig tabel

Navn	Adresse	By	Postnummer	Fødselsdato
.....	.....	.....	.....	.....
Birgitte Kofoed	**Kalmarvej 5**	**Rønne**	**3700**	**16/01/64**
.....	.....	.....	.....	.....

Tabel 1 og Tabel 2 er et fiktivt eksempel på hvordan re-identifikation kan ske ved direkte at koble delte attributter[1] (Ciriani et al. 2007). Det var denne form for identifikationsteknik, der blev brugt til at re-identificere medicinsk information for en guvernør i den amerikanske stat Massachusetts (Sweeney 2002). Ydermere viste en undersøgelse fra USA, at 87 % af den amerikanske befolkning unikt kan identificeres på baggrund af; køn, fødselsdato og 5-cifret postnummer (Sweeney 2000).

En teknisk løsning, der forhindrer direkte datakobling med ekstern data, er *k*-anonymitet. Her er oplysninger i datasættet aggregeret og transformeret på en sådan måde, at det ikke længere er muligt at identificere enkeltindviders data (Samarati et al. 1998).

I Tabel 3 er anført betegnelser og tilhørende eksempler for attributter associeret med *k* -anonymitet.

Tabel 3: Eksempler på klassificering af atrributter

Attributter:	Navn, CPR-nummer, køn, fødselsår, postnummer, civilstatus
Eksplicitte identifikationer:	Navn, CPR-nummer
Sensitive attributter:	Sygdomme, telefon nummer
Quasi-identifikatorer:	Køn, fødselsår, postnummer, civilstatus

Attributter er egenskaberne, der listes i tabellens kolonner (Holohan et al. 2017); eksplicitte indikatorer er unikke identifikationsværdier af individer i tabellens rækker (Holohan et al. 2017); sensitive attributter indeholder personfølsom data, som skal beskyttes (Machanavajjhala et al. 2006); quasi-identifikatorer er de ikke-sensitive attributter, som kan kobles med ekstern data til unikt at identificere individer i en population (Domingo-Ferrer et al. 2005).

Formelt er *k*-anonymitet defineret som følgende:

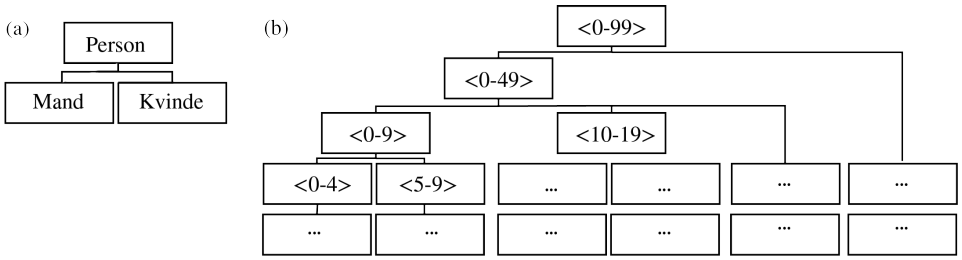
Definition 1. (k -anonymitet): *Lad T (A_1, ..., A_n) være en tabel og quasi-identifikatorer associeret med den. Tabellen siges at være k-anonym, hvis og kun hvis hver quasi-identifikator sekvens af værdier optræder med mindst k tilfælde (Samarati et al. 1998).*

Det vil sige, betingelsen for at et datasæt er *k*-anonymiseret er, at enhver kombination af værdier for en quasi-identifikator deles af mindst *k* individer. (Ciriani et al. 2007). Hvis *k* = 10 kan man sige, at hver person kan identificeres som en medlem af en gruppe på mindst 10 personer (denne gruppe kaldes også 'anonymization set').

De mest udbredte implementeringsteknikker for *k*-anonymitet er, at transformere datasættet ved hjælp af *generalisering og suppression* (El Emam et al. 2008).

Generalisering er en metode, hvor værdierne for en given attribut substitueres med en mere generel værdi (Ciriani et al. 2007), som deles af flere individer.

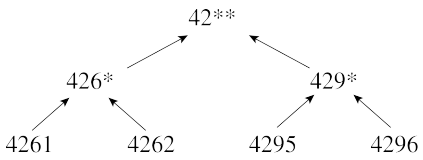
Figur 1: Eksempler på generaliserings hierarkier (a) og (b) med to almindelige quasi-identifikatorer: (a) køn, (b) alder i år.



På figur 2 illustreres hvorledes man kan benytte generalisering (Ciriani et al. 2007).

Suppression er en metode, hvor værdier for en bestemt attribut fjernes eller erstattes med en ikke-informativ værdi. Det gøres oftest med notationen '*' (Podgursky 2011).

Figur 2: Eksempel på suppression hierarki med postnumre som quasi-identifikatorer.



På figur 2 illustreres hvorledes man kan benytte suppression (Ciriani et al. 2007). Målet er at anonymisere datasættet, men samtidig minimere brugen af suppression og generalisering, for at tilstræbe så informationsrig data som muligt (G. Aggarwal et al. 2005).

Tabel 5 er et eksempel hvorpå 3-anonymitet af tabel 4 opnås (Machanavajjhala et al. 2006). I dette tilfælde er quasi-identifikatorne; postnummer, alder og køn. Ligeledes ses det, at hver kombination af quasi-identifikatornes værdier optræder mindst 3 gange i tabel.

Tabel 4: Patient tabel

	Ikke-sensitive informationer			Sensitive informationer
	Postnummer	Alder	Nationalitet	Sygdom
1	3700	28	Russisk	Hjerte sygdom
2	3730	29	Amerikansk	Hjerte sygdom
3	3751	21	Japansk	Viral infektion
4	2670	50	Indisk	Cancer
5	2660	55	Russisk	Hjerte sygdom
6	2650	47	Amerikansk	Viral infektion
7	4100	31	Amerikansk	Cancer
8	4180	37	Indisk	Cancer
9	4200	36	Japansk	Cancer

Tabel 5: 3-anonymiseret patient tabel

	Ikke-sensitive informationer			Sensitive informationer
	Postnummer	Alder	Nationalitet	Sygdom
1	37**	<30	*	Hjerte sygdom
2	37**	<30	*	Hjerte sygdom
3	37**	<30	*	Viral infektion
4	26**	2' 40	*	Cancer
5	26**	2' 40	*	Hjerte sygdom Influenza
6	26**	2' 40	*	
7	4***	3*	*	Cancer
8	4***	3*	*	Cancer
9	4***	3*	*	Cancer

Opsummering
Ved brug af *k*-anonymitet kan man dele data, men samtidig sløre enkeltindivider eller gruppers personlige data.

Styrker:
- Graden af beskyttelse er intuitivt forståeligt

Svagheder:
- *k*-anonymitet kan medføre uacceptabelt tab af information i databaser med mange attributter (C. C. Aggarwal 2005)
- Det er uklart, hvor stor *k* skal være for at give effektiv beskyttelse.
- *k*-anonymitet giver ikke garanti for beskyttelse mod senere fremkomne data, der bryder anonymiteten (fx at data fra andre 'medlemmer' af en *k*-gruppe offentliggøres) (Sweeney 2002)

Scenarier set fra virkeligheden:
- **Baggrundsviden:** Hvis person A kender person B, og A ved at B indgår i tabel 5. Så kender A, B's postnummer, alder og køn. Lad os sige B er 31 år, så kan A konkludere, at B har cancer (Machanavajjhala et al. 2006)
- **Usorteret deling:** Denne trussel baserer sig på rækkefølgen, hvormed hver tupel[2] optræder i en delt tabel. Hvis dataen i figur 1 deles i to forskellige anonymiserede versioner, men rækkefølgen af hver tupel forbliver den samme, kan dette potentielt være med til at genskabe det originale datasæt (Sweeney 2002)

For at imødegå *k*-anonymitets svagheder, er der foreslået modificerede versioner af systemet (Machanavajjhala et al. 2006; Li et al. 2007) og kombinationer med andre tekniske løsningsformer (Holohan et al. 2017), men der er også blevet introduceret nye tekniske løsninger, blandt disse er differential privacy (Dwork 2006).

2 Matematisk begreb for rækker i en matrix.

3. Differential Privacy

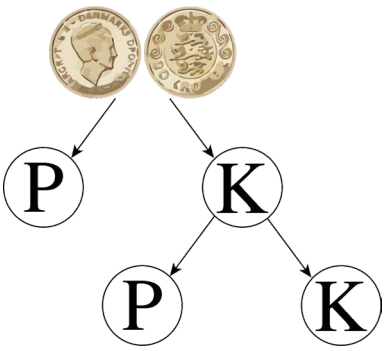
Hvis en statistisk database er en repræsentativ stikprøve for en population, er målet at lære og/eller offentligøre egenskaberne for populationen som en helhed, men uden at kompromittere anonymiteten eller privacy for de individuelle respondenter i stikprøven (Dwork og Smith 2010).

Dette førte til et tidligt desideratum for statistiske databaser. Det lød: "*nothing about an individual should be learnable from the database that cannot be learned without access to the database*" (Nguyen 2003). Det viser sig, at et privacy-system som dette ikke er muligt (Dwork 2006). Dette skyldes den eksterne information, der går udover oplysningerne, der fremgår i statistiske databaser (Ganta et al. 2008).

Et eksempel kan være, hvis det formodes, at højden på en person betragtes som sensitiv information, og afsløring af et individs højde er en krænkelse af privacy. Antag nu, at en database indeholdt gennemsnitshøjder fra kvinder fra forskellige nationaliteter. Hvis en person har adgang til databasen, og har den eksterne information: Lone Hansen er 2 cm højere end den gennemsnitlig tyske kvinde, da lærer den udefrakommende aktør Lone Hansens højde, mens alle personer, som kun lærer den eksterne information, uden adgang til databasen, lærer relativt lidt (Hilton 2012).

I eksemplet er et vigtigt aspekt, at uanset om Lone Hansen er en del af den statistiske database, er udfaldet det samme. Dette har ført til et nyt desideratum for statiske databaser; "*the risk to one's privacy, or in general, any type of risk, such as the risk of being denied automobile insurance, should not substantially increase as a result of participating in a statistical database*" (Dwork 2006).

Differential privacy bygger på ovenstående koncept, og for at garantere enkelt-personers privacy tilføjes støj til dataet, der indgår i den statistiske database. Ved at sløre dataet kan enkeltpersoner afvise, at netop deres data indgår i databasen (Inan et al. 2010). Et eksempel på, hvordan støj kan tilføjes til et en database, er at benytte en randomiseret funktion.



Figur 3: Møntkast algoritmen for spørgsmålet: Har du attribut A? 1) Slå plat eller krone, hvis plat (P) svar ærligt på spørgmålet (Ja/Nej), hvis krone (K) udføres kastet igen. 2) Ved andet kast: Hvis plat svar "Ja" hvis krone svar "Nej". Sandsynligheden i første kast er således 50% for både plat og krone, mens sandsynligheden for plat og krone i andet kast er 25%.

I figur 3 illustreres den randomiserede møntkast algoritme, der ved hjælp af tilfældig støj slører respondenters svar. Praktisk får respondenter spørgsmålet, har du attribut A? Derefter slås der plat eller krone, hvis plat skal respondenten svare ærligt på spørgmålet (Ja/Nej), hvis krone udføres kastet igen. Slås der i andet kast plat skal respondenter svare "Ja" og modsat "Nej" hvis krone. Svaret "Ja" kan således forventes at optræde hos 1/4 af de respondenter der *ikke* har attribut A, plus 3/4 af de respondenter, der ret faktisk har attribut A,

$$\frac{1}{4} \cdot (1 - \frac{x}{n}) + (\frac{3}{4}) \cdot \frac{x}{n} = \frac{1}{4} + 2 \cdot \frac{x}{n} \quad (1)$$

hvor *x* er antallet af respondenter, der har svaret "Ja", og *n* er antal respondenter i stikprøven.

Her sikres respondentens privacy gennem sandsynlighedsnægtelse *('plausible deniability')* af udfaldene. Hvis det at have attribut A er kriminelt, vil svaret "Ja" modsat ikke være kriminelt, da dette svar optræder tilfældigt med 1/4 sandsynlighed, uanset om respondenter faktisk har attribut A (Dwork og Roth 2014). Samtidig kan det faktiske antal personer, der har attribut A i en populationen, estimeres (Dwork og Pottenger 2013). For møntkast algoritmenten kan fraktionen af respondenter, der har attribut A *(A/n)*, estimeres til at være to gange fraktionen der har svaret "Ja" minus en halv:

$$\frac{A}{n} = 2 \cdot \frac{x}{n} - \frac{1}{2} \quad (2)$$

Ovenstående er et eksempel på differential privacy mekanisme, som formelt defineres således:

Definition 2. (Differential privacy): *En randomiseret funktion K giver ϵ-differential privacy hvis for alle datasæt D1 og D2 er forskellig med højst et element og alle S ⊆ Range(K) (Dwork 2006)*

$$Pr[K(D_1) \in S] \leq exp(\epsilon) \times Pr[K(D_2) \in S] \quad (3)$$

hvor *Pr* er sandsynlighedsfeltet *('probability space')* for hvert tilfælde over den randomiserede funktion *K* (Dwork og Pottenger 2013); *S* er delmængden, fx ϵ *{Ja, Nej}* (Dwork og Smith 2010); ϵ er den statistiske afstand *('statistical distance')* som bruges til at definere styrken af den opnåede privacy, hvor $\epsilon = 0$ giver stærkest mulig privacy og $\epsilon \rightarrow \infty$ ikke garanterer nogen form for privacy (D. P. T. Apple 2017). Styrken af møntkast algoritmen er således (ln(3))-differential privacy:

$$\frac{Pr[Svar = Ja|Sandhed = Ja]}{Pr[Svar = Ja|Sandhed = Nej]} = \frac{Pr[Svar = Nej|Sandhed = Nej]}{Pr[Svar = Nej|Sandhed = Ja]} = \frac{3/4}{1/4} = 3 \quad (4)$$

Differential privacy kan implementeres på forskellig vis. To effektive teknikker er at benytte Laplace støj eller ekspotential mekanismen på den rå data (Zhou et al. 2009). Her kan det på baggrund af dataets sensibilitet vælges ϵ værdier så forskellig styrke af differential privacy opnås. Sensibilitet henviser til forskellen mellem interne værdi størrelser i dataet (Dwork 2006).

Machine learning algoritmer med indbygget differential privacy er et aktivt forskningsfelt. Metoder er udviklet for de mest anvendte machine learning algoritmer, herunder såkaldt deep learning metoder (Abadi et al. 2016).

Flere virksomheder og organisationer ser et potentiale ved differential privacy (Erlingsson et al. 2014), heriblandt Apple Inc. som har implementeret differential privacy teknologi i deres software (D. P. T. Apple 2017). Med brugerens samtykke indsamler Apple forbrugs- og adfærdsdata (Apple 2018). Differential privacy muliggør, at Apple kan lære egenskaber omkring alle deres brugeres adfærd og forbrug, men i et format som gør, at de ikke kan udtrække egenskaber om det enkelte individs forbrug eller adfærd.

Opsummering: Differential privacy giver mulighed for at sløre modelberegninger og afledte resultater fra en populationsdatabase, således at det ikke kan afgøres, om givne enkeltindivider eller gruppers data er indgået i beregningen.

Styrker

- Differential privacy sikrer beskyttelse mod senere fremkomne data.
- Tillader indsamling af data fra en service, men uden at serviceudbyderen eller andre aktører med sikkerhed kan identificere eller lære egenskaber af enkelte individer i dataet.
- Differential privacy er 'provable security', hvilket betyder, at algoritmens sikkerhedsegenskaberne kan bevises matematisk (Commission on Evidence-Based Policymaking 2017).

Svagheder

- Differential privacy tillader ikke deling af individuelle svar, men data aggregeres til et samlet beregningsresultat.
- Valg af ϵ kan være intuitivt svært at forstå (Dwork og Pottenger 2013).
- Differential privacy giver stærkest privacy-garanti for datasæt baseret på mange personers data.

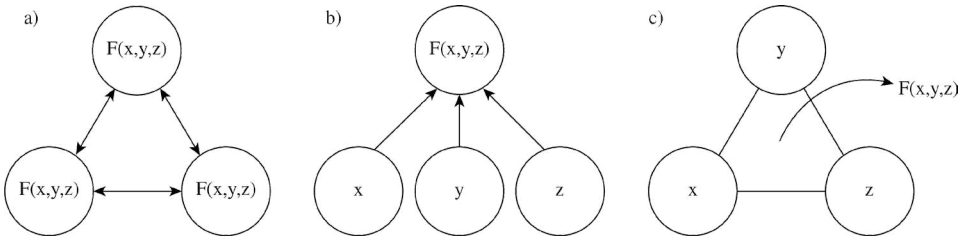
4. Multiparty Computation

Potentialet for data mining er stort, og særligt inden for sundhedssektoren er big data analyser et vigtigt redskab, der i fremtiden skal hjælpe med at skabe nye behandlingsformer samt reducere sundhedssektorens omkostninger (Peter et al. 2013).

Selvom big data analyser er essentielle, er en af udfordringerne i sundhedsektoren at sundhedsdata oftest er personfølsom. Ligeledes kan oplysninger være spredt ud i forskellige databaser (Veeningen et al. 2018). For eksempel hvis det ønskes at undersøge, om der var en korrelation mellem skattesnyd og stress-symptomer, ville det kræve adgang til både hospitalets- og SKATs database.

Der findes metoder, der gør, at en udregning mellem forskellige databaser kan foretages, men uden at sammenkøre databaser. Der kan gøres brug af en troværdig tredjepart, som modtager dataet. Den troværdige tredjeparten udfører så beregningen, og aktørerne får kun oplyst resultatet (Liu et al. 2016). Det kan dog være besværligt at nå til enighed om tredjeparten, og ligeledes er det økonomisk belastende (Damgård et al. 2017). Ydermere er både sundhedssektoren, organisationer og virksomheder blevet mere tilbageholdende med at dele deres data (Veeningen et al. 2018). For at lave data analyser på tværs af databaser, men samtidig undgå tredjepart, kan opgaven også løses teknisk.

Multiparty computation (MPC) er et teknisk redskab, der muliggør data analyse på tværs af databaser, men uden at de bagvedliggende data afsløres. MPC teknologier er baseret på kryptografi, og resultaterne beregnes på baggrund af inputs fra flere databaser, der kan være kontrolleret af forskellige aktører (Commission on Evidence-Based Policymaking 2017). Her skal det forstås, at MPC er et veldefineret teknisk redskab, som bygger på flere forskellige algoritmer (Archer et al. 2018). De forskellige variationer garanterer allesammen, at individuelle aktører ikke behøver dele databaser med hinanden. Dette betyder, at flere aktører kan bidrage med datainputs til data analyser med en teknisk garanti for, at deres datainput ikke kan dekrypteres af andre end dem selv (Veeningen et al. 2018; Commission on Evidence-Based Policymaking 2017).



Figur 4: Forskellige modeller for hvordan databaser kan sammenkøres: (a) alle aktører deler databaser med hinanden, (b) aktørerne finder en troværdig

tredjepart som får tilgang til alle databaser og (c) aktørerne benytter multiparty computaion, hvor det ikke er nødvendigt at sammenkøre databaser, men udelukkende bidrager med et krypteret datainput.

Figur 4 illustrerer tre metoder hvorpå fælles beregninger på tværs af databaser kan foretages. Her tages der udgangspunkt i figur 4 c): antag at tre personer ønsker at beregne deres gennemsnitlige løn, men hverken vil afslører deres løn til hinanden eller en tredjepart. Dette viser sig ikke at være et problem. For at lave beregningen generer hver person to tilfældige tal, og giver et af de tilfældigt generede tal til hver af de andre personer. Dernæst udføres følgende beregninger:

$$\begin{aligned} X_1 &= L_1 + (R_{12} + R_{13}) - (R_{21} + R_{31}) \\ X_2 &= L_2 + (R_{21} + R_{23}) - (R_{12} + R_{32}) \\ X_3 &= L_3 + (R_{31} + R_{32}) - (R_{13} + R_{23}) \end{aligned} \quad (5)$$

Hvor *Li* er den sande løn for person *i*; *Rij* er det randomiserede tal generet af person *i* og givet til person *j*; *Xi* er det resultat, hver person *i* har udregnet. Hver person rapportere nu deres udregnede *Xi*. Det viser sig nemlig, at ved at summere alle *X*'er annullerer de tilfældigt generede tal hinanden ud. Dette betyder, at ved at summere *X*'erne og dividere det med antal personer finder de den gennemsnitlige løn:

$$\frac{X_1 + X_2 + X_3}{3} = \frac{L_1 + L_2 + L_3}{3} \quad (6)$$

Samtidig er det ikke muligt at beregne den sande løn for de andre personer alene på baggrund af Xi. MPC sætter således alle aktører i kontrol over egne data, da den eneste, der kan dekryptere aktørens datainput, er aktøren selv.

Ovenstående er et eksempel på en MPC algoritme (Goroff et al. 2018), men der eksisterer mere avancerede MPC algoritmer som blandt andet muliggør beregninger som: kreditvurderinger af landmænd (Damgård et al. 2017), korrelation mellem studerenes uddannelseslængder og mængden af fritidsarbejde ved siden af studiet (Bogdanov et al. 2016) samt pilot projekter, hvor databaser på tværs af hospitaler og forsikringsselskaber er blevet sammenkørt (Veeningen et al. 2018).

Opsummering: I ovenstående er MPC beskrevet, men som allerede nævnt er det vigtigt at være opmærksom på, at MPC dækker over mange forskellige variationer over temaet. MPC er et aktivt forsknings- og udviklingsområde, og mange nye løsninger er på vej.

Styrker

- MPC muliggør dataanalyser på tværs af databaser med garanti for, at det ønskede beregningsresultat er det eneste, hver deltager har lært efter beregningen.
- Alle aktører har kontrol over egne data.
- Data kan opbevares i flere databaser.

- MPC er 'provable security', hvilket betyder at algoritmens sikkerhedsegenskaber kan bevises matematisk (Commission on Evidence-Based Policymaking 2017).

Svagheder

- Et MPC resultat beskytter nødvendigvis ikke privacy for respondenterne (Goroff et al. 2018).
- MPC algoritmer skal integreres i softwaret.
- Beregningsoverhead i form af den ekstra tid og beregning, det måtte tage at anvende MPC.

Sidst nævnte svaghed forudsiges at blive løst ved hjælp af bedre algoritmer og mere professionel implementering (Orlandi 2011). Eftersom MPC udregninger ikke tager højde for resultatets sensibilitet, kan det være nødvendigt at kombinere teknologien med andre tekniske redskaber, som for eksempel differential privacy, så respondenternes privacy er sikret.

5. Ukoblet Pseudonymitet

Der er et stigende antal mennesker der benytter sig af elektroniske medier, såsom Facebook, LinkedIn eller Google+ (Camenisch, Karjoth et al. 2013), og ligeledes foretages et øget antal daglige gøremål elektronisk, alt fra informationsøgning, tøjindkøb og rejsebestillinger. Alle disse elektroniske interaktioner betyder, at der dagligt indsamles et overflod af personlige oplysninger, som videregives til serviceudbyderne, men ofte tillader vi også tredjeparter adgang til oplysningerne (Camenisch, et al. 2005).

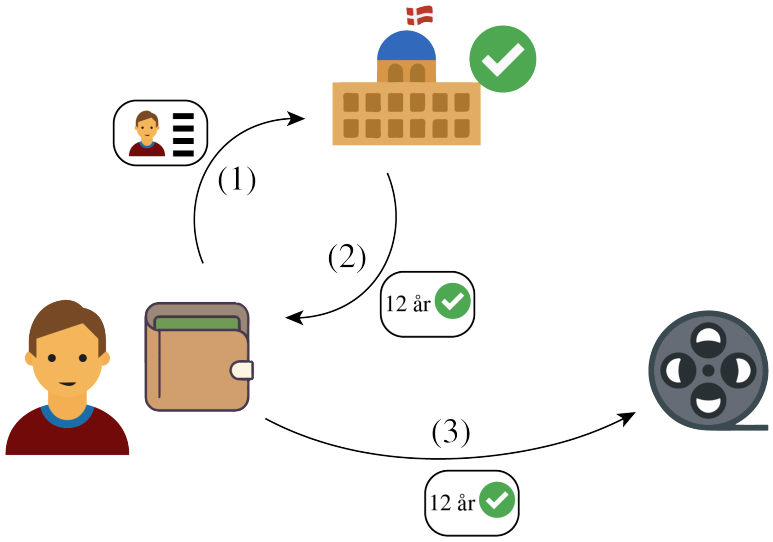
På nuværende tidspunkt er det praktisk talt umuligt at fjerne data fra internettet, når først det er delt, og det er umuligt at vide og forudse alle de potentielle formål, som data vil kunne blive brugt til (Camenisch, Dubovitskaya et al. 2011).

Politisk kan man forsøge at løse problemet gennem lovgivning, men der er altid en risiko for, at det viser sig at have en mindre effekt end ønsket (Garfinkel 2015). Teknisk eksisterer der en fundamental anderledes tilgang til det, kendt som pseudonymitet. Der eksisterer forskellige variationer og styrker af pseudonymsystemer, eksempelvis benyttes der et pseudonym for patientens CPR-nummer, når genetiske prøver sendes til sekventering på et laboratorium. Indenfor elektroniske valuta, heriblandt Bitcoin, bruges pseudonymer (Miers et al. 2013). Ligeledes er det østrigske eID, deres NemID system, understøttet af pseudonymer (Camenisch og Lehmann 2015).

De mest avancerede og sikre pseudonymsystemer bygger på ukoblet ('unlinkable') pseudonymitet. Ukoblet pseudonymitet er en særlig form for pseudonymitet, der gør, at en bruger i forskellige sammenhænge er kendt under forskellige pseudonymer. Pseudonymerne er tilfældigt valgt, og man kan derfor ikke knytte data til en bestemt person, heller ikke selvom man samkører data fra forskellige databaser (Camenisch og Lehmann 2015).

To eksempler på systemer, der benytter ukoblet pseudonymitet, er U-prove (Paquin 2013) og Idendity Mixer (Camenisch, Mödersheim et al. 2010), henholdsvis udviklet af Microsoft og IBM. Begge systemer tillader brugeren selektivt at udvælge, hvilke attributter de ønsker at afslører om dem selv, uden at afgive andre oplysninger end højst nødvendigt (Bournez et al. 2011).

Figur 5: Illustration af Identity Mixer: Personen NN ønsker adgang til en filmtjeneste, som har en aldersgrænsen på 12 år, (1) NN sender dokumentation til et certificeret domæne, (2) dernæst tjekker det certificerede domæne, at NN er 12 år, og udsender et certifikat med bekræftelse på, at NN er 12 år, (3) NN bruger certifikatet på filmtjenestens domæne som bevis for, at NN er 12 år gammel. Figuren er inspireret af IBM (Identity Mixer n.d.)



Identity Mixer er i figur 5 illustreret. Systemet bygger på princippet, at der foretages autentifikation uden identifikation. Antag at en person, NN, ønsker adgang til en filmtjeneste med en aldersgrænse på 12 år. I stedet for at oprette en bruger, hvor NN skal opgive oplysninger som navn, adresse og fødselsdato, får NN udsendt et certifikat, a la NemID, fra et certificeret domæne, svarende til DanID. Med certifikatet kan NN bevise at være 12 år gammel, men uden at give andre oplysninger til filmtjenesten.

NN kan således have flere certifikater, såsom statsborgerskab, kvalifikationsniveau eller medlemskaber. Selv hvis filmtjenenesten eller et andet domæne bliver hacket, kan ingen af NNs certifikater kobles, da de alle har tilfældigt valgte pseudonymer. Selv ikke det certifikerede domæne kan genskabe NNs identitet ud fra certifikaterne, selvom det var dem, der udstedte dem i starten (Camenisch, Mödersheim met al. 2010; Identity Mixer n.d.).

Opsummering: Ukoblet pseudonymisering kan give mulighed for at afgive data til populationsmodeller, uden at de kan linkes til en given bruger.

Styrker

- Privacy-by-Design opnås ved at give brugeren fuld kontrol egen data.
- Borgerens data i et domæne kan ikke kobles til andre domæner, hvilket giver en stærk privacy garanti.

Svagheder

- Udfordringer med kompatibilitet med andre systemer.
- Opgaven med at beskytte privatlivet lægges over på brugeren: det kan være komplekst at vurdere, hvad man giver tilladelse til ved samkøring.
- Metoden giver ikke en løsning (endnu) på situationer, hvor data ejes af flere.
- Der kan være et stort teknisk/økonomisk overhead ved implementering.

6. Opsummering

I de forrige afsnit er fire systemer/tekniske redskaber blevet præsenteret, med en beskrivelse af deres styrker og svagheder. Disse tekniske redskaber kan blive vigtige for tekniske løsninger, der skal beskytte privacy gennem design i tilfælde, hvor privatpersoner ønsker at få adgang til services og benytte sundhedsteknologier, såsom wearables, uden at dele alle sine private oplysninger, eller i hvertfald selv styre, hvor stort et tab af privatliv en bestemt service eller sundhedsteknologi vil indebære. Dette skal gøres samtidig med at forhindre, at forsøgspersoners data i sundhedsplatforme kan re-identificeres. Det er vigtigt at forstå, at de forskellige tekniske redskaber ikke nødvendigvis er en forbedring af hinanden, men at de hver især kan løse forskellige problemstillinger:

- *k*-anonymitet og differential privacy er sammenlignelige, fordi de begge handler om, hvordan en database svarer på forespørgsler, så man beskytter de personer, hvis oplysninger er i databasen.
- Multipart computation er et redskab, der løser et andet problem, nemlig to eller flere dataejere går sammen og beregner et resultat, der afhænger af den totale mængde af data.
- Ukoblet pseudonymitet løser et tredje problem, nemlig hvordan brugere er identificeret.

På nuværende tidspunkt har vi ikke kendskab til et system eller et teknisk redskab, der kan forhindre, at privatpersoners data opsamles, identificeres og kombineres med henblik på profilering, hvis ikke servicen selv har implementeret det i deres system. Privatpersoners privacy kan ikke sikres, når først en service har din data. Det er derfor vigtigt, at brugeren undersøger og gør sig overvejelser om, hvilken sikkerhedsgaranti og tekniske redskaber en elektronisk service tilbyder.

Fremtidige løsninger:

Her er et par eksempler på mulige systemer og tekniske redskaber, som kunne blive aktuelle i fremtiden.

Fuldstændig homomorf kryptering

Fuldstændig homomorf kryptering *(fully homomorphic encryption)* er en særlig avanceret form for kryptering, der minder om MPC men med den forskel, at outputtet også er krypteret. Dette betyder, at et individ i praksis kan sende oplysninger til en organisation, som kan foretage en beregning. Ved at både input og resultat er krypteret, lærer organisationen intet om respondenten. Det krypterede resultat kan således sendes tilbage til respondenten, som selv dekrypterer svaret. Fuldstændig homomorf kryptering er i dag stadig for langsomme til at fungere i en kommercielle sammenhænge (Goroff et al. 2018).

Samlet Infrastruktur

Det er realistisk at forvente variationer af samlede kommercielle elektroniske infrastrukturer som sikrer privacy gennem design.

Et eksempel kunne være projektet General Data Protection Infrastructure (GDPI), hvor blandt andet Aarhus universitet, Partisia og IBM i samarbejde udvikler en samlet elektronisk infrastruktur. GPDI er baseret på *security* og *Privacy-by-Design* og kombinerer pseudonymitet, kryptering og multi-party teknologier til at balancere mellem muligheden for at anvende og beskytte borgerens data.

Acknowledgement

Vi vil gerne takke Ivan Damgård, Gert Læssøe Mikkelsen, Kurt Nielsen og Jakob Illeborg Pagter for at være behjælpelige med input og diskussion til notatet.

Referencer

Abadi, Martin, Andy Chu, Ian Goodfellow, H Brendan McMahan, Ilya Mironov, Kunal Talwar og Li Zhang (2016). "Deep Learning with Differential Privacy". I: *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16.* ACM. New York, New York, USA: ACM Press, s. 308–318.

Aggarwal, Charu C. (2005). "On K-anonymity and the Curse of Dimensionality". I: *Proceedings of the 31st International Conference on Very Large Data Bases.* VLDB '05. Trondheim, Norway: VLDB Endowment, s. 901–909.

Aggarwal, Gagan, Tomas Feder, Krishnaram Kenthapadi, Rajeev Motwani, Rina Panigrahy, Dilys Thomas og An Zhu (2005). "Approximation Algorithms for k-Anonymity". I: *Proceedings of the International Conference on Database Theory (ICDT 2005).*

Apple (2018). "iOS Security". I: *iOS Security Guide—White Paper*, s. 1–54.

Apple, Differential Privacy Team (2017). "Learning with Privacy at Scale". I: *Machine Learning Journal* 1, s. 1–25.

Archer, David W., Dan Bogdanov, Y. Lindell, Liina Kamm, Kurt Nielsen, Jakob Illeborg Pagter, Nigel P. Smart og Rebecca N. Wright (2018). *From Keys to Databases – Real-World Applications of Secure Multi-Party Computation.* https://eprint.iacr.org/2018/450.

Bogdanov, Dan, Liina Kamm, Baldur Kubo, Reimo Rebane, Ville Sokk og Riivo Talviste (2016). "Students and Taxes: a Privacy-Preserving Study Using Secure Computation". I: *Proceedings on Privacy Enhancing Technologies* 2016.3, s. 117–135.

Bournez, Carine og Claudio A. Ardagna (2011). "Policy Requirements and State of the Art". I: *Privacy and Identity Management for Life.* Udg. af Jan Camenisch, Simone Fischer-Hübner og Kai Rannenberg. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 295–312.

Camenisch, Jan (2012). "Information Privacy?!" I: *Computer Network* 56.18, s. 3834–3848.

Camenisch, Jan, abhi shelat abhi, Dieter Sommer, Simone Fischer-Hübner, Marit Hansen, Henry Krasemann, Gérard Lacoste, Ronald Leenes og Jimmy Tseng (2005). "Privacy and Identity Management for Everyone". I: *Proceedings of the 2005 Workshop on Digital Identity Management.* DIM '05. Fairfax, VA, USA: ACM, s. 20–27.

Camenisch, Jan, Maria Dubovitskaya, Markulf Kohlweiss, Jorn Lapon og Gregory Neven (2011). "Crypto-graphic Mechanisms for Privacy". I: *Privacy and Identity*

Management for Life. Udg. af Jan Camenisch, Simone Fischer-Hübner og Kai Rannenberg. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 117–134.

Camenisch, Jan, Günter Karjoth, Gregory Neven og Franz-Stefan Preiss (2013). "Anonymously Sharing Flickr Pictures with Facebook Friends". I: *Proceedings of the 12th ACM Workshop on Workshop on Privacy in the Electronic Society.* WPES '13. Berlin, Germany: ACM, s. 13–24.

Camenisch, Jan og Anja Lehmann (2015). "(Un)Linkable Pseudonyms for Governmental Databases". I: *Proceedings of the 22Nd ACM SIGSAC Conference on Computer and Communications Security.* CCS '15. Denver, Colorado, USA: ACM, s. 1467–1479.

Camenisch, Jan, Sebastian Mödersheim og Dieter Sommer (2010). "A Formal Model of Identity Mixer". I: *Formal Methods for Industrial Critical Systems.* Udg. af Stefan Kowalewski og Marco Roveri. Berlin,Heidelberg: Springer Berlin Heidelberg, s. 198–214.

Castelluccia, Claude (2012). "Behavioural Tracking on the Internet: A Technical Perspective". I: *European Data Protection: In Good Health?* Udg. af Serge Gutwirth, Ronald Leenes, Paul De Hert og Yves Poullet. Dordrecht: Springer Netherlands, s. 21–33.

Cavoukian, Ann (2010). "Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D". I: *Identity in the Information Society* 3.2, s. 247–251.

Chester, Jeff (2012). "Cookie Wars: How New Data Profiling and Targeting Techniques Threaten Citizens and Consumers in the "Big Data" Era". I: *European Data Protection: In Good Health?* Udg. af Serge Gutwirth, Ronald Leenes, Paul De Hert og Yves Poullet. Dordrecht: Springer Netherlands, s. 53–77.

Ciriani, V., S. De Capitani di Vimercati, S. Foresti og P. Samarati (2007). "*k*-Anonymity". I: *Secure Data Management in Decentralized Systems.* Udg. af Ting Yu og Sushil Jajodia. Boston, MA: Springer US, s. 323–353.

Commission on Evidence-Based Policymaking (2017). *The Promise of Evidence-Based Policymaking: Report of the Commission on Evidence-Based Policymaking.* Tek. rap. Washington, DC, s. 1–138.

Damgård, Ivan, Kasper Damgård, Kurt Nielsen, Peter Sebastian Nordholt og Tomas Toft (2017). "Confidential Benchmarking Based on Multiparty Computation". I: *Financial Cryptography and Data Security.* Udg. af Jens Grossklags og Bart Preneel. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 169–187.

Domingo-Ferrer, Josep og Vicenc ̧ Torra (2005). "Ordinal, Continuous and Heterogeneous *k*-Anonymity Through Microaggregation". I: *Data Mining and Knowledge Discovery* 11.2, s. 195–212.

Dwork, Cynthia (2006). "Differential Privacy". I: *Automata, Languages and Programming.* Udg. af Michele Bugliesi, Bart Preneel, Vladimiro Sassone og Ingo Wegener. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 1–12.

Dwork, Cynthia og Rebecca Pottenger (2013). "Toward practicing privacy". I: *Journal of the American Medical Informatics Association* 20.1, s. 102–108.

Dwork, Cynthia og Aaron Roth (2014). "The Algorithmic Foundations of Differential Privacy". I: *Foundations and Trends® in Theoretical Computer Science* 9.3–4, s. 211–407.

Dwork, Cynthia og Adam Smith (2010). "Differential Privacy for Statistics: What we Know and What we Want to Learn". I: *Journal of Privacy and Confidentiality* 2, s. 135–154.

Eckersley, Peter (2010). "How Unique Is Your Web Browser?" I: *Privacy Enhancing Technologies.* Udg. af Mikhail J. Atallah og Nicholas J. Hopper. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 1–18.

El Emam, Khaled og Fida Kamal Dankar (2008). "Protecting Privacy Using *k*-AnonymityW. I: *Journal of the American Medical Informatics Association* 15.5, s. 627–637.

Erlingsson, Úlfar, Vasyl Pihur og Aleksandra Korolova (2014). "RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response". I: *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.* CCS '14. Scottsdale, Arizona, USA: ACM, s. 1054–1067.

European Commission (2018). "A new era for data protection in the EU". I: May.

Ganta, Srivatsava Ranjit, Shiva Prasad Kasiviswanathan og Adam Smith (2008). "Composition Attacks and Auxiliary Information in Data Privacy". I: *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining.* KDD '08. Las Vegas, Nevada, USA: ACM, s. 265–273.

Garfinkel, Simson L (2015). "De-identification of personal information". I: *NISTIR* 8053, s. 1–46.

Goroff, Daniel, Jules Polonetsky og Omer Tene (2018). "Privacy Protective Research: Facilitating Ethically Responsible Access to Administrative Data". I: *The ANNALS of the American Academy of Political and Social Science* 675.1, s. 46–66.

Hilton, Michael (2012). "Differential Privacy: A Historical Survey". I: Cal Poly State University, s. 1–4.

Holohan, Naoise, Spiros Antonatos, Stefano Braghin og Pol Mac Aonghusa (2017). "Anonymity with ⊠-Differential Privacy". I: *CoRR abs*/1710.01615.

Househ, Mowafa, Rebecca Grainger, Carolyn Petersen, Panagiotis Bamidis og Mark Merolli (2018). "Balancing Between Privacy and Patient Needs for Health Information in the Age of Participatory Health and Social Media: A Scoping Review". I: *Yearbook of Medical Informatics.*

Højgaard, Betina og Jakob Kjellberg (2017). "Fem megatrends der udfordrer fremtidens sundhedsvæsen". I: *KORA: Det Nationale Institut for Kommuners og Regioners Analyse og Forskning* 28.

Identity Mixer, Zurich (n.d.). *Identity Mixer.* url: https:// www. zurich. ibm. com/ identity_ mixer/. (accessed: 05.06.2018).

Inan, Ali, Murat Kantarcioglu, Gabriel Ghinita og Elisa Bertino (2010). "Private Record Matching Using Differential Privacy". I: *Proceedings of the 13th International Conference on Extending Database Technology.* EDBT '10. Lausanne, Switzerland: ACM, s. 123–134.

Li, N., T. Li og S. Venkatasubramanian (2007). "t-Closeness: Privacy Beyond k-Anonymity and l-Diversity". I: *2007 IEEE 23rd International Conference on Data Engineering*, s. 106–115.

Liu, Xin, Shundong Li, Jian Liu, Xiubo Chen og Gang Xu (2016). "Secure multiparty computation of a comparison problem". I: *SpringerPlus* 5.1, s. 1–1489. "

Machanavajjhala, Ashwin, Daniel Kifer, Johannes Gehrke og Muthuramakrishnan Venkitasubramaniam (2006). "L-diversity: privacy beyond *k*-anonymity". I: *22nd International Conference on Data Engineering* (ICDE'06), s. 24–24.

Mao, Ziqing, Ninghui Li og Ian Molloy (2009). "Defeating Cross-Site Request Forgery Attacks with Browser-Enforced Authenticity Protection". I: *Financial Cryptography and Data Security.* Udg. af Roger Dingledine og Philippe Golle. Berlin, Heidelberg: Springer Berlin Heidelberg, s. 238–255.

McKinley, K. (2008). *Cleaning up after cookies.* Technical report, iSEC PARTNERS.

Miers, I., C. Garman, M. Green og A. D. Rubin (2013). "Zerocoin: Anonymous Distributed E-Cash from Bitcoin". I: *2013 IEEE Symposium on Security and Privacy*, s. 397–411.

Orlandi, Claudio (2011). "Is multiparty computation any good in practice?" I: *2011 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, s. 5848–5851.

Paquin, Christian (2013). *U-Prove Technology Overview V1.1 (Revision 2).*

Peter, Groves, Basel Kayyali, David Knott og Steve Van Kuiken (2013). "The 'big data' revolution in healthcare: Accelerating value and innovation". I: January, s. 1–22.

Podgursky, Benjamin (2011). "Practical K-anonymity on Large Datasets". Ph.d.-afh. Vanderbilt University.

Samarati, Pierangela og Latanya Sweeney (1998). *Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression.* Tek. rap. Technical report, SRI International.

Sweeney, Latanya (2000). "Simple demographics often identify people uniquely". I: *Health (San Francisco)* 671, s. 1–34.

– (2002). "*k*-ANONYMITY: A MODEL FOR PROTECTING PRIVACYW. I: *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems* 10, s. 557–570.

The National IT and Telecom Agency (2011). "New Digital Security Models". I: København: Digitaliseringsstyrelsen.

Veeningen, M., S. Chatterjea, A.Z. Horváth, G. Spindler, E. Boersma, P. Van Der Spek, O. Van Der Galién, J. Gutteling, W. Kraaij og T. Veugen (2018). "Enabling analytics on sensitive medical data with secure multi-party computation". I: *Studies in Health Technology and Informatics* 247, s. 76–80.

Zhou, S., K. Ligett og L. Wasserman (2009). "Differential privacy with compression". I: *2009 IEEE International Symposium on Information Theory*, s. 2718–2722.

DET ETISKE RÅD
kontakt@etiskraad.dk
Tel: +45 72 21 68 70
etiskraad.dk

DET ETISKE RÅD