CompLex

Senter for rettsinformatikk / Avdeling for forvaltningsinformatikk

Jens Andresen Osberg

Innsyn i automatiserte avgjørelser etter personvernforordningen

Hva er en automatisert avgjørelse og hva er «relevant informasjon om den underliggende logikken» for avgjørelsen?

2/2019

UiO : Det juridiske fakultet

Henvendelser om denne bok kan gjøres til:
Senter for rettsinformatikk
Postboks 6706 St. Olavs plass
0130 Oslo
Tlf. 22 85 01 01
http://www.jus.uio.no/ifp/om/organisasjon/seri/

ISBN 978-82-72261-70-1
ISSN 0806-1912

Grafisk produksjon: 07 Media AS – 07.no

Forord

Grunnlaget for denne artikkelen er min masteroppgave i rettsvitenskap som ble levert 25. april 2019. Det er ikke gjort nevneverdige endringer fra da masteroppgaven ble levert.

Bakgrunnen for valg av problemstilling er at jeg parallelt med masteroppgaven, har gått første året av en bachelorgrad i «Informatikk: programmering og systemarkitektur» ved UiO. Dette gjorde at jeg ønsket å skrive en oppgave innen rettsinformatikk. Etter tips fra min veileder Dag Wiese Schartum, landet jeg på innsyn i automatiserte avgjørelser etter EUs nye personvernforordning (GDPR[1]) artikkel 15 nr. 1 bokstav h, jf. artikkel 22. Det tidligere personverndirektivet hadde liknende bestemmelser, men disse var lite brukt.[2] Med stadig flere og mer komplekse automatiserte avgjørelser i samfunnet, var og er det grunn til å tro at bestemmelsene i personvernforordningen oftere vil bli påberopt. Problemstillingen fremstod dermed som aktuell. Denne aktualiteten ble bekreftet da jeg så et foredrag på JavaZone 2018 om «Interpretable Machine Learning: Techniques to explain black box models».[3] Her var det tydelig at innsyn i automatiserte avgjørelser var aktuelt fra et informasjonsteknologisk perspektiv, særlig ved bruk av maskinlæring. Aktualiteten ble også bekreftet da forslaget til ny forvaltningslov og forslaget til ny arkivlov ble lagt frem. Her var automatiserte avgjørelser og dokumentasjon av slike avgjørelser behandlet.[4]

Jeg vil takke Dag Wiese Schartum for tips til tema, og for svært god veiledning. Videre vil jeg takke BAHR Leap for skriveplass, samt for verdifulle diskusjoner, både om de rettslige og teknologiske sidene ved problemstillingen. Jeg vil også takke Christian Frederik Mathiessen og Are Stenvik for gjennomlesing og gode innspill.

Oslo, 5. august 2019

Jens Andresen Osberg

1 Personvernforordningen (engelsk).
2 Personverndirektivet artikkel 15 nr. 1 og artikkel 12 bokstav a. Se Bygrave (2019) s. 1.
3 Bertani-Økland (2018).
4 NOU 2019:5 § 12 s. 20 og NOU 2019:9 § 10 s. 18.

Innhold

1 Innledning

Stadig flere avgjørelser tas av datamaskiner. Ny teknologi gjør det mulig for datamaskiner å ta mer kompliserte avgjørelser enn tidligere. Samtidig bringer slike automatiserte avgjørelser med seg rettsikkerhetsutfordringer. Et illustrerende eksempel er i den amerikanske staten Arkansas. Her opplevde funksjonshemmede med behov assistanse å få denne dramatisk redusert som følge av automatiserte avgjørelser. I en påfølgende rettssak ble det argumentert med at de berørte ikke hadde forutsetninger for å forstå datamaskinprogrammet som hadde blitt brukt. De hadde dermed ingen effektive muligheter til å overprøve de automatiserte avgjørelsene. Under rettssaken ble en sakkyndig bedt om å sjekke en av avgjørelsene manuelt. Da viste det seg at reduksjonen skyldtes en feil i algoritmen som lå til grunn for datamaskinprogrammet.[5]

Den 20. juli 2018 trådte EUs nye personvernforordning (GDPR[6]) i kraft[7] i Norge (heretter: personvernforordningen og forordningen[8]). Forordningen er en omfattende revisjon av personvernregelverket i Europa. Den etterfulgte og opphevet personverndirektivet,[9] som i Norge var gjennomført ved personopplysningsloven fra 2000.[10] Personvernforordningen skal sørge for større harmonisering mellom EU-landene[11] og et regelverk som skal kunne møte ny teknologi.[12] Forordningen har en innsynsbestemmelse som gir den registrerte krav på «relevant informasjon om den underliggende logikken»[13] dersom det er tatt en «en avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende».[14] Personverndirektivet hadde liknende bestemmelser, men disse var lite brukt.[15] Med flere automatiserte avgjørelser, kan det være

5 Eksempelet er hentet fra Lecher (2018). Eksempelet er ikke fra EU, men er egnet til å illustrere rettsikkerhetsutfordringer ved automatisert behandling.

6 Personvernforordningen (engelsk).

7 Forskrift om ikraftsetting, jf. meddelelse om ikrafttredelse.

8 Når denne oppgaven omtaler «Personvernforordningen» uten nærmere spesifisering, refererer det til den norske oversettelsen som er en del av personopplysningsloven. Se nærmere om språkversjon i punkt 2.2

9 Personverndirektivet.

10 Personopplysningslov av 2000 (opphevet).

11 Personvernforordningen fortale avsnitt 3.

12 Personvernforordningen fortale avsnitt 6 og 7.

13 Personvernforordningen Artikkel 15 nr. 1 bokstav h.

14 Personvernforordningen Artikkel 22 nr. 1.

15 Personverndirektivet artikkel 15 nr. 1 og artikkel 12 bokstav a. Se Bygrave (2019) s. 1.

grunn til å anta et større behov for innsynsbestemmelsen i personvernforordningen.

Temaet for denne oppgaven er retten til «relevant informasjon om den underliggende logikken» etter personvernforordningen artikkel 15 nr. 1 bokstav h for automatiserte avgjørelser som nevnt i artikkel 22 nr. 1 og 4. Hovedspørsmålene er hva en slik automatisert avgjørelse er, og hva som er «relevant informasjon om den underliggende logikken» for denne avgjørelsen.

Oppgaven tre hoveddeler. Den første er en oversikt over artikkel 15 nr. 1 bokstav h, herunder en drøftelse av hensyn og forholdet til andre relevante bestemmelser. Den andre er drøftelsen av hva som er en automatisert avgjørelse etter artikkel 22 nr.1 og 4. Den tredje er drøftelsen av hva som ligger i vilkåret «relevant informasjon om den underliggende logikken». Etter å ha besvart disse spørsmålene kan jeg til slutt vurdere om personvernforordningen artikkel 15 nr. 1 bokstav h, jf. artikkel 22 nr. 1 og 4 gir den registrerte et effektivt verktøy for å forsikre seg om at den automatiserte behandlingen har skjedd på en lovlig og rettferdig måte.[16]

16 Personvernforordningen Artikkel 5 nr. 1 bokstav a.

2 Metoden og rettskildene

2.1 Utgangspunktet

Det er få tilgjengelige rettskilder som kan belyse de rettslige spørsmålene som reises i oppgaven. Særlig fremtredende er det at det ikke eksisterer relevant rettspraksis.[17] Verken EU-domstolen eller Høyesterett har tatt stilling til denne typen spørsmål.

Oppgaven skal analysere vilkår fra en EU-forordning. Utgangspunktet er at personvernforordningen ikke har direkte virkning i norsk rett. Forordningen er imidlertid inkorporert i norsk lov gjennom personopplysningslovens § 1, jf. EØS-avtalen art. 7 bokstav a.[18] Den er dermed et av vedleggene til EØS-avtalen. Forordningen er ved motstrid med norsk rett gitt forrang.[19]

Hovedmålet med EØS-avtalen er å sikre ensartethet (homogenitetsmålsettingen).[20] En forordning er en type lovgivning som særlig sikter på en slik ensartethet. EØS-avtalen sier at en «forordning skal som sådan gjøres til del av avtalepartenes interne rettsorden».[21] (min understrekning). For å nå målet om ensartethet og for å oppfylle vilkåret «som sådan»[22] er det nødvendig å tolke personvernforordningen i lys av de samme rettskildene som vil bli lagt til grunn ved tolkningen av forordningen i resten av EU.

Homogenitetsprinsippet har sine grenser ettersom EØS-avtalen ikke fullt ut bygger på de samme hensyn som ligger til grunn for EU-samarbeidet.[23] Dermed blir den EØS-rettslige metoden en todelt prosess.[24] Først skal den EU-rettslige regelen klarlegges. Deretter skal tolkningen overføres til en EØS-rettslig sam-

17 Bygrave (2019) s. 3 og note 1. På samme sted viser Bygrave til en tysk avgjørelse vedrørende SCHUFA, et tysk kredittselskap og bruken av et system for automatisert kredittsjekk. Dommen synes ikke å være relevant for denne oppgaven.

18 Når det i denne oppgaven henvises til EØS-avtalen, menes EØS-avtalen slik den er vedlagt i EØS-loven.

19 Jf. EØS-loven § 2 og Personopplysningsloven § 2 (4).

20 EØS-avtalens artikkel 1 og Sejersted (2011) s. 87 og s. 223.

21 EØS-avtalens artikkel 7 bokstav a.

22 EØS-avtalen artikkel 7 bokstav a.

23 Arnesen i Sejersted (2011) s. 224.

24 Fredriksen i Arnesen (2018) s. 126 og Fredriksen (2012) s. 190.

menheng i lys av homogenitetsprinsippet.[25] Denne prosessen vil normalt lede til at den ferdig tolkede EU-regelen overføres som sådan til EØS-retten.[26] Dette vil i stor grad være tilfellet for spørsmålene i denne oppgaven.

2.2 Språket i forordningen

EØS-avtalens artikkel 129 nr. 1 sier at EØS-avtalens vedlegg, deriblant personvernforordningen, har samme gyldighet på alle EU-språkene og det skal «utarbeides tekster på islandsk og norsk som skal gis samme gyldighet og kunngjøres i EØS-tillegget til Den europeiske unions tidende». Forordningen er oversatt til norsk og den offisielle norske oversettelsen er en del av personopplysningsloven.[27] I det følgende vil jeg ta utgangspunkt i den norske oversettelsen. Dersom det skulle være ord og uttrykk i den norske oversettelsen som gir grunnlag for andre tolkninger enn noen av EU-språkversjonene, oppstår det et spørsmål om hvordan dette skal håndteres.[28] Som Arnesen påpeker, er det to mulige tilnærminger.[29] Den første er å forsøke å tilpasse tolkningen av den norske oversettelsen til en eller flere av EU-språkversjonene. Den andre er å forsøke å tolke den norske oversettelsen slik man antar at EU-domstolen eller EFTA-domstolen ville tolket den. Siden det i utgangspunktet er få tilgjengelige rettskilder for spørsmålene i denne oppgaven, finner jeg det mest hensiktsmessig med det første alternativet, ettersom det er høyst usikkert hvilken tolkning domstolene ville velge.[30]

I denne oppgaven oppstår det et slikt språkspørsmål i forbindelse med analysen av ordet «relevant», se punkt 5.3.1.

2.3 Det europeiske personvernrådets retningslinjer

Det europeiske personvernrådet, «The European Data Protection Board» (heretter: Personvernrådet) er et nytt organ som har blitt opprettet i medhold av personvernforordningen.[31] Personvernrådet er et uavhengig «EU-organ med

25 Fredriksen i Arnesen (2018) s. 126 og Fredriksen (2012) s. 219.
26 Fredriksen i Arnesen (2018) s. 126.
27 EØS-tillegg (2018).
28 Arnesen (2015) punkt 3.2.2.
29 Arnesen (2015) punkt 3.2.2.
30 Dette synes også å være tilnærmingen Arnesen tar til orde for, jf. Arnesen (2015) punkt 3.2.2 og punkt 5.
31 Personvernforordningen artikkel 68 flg.

status som juridisk person».[32] Personvernrådet var under personverndirektivet[33] kjent som Artikkel 29-gruppen «Article 29 Working party» (heretter: Artikkel 29-gruppen). Med forordningen har Artikkel 29-gruppen opphørt, og er blitt til Personvernrådet.

Rådet består blant annet av representanter for medlemsstatenes tilsynsmyndigheter,[34] og har som hovedoppgave å «sikre ensartet anvendelse» av personvernforordningen.[35] I arbeidet med dette, skal rådet utstede retningslinjer for anvendelsen av forordningen.[36] Artikkel 29-gruppen utstedte også slike retningslinjer. I denne oppgaven er det særlig to sett med retningslinjer som er relevante. Den første er retningslinjer for tolkningen av bestemmelser i forordningen som omhandler automatiserte avgjørelser og profilering.[37] Den andre er retningslinjer for bestemmelsene om innsyn.[38] Retningslinjene er opprinnelig forfattet av Artikkel 29-gruppen, men Personvernrådet har ved sitt første plenumsmøte gitt sin tilslutning til dem.[39]

Retningslinjene er ikke rettslig bindende dokumenter. Retningslinjene gir uttrykk for synspunktene til Personvernrådet. Samtidig er Personvernrådet, gjennom forordningen selv, gitt i oppgave å utstede slike retningslinjer.[40] Det er et tydelig ønske fra lovgiver at de utstedes, hvilket taler for at retningslinjene skal ha noe større tyngde enn andre uttalelser fra et EU-organ.

Vekten av retningslinjene må også sees i lys av at personvernforordningen gir tilsynsmyndighetene kraftige verktøy mot overtredelser.[41] Tilsynsmyndighetene har etter artikkel 58 myndigheten til å gjennomføre en rekke tiltak, både for å undersøke overtredelser og for å korrigere overtredelser. Tiltakene kan være ressurskrevende for en behandlingsansvarlig. Det er nok likevel overtredelsesgebyrene[42] som har skapt mest frykt blant behandlingsansvarlige. I denne forbindelse skriver Casey m. fl.:

---

32 Personvernforordningen artikkel 68 nr. 1, jf. artikkel 69.
33 Personverndirektivet.
34 Personvernforordningen artikkel 68.
35 Personvernforordningen artikkel 70 nr. 1 første punktum.
36 Personvernforordningen artikkel 70 nr. 1 bokstav e flg. Det er faktisk lovfestet at Personvernrådet skal utstede retningslinjer «for å presisere kriteriene og vilkårene for avgjørelser basert på profilering i henhold til artikkel 22 nr. 2», jf. bokstav f.
37 A29WP (2018a).
38 A29WP (2018b).
39 EDPB (2018).
40 Personvernforordningen artikkel 70 avsnitt 1 bokstav e flg.
41 Casey (2018) s. 28.
42 Personvernforordningen artikkel 58 nr. 2 bokstav i, jf. artikkel 83

«With great power, of course, comes great interpretive responsibility. After all, what better source of guidance could there be for companies seeking to ensure compliance with the GDPR's "right to explanation" than the data authorities likeliest to bring enforcement action against them?».[43]

Sitatet stammer fra diskusjonen om «right to explanation» (se punkt 5.3.5), men poenget gjelder også utover denne diskusjonen. Det er grunn til å tro at behandlingsansvarlige vil sikre seg mot tiltak fra tilsynsmyndighetene, og i dette ta utgangspunkt i det som trolig blir tilsynsmyndighetens tolkning av forordningen. Tilsynsmyndighetene er forpliktet til å «bidra til en ensartet anvendelse»[44] av denne forordningen. Siden Personvernrådet også består av representanter for de ulike tilsynsmyndighetene, er det god grunn til å tro at Personvernrådets og Artikkel 29-gruppens retningslinjer vil ligge til grunn ved tilsynsmyndighetenes tolkning av forordningen. Tilsynsmyndighetenes avgjørelse er til syvende og sist gjenstand for prøving av domstolene,[45] både nasjonalt og på EU/EFTA-nivå. Samtidig er det nok ikke til å komme unna at retningslinjene i praksis vil få stor betydning for tolkningen av forordningen.[46]

I en EØS-rettslig sammenheng har også Datatilsynet gitt uttrykk for at de legger vekt på uttalelsene fra Artikkel 29-gruppen.[47] Homogenitetsprinsippet understøtter dette. Jeg legger derfor til grunn at retningslinjene har den samme vekten når den EU-rettslige regelen skal vurderes som en EØS-regel.

2.4 Andre relevante rettskilder

Personvernforordningens fortale[48] har flere avsnitt som er relevante for spørsmålene i denne oppgaven. Fortalen er også oversatt til norsk og er inntatt i personopplysningsloven. I EU-rettslig sammenheng har fortalen generelt nokså stor vekt.[49] Fortalen har imidlertid bare vekt som et verktøy for å tolke uklare bestemmelser: «Whilst a recital in the preamble to a regulation may cast light on the interpretation to be given to a legal rule, it cannot in itself constitute such a rule».[50] EØS-avtalens Protokoll 1 om gjennomgående tilpasning nr. 1 omtaler

43 Casey (2018) s. 28.

44 Personvernforordningen artikkel 51 nr. 2 og artikkel 63 flg.

45 Casey (2018) s. 28.

46 Casey (2018) s. 28.

47 Datatilsynet 2018 s. 3.

48 Personvernforordningen fortale, jf. TEUV artikkel 296 nr. 2.

49 Sejersted (2011) s. 53 og 57.

50 Case 215/88 Casa Fleischhandels avsnitt 31. Dette sitatet er trukket frem av Wachter (2017) s. 80. Se også Case 162/97 Nilsson and Others avsnitt 54 og Case 308/97 Manfredi v Regione Puglia avsnitt 29–30. De to sistnevnte er trukket frem av Mendoza og Bygrave (2017) note 30.

bruken av fortaler i en EØS-rettslig sammenheng. Denne synes ikke å reise noen spørsmål for personvernforordningens fortale.[51] Homogenitetsprinsippet står sterkt ved tolkningen av EØS-regler.[52] Derfor må fortalen ha tilsvarende vekt når EU-regelen vurderes i en EØS-rettslig sammenheng.

Formålsbetraktninger og kontekstuelle betraktninger er generelt relevante rettskilder ved fortolkningen av EU-rettslige bestemmelser.[53] EU-domstolen uttaler at tolkningen av en bestemmelse skal skje med «regard to the context of the provision and to objective pursued by the legislation in question».[54] Vekten av formålsbetraktninger og kontekstuelle betraktninger er generelt nokså stor.[55] For personvernforordningen artikkel 15 nr. 1 bokstav h omtales formålene og hensynene nærmere under punkt 3.2 og forholdet mellom artikkel 15 nr. 1 bokstav h og andre bestemmelser i personvernforordningen i punkt 3.3.

Den formelle vekten av juridisk litteratur er liten.[56] Rettsreglene som diskuteres i denne oppgaven kan dermed ikke begrunnes i litteraturen. Litteraturen kan imidlertid være en kilde til systematisering av øvrige rettskilder og nyttige argumenter. Litteraturen vil bli brukt til dette.

Personvernforordningen må harmoniseres med Grunnlovens § 102 og Norges øvrige menneskerettslige forpliktelser, blant annet EMK artikkel 8 og Europarådets konvensjon nr. 108.[57] Sistnevnte er forslått modernisert,[58] og den er nå åpen for signaturer. Disse kildene har få bestemmelser som tilsvarer de tekniske bestemmelsene i personvernforordningen artikkel 15 nr. 1 bokstav h og artikkel 22. I den grad slike bestemmelser eksisterer,[59] gir de få tolkningsmomenter utover det som kan utledes av personvernforordningen selv og tilhørende rettskilder. Dermed skaper heller ikke disse kildene noen harmoniseringsutfordringer med hensyn til spørsmålene i oppgaven.

Personverndirektivet hadde bestemmelser som lignet de som skal behandles i denne oppgaven, se punkt 1. For enkelte spørsmål kan det være interessant å se hen til disse bestemmelsene. Personvernforordningen er imidlertid en revisjon

51 EØS-avtalens Protokoll 1 om gjennomgående tilpasning nr. 1. Protokollen er integrert del av EØS-avtalen, jf. EØS-avtalen artikkel 119.

52 EØS-avtalens artikkel 1.

53 Fredriksen (2012) s. 198–199.

54 Case 316/05 Nokia (2005) avsnitt 21. Dommen er også vist til av Fredriksen (2012) s. 198, men i den danske språkversjonen.

55 Fredriksen (2012) s. 198–199.

56 Sejersted (2011) s. 58–59.

57 Convention 108. Nærmere om denne i Schartum og Bygrave (2016) s. 90.

58 Convention 108+.

59 Convention 108+ artikkel 8 nr. 1 bokstav e, jf. artikkel 9 nr. 1 bokstav c.

av det tidligere regelverket. Man vil kunne risikere å undergrave det økte vernet personvernforordningen sikter mot, dersom forordningen tolkes i samsvar med det tidligere direktivet. Dette er spesielt viktig når det er snakk om automatiserte avgjørelser. Personverndirektivet er fra 1995, og grunnlaget for direktivet ble lagt enda tidligere. Det har skjedd store endringer i teknologien og automatiserte avgjørelser siden den gang.

3 En oversikt over personvernforordningens artikkel 15 nr.1 bokstav h

3.1 Generelt

Personvernsforordningens artikkel 15 har tittelen «Den registrertes rett til innsyn». Bestemmelsen gir rett til innsyn i informasjon som databehandleren har om den registrerte, samt en del tilhørende informasjon. Et innledende vilkår for at innsynsrettighetene i artikkel 15 kommer til anvendelse, er at det behandles personopplysninger om den registrerte. Artikkel 15 gir altså kun grunnlag for en innsynsrett for den registrerte, og er ikke en generell innsynsbestemmelse. Personvernforordningen og innsynsbestemmelsen gjelder både for private aktører og den offentlige forvaltning.[60]

Artikkel 15 nr. 1 bokstav h er en særbestemmelse som kun gjelder for helt automatiserte avgjørelser etter artikkel 22 nr. 1 og 4. Artikkel 15 nr. 1 bokstav h gir den registrerte rett til å få:

1. informasjon om «forekomsten» av avgjørelser som nevnt i artikkel 22.
2. «relevant informasjon om den underliggende logikken» for slike avgjørelser.
3. informasjon om «betydningen og de forventede konsekvensene».

Det er kun «relevant informasjon om den underliggende logikken» som er tema for denne oppgaven. Resten av bestemmelsen vil imidlertid bli trukket inn der slike kontekstuelle betraktninger er viktige for tolkningen.

3.2 Formål og hensyn

Når formålene som begrunner personvernforordningen artikkel 15 nr. 1 bokstav h skal identifiseres er det, som EU-domstolen viser,[61] nødvendig å finne de formål som begrunner den spesifikke regelen, og de overordnede formål som

60 Personvernforordningen artikkel 2 nr. 1.

61 Case 73/07 Satamedia avsnitt 51, 52 og 54. Dommen er lagt til grunn av Fredriksen (2012) s. 204 for å illustrere dette poenget.

ligger til grunn for forordningen.[62] Formålene kan finnes flere steder, i forordningen eller direktivet selv, og i fortalen.[63]

De overordnede formålene i personvernforordningen er nedfelt i artikkel 1. Av denne fremgår det at personvernforordningen skal sikre fri utveksling av personopplysninger, men samtidig sørge for at dette skjer på en måte som ivaretar «fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger».[64]

Innsyn i automatiserte avgjørelser, bør sees i sammenheng med artikkel 5 nr. 1 bokstav a. Denne gir et godt grunnlag for å forstå innsynsbestemmelsens funksjon i personvernforordningen. Dermed gir den også uttrykk for formålet med innsynsbestemmelsen. Artikkel 5 nr. 1 bokstav a sier at personopplysninger skal «behandles på en lovlig, rettferdig og åpen måte med hensyn til den registrerte («lovlighet, rettferdighet og åpenhet»)».

At behandlingen må være lovlig tilsier at den både må ha et rettslig grunnlag[65] og må være i overenstemmelse med andre relevante rettsregler. Behandlingen kan for eksempel ikke medføre ulovlig forskjellsbehandling.[66] Hva som er lovlig henger tett sammen med hva som er rettferdig, men vilkårene behøver ikke å peke på det samme. Kravet til rettferdighet kan etter sin ordlyd også rette seg mot former for behandling hvor det er elementer eller resultater som fremstår som klart urettferdig, men ikke er rettslig regulert. Dette kan være praktisk ved innsyn i automatiserte avgjørelser, da teknologien kan utvikle seg raskere enn den rettslige reguleringen.

Åpenhet henger tett sammen med rettferdighet[67] og lovlighet. Bare ved tilstrekkelig åpenhet kan den registrerte forvisse seg om at behandlingen skjer på en lovlig og rettferdig måte. Hvis den registrerte mener at behandlingen ikke er lovlig og rettferdig, gjør en slik åpenhet det mulig for den registrerte å kunne håndheve sine øvrige rettigheter etter personvernforordningen.[68] Åpenheten bygger på to elementer, se punkt 5.3.1. Den registrerte må få tilgang til den nødvendige informasjonen og denne informasjonen må presenteres på måte som den registrerte har forutsetninger for å forstå.

62 Se også Fredriksen (2012) s. 204 og 205.
63 Fredriksen (2012) s. 206.
64 Personvernforordningen artikkel 1 nr. 2.
65 Personvernforordningen artikkel 6.
66 A29WP (2018a) s. 10 og likestillings og diskrimineringslovens § 6 flg.
67 A29WP (2018b) s. 5 og personvernforordningen fortale punkt 39.
68 Eksempelvis artikkel 22 nr. 2 bokstav a og c, jf. artikkel 22 nr. 3.

I fortalens punkt 6 og 7 pekes det på at «det er viktig å skape den nødvendige tillit som vil gjøre at den digitale økonomien kan utvikle seg i det indre marked»[69] (min understrekning). Tillit er altså et sentralt hensyn. I fortalen er tillit nevnt i sammenheng med utviklingen av det indre marked, men det er ingen tvil om at tillit er et sentralt formål også for den offentlige forvaltning.[70] Artikkel 29-gruppen legger tillit til grunn som et sentralt hensyn i retningslinjene om gjennomsiktighet.[71]

For automatiserte avgjørelser er nettopp tillit og åpenhet sentrale hensyn. Hvordan en datamaskin virker er komplisert og utilgjengelig informasjon for de fleste.[72] Faren stor for at en kan oppleve å være i en «Kafka-prosess»,[73] dersom en datamaskin tar en betydningsfull avgjørelse som den berørte ikke kan forstå. For å motvirke dette, bør man etterstrebe åpenhet. Dette bidrar til å sikre tilliten til både offentlige og private aktører.

3.3 Sammenhengen mellom artikkel 15 nr. 1 bokstav h og andre bestemmelser i personvernforordningen

3.3.1 Forholdet til personvernforordningen artikkel 2 nr. 1

Personvernforordningen får «anvendelse på helt eller delvis automatisert behandling av personopplysninger», jf. artikkel 2 nr. 1. Det er to spørsmål det er grunn til å se nærmere på. Det første er hvor artikkel 15 nr. 1 bokstav h skal plasseres i forhold til «helt eller delvis». Det andre er hva som egentlig ligger i «automatisert behandling». Det er grunn til å anta at «automatisert behandling» er det samme i artikkel 2 nr. 1 og artikkel 15 nr. 1 bokstav h. Drøftelsen her vil derfor være bestemmende for forståelsen av artikkel 15 nr. 1 bokstav h.

Formuleringen «helt eller delvis» synes å dekke alle former for automatisert behandling. Til tross for dette bruker artikkel 22 nr. 1, som artikkel 15 nr.1 bokstav h viser til, en egen formulering: «avgjørelse som utelukkende er basert på automatisert behandling» (min understrekning). Det er vanskelig å se hva «utelukkende» i artikkel 22 nr. 1 tilfører i forhold til ordet «helt» i artikkel 2 nr. 1. Rent språklig er det naturlig å lese ordet «utelukkende» som et sterkere uttrykk for at det ikke er mennesker involvert i behandlingen enn ordet «helt». Samtidig gir det ikke uttrykk for noen realitetsforskjell. Forholdet mellom disse to ordene er ikke nevnt i verken forordningen selv, fortalen eller av Artikkel 29-gruppen.

69 Personvernforordningens fortale punkt 6 og 7.
70 Offentleglova § 1.
71 A29WP (2018b) s. 4.
72 Burell (2016) s. 4.
73 Borgesius (2018) s. 22 nevner at artikkel 22 av og til kalles Kafka-bestemmelsen.

Ettersom det er vanskelig å se noen realitetsforskjell, må det legges til grunn at disse ordene gir utrykk for det samme.

Vilkåret «automatisert behandling» indikerer etter sin ordlyd at det må være en behandling av data som skjer av seg selv. Utover dette sier ikke ordlyden noe om hvordan behandlingen skal skje eller hvilken teknologi som benyttes i en slik automatisering. Dette tilsier at alle teknologier som kan gi grunnlag for en automatisert behandling, skal være omfattet av bestemmelsen. Dette understøttes av fortalens avsnitt 15 som sier at «For å unngå at det oppstår en alvorlig risiko for at bestemmelsene omgås bør vernet av fysiske personer være teknologisk nøytralt og ikke avhenge av teknikkene som benyttes».

Med dagens teknologi vil digital prosessering være den mest aktuelle automatiserte behandlingen. Med digital prosessering menes bearbeiding av informasjon representert ved tall. Dette omfatter alle informasjonsteknologisystemer, fra smartklokker og smarttelefoner til stasjonære datamaskiner og mer omfattende datasystemer. I det følgende vil jeg bruke betegnelsen «datamaskin» om alle slike informasjonsteknologisystemer, selv om noen av disse er så omfattende at begrepet «datamaskin» kan høres fremmed ut. Dette gjøres som et pedagogisk grep for å unngå forvirring. Videre i dette punktet skal jeg utdype hvordan en datamaskin brukes til «automatisert behandling». Dette har betydning for lovtolkningen i resten av oppgaven. For å holde fremstillingen enklest mulig, vil noen tekniske detaljer og nyanser være plassert i fotnotene.

For at en datamaskin skal kunne brukes til «automatisert behandling», må den programmeres. Dette betyr at den må gis instruksjoner om hvordan den skal gjennomføre en slik behandling. Det finnes mange tilnærminger til programmering av en datamaskin.[74] Tradisjonelt har en datamaskin blitt programmert av en fysisk person som bruker logiske operasjoner til å finne resultatene. Disse logiske operasjonene er ikke så ulike det en finner i et lovverk. Her vil en ofte måtte vurdere om rettsfakta er oppfylt, for å se hvilke rettsvirkninger dette medfører.[75] Programmereren skriver disse logiske operasjonene i et eller flere programmeringsspråk. Slike programmeringsspråk stiller strenge krav til syntaks og logikk, sammenliknet med vanlige språk. Teksten som programmereren skriver kalles kildekode. På grunn av disse strenge kravene kan denne kildekoden konverteres til instruksjoner som en datamaskin kan forstå, og dermed bli et datamaskinprogram som datamaskinen kan «kjøre».[76] Når programmereren,

74 Det skillet jeg legger til grunn her, baserer seg på Kashyap (2017) s. 6 og Molnar (2019) punkt 1.3.

75 Schartum (2018a) kapittel 8, og spesielt kapittel 8.3.

76 Ved hjelp av en kompilator konverteres denne kildekoden til maskinkode PCmag (2019) og Kjos (2019) s. 342.

eller et stort team med programmerere, har skrevet ferdig et datamaskinprogram, kan dette brukes til «automatisert behandling» etter artikkel 2 nr. 1, artikkel 22 nr. 1 og dermed også artikkel 15 nr. 1 bokstav h.

I forbindelse med datamaskinprogrammer snakkes det ofte om algoritmer. Artikkel 29-gruppen bruker også dette begrepet i sine retningslinjer.[77] Med algoritme menes en «fullstendig og nøyaktig beskrivelse av fremgangsmåten for løsning av en beregningsoppgave eller en annen oppgave».[78] Det er altså tale om oppskriften for datamaskinprogrammet. Denne kommer til uttrykk i kildekoden.[79]

En annen tilnærming til programmering av datamaskinprogrammer som skal brukes til «automatisert behandling» er maskinlæring. De siste årene har det i informatikkmiljøer[80] og i forretningslivet vært mye snakk om «Artificial intelligence», «AI» og den norske oversettelsen «kunstig intelligens».[81] Når det snakkes om AI og kunstig intelligens i en informasjonsteknologisk sammenheng, er det gjerne maskinlæring det siktes til.[82] Maskinlæring er, som begrepet antyder, idéen om at en maskin kan lære. Det den lærer av er informasjon. Svensson og Söderberg definerer maskinlæring som:

> «Machine learning (ML) is concerned with the design and development of algorithms and techniques that allow computers to "learn." The major focus of ML research is to extract information from data automatically, by computational and statistical methods.»[83]

Maskinlæring som teknologi er ikke noe nytt.[84] Grunnen til den store oppmerksomheten de siste årene, er tilgangen på enorme mengder informasjon og tilgangen på tilstrekkelig prosesseringskraft.[85] Som det fremgår av sitatet, er ikke maskinlæring en spesifikk ting. Maskinlæring er et samlebegrep på de ulike algoritmene og teknikkene som benyttes. Fra et teknisk perspektiv blir maskinlæring omtalt som et paradigmeskifte fra tradisjonell programmering.[86] Som nevnt, forutsetter den tradisjonelle programmeringen at noen gir datamaskinen instruksjoner om hvordan datamaskinprogrammet skal fungere. For maskin-

77 Eksempelvis A29WP (2018a) s. 25.
78 SNL (2018a).
79 SNL (2018a).
80 Eksempelvis West (2018) som holder foredrag om maskinlæring på JavaZone 2018.
81 Kashyap (2017) s. 11 og s. 3.
82 Kashyap (2017) s. 5, Intel (2016).
83 Svensson (2008) s. 29.
84 Datatilsynet (2018) s. 4.
85 Kashyap (2017) s. 12.
86 Molnar (2019) punkt 1.3.

læringen blir dette snudd på hodet. Her gir man datamaskinen informasjon, og lar det være opp til datamaskinen selv å finne datamaskinprogrammet på bakgrunn av denne informasjonen. Denne prosessen kalles ofte å «trene» datamaskinprogrammet.[87]

Datamaskinprogrammet som datamaskinen selv har funnet, kalles en modell.[88] Dette er altså en modell for løsningen på et problem. Når datamaskinen har funnet en modell, kan dette være grunnlag for «automatisert behandling», jf. artikkel 2 nr. 1, artikkel 22 nr. 1 og dermed også artikkel 15 nr. 1 bokstav h. Hvordan og hvor godt modellen virker, avhenger blant annet av hvilken maskinlæringsalgoritme som er brukt og hvilken informasjon man har gitt til datamaskinen.[89] Dette bestemmes igjen av hva man ønsker å oppnå med den «automatiserte behandlingen». For automatiserte avgjørelser etter artikkel 22 nr. 1 er det grunn til å anta at klassifisering vil være aktuelt. Med klassifisering menes å plassere noe i en kategori. Dette kan være å plassere den registrerte i en kategori, slik som krav/ikke-krav, egnet/ikke-egnet osv. Slik klassifisering kan også være å vurdere om et vilkår er oppfylt eller ikke. Mange maskinlæringsalgoritmer er godt egnet til klassifisering.[90] Det kan være nyttig å illustrere dette med et eksempel:

En datamaskin blir gitt 100 000 tilfeller av personer som har misligholdt lånet sitt og 100 000 tilfeller av personer som ikke har misligholdt lånet sitt. Hvert tilfelle består av mange parametere (opplysninger) om personen. I tillegg gis datamaskinen svaret på om personen har misligholdt lånet eller ikke. For hvert tilfelle datamaskinen gjennomgår, justerer den vektingen av parameterne for finne sammenhenger mellom parameterne og hvorvidt personen har misligholdt lånet. Når treningen er ferdig, kan modellen brukes til å løse nye tilfeller. Den vil for eksempel kunne si at det er «62.8 % sannsynlig» at en person tilhører kategorien «personer som har misligholdt lånet» eller «93,7 % sannsynlig» at personen tilhører «personer som ikke har misligholdt lånet». Dette resultatet kan igjen benyttes til å avgjøre om personen skal innvilges lån. På mange måter kan dette sammenliknes med en saksbehandler, som med erfaring lærer hvilke egenskaper ved en låntaker som kan si noe om evnen til å tilbakebetale lånet.

87 Eksempelvis Datatilsynet (2018) s. 10

88 Datatilsynet (2018) s. 9.

89 Det er vanlig å dele de ulike maskinlæringsalgoritmene inn i tre kategorier: «supervised learning», «unsupervised learning» og «reinforcement learning». Se blant annet Datatilsynet (2018) s. 7–9, West (2018) på 27:15. Disse tre kategoriene omfatter mange forskjellige algoritmer. I denne oppgaven tar jeg utgangspunkt i klassifiseringsalgoritmer under kategorien «supervised learning».

90 Flere eksempler er nevnt i Kashyap (2017) s. 96–98.

Vilkåret «automatisert behandling» i denne oppgaven, tar altså utgangspunkt i en prosessering av informasjon av en datamaskin som er programmert enten på tradisjonelt vis eller ved hjelp av maskinlæring. Begrunnelsen for dette skillet mellom tradisjonell programmering og maskinlæring, er at «automatisert behandling» basert på visse typer maskinlæring skaper særlige utfordringer når det gjelder innsyn. Visse maskinlæringsalgoritmer gir modeller som er ugjennomsiktige og som ikke lar seg forklare. Dette omtales nærmere i punkt 5.3.6.

3.3.2 Forholdet til personvernforordningen artikkel 13 og artikkel 14

Artikkel 15 har en nær sammenheng med artikkel 13 og 14. Disse tre bestemmelsene utgjør til sammen avsnitt to, «Informasjon og innsyn i personopplysninger», under kapittelet om den registrertes rettigheter i forordningen. Artikkel 15 nr. 1 bokstav h har sin parallell i artikkel 13 nr. 2 bokstav f og 14 nr. 2 bokstav g, som er helt likelydende.

Det faktum at bestemmelsene har helt lik ordlyd, tilsier at de må forstås på samme måte. De tre bestemmelsene retter seg imidlertid mot tre ulike situasjoner. Artikkel 13 er aktuell når personopplysningene er hentet fra den registrerte selv. Artikkel 14 er aktuell når personopplysningene ikke er hentet fra den registrerte selv. Begge disse bestemmelsene retter seg mot den innledende fasen i behandlingssyklusen.[91] Artikkel 15 er derimot en innsynsbestemmelse og har ingen tidsavgrensning. Behovet for innsyn kan dermed knytte seg til konkrete omstendigheter.

Artikkel 29-gruppen gir uttrykk for at informasjonen som skal gis etter artikkel 15 nr. 1 bokstav h er den samme som skulle vært gitt etter artikkel 13 nr. 2 bokstav f.[92] Artikkel 29-gruppens standpunkt er ikke begrunnet. En vesentlig svakhet ved dette standpunktet er at dette gjør bestemmelsen i artikkel 15 nr. 1 bokstav h overflødig. Det gir lite mening å inkludere en likelydende bestemmelse i artikkel 15 nr. 1 bokstav h, dersom denne er uten betydning. Artikkel 29-gruppen bruker selv argumentet om at bestemmelser skal tolkes slik at de ikke blir overflødige når artikkel 22 nr. 1 diskuteres.[93]

Artikkel 15 nr. 1 bokstav h altså bør anses å ha en selvstendig betydning. I punkt 5.3.1 konkluderes det med at utgangspunktet for vurderingen av «relevant informasjon» er en konkret vurdering av hva som er relevant for den registrerte. Dermed kan det tenkes at informasjonen som kan kreves etter artikkel 15 nr. 1 bokstav h er noe annet eller mer enn det en behandlingsansvarlig er forpliktet å gi

91 A29WP (2018b) s. 14.
92 A29WP (2018a) s. 27.
93 A29WP (2018a) s. 35.

etter artikkel 13 eller 14, nettopp fordi en innsynsbegjæring som regel vil være konkret begrunnet. Fordi bestemmelsene er likelydende, er det likevel naturlig å se dem i sammenheng når vilkårene skal tolkes.

3.3.3 Forholdet til personvernforordningen artikkel 22

Artikkel 15 nr. 1 bokstav h viser eksplisitt til artikkel 22 nr. 1 og nr. 4 og må naturligvis tolkes i samsvar med disse bestemmelsene. En rett til innsyn i automatiserte avgjørelser etter artikkel 15 nr. 1 bokstav h må imidlertid også tolkes i sammenheng med artikkel 22 nr. 2 og nr. 3. Artikkel 22 nr. 4, som artikkel 15 nr. 1 bokstav h også viser til, leder til avgjørelser i artikkel 22 nr. 2.

Artikkel 22 nr. 2 oppstiller tre unntak fra hovedregelen i artikkel 22 nr. 1. I forlengelsen av unntakene oppstilles det krav til rettsikkerhetsgarantier som må være på plass dersom unntakene kommer til anvendelse. I første omgang oppstilles det at den behandlingsansvarlige eller medlemsstaten skal sørge for «egnede tiltak for å verne den registrertes rettigheter og friheter og berettigede interesser».[94] I de tilfellene hvor denne plikten påhviler den behandlingsansvarlige, er plikten videre utdypet. Den skal også omfatte «retten til menneskelig inngripen fra den behandlingsansvarlige, til å uttrykke sine synspunkter og til å bestride avgjørelsen».[95] Til tross for at plikten bare er utdypet for artikkel 22 nr. 2 bokstav a og c,[96] synes fortalen å gi uttrykk for at rettsikkerhetsgarantiene skal gjelde for alle automatiserte avgjørelser som nevnt i artikkel 22 nr. 1.[97] Rettsikkerhetsgarantiene, særlig retten til å bestride avgjørelsen, er nært knyttet til de formålene som ligger til grunn for innsynsbestemmelsen. Som nevnt i punkt 3.2, er en innsynsbestemmelse en forutsetning for å kunne hevde enkelte andre rettigheter etter personvernforordningen. Denne sammenhengen fremkommer også tydelig av fortalens avsnitt 71 som omtaler informasjon og forklaring av avgjørelsen som en viktig del av rettsikkerhetsgarantiene. Se mer om dette i punkt 5.3.5.

Et vanskelig tolkningsspørsmål som oppstår med artikkel 22 er hvorvidt hovedregelen i artikkel 22 nr. 1 skal forstås som et forbud mot automatisert behandling eller en rett til å protestere mot slik behandling. For det tilfellet at artikkel 22 nr. 1 anses som et forbud mot automatisert behandling, vil rettsikkerhetsgarantiene alltid måtte være iverksatt før en krever innsyn. Dette er fordi et av disse unntakene må komme til anvendelse for at det skal kunne foreligge en slik automatisert avgjørelse som berettiger innsyn etter artikkel 15 nr. 1 bokstav h.

94 Personvernforordningen artikkel 22 nr. 2 og artikkel 22 nr. 3.
95 Personvernforordningen artikkel 22 nr. 2 bokstav a og c, jf. artikkel 22 nr. 3.
96 Personvernforordningen artikkel 22 nr. 3.
97 Personvernforordningen fortale avsnitt 71.

For det tilfellet at artikkel 22 nr. 1 anses som en rett til å protestere på en slik behandling er ikke innsyn etter artikkel 15 nr. 1 bokstav h avhengig av at unntakene kommer til anvendelse. Dermed kan det foreligge en automatisert avgjørelse, uten at det samtidig foreligger plikt til å gjennomføre rettsikkerhetsgarantiene.

Hvorvidt artikkel 22 nr. 1 er et forbud eller en rett, har blitt grundig diskutert i juridisk litteratur.[98]Artikkel 29-gruppen har også tatt eksplisitt stilling til dette.[99] Det er mange gode argumenter for begge de to tolkningsmåtene.[100] Ordlyden taler for at artikkel 22 nr. 1 skal anses som en rett til å protestere. Denne sier at den registrerte har en rett. Videre kan artikkel 13 nr. 2 bokstav f og 14 nr. 2 bokstav g også tale for å forstå bestemmelsen som en rett. Informasjonen som skal gis etter disse bestemmelsene skal, som nevnt i punkt 3.3.2, gis i den innledende fasen av behandlingssyklusen. Det kan virke fremmed at det skal gis informasjon om forekomsten av automatiserte avgjørelser og informasjon om den underliggende logikken, før det er adgang til å ta en slik avgjørelse, hvilket vil være tilfellet dersom artikkel 22 nr. 1 anses som et forbud. Som det straks skal forklares, behøver likevel ikke dette å være problematisk. Til fordel for at 22 nr. 1 anses som en rett taler også at helautomatisert behandling allerede benyttes i stor grad. For at en slik behandling skulle fortsette å være lovlig, ville måtte få lovfestet et unntak.[101]

Til fordel for at artikkel 22 nr. 1 skal anses som et forbud taler først og fremst Artikkel 29-gruppens uttalelser som sier at bestemmelsen skal forstås som et forbud.[102] Gruppen begrunner dette med kontekstuelle betraktninger, samt at et forbud gir den beste logiske sammenhengen med samtykke-unntaket i artikkel 22 nr. 2 bokstav c.[103] Selv om det er litt kunstig å formulere et forbud som «en rett til ikke å være gjenstand for»,[104] utelukker ikke ordlyden at bestemmelsen leses som et forbud. Når det gjelder sammenhengen til artikkel 13 nr. 2 bokstav f og 14 nr. 2 bokstav g, er ikke en tolkning av 22 nr. 1 som et forbud til hinder for at disse bestemmelsene gir mening. Som uttalt i punkt 3.3.2, må disse bestemmelsene leses ut fra den situasjonen de retter seg mot. I den innledende delen av behandlingssyklusen, er det mulig å gi informasjon om forekomsten av automatiserte avgjørelser. Det er også mulig å beskrive den underliggende logikken i

98 Mendoza og Bygrave (2017) s. 9–10, Larsen (2018) s. 18, Schartum (2018b) s. 4, Bygrave (2019) s. 6.
99 A29WP (2018a) s. 19.
100 Bygrave (2019) s. 6.
101 Schartum (2018b) s. 5.
102 A29WP (2018a) s. 19.
103 A29WP (2018a) s. 35.
104 Artikkel 22 nr. 1.

generelle trekk. Dette kan faktisk fremstå som den mest hensiktsmessige tilnærmingen. Det er først etter å ha fått informasjon i medhold av artikkel 13 nr. 2 bokstav f og 14 nr. 2 bokstav g, den registrerte har tilstrekkelig informasjon til å samtykke etter artikkel 22 nr. 2 bokstav c. Enkelte argumenterer også for at en tolkning av bestemmelsen som et forbud, best styrker bestemmelsens formål.[105] Rettsikkerhetsgarantiene henger dessuten tett sammen med formålene bak innsynsbestemmelsen i artikkel 15 nr. 1 bokstav h. Dermed er det kunstig om innsynsbestemmelsen kan gjelde uten at rettsikkerhetsgarantiene er satt i verk, noe som kan være konsekvensen om artikkel 22. nr. 1 anses som en rett. Til slutt kan det nevnes at flertallet i forvaltningslovutvalget anser artikkel 22 nr. 1 som et forbud, selv om dette ikke nødvendigvis er en vektig kilde ved vurderingen av en EU/EØS-regel.[106]

Samlet sett finner jeg at artikkel 22. nr. 1 må leses som et forbud. Rettsikkerhetsgarantiene må dermed være satt i verk for at det kan foreligge en slik avgjørelse som gir grunnlag for innsyn etter artikkel 15 nr. 1 bokstav h. Dette synliggjør sammenhengen mellom rettsikkerhetsgarantiene, særlig retten til å «bestride avgjørelsen», og artikkel 15 nr. 1 bokstav h.

105 Mendoza og Bygrave (2017) s. 10.
106 NOU 2019:5 s. 261 og 262.

4 Hva er en helautomatisert avgjørelse etter artikkel 22 nr. 1 og nr. 4?

4.1 Oversikt over bestemmelsen

Artikkel 15 nr.1 bokstav h gjelder en automatisert avgjørelse som nevnt i Artikkel 22 nr. 1 og nr. 4. Artikkel 22 nr. 1 gir uttrykk for hva en slik avgjørelse er. Artikkel 15 nr. 1 bokstav h viser imidlertid også til artikkel 22 nr. 4. Dette er en bestemmelse som stiller særlige krav til det rettslige grunnlaget for automatiserte avgjørelser som bygger på «særlige kategorier av personopplysninger nevnt i artikkel 9 nr. 1».[107] Bestemmelsen påvirker ikke formuleringen av den automatiserte avgjørelsen i artikkel 22 nr. 1, og det er derfor ikke nødvendig å drøfte denne nærmere for å klarlegge hva som ligger i en automatisert avgjørelse.

Etter artikkel 22 nr. 1 taler om en «avgjørelse som utelukkende er basert på automatisert behandling, herunder profilering, som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende». Artikkel 22 nr. 1 kan brytes ned til fem vilkår. De tre første må være oppfylt. De to siste er alternative, så det er tilstrekkelig at et av dem er oppfylt. Det må foreligge en «avgjørelse». Denne avgjørelsen må være «utelukkende» basert på «automatisert behandling». Til slutt må det enten være en avgjørelse som har «rettsvirkning» for den registrerte eller «på tilsvarende måte i betydelig grad påvirker vedkommende».

I det følgende tar jeg utgangspunkt i disse fem vilkårene for å analysere artikkel 22 nr. 1, og dermed «automatisert avgjørelse» i artikkel 15 nr. 1 bokstav h. Det er imidlertid flere sammenhenger mellom vilkårene som er viktige å få frem. Enkelte sammenhenger vil bli drøftet i forbindelse med analysen av de fem vilkårene. Andre sammenhenger vil bli drøftet i punkt 4.6 og punkt 4.7.

Hva som ligger i vilkåret «automatisert behandling» er drøftet i punkt 3.3.1, og behandles ikke her. Artikkel 22 nr. 1 nevner også «herunder profilering». Det er litt uklart hvordan det er ment at «profilering» forholder seg til «automatisert behandling». Dette behandles i punkt 4.3.

107 Personvernforordningen artikkel 22 nr. 4.

4.2 Vilkåret «avgjørelse»

Det første vilkåret som må analyseres er «avgjørelse». Dette er et nokså generelt begrep. En naturlig språklig forståelse av «avgjørelse» tilsier at det skal gjøres et valg som medfører et eller flere utfall. Utover hva som kan hentes ut fra ordlyden, er det få rettskilder som kan si noe om dette vilkåret. Personvernforordningen har ingen definisjon av «avgjørelse». Det foreligger heller ingen dommer som presiserer begrepet, og det er ikke berørt i fortalen. Artikkel 29-gruppen har knyttet noen kommentarer til hva som er en automatisert avgjørelse, men har ikke presisert hva som ligger i selve begrepet «avgjørelse».

Begrepet er innarbeidet i dagligtalen. I mange sammenhenger vil det ikke være behov for å fastlegge nærmere hva «avgjørelse» omfatter. Det kan spørres om det i selve vilkåret «avgjørelse» ligger en terskel, slik at det bare er avgjørelser av en viss betydning som omfattes. Ettersom artikkel 22 nr. 1 gjelder en avgjørelse «som har rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende», (min understrekning) er det nok liten grunn til å innfortolke en slik terskel i selve vilkåret «avgjørelse».

Vilkåret «avgjørelse» favner altså vidt, og det skal trolig lite til før noe er omfattet. Følgelig må det anses som nokså klart at enkeltvedtak[108] er omfattet. For vedtak og beslutninger som ikke på samme måte er definert, vil hva som er en «avgjørelse» bero på en konkret vurdering av selve vedtaket eller beslutningen. Forholdet til prosessledende beslutninger behandles i punkt 4.5.

Et relevant spørsmål er om en «avgjørelse» skal forstås som et sluttresultat eller en avgjørelsesprosess.[109] Dersom «avgjørelse» forstås som et sluttresultat, referer det kun til selve valget som tas. Dersom «avgjørelse» forstås som en avgjørelsesprosess, omfatter det også noen av de prosessene som ledet til valget. Som nevnt, tilsier en naturlig språklig forståelse av ordlyden at det skal gjøres et valg som medfører et eller flere utfall. Rent språklig kan dette trekke i retning av at «avgjørelse» refererer til et sluttresultat. Dette harmonerer imidlertid dårlig med realiteten. Hva som blir resultatet av en avgjørelse er betinget av informasjonen som er tilgjengelig og hvordan denne er bearbeidet. Et datamaskinprogram som bare gjør et valg på bakgrunn av informasjon det blir gitt, kan være svært enkelt: «HVIS det er mer enn 75 % sannsynlig at personen tilhører kategorien «personer som har misligholdt lånet», SÅ skal lån avslås». (Dette baserer seg på eksempelet i punkt 3.3.1). Her har naturligvis også beregningen som ledet til 75 % vært

108 Forvaltningsloven (fvl.) § 2 (1) bokstav a og b.

109 Schartum og Bygrave (2016) s. 209 legger til grunn, i tilknytning den forrige personopplysningslovens § 22, at innsynet skal gis i «både de deler av programmene som styrer informasjonsinnsamlingen, og de deler som styrer den videre behandlingen frem til endelig avgjørelse».

bestemmende for avgjørelsen. Tilsvarende er det også for avgjørelser som ikke er automatisert. Dersom en saksbehandler eksempelvis sier at «vi har gitt deg avslag på lån, fordi du blir ansett som lite betalingsdyktig», er avgjørelsen naturligvis betinget av vurderingen av betalingsdyktighet.

Det er dermed gode grunner til å tolke «avgjørelse» slik at det anses som en prosess. Formålene understøtter dette. Hvis det skal være noen realitet i vernet som artikkel 22 nr. 1 og innsynsbestemmelsen i artikkel 15 nr. 1 bokstav h gir, må bestemmelsen omfatte de prosessene i en «avgjørelse» som faktisk har vært bestemmende for avgjørelsen. Hvordan en skal dele inn de prosessene som leder frem til en avgjørelse, er det vanskelig å si noe generelt om. Dette må vurderes konkret da det er store variasjoner på hvilke programmer en datamaskin består av og hvordan disse er organisert.

4.3 Vilkåret «profilering»

Vilkåret «profilering» har en egen legaldefinisjon i artikkel 4 punkt 4. Personvernforordningen er ikke konsekvent med plasseringen av «profilering» i forhold til en automatisert avgjørelse. Legaldefinisjonen gir utrykk for at «profilering» er en form for automatisert behandling.[110] Artikkel 15 nr. 1 bokstav h og artikkel 22 nr. 1 synes derimot å plassere «profilering» som en underkategori av en automatisert avgjørelse. Bestemmelsene taler om «[automatiserte avgjørelser],[111] herunder profilering». Dette indikerer at profilering er noe litt annet enn en automatisert avgjørelse.

Om forholdet mellom automatiserte avgjørelser og profilering, skriver Artikkel 29-gruppen at «Automated decision-making has a different scope and may partially overlap with or result from profiling».[112] Artikkel 29-gruppen ser altså ut til å mene at automatiserte avgjørelser og profilering er to forskjellige ting, selv om de til tider vil være overlappende.

Mot dette står flere uttalelser i personvernforordningens fortale. I avsnitt 63 i fortalen står det «logikken som ligger bak en eventuell automatisk behandling av personopplysningene […], i det minste dersom den er basert på profilering» (min understrekning og tilpasning). I avsnitt 71 står det to ting. For det første: «En slik behandling omfatter «profilering», som består av enhver form for auto-

110 Personvernforordningen artikkel 4 nr. 4.

111 Personvernforordningen artikkel 22 nr. 1 bruker riktignok ikke formuleringen «automatisert avgjørelse», men «avgjørelse som er utelukkende basert på automatisert behandling». Dette synes å være en mer spesifikk form for «automatisert avgjørelse».

112 A29WP (2018a) s. 8.

matisert behandling» (min understrekning). For det andre: «Avgjørelser som treffes på grunnlag av slik behandling, herunder profilering» (min understrekning).

Både formuleringen i legaldefinisjonen og formuleringene i fortalen indikerer at en profilering er en form for automatisert behandling som kan lede til en avgjørelse. Det er dessuten vanskelig å se hva som er nytten av å skille mellom profilering og en automatisert avgjørelse. Det er uklart hva profilering ville fanget opp, som ikke ellers ville være omfattet av begrepet automatisert avgjørelse. All den tid profilering handler «å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person»,[113] vil dette innebære at det tas en avgjørelse. Det vil enten bli tatt en avgjørelse om å plassere den registrerte i en kategori, eller det vil bli tatt en avgjørelse på bakgrunn av en slik kategorisering. Basert på legaldefinisjonen,[114] kan en slik avgjørelse for eksempel være å plassere den registrerte i kategorien «dårlig helse» eller «sannsynlige betalingsvansker», eller avgjørelsen kan være at denne kategoriseringen skal medføre avslag på en søknad eller liknende. Uansett hvilken av disse to innfallsvinklene en velger, vil avgjørelsen innbefatte profileringen.

Samlet sett gir ikke ordlyden i legaldefinisjonen og uttalelsene i fortalen uttrykk for et skille mellom en «automatisert avgjørelse» og «profilering», slik Artikkel 29-gruppen gjør. På bakgrunn av dette er det naturlig å se det slik at profilering er en form for automatisert behandling som kan lede til en avgjørelse. Dette fremstår også som den logiske løsningen fra et informatikkperspektiv.

Bygrave og Mendoza tar til orde for at «herunder», på engelsk «including», bør forstås som «involverer».[115] På denne måten vil kun avgjørelser som involverer «profilering» være dekket av artikkel 22 nr. 1. Bygrave og Mendoza anser denne tilnærmingen som mer hensiktsmessig enn å måtte operere med forordningens uklare plassering av «profilering.[116] Begrunnelsen for deres standpunkt synes å være at virkeområdet for artikkel 22 nr. 1 vil bli svært vidt dersom det også omfatter automatiserte avgjørelser som ikke er basert på profilering, samt at dette vil være mest i tråd med bestemmelsens begrunnelse og bakgrunn.[117] Bygrave understreker at argumentet deres er tynt.[118] Det er vanskelig å se nytten av Bygrave og Mendozas tolkning. Denne åpner for en vanskelig grenseoppgang mellom automatisert behandling med og uten profilering. Dette gjør det van-

113 Personvernforordningen artikkel 4 nr. 4.
114 Personvernforordningen artikkel 4 nr. 4.
115 Bygrave og Mendoza (2017) s. 13–14 og Bygrave (2019) s. 5.
116 Bygrave og Mendoza (2017) s. 14.
117 Bygrave og Mendoza (2017) s. 13–14 og Bygrave (2019) s. 5.
118 Bygrave (2019) s. 5.

skeligere nå formålet om at bestemmelsen skal bidra til åpenhet og tillit. Når det gjelder bestemmelsens virkeområde avgrenses dette best av terskelen «rettsvirkning for eller på tilsvarende måte i betydelig grad påvirker vedkommende».[119]

4.4 Vilkåret «utelukkende»

Vilkåret «utelukkende» er ikke nærmere definert utover det man kan hente fra ordlyden. En naturlig språklig forståelse av «utelukkende» tilsier at avgjørelsesprosessen ikke skal involvere noen form for menneskelig behandling. Vilkåret er ikke oppfylt om så den menneskelige involveringen bare er symbolsk. En slik tolkning harmonerer imidlertid dårlig med bestemmelsens formål.

En annen mulighet er å tolke «utelukkende» litt mindre strengt, og heller rette fokuset på hva som faktisk er avgjørende for beslutningen. På denne måten vil det avgjørende være hva eller hvem som i realiteten fattet avgjørelsen. Artikkel 29-gruppen gir i sine retningslinjer uttrykk for denne forståelsen, hvor de sier at «The controller cannot avoid the Article 22 provisions by fabricating human involvement».[120] Menneskelig inngripen skal være «meaningful, rather than just a token gesture».[121] Videre skal personen som er involvert ha «authority and competence to change the decision» og skal «consider all the relevant data».[122] Når bestemmelsens formål og Artikkel 29-gruppens retningslinjer sammenholdes, synes det nokså klart at en slik tolkning må legges til grunn.

I punkt 4.2 konkluderte jeg med at «avgjørelse» måtte forstås slik at det omfatter noen av de prosessene som leder frem til et valg. Den tolkningen av «utelukkende» som er skissert her, må i utgangspunktet gjelde for alle disse prosessene. Samtidig kan det oppstå vanskelige tvilstilfeller. I de innledende prosessene, slik som datainnsamlingen, kan det være mennesker involvert og dette kan ha betydning for resultatet. I noen slike situasjoner, vil det ikke være naturlig å unnta denne avgjørelsen under henvisning til at vilkåret «utelukkende» ikke er oppfylt. Et eksempel kan være at en datamaskin bruker et spørreskjema for å innhente informasjonen. Datamaskinen ber brukeren fylle ut de kategoriene med data som maskinen trenger. Et annet eksempel kan være at en fysisk person har bygget opp en digital database, som maskinen igjen henter informasjonen fra. I disse eksemplene er det ikke tvilsomt at den fysiske personen vil kunne ha betydning for resultatet. Samtidig harmonerer det dårlig med bestemmelsens

119 Personvernforordningen artikkel 22 nr. 1.
120 A29WP (2018a) s. 20–21.
121 A29WP (2018a) s. 21.
122 A29WP (2018a) s. 21.

formål om å gi den registrerte vern mot automatiserte avgjørelse, dersom alle slike avgjørelser skulle falle utenfor.

Det kan være interessant å vurdere hvordan «utelukkende» forholder seg til skjønnsmessige avgjørelser. Boe definerer skjønn som: «Regelen bestemmer at hvis fakta er slik som regelen sier, så kan det ene eller annet vedtak treffes, bare det ligger innenfor lovens ramme».[123] Skjønnet den offentlige forvaltning har, omtales ofte som «forvaltningens frie skjønn».[124] Til tross for betegnelsen, er dette aldri et helt fritt skjønn.[125] Det vil alltid være begrensninger og rammer for hvordan dette skjønnet skal utøves.[126] Det er dessuten vanlig at det oppstilles retningslinjer for skjønnet.[127] For private er skjønnet friere, selv om det også her finnes begrensninger for hva som kan vektlegges ved en avgjørelse.[128]

Datamaskiner bygger på logikk. Det er derfor ikke mulig for en datamaskin å gjennomføre en skjønnsmessig avgjørelse.[129] Ved tradisjonell programmering av en datamaskin, kan man programmere inn alle retningslinjene og begrensningene for skjønnet. Selve kjernen i skjønnet, at konkrete omstendigheter som en ikke hadde tenkt på tidligere kan tas med i betraktningen, er det imidlertid ikke mulig å programmere. Også for systemer som bruker maskinlæringsalgoritmer forutsettes det at det er mulig å finne et mønster, altså en korrelasjon mellom data som sendes inn og resultatet. Maskinlæringsalgoritmene lærer av historiske data. Et forvaltningsorgan kan trene en maskinlæringsmodell til å klassifisere på bakgrunn av alle tidligere saker. Deretter kan de ta i bruk denne modellen for å erstatte skjønnet. Selv om dette skulle være vellykket, vil den delen av skjønnet som innebærer en konkret vurdering av en sak være borte.

Dersom det foreligger en plikt til å kunne bruke skjønnet, og en «automatisert behandling» ikke kan gjennomføre et slikt skjønn, er vilkåret «utelukkende» til hinder for at artikkel 22 nr. 1 kan omfatte skjønnsmessige avgjørelser.[130]

123 Boe (2010) s. 82.
124 Rt. 2007 s. 257 avsnitt 36.
125 Smith (2011) s. 382.
126 Smith (2011) s. 382.
127 Eksempelvis Kriminalomsorgen (2008).
128 Se blant annet likestillings- og diskrimineringsloven § 6.
129 Se også Schartum (2018a) s. 117.
130 Se nærmere om automatiseringsvennlig lovgivning i Schartum (2018a) kapittel 12.

4.5 De alternative vilkårene «har rettsvirkning for» og «på tilsvarende måte i betydelig grad påvirker vedkommende»

Til slutt må et av de alternative vilkårene være oppfylt. Disse vilkårene oppstiller en terskel og viser at ikke alle helautomatiserte avgjørelser skal utløse vernet i artikkel 22 og tilhørende rettigheter. Vilkåret «har rettsvirkning for» gjelder avgjørelser som kan endre et individs rettsposisjon, slik som offentlige vedtak og endringer av kontraktsposisjon.[131] Ordlyden er «har rettsvirkning» (min understrekning). Formålet tilsier at dette må forstås som «kan ha». Avslag på et vedtak kan ha like stor betydning som at det blir truffet et vedtak.

Vilkåret «har rettsvirkning for» gjelder etter sin ordlyd uavhengig av grad. Den etterfølgende delen av bestemmelsen, kan imidlertid tyde på at også rettsvirkningene må være betydelige. Artikkel 29-gruppen gir uttrykk for at artikkel 22 nr. 1 gjelder betydningsfulle avgjørelser, og viser til rettsvirkninger som generelt kan sies å være av nokså stor betydning for den registrerte.[132] Samtidig vurderer de kun terskelen i forbindelse med vilkåret «på tilsvarende måte i betydelig grad».[133] Det er dermed noe uklart om alle «rettsvirkninger» er omfattet eller bare betydelige rettsvirkninger.

Vilkåret «på tilsvarende måte» antyder at vilkåret også gjelder faktiske virkninger som ligner på rettsvirkninger. Ordene «i betydelig grad» legger tydelige føringer på graden, og tilsier at det er en nokså høy terskel. Artikkel 29-gruppen inntar samme standpunkt.[134] Før gruppen presiserer at det er vanskelig å si noe presist om terskelen, lister de opp følgende tre punkter for nærmere å klarlegge denne:[135]

- «significantly affect the circumstances, behaviour or choices of the individuals concerned»;
- «have a prolonged or permanent impact on the data subject; or»
- «at its most extreme, lead to the exclusion or discrimination of individuals.»

Fortalens punkt 71 lister opp «automatisk avslag på en søknad om kreditt på internett eller e-rekruttering uten menneskelig inngripen»[136] som eksempler på avgjørelser som kan oppfylle vilkåret. Artikkel 29-gruppen referer til de samme

131 A29WP (2018a) s. 21.
132 A29WP (2018a) s. 21.
133 A29WP (2018a) s. 21.
134 A29WP (2018a) s. 21–22.
135 A29WP (2018a) s. 21.
136 Personvernforordningen fortalen avsnitt 71.

eksemplene, men legger også til «tilgang til helsetjenester» og «tilgangen til utdanning» (min oversettelse).[137]

Det er også et spørsmål om «på tilsvarende måte i betydelig grad»[138] er en objektiv eller en subjektiv vurdering fra den registrertes standpunkt. På dette punktet gir ordlyden lite veiledning. Artikkel 29-gruppen tar utgangspunkt i at dette er en subjektiv vurdering.[139] De gir som eksempel at markedsføring for forbrukslån kan være en avgjørelse som «på tilsvarende måte i betydelig grad påvirker vedkommende», dersom den spesifikt rettes mot mennesker som er eller sannsynligvis er i en dårlig økonomisk situasjon.[140]

Med den vide forståelsen av «avgjørelse» som er nevnt i punkt 4.2, vil nok prosessledende beslutninger i den offentlige forvaltning omfattes av ordet «avgjørelse». Slike beslutninger vil imidlertid ikke produsere rettsvirkninger for individer og vil derfor, i mange tilfeller, ikke være omfattet av artikkel 22 nr. 1. Slike avgjørelser kan imidlertid «på tilsvarende måte i betydelig grad påvirke[r] vedkommende».[141]

4.6 Gitt samme input, vil utfallet av avgjørelsen også være den samme

Et poeng som kommer frem når en ser vilkårene «avgjørelse», «utelukkende» og «automatisert behandling» i sammenheng, er at avgjørelser som nevnt i artikkel 22 nr. 1 er forutsigbare.[142] Når alle stegene i avgjørelsesprosessen utelukkende er basert på automatisert behandling som ikke kan gjennomføre skjønn, vil fremgangsmåten for avgjørelsen være nøyaktig fastsatt før avgjørelsen tas. Fremgangsmåten er altså algoritmen for det eller de datamaskinprogrammene som gjennomfører avgjørelsen. Dermed er det bare å gi algoritmen den inputen den er avhengig av, så vil en få resultatet. Dette betyr også at dersom datamaskinen på nytt får den samme inputen, vil avgjørelsen alltid bli den samme.

En automatisert avgjørelse er forutsigbar både der den er basert på tradisjonell programmering, og der den er basert på maskinlæring. Ved tradisjonell programmering vil en skrive algoritmen basert på retningslinjer eller tolkede retts-

137 A29WP (2018a) s. 22.
138 Personvernforordningen artikkel 22 nr. 1.
139 A29WP (2018a) s. 22.
140 A29WP (2018a) s. 22.
141 Personvernforordningen artikkel 22 nr. 1.
142 Dette synes også å være et av Selbst og Powels sentrale poeng i forbindelse med diskusjonen om «right to explanation», se Selbst (2017) s. 239 og punkt 5.3.5.

regler. Ved maskinlæring er det datamaskinen selv som finner algoritmen på bakgrunn av treningsprosessen. Algoritmen er uansett fastsatt før avgjørelsen tas. Dersom maskinlæringsmodellen lar seg forklare, kan en se hva som vil bli vektlagt før avgjørelsen blir tatt. Visse maskinlæringsalgoritmer er det imidlertid ikke mulig å få en forklaring fra,[143] se punkt 5.3.6.

Innebygget personvern er en målsetning etter artikkel 25. Fordi helautomatiserte avgjørelser etter artikkel 22 er forutsigbare, er det mulig å bygge inn løsninger for å presentere informasjon etter artikkel 15 nr. 1 bokstav h. Dette omtales nærmere i punkt 5.3.2.

4.7 Eksempel fra Lånekassen

Med denne forståelsen av artikkel 22 nr.1, kan være interessant å nevne et eksempel på bruk av automatiserte avgjørelser. Lånekassen bruker maskinlæring til å redusere utvalget av kunder som skal vurderes trukket ut til bo-kontroll.[144] Dette gjøres ved hjelp av en maskinlæringsteknikk kalt «gradient boosting», som baserer seg på beslutningstrær.[145] Selve bo-kontrollen er imidlertid ikke automatisert.[146] Det må forutsettes at denne manuelle behandlingen har eller kan ha reell påvirkning på resultatet, slik det er nevnt i punkt 4.4. Lånekassen oppgir selv at den automatiserte behandlingen faller utenfor artikkel 22 nr. 1, fordi den ikke har rettsvirkning for den registrerte.[147] Dette er i tråd med forståelsen nevnt i punkt 4.5, da det å gjøre et slikt utvalg må kunne sees på som en prosessledende beslutning som heller ikke «i betydelig grad påvirker vedkommende».[148] Når selve avgjørelsen også involverer manuell behandling med reell innflytelse, vil heller ikke vilkåret «utelukkende» være oppfylt.

Dersom Lånekassen også automatiserer den manuelle delen av avgjørelsesprosessen, vil vilkårene i artikkel 22 nr. 1 være oppfylt. Avgjørelsen vil da være «utelukkende basert på automatisert behandling». Avgjørelsen vil også medføre rettsvirkninger, ved at den registreres rettslige posisjon i forhold til Lånekassen endres. Dersom denne manuelle delen blir automatisert, vil det være i tråd med hensynene at denne avgjørelsen er underlagt særreglene i artikkel 22 og 15. Det er viktig for tilliten til Lånekassen at en helautomatisert avgjørelse er åpen og etterprøvbar.

143 Selbst (2017) s. 239 understrekker også dette i sin note 39.
144 Lånekassen (2019) og Lånekassen (2018).
145 Lånekassen (2017) s. 21 og Lånekassen (2018).
146 Lånekassen (2017) s. 21.
147 Lånekassen (2018).
148 Personvernforordningen artikkel 22 nr. 1.

5 Hva er «relevant informasjon om den underliggende logikken» for en automatisert avgjørelse?

5.1 Fremstillingen videre

Artikkel 15 nr. 1 bokstav h gir en rett til «relevant informasjon om den underliggende logikken» for en automatisert avgjørelse, slik dette er redegjort for i punkt 4. På et overordnet nivå kan det være hensiktsmessig å dele «relevant informasjon om den underliggende logikken» i to deler. Den første er hva «informasjon om den underliggende logikken» referer til, se punkt 5.2. Den andre delen er hva som er «relevant informasjon» om denne «underliggende logikken», se punkt 5.3. Til slutt er det interessant å vurdere om den behandlingsansvarlige har en plikt til å ha dokumentasjon som gir uttrykk for «relevant informasjon om den underliggende logikken», se punkt 5.4.

5.2 Hva er «den underliggende logikken»?

Verken forordningen, fortalen utdyper eller Artikkel 29-gruppen nevner direkte hva den «underliggende logikken» referer til.[149] Det naturlige utgangspunktet må være algoritmen som ligger til grunn for det eller de datamaskinprogrammene som har gjennomført den «automatiserte behandlingen» som ledet til avgjørelsen. En beskrivelse av denne algoritmen vil kunne forklare hvordan datamaskinprogrammet har lest personopplysningene, hvilke andre opplysninger og programmer som har blitt benyttet og hvordan datamaskinen har arbeidet med denne informasjonen.

Det mest presise og detaljerte uttrykket for algoritmen er kildekoden, se 3.3.1. Kildekoden brukes av datamaskinen for å kjøre programmet. Ved å lese kildekoden, kan en se den fulle algoritmen for den «automatiserte behandlingen» som ligger til grunn for avgjørelsen. Dermed har man også nøyaktig informasjon om «den underliggende logikken». Kildekoden har to roller. Den er både en del av «den underliggende logikken», og en kilde til informasjon om «den underliggende logikken». Det er imidlertid ikke alltid en hensiktsmessig kilde til informasjon, se neste punkt 5.3.2. For automatisert behandling som er basert på maskinlæring, vil ikke kildekoden gi et fullt uttrykk for algoritmen som lig-

149 Personvernforordningen artikkel 15 nr. 1 bokstav h.

ger til grunn. Fordi maskinlæringsalgoritmer er avhengig av trening, må kildekoden suppleres med datasettet som er benyttet ved treningen av maskinlæringsmodellen.

Vilkåret «den underliggende logikken» kan forstås svært vidt ved automatiserte avgjørelser. Datamaskiner bygger gjennomgående på logikk, og «den underliggende logikken» finnes flere steder. Datamaskinprogrammet som algoritmen gir uttrykk for virker i et samspill med flere andre elementer når programmet «kjøres». I informatikken er det vanlig å dele en datamaskin inn i flere elementer.[150] Englander deler datamaskinarkitekturen inn i hardware-elementet, software-elementet, data-elementet og kommunikasjons-elementet.[151] Algoritmen til det aktuelle datamaskinprogrammet er en av de mange tingene man finner i software-elementet. Et mer usikkert spørsmål er om «den underliggende logikken» også kan omfatte informasjon om de øvrige elementene, og ikke bare den delen av software-elementet som gjelder det aktuelle datamaskinprogrammet. Det er eksempelvis mulig å se for seg at det ikke er noe galt med algoritmen eller kildekoden, men en feil i prosessoren (hardware-elementet) gjør at beregningene i datamaskinen ikke blir riktig,[152] og at dette kan påvirke avgjørelsen. Dersom man bare tar utgangspunkt i ordlyden vil også øvrige elementer være en del av «den underliggende logikken». Den «underliggende logikken» vil dessuten avgrenses av hva som er «relevant informasjon», hvilket kan tilsi at det ikke er behov for å avgrense «den underliggende logikken» til å bare gjelde det aktuelle datamaskinprogrammet. Samtidig er det vanskelig å se for seg at den registrerte vil ha behov for teknisk og detaljert informasjon om de øvrige elementene i datamaskinen. I dagens datamaskiner er de fleste delene i de ulike elementene masseprodusert. Dersom det er feil ved disse delene, og dette har betydning for avgjørelsen, vil en nok få klarhet i dette ved å analysere kildekoden. Ved å analysere kildekoden, vil en nemlig kunne få informasjon om forventet resultat. I dag fremstår derfor dette som en mindre relevant problemstilling, og denne delen av den «underliggende logikken» vil ikke bli behandlet videre. Fordi forordningen skal være teknologinøytral,[153] kan dette tenkes å være en problemstilling ved mer eksperimentell teknologi i tiden fremover.

150 Englander (2014) s. 2 og s. 11–19.
151 Englander (2014) s. 2 og s. 11–19.
152 Eksempelvis Athow (2014).
153 Personvernforordningen fortale avsnitt 15.

5.3 Hva er «relevant informasjon» om den underliggende logikken?

5.3.1 Noen utgangspunkter

Den registrerte kan kreve «relevant informasjon» om den underliggende logikken. Her er det grunn til å se på ordlyden i den tilsvarende bestemmelsen i personvernforordningen slik den fremkommer på noen av de øvrige EU-språkene. Den engelske versjonen bruker begrepet «meaningful information»,[154] og ikke «relevant informasjon». Det samme gjelder for den danske og svenske versjonen, som bruker henholdsvis «meningsfulde oplysninger»[155] og «meningsfull information»[156]. Den tyske versjonen bruker begrepet «aussangekräftige Informationen»,[157] hvilket kan oversettes til «meningsfull informasjon». Den franske versjonen bruker begrepet «des informations utiles»,[158] som kan oversettes til «nyttig informasjon». Betydningen av ordet «nyttig» ligger nærmere betydningen av «meningsfull» enn betydningen av «relevant».

Både «meningsfull» og «relevant» er relative begreper. Det beror på situasjonen og adressaten hvorvidt noe er «relevant» eller «meningsfullt». Samtidig gir ordet «meningsfull» uttrykk for en større grad av subjektivitet enn det relevant gjør. Ordet «meningsfull» tilsier at informasjonen skal gi mening for den registrerte, hvilket innebærer at informasjonen må kunne forstås. Her skiller «meningsfull» seg fra «relevant» – informasjon kan være relevant for den registrerte, selv om den registrerte ikke forstår informasjonen. I uttrykket «meningsfull informasjon» synes det dermed å ligge en plikt til å gjøre informasjonen forståelig der den registrerte har behov for det. Dette harmonerer godt med artikkel 12 nr. 1, som sier at all informasjon og kommunikasjon etter artikkel 15 skal presenteres på «en kortfattet, åpen, forståelig og lett tilgjengelig måte og på et klart og enkelt språk». Avsnitt 58 i fortalen understreker at dette er av særlig betydning der kompleks teknologi er involvert.

Forarbeidene til personopplysningsloven har ingen uttalelser om bakgrunnen for valget av ordet «relevant».[159] Det er antakelig ikke en bevisst fravikelse av uttrykket «meaningful». I lys av homogenitetsmålsetningen er det uansett naturlig å forstå «relevant informasjon» som uttrykk for den samme rettsregelen som i de øvrige språkversjonene. Jeg velger derfor å tolke den norske oversettelsen i lys av de andre språkversjonene. Begrepet «relevant» bør forstås som

154 Personvernforordningen (engelsk) artikkel 15 nr. 1 bokstav h.
155 Personvernforordningen (dansk) artikkel 15 nr. 1 bokstav h.
156 Personvernforordningen (svensk) artikkel 15 nr. 1 bokstav h.
157 Personvernforordningen (tysk) artikkel 15 nr. 1 bokstav h.
158 Personvernforordningen (fransk) artikkel 15 nr. 1 bokstav h.
159 Et aktuelt sted ville vært Prop.56 LS (2017–2018) punkt 10.2.2.

«meningsfull»,[160] som er oversettelsen av den engelske, tyske, svenske og danske språkversjonen. Hvorvidt det er noen forskjell mellom «meningsfull» og den franske «nyttige», behandles ikke videre her.

Ordet «meningsfull» gir uttrykk for en konkret vurdering av hva som er meningsfull informasjon for den registrerte. Dette harmonerer med den etterfølgende delen av artikkel 15 nr. 1 bokstav h, som sier at det skal gis informasjon om «betydningen og de forventede konsekvensene av en slik behandling for den registrerte»[161] (min understrekning). Artikkel 29-gruppen synes også å gi uttrykk for dette, ved at de nevner at informasjonen skal være nyttig for den registrerte.[162]

Når utgangspunktet er en konkret vurdering av hva som er meningsfullt for den registrerte, kan informasjonen som skal gis variere med hvem den registrerte er og grunnlaget for innsynsbegjæringen. Det er viktig å understreke at det fortsatt er rettsanvenderen som må vurdere om informasjonen er meningsfull for den registrerte. Det er altså snakk om en objektiv vurdering av det konkrete tilfellet.

Til tross for at utgangspunktet er en konkret vurdering, kan det oppstilles visse retningslinjer for hvilken informasjon som normalt vil være «[meningsfull] informasjon» for den registrerte. I det følgende vil jeg først se nærmere på hvilken informasjon som normalt er meningsfull for den registrerte. Deretter vil jeg se nærmere på situasjoner hvor den registrerte etterspør spesifikk informasjon. Her er trolig innsyn i kildekoden det mest aktuelle, og fremstillingen i punkt 5.3.3 begrenses til dette. I punktene 5.3.4, 5.3.5 og 5.3.6 drøfter jeg tre spørsmål som har betydning for all informasjon etter artikkel 15 nr. 1 bokstav h.

5.3.2 Informasjon som normalt vil være meningsfull informasjon for den registrerte

Informasjon som normalt vil være meningsfull informasjon for den registrerte kan ikke være for teknisk. Dette følger av både ordlyden, formålene og uttalelsene fra Artikkel 29-gruppen.[163] Kildekoden og detaljerte beskrivelser av algoritmen vil normalt ikke være meningsfull informasjon.[164] Forenklede beskrivelser av algoritmen kan derimot være meningsfull informasjon. Det er todelt spørsmål

160 I det følgende vil jeg av og til sette meningsfull i klammeparentes for å synliggjøre at dette ordet ikke står i den norske forordningen. Dette er tilføyd av meg. For å holde fremstillingen ryddig, kommer jeg ikke til å kommentere «(min tilpasning)» for hver gang jeg skriver «[meningsfull]».

161 Personvernforordningen artikkel 15 nr. bokstav h.

162 Se blant annet A29WP (2018a) s. 26 og s. 27.

163 A29WP (2018a) s. 25.

164 A29WP (2018a) s. 25.

hva disse beskrivelsene er. Først er det et spørsmål om hvilke deler av algoritmen som skal beskrives. Deretter er det et spørsmål om hvordan disse beskrivelsene skal presenteres for den registrerte.

Når det gjelder hvilke deler av algoritmen som skal presenteres, er formålet et godt utgangspunkt for vurderingen. Formålet med innsynsbestemmelsen i artikkel 15 nr. 1 bokstav h er blant annet at den registrerte skal kunne forvisse seg om behandlingen har skjedd på en lovlig og rettferdig måte.[165] Artikkel 29-gruppen gir uttrykk for at informasjonen må være tilstrekkelig omfattende til at den registrerte forstår «the reasons for the decision».[166] Dersom den registrerte mener at avgjørelsen ikke har foregått på en lovlig og rettferdig måte, skal han eller hun ha tilstrekkelig informasjon til å kunne bestride avgjørelsen i tråd med sine øvrige rettigheter i personvernforordningen. Dette understøttes av Artikkel 29-gruppens uttalelser om at den registrerte fullt ut må kunne forstå hvordan og på hvilket grunnlag en avgjørelse er tatt for å være i stand til å uttrykke seg eller prøve denne.[167] Artikkel 29-gruppen har flere uttalelser som nærmere konkretiserer hva denne informasjonen vil være:

Den registrerte skal få informasjon om begrunnelsen og kriteriene som er lagt vekt på for å finne resultatet.[168]

Den registrerte bør i tillegg få generell informasjon om faktorene som er tatt i betraktning ved avgjørelsen, og deres vekt på et aggregert nivå.[169] Hva som ligger i dette er noe uklart. Faktorene som er tatt i betraktning, må forstås som merkelappen på hver av kategoriene med personopplysninger og annen informasjon som benyttes i dataprogrammet, for eksempel at programmet eller modellen vurderer «inntekt», «utdanning», «bostedsområde». Vekten på et aggregert nivå, må trolig forstås som de generelle tendensene for hvordan faktorene påvirker avgjørelsen.[170]

Artikkel 29-gruppen liste i sine «good practice recommendations» opp flere eksempler på informasjon som kan gis til den registrerte.[171] Her nevnes kategoriene med data som har blitt brukt, hvorfor disse er relevante, hvordan en profil

165 Artikkel 5 nr. 1 bokstav a.
166 A29WP (2018a) s. 25.
167 A29WP (2018a) s. 27 Artikkel 29-gruppens uttalelse her er tilknytning til rettsikkerhetsgarantiene i artikkel 22 nr. 2 bokstav a og b og artikkel 22 nr. 3 og det tilhørende avsnitt 71 i fortalen. Som nevnt i punkt 3.3.3 er rettsikkerhetsgarantiene nært knyttet til formålet med innsynsbestemmelsen.
168 A29WP (2018a) s. 25.
169 A29WP (2018a) s. 27.
170 Se Dvergsdal (2018a) om aggregat innen IT.
171 A29WP (2018a) s. 31.

bygges opp (inkludert statistikken brukt i analysen), hvorfor profilen er relevant og til slutt hvordan denne profilen har blitt brukt til å ta en avgjørelse om den registrerte.

Informasjonen bør altså presenteres uten å fremlegge selve kildekoden. Informasjon om algoritmen kan blant annet gis ved muntlige forklaringer, andre tekstlige beskrivelser, pseudokode,[172] figurer, illustrasjoner og videoklipp.[173] Innebygget personvern er aktuelt for å gi informasjon om den «underliggende logikken» for en automatisert avgjørelse. Forvaltningslovutvalget forslår simulering av vedtak som en mulig løsning.[174] På denne måten kan den registrerte selv justere og endre parametere for å se hvordan dette ville påvirket avgjørelsen. En annen mulig løsning, er automatisk genererte forklaringer. Disse kan gjerne komme i forskjellige detaljnivåer, slik at den registrerte selv kan velge detaljnivå. Personvernforordningen synes ikke å legge noen begrensninger på hvilke løsninger for innebygget personvern som kan benyttes for å gi «[meningsfull] informasjon om den underliggende logikken», så lenge dette fremmer idealene i artikkel 5 nr. 1 bokstav a. Det ser heller ut til at det oppfordres til kreative løsninger som kan fremme artikkel 5 nr. 1 bokstav a.[175]

5.3.3 Kan den registrerte kreve innsyn i kildekoden?

Det er mulig at kildekoden også fremstår som meningsfull informasjon for enkelte registrerte. Dette er nok særlig aktuelt dersom den registrerte er i tvil om det er en feil i datamaskinprogrammet. Som eksempelet i innledningen (punkt 1) viste, kan det være nødvendig å undersøke kildekoden for å avdekke feil.

Hva som er meningsfull informasjon, beror i utgangspunktet på en konkret vurdering av hva som er meningsfull informasjon for den registrerte, se punkt 5.3.1. Dersom kildekoden faktisk er «[meningsfull] informasjon om den underliggende logikken»[176] for den registrerte, taler ordlyden for at kildekoden skal gis.

Formålet med innsynsbestemmelsen kan tilsi at den registrerte bør kunne få se kildekoden. Hensynet til åpenhet og tillit trekker i denne retningen. Dersom innsyn i kildekoden er nødvendig for å vurdere om behandlingen er lovlig og rettferdig, jf. artikkel 5 nr. 1, bør det være mulig å se kildekoden. Vekten av formålsbetraktningene kan imidlertid reduseres noe av at personvernforordnin-

172 Dvergsdal (2018b) og Schartum (2018a) s. 284.
173 Pound (2017) Dr. Mike Pound ved Universitetet i Nottingham forklarer i denne videoen en nokså komplisert algoritme på en lettfattelig måte.
174 NOU 2019:5 s. 264.
175 A29WP (2018a) s. 31
176 Personvernforordningen artikkel 15 nr. 1 bokstav h

gen gir grunnlag for flere nivåer med kontroll av algoritmen.[177] For det første har tilsynsmyndighetene krav på å få tilgang til «all informasjon som er nødvendig»[178] når denne skal gjennomføre tilsyn eller personvernrevisjoner.[179] I Norge har Datatilsynet denne tilsynsmyndigheten.[180] For det andre må den behandlingsansvarlige selv ha informasjon i forbindelse med en vurdering av personvernkonsekvenser,[181] og i forbindelse med at den behandlingsansvarlige skal kunne sørge for «menneskelig inngripen fra den behandlingsansvarlige».[182] Personen som foretar den menneskelige inngripen skal vurdere «all the relevant data».[183] For det tredje nevner Artikkel 29-gruppen at det kan være hensiktsmessig å bruke uavhengige tredjeparter til å revidere algoritmen.[184] Gruppen forslår at disse tredjepartene gis all nødvendige informasjonen om hvordan systemene virker. På denne bakgrunnen kan det kontrolleres at algoritmen ikke gir diskriminerende, urettferdige eller andre uriktige resultater.

Systematisk kontroll med algoritmen er med på å styrke idealene i artikkel 5 nr. 1 bokstav a. For mange individer vil det også være mer hensiktsmessig å vite at en algoritme er godkjent av en uavhengig tredjepart enn å skulle gjøre disse vurderingene selv.[185] Systematisk kontroll ivaretar imidlertid bare delvis tillitshensynet.[186] Det ligger trolig en verdi i at den registrerte selv kan få undersøke den underliggende logikken. Dersom den registrerte etterspør kildekoden og dette anses som «[meningsfull] informasjon», er det lite tilfredsstillende for den registrerte om innsynet blir avslått under henvisning til at systemet er grundig kontrollert.

Artikkel 29-gruppen uttaler at «The GDPR requires the controller to provide meaningful information about the logic involved, not necessarily a complex explanation of the algorithms used or disclosure of the full algorithm».[187] Ettersom kildekoden er det mest presise og komplette uttrykket for algoritmen, må det antas at det er kildekoden Artikkel 29-gruppen sikter til med «full algorithm». Uttalelsen synes først og fremst å adressere at teknisk informasjon ikke vil være relevant for de fleste. Bruken av ordet «necessarily» kan imidlertid indikere at slik informasjon unntaksvis kan gis.

177 Den følgende tredelingen bygger på Kaminski (2018) s. 23–24.
178 Personvernforordningen artikkel 58 nr. 1 bokstav e, jf. artikkel 58 nr. 1 bokstav a.
179 Personvernforordningen artikkel 57 nr. 1 bokstav a og artikkel 58 nr. 1 bokstav b.
180 Se nærmere om denne typen tilsyn i Datatilsynet (2018) s. 22–23.
181 Personvernforordningen artikkel 35 nr. 3 bokstav a.
182 Personvernforordningen artikkel 22 nr. 2 og nr. 3.
183 A29WP (2018a) s. 27.
184 A29WP (2018a) s. 32. Se også Kaminiski (2018) s. 23–24.
185 A29WP (2018a) s. 31.
186 Se punkt 3.2.
187 A29WP (2018a) s. 25.

Det er uvisst hvor mange som benytter seg av en slik innsynsmulighet, og det er naturligvis ikke mulig å vite hvor mange som vil benytte dette i tiden fremover. Den forrige bestemmelsen i personverndirektivet var lite brukt, se punkt 1. De norske forarbeidene til personvernforordningen uttaler også at det er usikkert hvor mange som vil benytte retten i artikkel 22.[188] Dersom det skulle bli mange som etterspør denne typen informasjon, vil det kunne komme inn ulike ressurshensyn og økonomiske hensyn som tilsier begrensninger i adgangen til å be om kildekoden. Fortalen gir uttrykk for at den behandlingsansvarlige kan be den registrerte om å «presiser[e] hvilke opplysninger eller behandlingsaktiviteter anmodningen gjelder»[189](min tilpasning). Dette kan gjøre det enklere for den behandlingsansvarlige å etterkomme en innsynsbegjæring, hvilket kan ivareta noen ressurshensyn.

Samlet synes det som om den registrerte kan ha rett til innsyn i kildekoden der hvor denne informasjonen faktisk fremstår som meningsfull for den registrerte. Det kan tenkes at ressurshensyn kan begrense denne retten. Hensynet til forretningshemmeligheter synes også å være aktuelt i denne sammenheng. Dette behandles i punkt 5.3.4.

5.3.4 Forholdet til vernet av forretningshemmeligheter

Ved tolkningen av «[meningsfull] informasjon»[190] er det nødvendig å vurdere hvordan hensynet til åpenhet skal harmoniseres med legitime hensyn som kan begrunne hemmelighold. Forretningshemmeligheter er et slikt hensyn.

På tidspunktet oppgaven blir skrevet finnes det ingen legaldefinisjon av forretningshemmelighet og regelverket om forretningshemmeligheter er fragmentert. Samtidig er et forslag til ny «lov om vern av forretningshemmeligheter» under behandling[191]. Loven skal gjennomføre EUs nye forretningshemmelighetsdirektiv.[192] I lovforslaget er det i § 2 et forslag til en legaldefinisjon.[193] Her er forretningshemmelighet definert som opplysninger som:

> «a) er hemmelige i den forstand at opplysningene ikke som helhet, eller slik de er satt sammen eller ordnet, er allment kjent eller lett tilgjengelig
>
> b) har kommersiell verdi fordi de er hemmelige
>
> c) innehaveren har truffet rimelige tiltak for å sikre hemmelighold av».

188 Prop.56 LS (2017–2018). Uttalelsen i forarbeidene er tilknyttet en vurdering av et mulig unntak i nasjonal rett fra retten til å protestere. Uttalelsen indikerer likevel generelt at det er usikkert i hvor stor grad artikkel 22 og de tilknyttede innsynsrettene vil bli påberopt.

189 Personvernforordningen fortale avsnitt 63.

190 Personvernforordningen artikkel 15 nr. 1 bokstav h.

191 Justis- og beredskapsdepartementet (2018).

192 Forretningshemmelighetsdirektivet.

193 Justis- og beredskapsdepartementet (2018) s. 139.

Fordi definisjonen gjenspeiler gjeldende rett,[194] finner jeg det hensiktsmessig å ta utgangspunkt i denne. Dersom en algoritme er utviklet på en måte som gjør at datamaskinprogrammet er eller kan inngå i en salgbar tjeneste, har datamaskinprogrammet en kommersiell verdi. Hvis algoritmen er hemmelig fordi tjenesten mister sin verdi om algoritmen blir kjent, og innehaveren derfor sikrer hemmeligholdet av algoritmen, er det algoritmen en forretningshemmelighet. Det gjelder i første rekke algoritmer i proprietære datamaskinprogrammer. Der hvor datamaskinprogrammet er basert på åpen kildekode,[195] er det naturligvis ikke behov holde algoritmen hemmelig.

Der algoritmen er en forretningshemmelighet, vil innsyn i algoritmen utfordre behovet for hemmelighold. Dette gjelder nok særlig der informasjonen om algoritmen presenteres ved fremleggelse av kildekoden. Enkelte algoritmer lar seg heller ikke forklare på andre måter uten samtidig å avsløre forretningshemmeligheten. Spørsmålet blir dermed hvordan «[meningsfull] informasjon» skal tolkes der algoritmen er en forretningshemmelighet.

Selve ordlyden «[meningsfull] informasjon» er såpass vid at det er mulig å si at informasjon om forretningshemmeligheter ikke er «[meningsfull] informasjon». Samtidig kan det oppstå situasjoner hvor informasjonen den registrerte etterspør åpenbart er meningsfull informasjon for vedkommende, selv om informasjonen også er en forretningshemmelighet. Hvordan hensynet til forretningshemmeligheter skal balanseres kan altså ikke løses på bakgrunn av ordlyden alene.

Personvernforordningens fortale har relevante uttalelser om innsyn i forretningshemmeligheter. I fortalens avsnitt 63 er det uttalt at innsynsretten ikke bør «ha negativ innvirkning på andres rettigheter eller friheter, herunder forretningshemmeligheter». Samtidig uttales det at «Disse hensynene bør imidlertid ikke føre til at den registrerte nektes innsyn i alle opplysninger». Artikkel 29-gruppen adresserer den førstnevnte uttalelsen i fortalen og understreker at den behandlingsansvarlige ikke kan bruke vernet av forretningshemmeligheter som en unnskyldning for å nekte tilgang eller å utlevere informasjon til den registrerte.[196]

Personvernforordningen artikkel 23, gir medlemsstatene adgang til å fastsette unntak fra blant annet artikkel 15. Artikkel 23 nr. 1 bokstav i, gir adgang til å gjøre unntak for «vern av […] andres rettigheter og friheter». (min tilpasning) Slike unntak må være lovfestet. Personopplysningsloven § l6 første ledd bokstav

194 Justis- og beredskapsdepartementet (2018) s. 22. Se også Irgens-Jensen (2019) punkt 3.
195 SNL (2018b).
196 A29WP (2018a) s. 17.

f lovfester unntaket i artikkel 23 nr. 1 bokstav i, og oppstiller en adgang til å gjøre unntak fra innsynet dersom «det vil være i strid med åpenbare og grunnleggende private eller offentlige interesser». Bestemmelsen likner veldig på paragraf 23 første ledd bokstav f i personopplysningsloven fra 2000,[197] og det fremgår av forarbeidene at § 16 første ledd bokstav f viderefører gjeldende rett etter denne bestemmelsen.[198] Derfor er det interessant å se rettstilstanden under paragraf 23 første ledd bokstav f i personopplysningsloven fra 2000.[199] Vilkårene her var strenge og unntaksadgangen var snever.[200] Hensynet til forretningshemmeligheter kunne tilsi et slikt unntak, men som Schartum og Bygrave påpekte «den konkurransemessige effekten […] må [trolig] være av vital betydning for bedrifter, og […] det ikke kan gjøres unntak i større omfang enn begrunnelsen rekker»[201] (mine tilpasninger). Unntaket kunne imidlertid være aktuelt for informasjon om behandlingsmåten.[202] Informasjon om den «underliggende logikken»[203] vil nok ofte være informasjon om behandlingsmåten. Samlet sett oppstilte paragraf 23 første ledd bokstav f bestemmelsen en snever adgang til å unnta forretningshemmeligheter fra innsyn, men unntaket kunne være aktuelt for informasjon om behandlingsmåten. Rettstilstanden er altså videreført til den nye personopplysningsloven § 16.

Det kan spørres om eksistensen av en unntaksbestemmelse i personvernforordningen artikkel 23, jf. personopplysningsloven § 16, tilsier at «[meningsfull] informasjon» i seg selv ikke behøver å harmoniseres med hensynet til forretningshemmeligheter. Fortalen og Artikkel 29-gruppens uttalelser tyder imidlertid på at en slik avveining også skal ligge i «[meningsfull] informasjon». Det er dermed to grunnlag for å ivareta hensynet til forretningshemmeligheter. Fordi det ikke bør være avgjørende for den registrertes rettigheter hvilket grunnlag som bli påberopt for ikke å gi informasjon, bør grunnlagene leses i sammenheng.

Samlet kan det sies at «[meningsfull] informasjon» må leses med et visst unntak for forretningshemmeligheter. Både fortalen og Artikkel 29-gruppen kan tas til inntekt for dette. Det samme gjør adgangen til unntak i artikkel 23 nr. 1 bokstav i. Fortalen og Artikkel 29-gruppen uttrykker samtidig at unntaket ikke gjelder betingelsesløst. Dette synes å være en forståelse som harmonerer nokså godt med ordlyden.

197 Personopplysningslov av 2000 (opphevet).
198 Prop.56 LS (2017–2018) s. 217.
199 Personopplysningslov av 2000 (opphevet).
200 Schartum og Bygrave (2016) s. 210 og Ot.prp.nr.92 (1998–1999) s. 122.
201 Schartum og Bygrave (2016) s. 210.
202 Ot.prp.nr.92 (1998–1999) s. 122.
203 Personvernforordningen artikkel 15 nr. 1 bokstav h.

Det kan se ut som det må foretas en interesseavveining mellom den behandlingsansvarliges behov for hemmelighold og den registrertes behov for innsyn. Dette minner om det utgangspunktet Schartum og Bygrave påpeker[204] i forbindelse med unntaket i den gamle personopplysningslovens § 23.[205] Denne typen interesseavveining finnes også i tvistelovens § 22-10[206]. Formålene bak innsynsbestemmelsen taler med styrke for at det bør skje en slik interesseavveining dersom «[meningsfull] informasjon» først skal tolkes innskrenkende. Det er kun den registrerte som kan kreve denne typen innsyn, og avgjørelsene som er omfattet av § 15 nr. 1 bokstav h er avgjørelser av nokså stor betydning for den registrerte,[207] se punkt 4.5. Hensynet til tillit og åpenhet utfordres om det treffes avgjørelser som den registrerte ikke kan få vite begrunnelsen for, der hvor denne avgjørelsen har stor betydning for den registrerte. Terskelen må altså være høy for hemmelighold.

Dersom man, etter en interesseavveining, kommer til at informasjonen skal fremlegges for den registrerte selv om den er vernet av forretningshemmeligheter, har hensynet til forretningshemmeligheter måttet vike for hensynet til åpenhet. Til tross for at hensynet ikke har i blitt ivaretatt fult ut, er det ikke nødvendigvis motstrid mellom de to regelsettene. Paragraf 3 i forslaget til ny lov om forretningshemmeligheter,[208] må nemlig leses med en rettstridsreservasjon:[209] «Når forretningshemmeligheten er tilegnet, brukt eller formidlet i overenstemmelse med annen nasjonal lovgivning, vil handlingen være rettmessig, og handlingen vil derfor ikke utgjøre et inngrep etter forslaget § 3».[210] All den tid personvernforordningen artikkel 15 nr. 1 bokstav h gir mulighet til innsyn i en forretningshemmelighet, er det tale om en forretningshemmelighet som blir «formidlet i overenstemmelse med annen nasjonal lovgivning».[211]

Dersom den behandlingsansvarlige må utlevere opplysninger som er forretningshemmeligheter, kan det oppstilles en taushetsplikt for den registrerte. Personvernforordningen nevner ikke en slik løsning, men det er en mulig løsning for ytterligere å ivareta hensynet til forretningshemmelighetene. Tvisteloven har en slik løsning.[212] Det er imidlertid ikke gitt at behandlingsansvarlig vil anse dette som et tilstrekkelig sikkerhetstiltak.

204 Schartum og Bygrave (2016) s. 210.
205 Personopplysningslov av 2000 (opphevet) § 23.
206 Tvisteloven § 22-10.
207 Personvernforordningen artikkel 22 nr. 1.
208 Justis- og beredskapsdepartementet (2018) s. 139.
209 Justis- og beredskapsdepartementet (2018) s. 51. Se også Irgens-Jensen (2019) punkt 4.
210 Justis- og beredskapsdepartementet (2018) s. 51.
211 Justis- og beredskapsdepartementet (2018) s. 51.
212 Tvisteloven § 22-12.

Definisjonen på forretningshemmeligheter i forslaget til ny lov om forretningshemmeligheter § 2[213] vil nok i stor grad utelukke at den offentlige forvaltning kan ha forretningshemmeligheter ved offentlig myndighetsutøvelse. Her er det vanskelig å se at offentlige forvaltning skal kunne vektlegge det kommersielle aspektet som er en forutsetning for forretningshemmeligheter. Dette bildet vanskeliggjøres nok noe i de situasjonene hvor det offentlige har kjøpt sin løsning fra kommersielle tredjeparter. For det tilfellet at det offentlige kan sies å ha forretningshemmeligheter, bør en interesseavveining tilsi en svært høy terskel for ikke å gi innsyn i disse opplysningene. Den registrerte vil som regel ikke ha noen valg når det kommer til offentlige avgjørelser. Hensynet til åpenhet er særlig viktig når det gjelder den offentlige forvaltning.[214] Dette tilsier at offentlig forvaltning i størst mulig grad baserer seg på gjennomsiktig automatisert behandling, slik som åpen kildekode.

5.3.5 En generell eller en spesifikk forklaring?

Et spørsmål som kan stilles ved analysen av «[meningsfull] informasjon om den underliggende logikken»,[215] er om den registrerte har krav på en spesifikk forklaring eller bare en generell forklaring. Med en spesifikk forklaring menes at den registrerte har rett til å få vite begrunnelsen for utfallet av avgjørelsen i sin sak. Med en generell forklaring menes at den registrerte kun har rett til å få en generell forklaring på hvordan datamaskinen tar slike avgjørelser.

Utgangspunktet er at den registrerte har krav på «[meningsfull] informasjon om den underliggende logikken».[216] Med den tolkningen som er lagt til grunn i punkt 5.3.1, må hva som er meningsfull informasjon avgjøres på bakgrunn av en konkret vurdering av hva som er meningsfull informasjon for den registrerte. Dersom en spesifikk forklaring er meningsfull informasjon, er dette i utgangspunktet informasjon som kan kreves. Dersom en generell forklaring er meningsfull informasjon, er dette også i utgangspunktet informasjon som kan kreves. Fortalens punkt 71 er relevant i denne sammenhengen. Her fremkommer det at en automatisert behandling slik som i artikkel 22 nr. 1:

> «[bør] under alle omstendigheter […] ledsages av nødvendige garantier som bør omfatte spesifikk informasjon til den registrerte og rett […] til å få en forklaring på avgjørelsen som er truffet etter en slik vurdering [..]»[217] (min understrekning og tilpasning).

213 Justis- og beredskapsdepartementet (2018) s. 139.
214 Offentleglova § 1.
215 Personvernforordningen artikkel 15 nr.1 bokstav h.
216 Personvernforordningen artikkel 15 nr.1 bokstav h.
217 Personvernforordningen fortale avsnitt 71.

Sitatet synes nokså klart å gi uttrykk for at det i rettsikkerhetsgarantiene skal ligge en adgang til å få en spesifikk forklaring.[218] Sitatet er i utgangspunktet tilknyttet artikkel 22 nr. 2 og nr. 3, men som nevnt i punkt 3.3.3 er det en nær sammenheng mellom artikkel 15 nr. 1 bokstav h og rettsikkerhetsgarantiene i artikkel 22 nr. 2 og nr. 3.

Ordlyden sammenholdt med fortalens avsnitt 71, gir altså uttrykk for at en slik spesifikk forklaring kan gis. Til tross for dette har det vært en diskusjon i litteraturen om personvernforordningen gir en rett til en spesifikk forklaring, en «right to an explanation», eller om bestemmelsene er begrenset til en generell forklaring.[219] Det er tre akademiske artikler det er særlig grunn til å trekke frem.[220]

Den første er en artikkel Bryce Goodman og Seth Flaxman.[221] Denne har blitt tatt til inntekt for at det eksisterer en rett til en spesifikk forklaring.[222] Forfatterne diskuterer hovedsakelig utfordringer ved klassifisering og profilering på bakgrunn av datasett og bruk av sensitive personopplysninger.[223] De analyserer i liten grad innholdet i bestemmelsene i personvernforordningen, men uttaler «The law will also effectively create a "right to explanation," whereby a user can ask for an explanation of an algorithmic decision that was made about them.»[224]

Flaxman og Goodmans artikkel fikk et tilsvar av Sandra Wachter, Brent Middelstadt og Luciano Floridi.[225] Wachter m.fl. oppstiller et rammeverk som opererer med to skiller.[226] Det første er at det må skilles mellom forklaringer av den generelle funksjonaliteten til et system, og forklaringer av spesifikke avgjørelser. Det andre er at man må skille mellom forklaringer gitt i forkant av en avgjørelse og forklaringer gitt i etterkant. Den eneste muligheten den registrerte har til å få en forklaring slik Goodman og Flaxman nevner,[227] en spesifikk forklaring, er hvis personvernforordningen hjemler en rett til forklaring av spesifikke avgjørelser i etterkant av avgjørelsen. Wachter m.fl. vurderer flere mulige hjemler i

218 Bygrave (2019) s. 8.
219 Se blant annet Goodman (2016) s.1–9, Wachter (2017) s. 76–99, Selbst (2017) s. 233–242, Casey (2018) s. 1–50, Kaminski (2018) s. 1–25.
220 Casey (2018) s. 18–22 trekker også frem disse tre artiklene når de gjengir denne diskusjonen. Bygrave (2019) s. 8 trekker frem to av de to siste av disse tre når omtaler problemstillingen.
221 Goodman (2016) s.1–9.
222 Wachter (2017) s. 79 og note 13.
223 Personvernforordningen art. 22 nr. 4, jf. art. 9 og fortalens avsnitt 71.
224 Goodman (2016) s. 1.
225 Wachter (2017) s. 76–99.
226 Wachter (2017) s. 78.
227 Goodman (2016) s. 1.

personvernforordningen,[228] men konkluderer med at ingen gir grunnlag for en slik rett. Wachter m. fl. fremholder likevel at det eksisterer en «right to be informed», og i dette ligger en generell forklaring av systemet.[229]

Wachter m.fl. fikk et kritisk tilsvar fra Andrew Selbst og Julia Powels.[230] Selbst og Powels deler sin kritikk i to. De er kritiske til lovtolkningen og vektingen av rettskildene, blant annet at Wachter m.fl. ikke på noe tidspunkt adresserer «[meningsfull] informasjon om den underliggende logikken».[231] Selbst og Powels er også kritiske til det analytiske rammeverket som Wachter m.fl. benytter. De påpeker at rammeverket er en teoretisk konstruksjon som bygger på en rekke implisitte antakelser om teknologien.[232] Dette innebærer at rammeverket faktisk ikke stemmer med hvordan datamaskiner fungerer. Selbst og Powels påpeker at datamaskiner er forutsigbare. I den grad det er mulig å få en generell forklaring av algoritmen, vil det i prinsippet ikke være noen forskjell mellom en generell forklaring og en spesifikk forklaring.[233]

Med en slik diskusjon i litteraturen kunne man håpet på at Artikkel 29-gruppen i sine retningslinjer ville adressere dette spørsmålet på en klar og entydig måte. Gruppen er kjent med diskusjonen, og i vedlegg 3 nevnes Wachter m.fl.[234] som litteratur som har blitt tatt i betraktning ved utformingen av retningslinjene.[235] Artikkel 29-gruppens uttalelser på dette punktet er imidlertid vage og lite konsekvente.

Det naturlige utgangspunktet i retningslinjene vil være hva Artikkel 29-gruppen uttaler i tilknytning til artikkel 15 nr.1 bokstav h. Her uttales det at «Article 15(1)(h) says that the controller should provide the data subject with information about the *envisaged consequences* of the processing, rather than an explanation of a *particular* decision.»[236] Sitatet i seg selv taler klart for at det ikke skal gis spesifikke forklaringer. Den logiske konsekvensen av dette må da bli at det bare skal gis generelle forklaringer. Samtidig er dette sitatet fra Artikkel 29-gruppen lite overbevisende. Forklaringen av en spesifikk avgjørelse settes opp mot informasjon om «de forventede konsekvensene»[237] av en slik behandling. En slik

228 Personvernforordningen artikkel 13 nr. 2 bokstav f, artikkel 14 nr. 2 bokstav g, artikkel 15 nr. 1 bokstav h og artikkel 22 nr. 2 og nr. 3.
229 Wachter (2017) s. 90.
230 Selbst (2017) s. 233–242.
231 Selbst (2017) s. 241.
232 Selbst (2017) s. 238.
233 Selbst (2017) s. 239.
234 Wachter (2017) s. 76–99.
235 A29WP (2018a) s. 37.
236 A29WP (2018a) s. 27.
237 Personvernforordningens artikkel 15 nr. 1 bokstav h.

motsetning har ingen støtte i ordlyden. Den norske oversettelsen sier: «[meningsfull] informasjon om den underliggende logikken samt om betydningen og de forventede konsekvensene av en slik behandling for den registrerte»[238] (min utheving). Artikkel 29-gruppen tar riktignok utgangspunkt i den engelske språkversjonen, men denne bruker heller ikke en formulering som kan begrunne deres motsetning. Her brukes uttrykket «as well as»[239] der den norske bruker «samt». Artikkel 29-gruppen synes å mene at fortalens avsnitt 63 kan begrunne deres standpunkt.[240] I fortalens avsnitt 63 er det imidlertid ingen ting som gir uttrykk for at informasjon om den «underliggende logikken» bare er spesifikk informasjon eller at den skal nedprioriteres til fordel for informasjon om «de forventede konsekvensene».

Artikkel 29-gruppen uttaler også i tilknytning til artikkel 15 nr.1 bokstav h at den registrerte har krav på generell informasjon om faktorene som er tatt i betraktning ved avgjørelsen, og deres vekt på et aggregert nivå.[241] (se punkt 5.3.2)

Det er altså to uttalelser fra Artikkel 29-gruppen som kan tyde på at det ikke skal gis en spesifikk forklaring. Særlig den første trekker i denne retningen. Til tross for dette har retningslinjene flere uttalelser som indikerer at «[meningsfull] informasjon» omfatter informasjon som er karakteristisk for forklaringer av spesifikke avgjørelser. Disse er omtalt i tilknytning til hvilken informasjon som normalt er meningsfull informasjon, se punkt 5.3.2.

Når både ordlyden, fortalen og retningslinjene holdes opp mot hverandre, kan ikke «[meningsfull] informasjon om den underliggende logikken» avgrenses til bare å gjelde en generell forklaring. Først og fremst gir ikke ordlyden grunnlag for en slik avgrensning. Dette er klart den mest tungtveiende rettskilden på dette området. Fortalen gir videre uttrykk for at det skal gis en spesifikk forklaring. Når Artikkel 29-gruppens retningslinjer er inkonsekvente og uklare på dette punktet, kan ikke disse tas til inntekt for et slikt skille. Muligheten for at det skal gis en spesifikk forklaring harmonerer også best med formålet bak innsynsbestemmelsen, ettersom en spesifikk forklaring trolig best fremmer tillitshensynet. Det harmonerer også med kravet om at informasjonen skal presenteres på en forståelig måte.

238 Personvernforordningens artikkel 15 nr. 1 bokstav h.
239 Personvernforordningen (engelsk) artikkel 15 nr. 1 bokstav h.
240 A29WP (2018a) s. 27.
241 A29WP (2018a) s. 27.

5.3.6 Forholdet til ugjennomsiktige maskinlæringsalgoritmer

Maskinlæring skaper særlige utfordringer når det gjelder innsyn i den «underliggende logikken». Den tradisjonelle programmeringen innebærer at programmene er skrevet av mennesker for maskiner, mens maskinlæringen gir programmer som er skrevet av maskiner for maskiner. Begge tilnærmingene kan gi svært komplekse dataprogrammer. Tradisjonell programmeringen er mulig å forstå for et menneske, selv om en kanskje må være ekspert på området. Modellene som visse maskinlæringsalgoritmer returnerer vil derimot være umulig å forstå. Disse modellene er så kompliserte at selv om det finnes en underliggende logikk, må modellene betegnes som ugjennomsiktige.[242]

Maskinlæring er ikke en bestemt ting (se punkt 3.3.1). Det finnes mange forskjellige maskinlæringsalgoritmer. Noen av disse er transparente, slik som for eksempel lineær regresjon, logistisk regresjon og beslutningstrær.[243] Andre maskinlæringsalgoritmer, slik som nevrale nett,[244] er ugjennomsiktige. En maskinlæringsmodell basert på et nevralt nett, vil i utgangspunktet ikke kunne vise de avgjørende momentene i en konkret sak. Eksempelvis er det ikke mulig å se om kjønn eller etnisitet er utslagsgivende ved avslag på en lånesøknad av en datamaskin bygget på et nevralt nett.

På denne bakgrunnen er det lett å tenke at en bare bør bruke transparente maskinlæringsalgoritmer. Maskinlæringsalgoritmer som nevrale nett har imidlertid vist seg nøyaktige og kraftige i dagens maskinlæring.[245]

Ugjennomsiktige maskinlæringsalgoritmer må vurderes særskilt i lys av innsynsbestemmelsen i artikkel 15 nr. 1 bokstav h. Spørsmålet er hvordan en ved tolkningen av «[meningsfull] informasjon om den underliggende logikken» skal forholde seg til at visse former for automatisert behandling ikke kan gi den informasjonen som i utgangspunktet anses som meningsfull informasjon. Det kan stilles spørsmål ved om det er grunnlag i rettskildene for å innfortolke et unntak i «[meningsfull] informasjon» for ugjennomsiktige maskinlæringsprogrammer.

Artikkel 29-gruppen nevner allerede i innledningen at maskinlæring kan være utfordrende fra et personvernperspektiv.[246] Dette gjentas også når «[meningsfull] informasjon om den underliggende logikken»[247] omtales i tilknytning til

242 Burrell (2016) s. 5–10.
243 Molnar (2019) punkt 4.
244 Burrell (2016) s. 5–7 og Datatilsynet (2018) s. 13.
245 Kashyap (2017) s. 124 og eksempelvis TensorFlow (2019).
246 A29WP (2018a) s. 5.
247 Retningslinjene er på engelsk, og bruker den engelske formuleringen.

artikkel 13 og 14.[248] I sine «good practice recommendations» gir Artikkel 29-gruppen uttrykk for at «Instead of providing a complex mathematical explanation about how algorithms or machine-learning work, the controller should consider using clear and comprehensive ways to deliver the information to the data subject».[249] Sitatet er til forveksling likt sitatet som er nevnt i punkt 5.3.3. Det er nok grunn til å lese sitatet på samme måte, nemlig at Artikkel 29-gruppen primært tar sikte på å unngå at den registrerte blir overlesset med kompleks informasjon. Det synes ikke å gi uttrykk for hva konsekvensen av ugjennomsiktige maskinlæringsalgoritmer bør være.

Unntak for ugjennomsiktige maskinlæringssystemer harmonerer dessuten dårlig med de øvrige rettskildene. Fortalen til personvernforordningen gir i avsnitt 15 uttrykk for at personvernforordningen skal være teknologinøytral. Dette taler klart for at forordningens bestemmelser skal gjelde på samme måte overfor alle former for automatisert behandling, uavhengig av den valgte teknologien. Formålene med innsynsbestemmelsen understøtter dette. Selv om det kanskje kan være teknologiske og forretningsmessige gevinster ved å bruke kraftige, men ugjennomsiktige maskinlæringsalgoritmer, strider det med tanken på åpenhet og tillit å innfortolke et slikt unntak i artikkel 15 nr. 1 bokstav h. Denne typen avgjørelser kan ha stor betydning for den registrerte. For mindre inngripende avgjørelser legger ikke denne innsynsbestemmelsen begrensninger på hvilken informasjon det må være mulig å hente ut.

Oppsummert gir ikke rettskildene grunnlag for å innfortolke et unntak i «[meningsfull] informasjon» for ugjennomsiktige maskinlæringssystemer. Den logiske konsekvensen av at det ikke er mulig å gi slik informasjon som den registrerte i utgangspunktet har krav på etter artikkel 15 nr. 1 bokstav h, vil være at ugjennomsiktige maskinlæringsalgoritmer ikke kan benyttes til avgjørelser som nevnt i artikkel 22 nr. 1. Det er imidlertid viktig å understreke at dette først og fremst er et praktisk problem. Problemet ligger i at visse typer «[meningsfull] informasjon» ikke er mulig å gi. Det er ikke sikkert at det er noe galt med maskinlæringssystemet, det er bare ikke mulig å kontrollere hvorvidt det er tilfellet. Dette betyr samtidig at dersom det blir utviklet teknologi som kan gi denne informasjonen, legger ikke innsynet begrensning på at systemet kan benyttes til avgjørelser som nevnt i artikkel 22. «Interpretable machine learning» er et felt det forskes på,[250] så det er mulig at algoritmer som i dag er ugjennomsiktige, kan bli tilstrekkelig transparente i relativt nær fremtid.

248 A29WP (2018a) s. 25.

249 A29WP (2018a) s. 31.

250 Molnar (2019) med videre referanser. Bertani-Økland (2018) gir i sin presentasjon oversikt over noen verktøy for Interpretable Machine Learning. Datatilsynet (2018) s. 26 nevner også noen slike verktøy.

5.4 Finnes det en plikt til å ha dokumentasjon som gir uttrykk for meningsfull informasjon om den underliggende logikken?

5.4.1 Problemstillingen

Etter å ha klarlagt hva som ligger i vilkåret «[meningsfull] informasjon om den underliggende logikken»[251] er det relevant å spørre om den behandlingsansvarlige har en plikt til å ha et dokument som gir uttrykk for denne informasjonen. Ettersom «[meningsfull informasjon] tar utgangspunkt i hva som er meningsfull informasjon for den registrerte, vil en slik dokumentasjon måtte basere seg på hva som normalt vil være meningsfull informasjon (se punkt 5.3.2). Begrepet dokumentasjon er i denne sammenhengen ikke begrenset til et fysisk dokument. Det kan også omfatte alternative tekniske løsninger og fremstillinger. Dokumentasjon kan tjene mange formål. I denne oppgaven er spørsmålet om det finnes dokumentasjon som kan ivareta den registrertes behov for innsyn.

Hvorvidt det foreligger en dokumentasjonsplikt er et spørsmål som må antas å ha nokså stor praktisk betydning for den registrerte. En ting er hva den registrerte har krav på. En annen ting er hvorvidt den registrerte faktisk får denne informasjonen. Dersom det ikke finnes en plikt til å ha dokumentasjon som gir uttrykk for «[meningsfull] informasjon om den underliggende logikken», er det vanskeligere for den registrerte å realisere rettigheten i artikkel 15 nr. 1 bokstav h. En dokumentasjonsplikt vil også gi den behandlingsansvarlig et utgangspunkt for innebyggede løsninger etter artikkel 25.

5.4.2 Finnes det en dokumentasjonsplikt i personvernforordningen?

Artikkel 15 nr. 1 bokstav h lest i sammenheng med artikkel 12 nr. 2 kan være et mulig grunnlag for en dokumentasjonsplikt. Artikkel 12 nr. 2 sier at «Den behandlingsansvarlige skal legge til rette for at den registrerte kan utøve sine rettigheter i henhold til artikkel 15-22». Utforming av dokumentasjon med «[meningsfull] informasjon om den underliggende logikken» kan tenkes å være en mulig tilrettelegging etter artikkel 12 nr. 2. Samtidig er bestemmelsen nokså generelt utformet. Den synes å være for generell til at det kan utledes en dokumentasjonsplikt.[252]

Artikkel 24 er den første bestemmelsen i kapittelet om den behandlingsansvarliges plikter. Bestemmelsens nr. 1 gir uttrykk for at den behandlingsansvarlige skal «gjennomføre egnede tekniske og organisatoriske tiltak for å sikre og påvise at behandlingen utføres i samsvar med denne forordning». Dersom en ser denne bestemmelsen i sammenheng med artikkel 5 nr. 1 bokstav a, gir bestemmelsen

251 Personvernforordningen artikkel 15 nr.1 bokstav h.

252 Se også Schartum (2018a) s. 278.

uttrykk for at den behandlingsansvarlige må ha tilstrekkelig dokumentasjon til å kunne «påvise» at behandlingen skjer på en «lovlig, rettferdig og åpen måte». Dette kan nok tas til inntekt for at den behandlingsansvarlige må ha slik informasjon som artikkel 15 nr. 1 bokstav h gir anvisning på. Samtidig er også denne bestemmelsen generelt utformet, slik at det er vanskelig å utlede en spesifikk plikt til å ha «[meningsfull] informasjon om den underliggende logikken».

Den behandlingsansvarlige skal vurdere personvernkonsekvenser for visse typer automatisert behandling etter artikkel 35 nr.1, jf. artikkel 35 nr. 3 bokstav a. Denne vurderingen skal minst inneholde «en systematisk beskrivelse av de planlagte behandlingsaktiviteter», jf. artikkel 35 nr. 7. Selv om bestemmelsen oppstiller en form for dokumentasjonsplikt, synes den ikke å gi et tilstrekkelig presist uttrykk for en dokumentasjonsplikt for «[meningsfull] informasjon om den underliggende logikken».

Den behandlingsansvarlige skal etter artikkel 22 nr. 2 og nr. 3 kunne sørge for «menneskelig inngripen fra den behandlingsansvarlige». Personen som kontrollerer den automatiserte avgjørelsen skal vurdere «all the relevant data».[253] Det er nærliggende å tenke at den behandlingsansvarlige må ha noe dokumentasjon for at menneskelig inngripen skal være mulig. Likevel synes også denne bestemmelsen å være for generell til at det kan oppstilles en dokumentasjonsplikt.

Samlet synes personvernforordningen å gi uttrykk for flere dokumentasjonsplikter. Det synes imidlertid ikke som om personvernforordningen oppstiller en dokumentasjonsplikt for «[meningsfull] informasjon om den underliggende logikken». En slik plikt er heller ikke nevnt i fortalen[254] eller av Artikkel 29-gruppen.

5.4.3 Teknisk dokumentasjon av datamaskinprogrammer

Ved utviklingen av datamaskinprogrammer utarbeides det ofte teknisk dokumentasjon.[255] Teknisk dokumentasjon brukes her som en samlebetegnelse på dokumentasjon som følger et datamaskinprogram og som kan gi uttrykk for hvordan programmet fungerer og hvordan det skal brukes. Jeg kjenner ikke til at det eksisterer en plikt til å utarbeide slik dokumentasjon, eller retningslinjer for slik dokumentasjon som er allment anerkjente i programvareutviklingsmiljøer. Teknisk dokumentasjon vil nok sjelden være utformet for å ivareta behovet for innsyn. Det er nok heller tiltenkt som veiledning for teknologer som skal

253 A29WP (2018a) s. 27.

254 Relevante avsnitt ville vært avsnitt 58 og 59.

255 Eksempelvis Django (2019), Oracle (2019) og Electron (2019).

bruke, feilsøke eller implementere det aktuelle programmet i egne datamaskinprogrammer. Hvorvidt slik teknisk dokumentasjon kan gi «[meningsfull] informasjon om den underliggende logikken», avhenger av innholdet og utformingen av den aktuelle dokumentasjonen.

5.4.4 Rettslig dokumentasjon av datamaskinprogrammer

Rettslig dokumentasjon er en dokumentasjon som er aktuell for datamaskinprogrammer som tar avgjørelser på bakgrunn av rettsregler. Dette er særlig aktuelt der den offentlige forvaltning bruker helautomatiserte avgjørelser i offentlig myndighetsutøvelse. Fremstillingen i dette punktet tar derfor utgangspunkt i dette.

Det finnes ikke i dag en alminnelig plikt å dokumentere det rettslige innholdet i den automatiserte behandlingen.[256] I forslaget til ny forvaltningslov og forslaget til ny arkivlov er det imidlertid foreslått en slik plikt.[257] Arkivlovutvalgets forslag til § 10 (1) oppstiller noen rammer for hva slik rettslig dokumentasjon kan inneholde. Det er særlig grunn til å nevne denne bestemmelsens bokstav c som sier at det skal dokumenteres «hvilke behandlingsregler som er utledet av rettsreglene og som er styrende for vedtakene».[258] For en helautomatisert avgjørelse som tas på bakgrunn av rettsregler, vil de utledede behandlingsreglene være den «underliggende logikken». Det er disse behandlingsreglene som implementeres i datamaskinprogrammet og disse behandlingsreglene som utgjør algoritmen. En slik dokumentasjon kan utarbeides på flere måter.[259] En praktisk tilnærming Schartum foreslår, er å få bekreftet at det er samsvar mellom den rettslige kravspesifikasjonen til datamaskinprogrammet og hvordan disse rettsreglene er implementert i datamaskinprogrammet.[260] Med rettslig kravspesifikasjon menes spesifiseringer av ferdig tolkede rettsregler som skal implementeres i datamaskinprogrammet.[261] Kravspesifikasjonen bør ideelt sett være uttrykt på et delvis formalisert språk, slik som pseudokode, figurer og likende.[262] Schartums tilnærming synes også å være utgangspunktet til forvaltningslovutvalget og utgangspunktet til arkivlovutvalget.[263]

Dersom det vedtas en dokumentasjonsplikt, vil slik rettslig dokumentasjon trolig være den primære kilden til «informasjon om den underliggende logikken»

256 Schartum (2018a) s. 278.
257 NOU 2019:5 § 12 s. 20 og NOU 2019:9 § 10 s. 18.
258 NOU 2019:9 § 10 s. 18.
259 Schartum (2018a) s. 283 flg.
260 Schartum (2018a) s. 211–212 og 283.
261 Schartum (2018a) s. 213.
262 Schartum (2018a) s. 214.
263 NOU 2019:5 s. 265 og NOU 2019:9 s. 156 note 12. Schartum er medlem av Arkivlovutvalget.

for forvaltningsorganene. Ettersom personvernforordningen artikkel 15 nr. 1 bokstav h er en EU-regel, vil nok ikke en dokumentasjonsplikt i norsk lov være en tilstrekkelig tungtveiende rettskilde til at bestemmelsen alltid skal tolkes slik at rettslig dokumentasjon alltid tilsvarer kravet etter «[meningsfull] informasjon om den underliggende logikken». Rettslig dokumentasjon vil nok imidlertid som regel oppfylle vilkåret i artikkel 15 nr. 1 bokstav h. Så fremt den rettslige dokumentasjonen er tilstrekkelig pedagogisk eller fremlegges tilstrekkelig pedagogisk, vil den være «[meningsfull] informasjon om den underliggende logikken».

6 Avslutning og rettspolitiske vurderinger

Retten til «[meningsfull] informasjon om den underliggende logikken» i artikkel 15 nr. 1 bokstav h gir i utgangspunktet den registrerte et effektivt verktøy for å kontrollere at avgjørelsen er lovlig og rettferdig, jf. artikkel 5 nr. 1 bokstav a. En automatisert avgjørelse etter artikkel 22 nr. 1 er forutsigbar.[264] Derfor gir informasjon om «den underliggende logikken» et godt og presist grunnlag for å forstå avgjørelsen. En helautomatisert avgjørelse kan faktisk være vel så gjennomsiktig som en ikke-automatisert avgjørelse. Innsyn i sakens dokumenter ved ikke-automatiserte avgjørelser gir ikke nøyaktig informasjon om saksbehandlerens tankeprosesser.

En effektiv innsynsrett forutsetter imidlertid at informasjonen formidles på en måte som er meningsfull for den registrerte. Innebygde løsninger for å formidle informasjonen[265] gir etter mitt syn et godt utgangspunkt for en transparent bruk av automatiserte avgjørelser. Slike innsynsløsninger må riktignok utvikles, noe som krever ressurser. Samtidig kan det være grunn til å tro at behandlingsansvarlige får færre innsynsbegjæringer. Dette kan være ressursbesparende. En velutviklet innsynsløsning kan dessuten være med på å øke tilliten til den behandlingsansvarlige.[266] Dette er viktig for både private og offentlige aktører.[267]

En effektiv innsynsrett forutsetter også at det er mulig å forklare «den underliggende logikken». Rettskildene gir ikke adgang til å gjøre unntak fra artikkel 15 nr.1 bokstav h for ugjennomsiktige maskinlæringsalgoritmer.[268] Dette medfører at den behandlingsansvarlige i praksis ikke kan benytte ugjennomsiktige maskinlæringsalgoritmer til avgjørelser etter personvernforordningen artikkel 22 nr. 1 og 4. Dette er etter mitt syn en riktig løsning. Samtidig kan det være gode grunner til å bruke kraftige, men ugjennomsiktige, maskinlæringsalgoritmer. Det kan blant annet være muligheter for effektivisering og ressursbesparing. Dette kan tilsi at en bør tenke annerledes om gjennomsiktighet for slike algoritmer. Det er for eksempel mulig å se for seg en klagebehandling som et alternativ til innsyn.[269] Man må imidlertid være sikker på at vilkårene i artikkel 5 nr. 1

264 Se punkt 4.6.
265 Se punkt 5.3.2.
266 Se punkt 3.2.
267 Personvernforordningens fortale avsnitt 6 og offentliglova § 1.
268 Se punkt 5.3.6.
269 Schartum (2018b) s. 7 sier at det kan hevdes at klagesaksbehandling reduserer behovet for vern etter art. 22 nr. 1, men konkluderer raskt med at rettskildene ikke kan tas til inntekt for dette.

bokstav a blir oppfylt ved alternative løsninger. Innsynsbestemmelser er i dag vel etablerte rettsikkerhetsverktøy. En bør ikke gå vekk fra disse før en er sikker på at alternativene er bedre. Forhåpentligvis kan videre forskning på «interpretable machine learning»[270] gjøre ugjennomsiktige algoritmer mer gjennomsiktige.

Den største utfordringen for en effektiv innsynsrett synes å være hensynet til forretningshemmeligheter. Personvernforordningen gir den behandlingsansvarlige adgang til å unnta forretningshemmeligheter fra innsyn.[271] Rettskildene kan riktignok tyde på at det skal foretas en interesseavveining. I første omgang vil den behandlingsansvarlige eller en representant for den behandlingsansvarlige være rettsanvenderen som skal foreta denne interesseavveiningen. Det er grunn til å tro at dette kan påvirke interesseavveiningen i favør av den behandlingsansvarlige. Samtidig kan det tenkes økt digitalisering gjør at potensielle kunder stiller større krav til åpenhet. For behandlingsansvarlige kan det derfor tenkes at åpne løsninger i seg selv har en forretningsmessig verdi. Dette kan kanskje medføre at behandlingsansvarlige strekker seg lengere for å gi «[meningsfull] informasjon om den underliggende logikken».

Offentlig forvaltning vil nok ikke kunne nekte innsyn på grunn av forretningshemmeligheter ved offentlig myndighetsutøvelse.[272] Her tas nok de automatiserte avgjørelsene med størst betydning for den registrerte. Forarbeidene til ny forvaltningslov og arkivlov foreslår en plikt til å dokumentere det rettslige innholdet i datamaskinprogrammet som skal ta avgjørelsen.[273] Hvis dette vedtas, har den offentlige forvaltning et godt utgangspunkt for å gi informasjon til den registrerte. Dette gir også et godt utgangspunkt for innebyggede løsninger, jf. artikkel 25. Dermed synes «[meningsfull] informasjon om den underliggende logikken»[274] å være et effektivt verktøy for å kontrollere at avgjørelsen er lovlig og rettferdig ved offentlig myndighetsutøvelse.[275]

270 Se punkt 5.3.6.
271 Se punkt 5.3.4.
272 Se punkt 5.3.4.
273 se punkt 5.4.4.
274 Artikkel 15 nr. 1 bokstav h.
275 Artikkel 5 nr. 1 bokstav a.

Litteraturliste

Litteratur

Arnesen (2018) — Arnesen, Finn og Halvard Haukeland Fredriksen, Hans Petter Graver, Ola Mestad, Christoph Vedder. *Agreement on the European Economic Area – A Commentary*, 1. utg., Baden-Baden/Munchen/Oxford/Portland/Oslo:C.H. Beck/Nomos/Hart/Universitetsforlaget, 2018.

Arnesen (2015) — Arnesen, Finn. "Om den babelske vending i norsk rett", *Lov og Rett* LOR-2015-344 (2015), 344-362. (Lest på Lovdata: https://lovdata.no/pro/#document/JUS/arnesen-f-2015-01).

Athow (2014) — Athow, Desire. *Pentium FDIV: The processor bug that shook the world.* (2014), https://www.techradar.com/news/computing-components/processors/pentium-fdiv-the-processor-bug-that-shook-the-world-1270773 [Sitert 22.04.2019].

Bertani-Økland (2018) — Bertani-Økland, Marco. Interpretable Machine Learning: Techniques to explain black box models. [videoklipp], (13.09.2018) [https://vimeo.com/album/5419780/video/289851689].

Boe (2010) — Boe, Erik Magnus. *Innføring i juss – Juridisk tekning og rettskildelære*, 3. utg., Oslo:Universtitetsforlaget, 2010.

Borgesius (2018) — Borgesius, Frederik Zuiderveen. "Discrimination, artificial intelligence, and algorithmic decision-making", *Report for the Anti-discrimination department of the Council of Europe,* (2018), s. 1–49 (tilgjengelig på https://rm.coe.int/discrimination-artificial-intelligence-and-algorithmic-decision-making/1680925d73).

Burrell (2016) — Burrell, Jenna. "How the machine 'thinks': Understanding opacity in machine learning algorithms", *Big Data & Society* January-June 2016 (2016), s. 1–12 (tilgjengelig på http://dx.doi.org/10.1177/2053951715622512).

Bygrave (2019) Bygrave, Lee A. ”Minding the Machine v2.0: The EU General Data Protection Regulation and Automated Decision Making”, *University of Oslo Faculty of Law Research Paper* No. 2019-01 (2019), s. 1–18 (tilgjengelig på http://dx.doi.org/10.2139/ssrn.3329868).

Casey (2018) Casey, Bryan og Ashkon Farhangi, Roland Vogl. ”Rethinking Explainable Machines: The GDPR's 'Right to Explanation' Debate and the Rise of Algorithmic Audits in Enterprise”, *Berkeley Technology Law Journal* Forthcoming (2018), s.1–50, tilgjengelig på https://ssrn.com/abstract=3143325 [sitert 13.01.2019].

Django (2019) Django. Django documentation. (2019), https://docs.djangoproject.com/en/2.1/ [Sitert 28.03.2019].

Dvergsdal (2018a) Dvergsdal, Henrik. *aggregat – IT*. (2018), https://snl.no/aggregat_-_IT [Sitert 06.03.2019].

Dvergsdal (2018b) Dvergsdal, Henrik. *pseudokode*. (2018), https://snl.no/pseudokode [Sitert 28.03.2019].

Eckhoff (2010) Eckhoff, Torstein og Eivind Smith. *Forvaltningsrett*, 9. utg., Oslo:Universtitetsforlaget, 2010.

Electron (2019) Electron. *Electron Documentation*. (2019), https://electronjs.org/docs [Sitert 28.03.2019].

Englander (2014) Englander, Irv. *The Architecture of computer hardware, system software, and networking: an information technology approach*, 5. utg., Hoboken:Wiley, 2014.

Fredriksen (2012) Fredriksen, Halvard Haukeland og Gjermund Mathisen. *EØS-rett*, 1. utg., Bergen:Fagbokforlaget, 2012.

Goodman (2017) Goodman, Bryce og Seth Flaxman. ”European Union Regulations on Algorithmic Decision-Making and a “Right to Explanation””, *AI Magazine* Vol 38, No 3 (2017), s.1–9 (tilgjengelig på http://dx.doi.org/10.1609/aimag.v38i3.2741).

Intel (2016) Intel. *Artificial Intelligence and Machine Learning: How Computers Learn*. (2016), https://iq.intel.com/artificial-intelligence-and-machine-learning/ [Sitert 06.02.2019].

Kaminski (2018) Kaminski, Margot E. ”The Right to Explanation, Explained”, *U of Colorado Law Legal Studies Research Paper* No. 18-24 (2018), s. 1–25 (tilgjengelig på http://dx.doi.org/10.2139/ssrn.3196985).

Kashyap (2017) Kashyap, Patanjali. *Machine Learning for Decision Makers – Cognitive Computing Fundamentals for Better Decision Making*, 1. utg., California:Apress, 2017 https://doi-org.ezproxy.uio.no/10.1007/978-1-4842-2988-0

Kjos (2009) Kjos, Bård (red.). *Informasjonsteknologi*, 6. utg., Trondheim:Tapir, 2009.

Larsen (2018) Larsén, Linus. ”Nu regleras artificiell intelligens på allvar ur ett dataskyddsperspektiv”, *Lov og Data* Nr. 133/ Nr. 1/2018 (2018), s. 17–20 (PDF-versjon hentet fra Lovdata).

Lecher (2018) Lecher, Colin. *What Happens When An Algorithm Cuts Your Health Care.* (2018), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy [Sitert 24.02.2019].

Lånekassen (2017) Lånekassen, v/Severin Hansen. *Sluttrapport fra konseptutredning av muligheter for effektivisering ved bruk av kunstig intelligens.* (2017), https://lanekassen.no/Global/Om%20organisasjonen/Sluttrapport%20konseptutredning%20kunstig%20intelligens%20L%C3%A5nekassen%202017.pdf [Sitert 03.04.2019].

Lånekassen (2018) Lånekassen, v/ Liv Simonsen og Severin Hansen. *”Kunstig intelligens i Lånekassen, slides til foredrag på seminaret ”Innovasjon i eget hus” i regi av Difi”.* (2018), https://www.difi.no/sites/difino/files/8_liv_simonsen_og_severin_hanssen_-_kunstig_intelligens_i_lanekassens.pdf [Sitert 16.01.2019].

Lånekassen (2019) Lånekassen. *Lånekassen bruker kunstig intelligens i bokontroll.* (2019), https://www.lanekassen.no/nb-NO/Om_Lanekassen/media-/nyheter1/Nyheter/lanekassen-bruker-kunstig-intelligens-i-bokontroll/ [Sitert 23.02.2019].

Mendoza og Bygrave (2017) — Mendoza, Isak og Lee A. Bygrave. "The Right Not to Be Subject to Automated Decisions Based on Profiling", *University of Oslo Faculty of Law Research Paper* No. 2017-20 (2017), s. 1–22 (tilgjengelig på https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2964855).

Molnar (2019) — Molnar, Christoph. *Interpretable machine learning. A Guide for Making Black Box Models Explainable*, 1 utg., Christoph Molnar/GitHub:Ukjent sted, 2019 https://christophm.github.io/interpretable-ml-book/

Oracle (2019) — Oracle (Java). *JDK 12 Documentation*. (2019), https://docs.oracle.com/en/java/javase/12/ [Sitert 28.03.2019].

PC-Mag (2019) — PC-Mag. *Encyclopedia: Definition of compiler*. (2019), https://www.pcmag.com/encyclopedia/term/40105/compiler [Sitert 20.02.2019].

Pound (2017) — Pound, Mike. Dijkstra's Algorithm – Computerphile. [videoklipp], (04.01.2017) [https://www.youtube.com/watch?v=GazC3A4OQTE].

Schartum og Bygrave (2016) — Schartum, Dag Wiese og Lee A. Bygrave. *Personvern i informasjonssamfunnet – En innføring i vern av personopplysninger*, 3. utg., Bergen:Fagbokforlaget, 2016.

Schartum (2018a) — Schartum, Dag Wiese. *Digitalisering av offentlig forvaltning – Fra lovtekst til programkode*, 1. utg., Oslo:Fagbokforlaget, 2018.

Schartum (2018b) — Schartum, Dag Wiese. "Personvernforordningen og helt automatiserte avgjørelser innen forvaltningsretten", *Lov og Data* Nr. 134/Nr. 2/2018 (2018), s. 4–7 (PDF-versjon hentet fra Lovdata).

Sejersted (2011) — Sejersted, Fredrik og Finn Arnesen, Ole-Andreas Rognstad, Olav Kolstad. *EØS-rett*, 3. utg., Oslo:-Universtitetsforlaget, 2011

Selbst (2017) — Selbst, Andrew D. og Julia Powles. "Meaningful information and the right to explanation", *International Data Privacy Law* Vol. 7, No. 4 article 233 (2017), s. 233–242, (tilgjengelig på https://ssrn.com/abstract=3039125).

SNL (2018a) Store Norske Leksikon, v/Johan F. Aarnes. *algoritme*. (2018), https://snl.no/algoritme [Sitert 28.03.2019].

SNL (2018b) Store Norske Leksikon, v/Thomas Gramstad. *åpen kildekode*. (2018), https://snl.no/åpen_kildekode [Sitert 20.04.2019].

Svensson (2008) Svensson, Martin og Joakim Söderberg. "Machine-learning technologies in telecommunications", *Ericsson Review* nr. 3 (2008), s. 29–33, (tilgjengelig på https://pdfs.semanticscholar.org/a367/f8cad03c1353e9fc36970e4cb-4b8edc21fc0.pdf).

TensorFlow (2019) TensorFlow. *Why TensorFlow – Case studies and mentions*. (2019), https://www.tensorflow.org/about/case-studies/ [Sitert 20.04.2019].

Wachter (2017) Wachter, Sandra og Brent Mittelstadt, Luciano Floridi. "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation", *International Data Privacy Law* Vol. 7, No. 2 (2017), s. 76–99 (tilgjengelig på http://dx.doi.org/10.2139/ssrn.2903469).

West (2018) West, Mark. A Practical(ish) Introduction to Data Science. [videoklipp], (13.09.2018) [https://vimeo.com/album/5419780/video/289705893].

Norske lover og forskrifter

1814 Kongerike Norges Grunnlov (Grunnloven) 17. mai 1814.

1967 Lov 10. februar 1967 nr. om behandlingsmåten i forvaltningssaker (forvaltningsloven).

1992 Lov 27. november 1992 nr. 10 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven).

2000 Lov 14. april 2000 nr. 31 om behandling av personopplysninger (personopplysningsloven).

2005 Lov 17. juni 2005 nr. 90 om mekling og rettergang i sivile tvister (tvisteloven).

2006 Lov 19. mai 2006 nr. 16 om rett til innsyn i dokument i offentleg verksemd (offentleglova).

2017 Lov 16. juni 2017 nr. 51 om likestilling og forbud mot diskriminering (likestillings- og diskrimineringsloven).

2018 Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

2018 Forskrift 15. juni 2018 nr. 38 om ikraftsetting av lov 15.juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

2018 Meddelelse 17. juli 2018 nr. 1195 om ikrafttredelse av lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

Andre norske rettskilder

Datatilsynet (2018) Datatilsynet. (2018) *Kunstig intelligens og personvern*, Januar 2018. [https://www.datatilsynet.no/globalassets/global/om-personvern/rapporter/rapport-om-ki-og-personvern.pdf] [Sitert 06.11.2018].

Irgens-Jensen (2019) Irgens-Jensen, Harald. (2019). *Høringssvar – Innspill til høringsnotat om forslag til ny lov om vern av forretningshemmeligheter*, 15.02.2019 [https://www.regjeringen.no/no/dokumenter/horing-om-utkast-til-ny-lov-om-vern-av-forretningshemmeligheter/id2620301/?uid=56c6aaec-4733-483b-b38f-612558f00e13] [Sitert 12.03.2019].

Justis- og beredskapsdepartementet (2018) Justis- og beredskapsdepartementet. (2018). *Høringsnotat – Høring om utkast til ny lov om vern av forretningshemmeligheter – gjennomføring av EUs forretningshemmelighetsdirektiv i norsk rett*, 26.11.2018 [https://www.regjeringen.no/contentassets/d1da66bb9e414ee28b41a95e993d1f90/horingsnotat-l955806.pdf] [Sitert 12.03.2019].

Kriminalomsorgen (2008)	Kriminalomsorgen. *Retningslinjer til straffegjennomføringsloven*. (2008), https://www.kriminalomsorgen.no/retningslinjer-til-straffegjennomfoeringsloven.411497.no.html [Sitert 23.04.2019].
NOU 2019:5	*Ny forvaltningslov — Lov om saksbehandlingen i offentlig forvaltning (forvaltningsloven).*
NOU 2019:9	*Fra kalveskinn til datasjø — Ny lov om samfunnsdokumentasjon og arkiver.*
Ot.prp.nr.92 (1998–1999)	*Om lov om behandling av personopplysninger (personopplysningsloven).*
Prop.56 LS (2017–2018)	*Lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.*

Rt. 2007 s. 257.

Forordninger, direktiver og traktater

Convention 108	Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. (ETS No.108. Strasbourg, 28/01/1981.)
Convention 108 +	Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (consolidatet text). (128th Session of the Committee of Ministers (Elsinore, Denmark, 17–18 May 2018)). Tilgjengelig på: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1
EMK	Konvensjon om beskyttelse av menneskerettighetene og de grunnleggende friheter, Roma 4. november 1950.

Forretnings-hemmelighets-direktivet	Dir 2016/943 DIRECTIVE (EU) 2016/943 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure.
Personvern-direktivet	Dir 95/46/EC Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.
Personvern-forordningen (dansk)	For 2016/679 EUROPA-PARLAMENTETS OG RÅDETS FORORDNING (EU) 2016/679 af 27. april 2016 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 (generel forordning om databeskyttelse).
Personvern-forordningen (engelsk)	For 2016/679 Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Personvern-forordningen (fransk)	For 2016/679 RÈGLEMENT (UE) 2016/679 DU PARLEMENT EUROPÉEN ET DU CONSEIL du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données).
Personvernf-orordningen (svensk)	For 2016/679 EUROPAPARLAMENTETS OCH RÅDETS FÖRORDNING (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmän data-skyddsförordning).

Personvern-forordningen (tysk)	For 2016/679 VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).
TEUV	Treaty on the Functioning of the European Union (Consolidated version 2016) (OJ C 202, 7.6.2016) [TEUV].

Rettspraksis fra EU

Case 215/88 Casa Fleischandels-GmbH v	ECLI:EU:C:1989:331.
Bundesanstalt fur landwirtscafliche Marktordung.	
Case 162/97 Criminal proceedings against Gunnar Nilsson,	ECLI:EU:C:1998:554.
Per Olov Hagelgren and Solweig Arrborn.	
Case 308/97 Guiseppe Manfredi v Regione Puglia.	ECLI:EU:C:1998:331.
Case 316/05 Nokia Corp v. Joacim Wardell.	ECLI:EU:C:2006:789.
Case 73/07 Tietosuojavaltuutettu v	ECLI:EU:C:2008:727.
Satakunnan Markkinaporssi Oy and Satamedia Oy.	

Andre EU-rettslige kilder

A29WP (2018a)	Article 29 Data Protection Working Party. (2018) *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679,* As last Revised and Adopted on 6 February 2018. [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612053] [Sitert 08.01.2019].

A29WP (2018b) Article 29 Data Protection Working Party. (2018) *Guidelines on transparency under Regulation 2016/679,* As last Revised and Adopted on 11 April 2018. [https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227] [Sitert 08.01.2019].

EDPB (2018) The European Data Protection Board. (2018) *Endorsement* 1/2018, 25.06.2018. [https://edpb.europa.eu/news/news/2018/endorsement-gdpr-wp29-guidelines-edpb_en] [Sitert 17.01.2019].

EØS-avtalens Protokoll 1 om gjennomgående tilpasning (hentet fra Lovdata).

EØS-tillegg (2018) EØS-tillegget til Den europeiske unions tidende, 25 årgang, nr. 46, 19.07.2018. Tilgjengelig på https://www.efta.int/sites/default/files/documents/eea-supplements/norwegian/2018-no/su-nr-46-no-19-07-2018.pdf