

Dansk persondataret



BENT OLE GRAM MORTENSEN (RED.)

Dansk persondataret

ExTuto
PUBLISHING
www.extuto.com

Bent Ole Gram Mortensen (red.), Carina Risvig Hamer, Daniel Hartfield-Traun, Lisa Hjerrild, Kent Kristensen, Jesper Kruse Markvart, Helene Arensbak Mørk, Jesper Løffler Nielsen, Ayo Næsborg-Andersen, Sten Schaumburg-Müller, Christian Højer Schjøler, Peter Starup, Jøren Ullits & Frederik Waage

Dansk persondataret

Første udgave, første oplag

Denne bog er udgivet i januar 2020 af EX TUTO PUBLISHING A/S. Grafisk tilrettelæggelse og sats af MERE.INFO A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis FRANTIŠEK ŠTORM i 2000 og ROBERT SLIMBACH i 1996. JAN TRZASKOWSKI har stået for forlagsredaktion og TOVE MØGELVANG-HANSEN har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m² af NARAYANA PRESS, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af BUCHBINDEREI S.R. BÜGE GMBH i Celle. Bogen er fagfællebedømt.

Ex Tuto A/S er medlem af Forening for Boghaandværk, og vi støtter bæredygtig skovforvaltning ved at anvende FSC-certificeret papir.

Copyright © 2020 the editor and the authors

Printed in Denmark 2020

ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S

Toldbodgade 55, 1.

DK-1253 København K

www.extuto.com



Udgivet med støtte fra

dreyersfond

Kapitelloversigt

DEL I: GENERELLE SPØRGSMÅL	1
1. Fra registerlov til databeskyttelsesforordning <i>Bent Ole Gram Mortensen</i>	3
2. Den centrale lovgivning på databeskyttelsesområdet <i>Peter Starup</i>	19
3. Hvornår er der tale om en personoplysning, og hvornår er det behandling af en sådan? <i>Sten Schaumburg-Müller</i>	29
4. Nærmere om persondatarettens dækning <i>Sten Schaumburg-Müller</i>	41
5. De overordnede principper for databehandling <i>Ayo Næsborg-Andersen</i>	55
6. Oplysningskategorier og behandlingsbetingelser <i>Sten Schaumburg-Müller</i>	75
7. Ytrings- og informationsfrihed <i>Sten Schaumburg-Müller</i>	117
8. Personbilleder <i>Sten Schaumburg-Müller</i>	127
9. Ansvarlighed og dokumentation <i>Jesper Løffler Nielsen & Helene Arensbak Mørk</i>	169
10. Ansvarssubjekter og aftaleregulering <i>Jesper Løffler Nielsen & Helene Arensbak Mørk</i>	177

11. Databeskyttelsesrådgiveren	191
<i>Lisa Hjerrild</i>	
12. Krav om konsekvensanalyse	203
<i>Lisa Hjerrild</i>	
13. De registreredes rettigheder	213
<i>Jøren Ullits, Ayo Næsborg-Andersen & Kent Kristensen</i>	
14. Sikkerhed og håndtering af databrud	229
<i>Daniel Hartfield-Traun</i>	
15. Tredjelandsoverførsler	255
<i>Jesper Løffler Nielsen & Helene Arensbak Mørk</i>	
16. Tilsynsmyndigheder og sanktioner	269
<i>Carina Risvig Hamer</i>	
DEL II: UDVALGTE RETSOMRÅDER	281
17. Persondatarettens anvendelse på forskningsprojekter	283
<i>Kent Kristensen & Jøren Ullits</i>	
18. Statistik	301
<i>Ayo Næsborg-Andersen</i>	
19. Behandlingen af personoplysninger ved domstolene	309
<i>Frederik Waage</i>	
20. Persondatabehandling i journalistisk øjemed	321
<i>Jøren Ullits & Sten Schaumburg-Müller</i>	
21. Kunstnerisk, litterær og akademisk virksomhed	343
<i>Sten Schaumburg-Müller</i>	
22. Markedsføring og personoplysninger	349
<i>Bent Ole Gram Mortensen</i>	
23. Forsyningsvirksomheder	367
<i>Bent Ole Gram Mortensen & Lisa Hjerrild</i>	
24. Geodata	377
<i>Lisa Hjerrild</i>	

25. Konkurrenceret	385
<i>Peter Starup & Jesper Kruse Markvart</i>	
26. Sundhedslovens behandlingsregler	429
<i>Kent Kristensen & Jøren Ullits</i>	
27. Forvaltningens samkøring af borgerdata	443
<i>Jøren Ullits</i>	
28. HR og persondataret	453
<i>Christian Højer Schjøler</i>	
Bibliografi	481
Stikordsregister	495

Sundhedslovens behandlingsregler

Kent Kristensen & Jøren Ullits

26.1. Indledning

Udviklingen inden for database- og programmeringsteknologien har øget mulighederne for at indsamle, opbevare og samkøre data. I takt med den teknologiske udvikling har patientjournalerne udviklet sig fra at være baseret på en enkelt it-plattform til at være digitale patientinformationssystemer, hvor sundhedsvæsenets aktører deler og tilgår data fra forskellige elektroniske platforme på tværs af organisatoriske grænser mellem flere dataansvarlige. Sundhedslovens behandlingsregler afspejler denne udvikling. Fra at være regler, der blev udviklet med en forståelse af patienters ret til selvbestemmelse og en ret til at få indflydelse på, hvem der kan få adgang til oplysningerne, er sundhedslovens behandlingsregler i højere grad udviklet med henblik på at udnytte mulighederne for at dele data. Det er samtidig en udvikling, der stiller krav om udarbejdelse af specifikke foranstaltninger til beskyttelse af den registrerede. Kapitlet omhandler disse regler og forholdet til databeskyttelsesforordningen.

Kapitlet indledes i afsnit 26.2 med en oversigtlig beskrivelse af den digitale infrastruktur og mulighederne for at dele sundhedsdata mellem sundhedsvæsenets forskellige aktører. Behandlingen af oplys-

ninger i den digitale infrastruktur er omfattet af sundhedslovens behandlingsregler og skal holde sig inden for rammerne af forordningens harmonisering. I afsnit 26.3 beskrives indledningsvist forholdet til forordningen og dernæst behandles de sundhedsretlige behandlingsregler. De øgede muligheder for at stille oplysninger til rådighed for andre stiller samtidig øgede krav til fastsættelse af specifikke beskyttelsesforanstaltninger. Kravene til beskyttelse af den registrerede behandles i afsnit 26.4.

26.2. Sundhedsvæsenets digitale infrastruktur

26.2.1. Introduktion

Sundhedspersoner har efter journalføringsreglerne pligt til at dokumentere patientbehandlingen. Patientjournalen og det at anvende og føre sundhedsfaglige optegnelser er traditionelt begrænset til behandlingsrelationen mellem patient og den pågældende sundhedsperson. Patientjournalerne har imidlertid udviklet sig fra elektroniske patientjournaler til informationssystemer, hvor de registrerede oplysninger lagres i databaser baseret på en fælles digital infrastruktur, som er tilgængelig på tværs af regioner og kommuner for forskellige aktører. Den øgede tilgængelighed af helbredsoplysninger forbedrer kvaliteten og sikkerheden i forbindelse med patientbehandlingen sammenlignet med de traditionelle former for sundhedsfaglig dokumentation.

26.2.2. Sundhedsvæsenets kildesystemer

Den digitale infrastruktur omfatter oplysninger fra sundhedsvæsenets forskellige kildesystemer, hvor oplysninger om patienters helbredsforhold løbende registreres.

Regionerne er dataansvarlige for de regionale (lokale) kildesystemer, og Sundhedsdatastyrelsen er dataansvarlig for de nationale kildesystemer. De fleste af de nationale sundhedsregistre er etableret på grundlag af oplysninger fra de regionale kildesystemer.

I Landspatientregistret registreres oplysninger om patienters undersøgelses- og indlæggelsesforløb, herunder diagnosekoder, laboratorieresvar, sengedage m.v. Registreringen af oplysninger sker dels manuelt ved indtastning og automatisk, hvor oplysninger overføres fra de

regionale sygehusjournaler. Medicinoplysninger, der er tilgængelige i Det Fælles Medicinkort (FMK), registreres først i patientjournalen i et selvstændigt modul og overføres derefter til FMK, der fungerer som en fælles national database, som er tilgængelig for sundhedspersoner i blandt andet hjemmesygeplejen, praktiserende læge, sygehus og apotekspersonale. Laboratoriesvar, prøvesvar på blod- og vævsprøver overføres fra de regionale kildesystemer til Laboratoriedatabasen, der er en fælles national database. Radiologiske røntgen- og skanningsbilleder registreres i billeddatabasen (PACS), der er en fælles regional database, og overføres herfra til et fælles Nationalt Billedindeks. Genetiske oplysninger i forbindelse med patientbehandling registreres i patientjournalen og overføres herfra til en fælles national gendatabase. Patient-rapporterede oplysninger, registreres i en database for klinisk integreret hjemme-monitorering (KIH-databasen), der fungerer som en national database for opsamling og deling af data opsamlet i patientens eget hjem på tværs af sundhedsvæsenets aktører.

26.3. Databeskyttelsesretten

26.3.1. Introduktion

Sundhedsdatastyrelsen er efter sundhedsloven dataansvarlig for at drive en fælles digitale infrastruktur til udveksling og registrering af oplysningerne om borgerens helbredsforhold og dermed også for opfyldelse af reglerne i databeskyttelsesforordningen (GDPR). Regionernes dataansvar er begrænset til de regionale kildesystemer. Der gælder efter GDPR artikel 9, stk. 1, et generelt forbud mod at behandle følsomme oplysninger. Der er imidlertid opregnet en række undtagelser, hvor der i forordningen er taget et særligt hensyn til behandlingen af oplysninger på sundhedsområdet. Medlemsstaterne har således efter databeskyttelsesforordningens en relativt stor manøvremargin til at opretholde eller indføre yderligere betingelser for behandlingen af helbredsoplysninger i national ret. Medlemsstaterne kan inden for rammerne af forordningens harmonisering præcisere anvendelsen af forordningsbestemmelser og kan på visse områder fastsætte en række yderligere begrænsninger for behandlingen af oplysninger. Indledningsvist belyses det retlige grundlag for behandling af oplysninger i den fælles digi-

tale infrastruktur, og derefter behandles sundhedsrettens særlige behandlingsregler.

26.3.2. Forordningen

Det retlige grundlag for behandlingen af oplysninger i den fælles digitale infrastruktur findes i sundhedslovens § 193 b.¹ Formålet med at behandle oplysninger kan sammenfattes som oplysninger, der er nødvendige for patientbehandling, forebyggende sygdomsbekæmpelse eller forvaltning af læge- og sundhedstjenester. Behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.² Formålsafgrænsningen svarer, med mindre forskelle, til databeskyttelsesforordningens artikel 9, stk. 2, litra h, og den korresponderende artikel 6, stk. 1, litra e. Bestemmelsen i artikel 9, stk. , litra h, er inddelt i to led. Første led omfatter behandling af helbredsoplysninger med henblik på forebyggende medicin, arbejdsmedicin, medicinsk diagnose, ydelse af social- og sundhedsomsorg eller -behandling eller forvaltning af social- og sundhedsomsorg og -tjenester. Andet led omfatter behandling af oplysninger i henhold til kontakt med en sundhedsperson.

Første led indeholder udover kravet om lovhjemmel tre yderligere betingelser, som skal være opfyldt. Behandlingen skal være formålsspecifik til de formål, der er opregnet i bestemmelsen, behandlingen skal endvidere være "nødvendig" for formålet, og endelig skal behandlingen foretages af en fagperson, der er underlagt tavshedspligt, jf. GDPR artikel 9, stk. 3. Andet led udgør et selvstændigt retligt grundlag for behandling af oplysninger og skal derfor "aktiveres" i enten EU-retten eller i national ret. Bestemmelsen skal som en undtagelsesregel fra det generelle forbud mod at behandle følsomme oplysninger fortolkes snævert begrænset til oplysninger, der er påkrævet for direkte at

-
1. Lov 273 af 26. marts 2019. Sundhedsministeren fastsætter tidspunktet for ikrafttrædelse af § 193 b.
 2. Sundhedslovens § 193 b, stk. 2. Oplysninger, der opbevares i den fælles digitale infrastruktur, må kun behandles, hvis det er nødvendigt med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje, patientbehandling eller forvaltning af læge- og sundhedstjenester, og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt.

levere de ydelser, der er truffet aftale om. Behandling af oplysninger til administrative formål er eksempelvis ikke omfattet. Den nationale digitale infrastruktur omfatter andre formål end den direkte patientbehandling. GDPR artikel 9, stk. 2, litra h, kan derfor ikke uden videre anvendes som behandlingshjemmel. Bestemmelsen i GDPR artikel 9, stk. 2, litra h, skal så at sige "aktiveres" i enten EU-retten eller national ret, for at behandlingsforbuddet kan anses for fraveget. Uden andet retligt grundlag udgør sundhedslovens § 193 b en sådan behandlingshjemmel. I og med at GDPR artikel 9, stk. 2, litra h, ikke uden videre kan anvendes som behandlingsgrundlag, kan medlemsstaterne lovgivningsmæssigt bestemme kun at aktivere dele af bestemmelsen.

I det omfang sundhedsloven ikke har aktiveret hele bestemmelsen i forordningens artikel 9, stk. 2, litra h, gælder forbuddet mod at behandle de pågældende oplysninger. Formålsafgrænsningen i sundhedslovens § 193 b omfatter ikke behandling af oplysninger vedrørende arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne og ydelse af social- og sundhedsomsorg. Behandlingen af oplysninger i den digitale infrastruktur skal dermed fortolkes mere snævert i retning af opgaver, der har direkte tilknytning til opgaver i sundhedsvæsenet. Formålsbestemmelsen giver dermed ikke hjemmel til, at eksempelvis de kommunale myndigheder behandler oplysninger til brug for planlægning af ydelser på det sociale område, som ikke har en direkte tilknytning til sundhedsområdet. Tilsvarende giver bestemmelsen ikke hjemmel til at behandle oplysninger til de arbejdsmedicinske klinikker til brug for vurderingen af arbejdsevnen.

Derudover følger det af formålsafgrænsningen i sundhedslovens § 193b, at oplysningerne ikke kan behandles til fastlæggelse af retskrav eller til forskningsformål. Det er af ordlyden ikke klart, at forbuddet mod at behandle oplysninger til fastlæggelse af retskrav ikke gælder for behandling af klage- og erstatningssager i medfør af lov om klage- og erstatningsadgang inden for sundhedsvæsenet eller til brug for Styrelsen for Patientsikkerheds varetagelse af tilsynsopgaver efter autorisationsloven eller sundhedsloven, sådan som det er præciseret i forarbejderne.³ Derudover skal det bemærkes, at formålsafgrænsningen gælder for den fælles digitale infrastruktur og ikke for de underliggende

3. FT 2018-19, L 127, A som fremsat, s. 47.

kildesystemer. Det er dermed ikke udelukket at behandle oplysninger i de regionale kildesystemer til formål, der ellers er udelukket efter formålsafgrænsningen i sundhedslovens § 193 b. Der vil herefter kunne behandles oplysninger fra de regionale kildesystemer til eksempelvis forskningsformål.

26.3.3. Sundhedsloven

Formålet med at behandle oplysninger i den fælles digitale infrastruktur er fastlagt i sundhedslovens § 193 b, mens adgangen til oplysninger følger af sundhedslovens indhentningsregler i §§ 42 a-e. Reglerne om indhentning af oplysninger omfatter adgangen til at foretage opslag i de elektroniske patientsystemer. Indhentningsreglerne omfatter den enkelte persons direkte online adgang til oplysninger. Det følger samtidig af formålsafgrænsningen, at oplysningerne kun kan indhentes til formål, der er i overensstemmelse med formålet med at behandle oplysninger i den digitale infrastruktur. Indhentningsreglerne er bygget op omkring en sondring mellem indhentning af helbredsoplysninger til patientbehandling og indhentning til andre formål. Indledningsvist omtales indhentning af helbredsoplysninger til patientbehandling og dernæst reglerne om indhentning af oplysninger til andre formål.

26.3.3.1. Behandling af patienten

Reglerne i § 42 a retter sig mod den enkelte sundhedsperson og giver en sundhedsperson adgang til uden patientens samtykke at indhente oplysninger om en patients helbredsforhold og andre fortrolige oplysninger, når det er nødvendigt i forbindelse med aktuel behandling af patienten. Sundhedspersoner skal forstås i overensstemmelse med sundhedslovens § 6 og omfatter autoriserede sundhedspersoner eller personer, der handler på vegne af en, der er autoriseret. Personer der ikke er autoriserede, men som får overdraget en sundhedsfaglig behandlingsopgave, anses dermed også for at være en sundhedsperson. Lægeseekretærer, der tager blodprøver, sygehjælper eller studerende, der deltager i patientbehandlingen på sygehuse, anses dermed også for sundhedspersoner.

Sundhedspersoner kan efter § 42 a, stk. 1, i *fornødent omfang* indhente helbredsoplysninger mv. elektronisk ved opslag, når det er *nødvendigt* i forbindelse med *aktuel behandling*.

Fornødent omfang indebærer, at de sundhedspersoner, der er omfattet af bestemmelsen, ikke må indhente oplysningerne i videre omfang end det, der er sagligt begrundet i forhold til behandlingen. Er systemet indrettet sådan, at sundhedspersonen ved opslag præsenteres for enten en oversigt eller en sammenfatning af oplysninger, giver reglen alene hjemmel til at foretage opslag i de oplysninger, hvor lægen ud fra oversigten vurderer, at der er et fagligt behov for de pågældende oplysninger.

Oplysningerne skal være *nødvendige* for behandlingen. Det er ikke et krav, at sundhedspersonen på forhånd har konstateret, at det er nødvendigt at få adgangen til de konkrete oplysninger. Det er tilstrækkeligt, at sundhedspersonen forinden har en begrundet formodning om, at oplysningerne kan være nødvendige for behandlingen.

Derudover er retten til at indhente oplysninger uden samtykke begrænset til oplysninger til brug for *aktuel behandling*. Der skal dermed foreligge en behandlingsmæssig relation mellem sundhedsperson og patient, og hvor den, der indhenter oplysninger, skal have en rolle i den aktuelle behandling. Det er ikke en betingelse, at den sundhedsperson, der indhenter oplysningerne, først har tilset patienten. Det er tilstrækkeligt, at patienten er henvist til forundersøgelse med henblik på evt. behandling. Sundhedspersonen må herefter på baggrund af henvisningen vurdere, hvilke oplysninger det er nødvendigt at indhente til brug for den planlagte undersøgelse.

Disse tre betingelser er ikke tilstrækkelige. Patienten må ikke efter sundhedslovens § 41 a, stk. 6, have udnyttet retten til at frabede sig, at sundhedspersonen indhenter oplysninger. Retten til at frabede sig indhentning af oplysninger skal ses i lyset af indsigelsesretten i forordningens artikel 21, hvor den registrerede til enhver tid har ret til, af grunde, der vedrører den pågældendes særlige situation, at gøre indsigelse mod behandlingen af sine personoplysninger.⁴ Den dataansvarlige må herefter ikke længere behandle oplysningerne, medmindre den dataansvarlige kan påvise vægtige legitime grunde til behandlingen, som går forud for den registreredes interesser.

Patienten skal informeres om retten til at sige fra. Det kan ske ved, at sundhedspersonen konkret informerer patienten om muligheden

4. FT 2006-07, A, L 431 som fremsat, s. 698.

eller mere generelt i form af udleveret patientinformationsmateriale eller anden skriftlig vejledning.

Patienter kan generelt frabede sig, at der indhentes oplysninger fra den fælles digitale infrastruktur.⁵ Retten til at frabede sig indhentning af oplysninger omfatter også bestemte sundhedspersoner, bestemte afdelinger, bestemte kategorier af oplysninger eller oplysninger fra et bestemt tidsrum. I nogle situationer kan udnyttelse af retten til at frabede sig indhentning af helbredsoplysninger indebære, at det er umuligt at behandle patienten. Patienten skal i disse tilfælde informeres om konsekvenserne af at frabede sig indhentning af helbredsoplysninger. Der er i sundhedsloven ikke nogen nærmere angivelse af, hvordan retten til at frabede sig indhentning af oplysninger skal udmøntes. Patienten er derfor i praksis henvist til at tage kontakt til den enkelte region, som herefter manuelt må spærre for adgangen til at indhente oplysningerne.

26.3.3.2. Andre formål

Der kan efter sundhedslovens § 42 a-e indhentes oplysninger til forskellige formål.

Der er i sundhedsloven hjemmel til at indhente oplysninger uden samtykke til brug for behandling af andre end patienten selv. Sundhedsloven § 41 a, stk. 2, giver hjemmel til at indhente oplysninger til brug for behandling af andre patienter, når det er nødvendigt til berettiget varetægelse af en åbenbar almen interesse. Bestemmelsen er udformet som en værdispringsregel, hvor hensynet til at indhente oplysninger klart skal overstige hensynet til fortrolighed. I sundhedslovens § 42 a, stk. 6, er retten til at indhente oplysninger udvidet til at omfatte oplysninger til brug for beslutningsstøtte. Bestemmelsen er udformet som en bemyndigelsesbestemmelse og giver hjemmel til at fastsætte regler om, at en autoriseret sundhedsperson kan indhente oplysninger fra elektroniske patientsystemer om andre patienter som et led i aktuel behandling af en anden patient. Indhentningen omfatter oplysninger om patienter med sammenlignelige tilstande med henblik på at støtte en sundhedsperson i at træffe sundhedsfaglige beslutninger. Bestemmelsen giver hjemmel til at indhente oplysninger i person-

5. SUU 2018-19, L 127 som fremsat, endeligt svar på spørgsmål 6.

henførbart form og omfatter enkelte patienter såvel som et meget stort antal patienter. Det er ikke et krav, at der skal foretages en konkret afvejning af hensynet til patienters ret til fortrolighed over for hensynet til oplysningernes væsentlighed til brug for behandling af en anden patient. Bestemmelsen giver dermed en mere lempelig adgang til at indhente oplysninger og vil i praksis erstatte værdispringsreglen som hjemmelsgrundlag. Indhentningen er personhenførbart, *anvendelsen* af oplysninger må derimod efter forarbejderne kun finde sted i pseudonymiseret form.⁶

I tillæg til de allerede nævnte regler er der i sundhedslovens § 42 d-e fastsat regler for behandling af oplysninger til brug for uddannelse, kvalitetssikring og akkreditering. Oplysninger kan efter bestemmelsen indhentes uden samtykke fra den registrerede.

26.4. Krav til udformningen af den digitale infrastruktur

26.4.1. Introduktion

Udviklingen af den fælles digitale infrastruktur har givet forskellige aktører mulighed for at få direkte adgang til en samling af helbredsoplysninger om en persons behandling fra sundhedsvæsenets kilder over et helt liv til brug for forskellige formål. Fortroligheden i læge-patientforholdet var oprindeligt begrænset til den enkelte læge. Den digitale infrastruktur overskrider derfor også den traditionelle grænse for fortroligheden i læge-patientforholdet. Den øgede tilgængelighed indebærer, at det i lovgivningen er nødvendigt at se på behovet for at fastsætte krav om mere specifikke foranstaltninger til beskyttelse af den registrerede.

Kravet om, at oplysningerne skal behandles af personer, der er underlagt tavshedspligt, udgør en væsentlig, men ikke tilstrækkelig beskyttelsesmekanisme i GDPR artikel 9, stk. 2, litra h. Der er således anført en række yderligere krav om, at behandlingen foruden at være nødvendig skal ske til brug for specifikke formål og have hjemmel i enten national ret eller i EU-retten. Det er derfor også i forbindelse med etableringen af den digitale infrastruktur relevant at se nærmere

6. FT 2018-19, A, L 127 som fremsat, s. 40.

på kravene til udformningen af det retlige grundlag for beskyttelse af den registrerede.

26.4.2. Beskyttelsesforanstaltninger

Artikel 29-Gruppen har i et arbejdsdokument formuleret nogle generelle anbefalinger til beskyttelse af personoplysninger i elektroniske patientsystemer.

For det første bør retten til selvbestemmelse efter Artikel 29- gruppen opfattelse tillægges væsentlig betydning som beskyttelsesmekanisme. *For det andet* bør der sondres mellem forskellige grader af muligheder for at udøve selvbestemmelsesretten i forhold til oplysningernes skadevirkning, og endelig peger Artikel 29-Gruppen *som det tredje* på, at det i lovgivningen bør være muligt at forhindre offentliggørelsen af helbredsoplysninger indsamlet i forbindelse med patientbehandlingen.

For så vidt angår selvbestemmelsesretten lægger artikel 29-Gruppen vægt på, at selvbestemmelsesretten bør spille en væsentlig rolle som beskyttelsesmekanisme med hensyn til spørgsmålet om, hvornår og hvordan oplysningerne behandles.⁷ Der ligger heri ikke en anbefaling om, at behandlingen af oplysninger skal være samtykkebaseret. Udøvelse af selvbestemmelsesretten kan også have form af en opt-out ordning, hvor patienten kan frabede sig behandling af oplysninger.⁸ Der skal som nævnt sondres mellem indlæsning og indhentning af oplysninger. Selvbestemmelsesretten er i den digitale infrastruktur udformet som en opt-out ordning, hvor patienten kan frabede sig indhentning af oplysninger. Retten til at fravælge indhentning af oplysninger er, jf. sundhedslovens § 42 a, stk. 6, begrænset til formål for patientbehandling og gælder kun patienten selv. Patienter kan dermed ikke frabede sig indhentning af oplysninger til andre formål. Indhentning af oplysninger til brug for behandlingen af andre patienter er ikke omfattet af sundhedslovens opt-out ordning. Det gælder indhentning af oplysninger efter værdispringsreglen i sundhedsloven § 41 a, stk. 2, og efter sundhedslovens § 41 a, stk. 6, som udvider hjemlen til at indhente oplysninger fra at omfatte patientbehandling til at omfatte oplysninger til brug for beslutningsstøtte til behandling af andre patienter.

7. Artikel 29-Gruppen WP 131, s. 14.

8. Ibid., s. 13.

Hvad angår oplysningernes skadevirkning, peger Artikel 29-Gruppen på, at der bør tages hensyn til, at adgangen til personoplysninger er omfattet af en ordning med stigende krav om “opt-in”, når der er tale om oplysninger, der udgør en særlig risiko for at kunne skade den registrerede og “opt-out” muligheder for mindre kompromitterende oplysninger.⁹ I Artikel 29-Gruppen fremhæves psykiatriske oplysninger og oplysninger om svangerskabsafbrydelse som oplysninger, der kræver en særlig beskyttelse.¹⁰ Den digitale infrastruktur omfatter somatiske, psykiatriske og genetiske oplysninger, og der sondres ikke mellem de forskellige kategorier af oplysninger vedrørende retten til at fravælge indlæsning af oplysninger. Der er imidlertid fastsat særlige regler for adgangen til at indhente genetiske oplysninger. Den registrerede kan vælge, at genetiske oplysninger ikke må bruges til andre formål end behandling af patienten selv, jf. sundhedslovens § 29, stk. 1.¹¹ Genetiske oplysninger er som nævnt heller ikke omfattet af sundhedslovens § 41 a, stk. 6, om indhentning af oplysninger til brug for beslutningsstøtte. Derudover finder de almindelige regler om edition efter straffetretten ikke anvendelse for genetiske oplysninger. Genetiske oplysninger kan efter sundhedslovens § 223 b, stk. 2, alene videregives til brug for efterforskning af en overtrædelse af straffelovens § 114 eller § 114 a om terrorisme og terrorlignende handlinger. Endelig følger det af formålsafgrænsningen for indsamlingen af genetiske oplysninger i sundhedslovens § 223 b, at genetiske oplysninger ikke kan indgå i fastlæggelse af retskrav efter GDPR artikel 9, stk. 2, litra f. Der peges i forarbejderne specifikt på, at genetiske oplysninger ikke ville kunne videregives, til brug for fastlæggelse af et retskrav i en forsikrings- eller pensionssag.¹²

Endelig bør det ifølge Artikel 29-Gruppen være muligt for patienter at forhindre fremvisningen af oplysninger. Det indebærer, at det i lovgivningen er nødvendigt at forholde sig til, hvordan det skal håndteres, at en patient har udnyttet muligheden for at frabede sig, at andre får adgang til oplysningerne. Der er i sundhedsloven ikke nærmere fastsatte regler for, hvordan retten til at frabede sig behandling af oplysning-

9. Ibid., s. 15.

10. Ibid., s. 14.

11. Indført ved lov 728/2018 om organiseringen i Sundheds- og Ældreministeriet.

12. FT 2017-18, L 146, B, s. 2.

ger skal udmøntes. Der er således ikke fastsat regler for, hvordan det skal fremgå, at den registrerede har ønsket at privatmarkere bestemte oplysninger, eller hvordan det skal håndteres, at oplysningerne kun er tilgængelige på bestemte vilkår. I tilknytning til retten til at frabede sig indhentning af oplysninger peger Artikel 29-Gruppen på, at der i lovgivningen skal tages stilling til muligheden for at slette oplysningerne. Der er i journalføringsbekendtgørelsen taget stilling til sletning af oplysninger. Det følger af bekendtgørelsen, at oplysninger i patientjournalen ikke må slettes eller gøres ulæselige. Der kan alene rettes eller tilføjes oplysninger, så den oprindelige tekst bevares. Det bagvedliggende hensyn er, at det er nødvendigt også at opbevare forkerte oplysninger for at kunne dokumentere grundlaget for patientbehandlingen. Journalføringsreglerne er i praksis fortolket sådan, at det er udelukket at slette oplysninger, som er åbenbart forkerte og helt uden betydning for patientbehandlingen.¹³

26.5. Konklusion

Sundhedsloven er udformet som en opt-out ordning, hvor patienten kan frabede sig indhentning, men ikke indlæsning af helbredsoplysninger. Det er ikke uden betydning, om retten til at frabede sig behandling af oplysninger udmøntes før eller efter, oplysningerne er indlæst. En opt-out ordning udformet som en ret til at indhente oplysninger, efter de er indlæst, beskytter ikke den registrerede mod den usikkerhed, der er forbundet med, at oplysninger der er indlæst, er til rådighed til brug for fremtidige ukendte formål.¹⁴ Der er samtidig sket en udvidelse af den kreds af personer, der har adgang til at indhente oplysninger. Kredsen af personer, der kunne indhente oplysninger, var oprindeligt begrænset til læger og sygehusansatte tandlæger,¹⁵ men er sidenhen løbende udvidet til nu at omfatte alle sundhedspersoner.¹⁶ Derudover er formålene med at indhente oplysninger udvidet fra at være direkte rela-

13. Kristensen 2018.

14. Artikel 29-Gruppen er af den opfattelse, at ingen bør kunne tvinges til at deltage i et EPJ-system, jf. Artikel 29-Gruppen WP 131, s. 14 (engelsk udgave).

15. Lov 431/2007 (it-anvendelse i sundhedsvæsenet og elektroniske helbredsoplysninger).

16. Lov 273/2019 (Bedre digitalt samarbejde i sundhedsvæsenet).

teret til behandlingen af den enkelte patient, til også at omfatte opgaver i tilknytning til patientbehandling (kvalitetsudvikling og akkreditering) og til formål for beslutningsstøtte til behandling af andre patienter. I takt med de øgede muligheder for at dele helbredsoplysninger er der i lovgivningen skabt det nødvendige retlige grundlag for at indhente oplysningerne til brug for forskellige formål. Den retlige regulering har dermed understøttet den teknologiske udvikling med henblik på deling af oplysninger. Den retlige udvikling yder samtidig kun den registrerede en begrænset beskyttelse. Den registrerede har således kun en begrænset mulighed for at fastsætte grænsen for retten til fortrolighed ved at forhindre adgang til oplysninger om vedkommende selv.