Dansk persondataret

Bent Ole Gram Mortensen (red.)

Dansk persondataret

Ex Tuto
PUBLISHING
www.extuto.com

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

Denne bog er udgivet i januar 2020 af Ex Tuto Publishing A/S. Grafisk tilrettelæggelse og sats af mere.info A/S, som har anvendt LibreOffice/Linux samt skrifterne Baskerville Original og Cronos designet af henholdsvis František Štorm i 2000 og Robert Slimbach i 1996. Jan Trzaskowski har stået for forlagsredaktion og Tove Møgelvang-Hansen har været ansvarlig for korrekturlæsning. Bogen er trykt på Munken Pure 100 g/m^2 af Narayana Press, der ligger på Gyllingnæs syd for Odder. Indbindingen er udført af Buchbinderei S.R. Büge GmbH i Celle. Bogen er fagfællebedømt.

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

Printed in Denmark 2020
ISBN 978-87-420-0033-5

Ex Tuto Publishing A/S
Toldbodgade 55, 1.
DK-1253 København K
www.extuto.com

MIX
Papir fra ansvarlige kilder
FSC® C010651
www.fsc.org

Udgivet med støtte fra
dreyersfond

FairPublishing

Kapiteloversigt

Kapitel 6

Oplysningskategorier og behandlingsbetingelser

Sten Schaumburg-Müller

6.1. Indledning

Et helt centralt element i persondataretten er kravet om hjemmel: Hvis en aktivitet er inden for persondatarettens brede område (se ovenfor kapitel 3), og hvis aktiviteten ikke er undtaget (se ovenfor kapitel 4), skal man have lov til at foretage den pågældende behandling. Sagt lidt mere teknisk: Behandlingen skal have hjemmel i en lovbestemmelse. Man skal altså ind i persondatarettens regler for at se, om man kan finde en bestemmelse, der giver mulighed for at foretage den behandling, man har tænkt sig at foretage. For private aktører er dette det modsatte af, hvad der normalt er tilfældet. Udgangspunktet i dansk ret er, at hvis en handling ikke er forbudt, så er den tilladt. Dette er helt åbenlyst i strafferetten: Her gælder det, at man kun kan straffes, hvis det udtrykkeligt følger af en straffebestemmelse.[1] Men i persondataretten er det anderledes: Hvis man er inden for persondatarettens dækningsområde, skal man have lov. Man skal kunne henvise til en bestemmelse, der muliggør, at man netop i dette tilfælde har ret til at foretage

1. Dette står tydeligt i straffelovens § 1: "Straf kan kun pålægges for et forhold, hvis strafbarhed er hjemlet ved lov, eller som ganske må ligestilles med et sådant."

netop den behandling, man påtænker (eller er i gang med at udføre eller allerede har udført).

Persondataretten inddeler personoplysninger i forskellige kategorier, og de forskellige kategorier opstiller ikke helt samme betingelser for at foretage en lovlig behandling. Det er derfor vigtigt, at man kan placere en oplysning i den rigtige kategori. Kategorierne behandles nedenfor i afsnit 6.3, henholdsvis særligt følsomme oplysninger i afsnit 6.3.1, almindelige oplysninger i afsnit 6.3.2, oplysninger om strafbare forhold i afsnit 6.3.3 og endelig to yderligere specifikke kategorier: CPR-numre og oplysninger om gæld i afsnit 6.3.4. Uden sådan kategorisering er det ikke muligt at finde den korrekte behandlingshjemmel.

Afsnit 6.6 omhandler herefter muligheden for at behandle oplysninger vedrørende strafbare forhold, og afsnit 6.4 ser på behandlingsbetingelser for "almindelige" personoplysninger.

Endelig i afsnit 6.7 behandles den persondatabehandling, der angår CPR-numre og oplysninger om gæld.

6.2. Behandling uden for persondataretten

Man skal være opmærksom på, at en del behandling af personoplysninger ikke falder ind under den almindelige persondataret. I sådanne tilfælde er det selvfølgelig uden betydning at kunne kategorisere en bestemt oplysning, eftersom man ikke behøver finde en behandlingsbetingelse. Den rent personlige eller familiemæssige behandling falder helt udenfor den persondataretlige regulering, strafferetlig efterforskning har sin egen regulering, og journalistisk og kunstnerisk behandling er stort set undtaget, mv. Der henvises til denne bogs kapitel 4 for nærmere detaljer.

6.3. Kategorier

Der findes forskellige kategorier af personoplysninger, og det er vigtigt at få placeret en oplysning i den rigtige kategori, eftersom mulighederne for lovlig behandling netop afhænger af, hvilken kategori af personoplysning der er tale om.

Helt overordnet er der to kategorier: de særlige oplysninger, ofte kaldet følsomme eller særligt følsomme, og resten, ofte blot kaldet almindelige oplysninger. Hertil kommer oplysninger om strafbare for-

hold, der er særskilt reguleret. Principielt hører oplysninger om strafbare forhold under de almindelige oplysninger, men netop fordi de er undergivet en særlig regulering, medtages de i denne fremstilling som en særskilt, tredje kategori.[2] Disse tre kategorier behandles nedenfor i afsnittene 6.3.1, 6.3.2, og 6.3.3. Hertil kommer nogle mere specifikke kategorier som CPR-numre og kreditoplysninger, ligesom forskellige områder er særligt reguleret. Det gælder nærmere bestemt retsinformationssystemer, videnskabelig og statistisk behandling, videregivelse til arkiv, særligt om ansættelsesforhold mv. Disse særligt regulerede områder behandles i afsnit 6.3.4.

6.3.1. Følsomme oplysninger

Kategorien "følsomme oplysninger" er en særligt kvalificeret kategori af personoplysninger, som er undergivet en strammere regulering end personoplysninger i almindelighed. Det hedder i GDPR artikel 9, stk. 1:

> "Behandling af personoplysninger om race eller etnisk oprindelse, politisk, religiøs eller filosofisk overbevisning eller fagforeningsmæssigt tilhørsforhold samt behandling af genetiske data, biometriske data med det formål entydigt at identificere en fysisk person, helbredsoplysninger eller oplysninger om en fysisk persons seksuelle forhold eller seksuelle orientering er forbudt."

Persondatarettens særlige reguleringsmåde træder her tydeligt frem: Behandling af denne kategori af personoplysninger er som udgangspunkt forbudt. Hertil kommer så en længere række undtagelser i stk. 2. Sagt på en anden måde skal man ned i stk. 2 for at finde en hjemmel til overhovedet at foretage en behandling af disse følsomme oplysninger. Som illustration kan nævnes, at det i udgangspunktet er forbudt at behandle oplysninger om personers politiske overbevisning. Man kunne her indvende, at det er mærkeligt, at man ikke må behandle oplysninger om en kendt folketingspolitikers politiske overbevisning. Men det

2. Efter tidligere dansk ret hørte oplysninger om strafbare forhold til en særlig kategori sammen med væsentlige sociale problemer og andre rent private forhold. Personoplysninger i denne kategori blev kaldt for semi-følsomme. Denne kategori eksisterer ikke længere.

må man netop også godt. Efter artikel 9, stk. 1, er det ganske vist forbudt at behandle de nævnte oplysninger, men stk. 2, litra e, lovliggør behandling, der "tydeligvis er offentliggjort af den registrerede".[3] En folketingspolitiker, og i det hele taget enhver, der stiller sin politiske opfattelse åbent til skue, må tåle at få netop denne type oplysning behandlet i alle mulige sammenhænge. Bemærk her, at der kan være andre regler, der begrænser behandlingen. Det kunne f.eks. være kravet om dataminimering og relevans efter GDPR artikel 5, stk. 1, litra c. Hvis man ejer en kiosk, og man jævnligt får besøg af en folketingspolitiker, der køber et par øl, har den pågældendes politiske overbevisning ikke umiddelbart nogen relevans. Man må gerne fortælle ude i baglokalet, at nu kom (NN) igen for at købe øl. Dette vil umiddelbart ikke være omfattet af persondataretten, da der er tale om ikke en ikke-automatisk persondatabehandling, der ikke er beregnet til et register. Men den følsomme oplysning, her om personens politiske overbevisning, bør ikke behandles i forbindelse med købet.[4]

Som kategori giver de særlige oplysninger ikke anledning til de store vanskeligheder. En oplysning om, at en bestemt person er "af afrikansk afstamning", "af nordisk type", "kineser" eller "født i Somalia og kommet til Danmark som 4-årig" er en oplysning om race og etnisk oprindelse. Der sondres ikke mellem race og etnisk oprindelse. Blot en af delene bliver oplyst, falder oplysningen i den særligt følsomme kategori. Desuden kan man sætte spørgsmålstegn ved, om begrebet "race" overhovedet giver mening. I betragtning 51 understreges det da også, at der med anvendelse af ordet "race" ikke gives tilslutning til nogen teori om, at menneskearten er opdelt i racer. Ideen er blot, at anvendes begrebet, falder oplysningen i den særlige kategori – hvorved erindres om, at en oplysning ikke behøver at være korrekt for at udgøre en oplysning i persondatarettens forstand (se herom kapitel 3, afsnit 3.3).

Politisk, religiøs eller filosofisk overbevisning indgår også i den særlige kategori. Især den første er relevant i forbindelse med individuelt rettede, politiske annoncer: Hvis man på baggrund af en persons adfærd, ikke mindst på nettet, mener at kunne udlede noget om den pågældendes politiske opfattelse, er der tale om en følsom oplysning,

3. Se nærmere om denne undtagelse nedenfor afsnit 6.5.
4. Se særskilt om profilering kapitel 3, afsnit 3.3.

hvis behandling skal følge reglerne i artikel 9.[5] En oplysning om, at en bestemt person går til fredagsbøn eller går til nadvers, udgør åbenlyst en oplysning om religiøs overbevisning, mens en oplysning om, at den pågældende "går i kirke", kan være, men ikke nødvendigvis er en følsom oplysning. Når "filosofisk overbevisning" er medtaget, skyldes, at også en stærk anti-religiøs overbevisning bør falde i den særlige kategori. At være "marxist" er både en politisk og en filosofisk overbevisning.

"Fagforeningsmæssigt tilhørsforhold" giver for så vidt sig selv, men man skal være opmærksom på, at der ikke behøver være tale om medlemskab. Det, at en bestemt person står udenfor en (relevant) fagforening, er også en følsom personoplysning.

Genetiske data kommer formentlig til at spille en stigende rolle inden for personligt designet medicin. Ideen med at kategorisere disse oplysninger som særligt følsomme er selvfølgelig ikke at hindre udviklingen af en bedrevirkende medicin, men at underlægge behandlingen af sådanne oplysninger de skrappere krav i artikel 9. Det samme kan siges at gælde både for biometriske data som f.eks. fingeraftryk, ansigtsgenkendelse, gang-genkendelse osv. og for helbredsoplysninger. Hvad de sidste angår, kan man overveje, om der er en bagatelgrænse: Hvad med forkølelser, forstuvede tæer, dårlige tænder og lignende? Det rigtigste er formentligt at betragte dem som de helbredsoplysninger, de er, og herefter vurdere behandlingen efter bestemmelserne i stk. 2. Går man på arbejde eller i skole med en bullen finger, eller har man briller på offentligt, har man offentliggjort en helbredsoplysning, jf. GDPR artikel 9, stk. 2, litra e (nærmere behandlet nedenfor afsnit 6.5.5). Om oplysningen herefter må behandles, afhænger af artikel 5 om dataminimering mv.

Oplysninger både om seksuelle forhold og om seksuel orientering udgør også følsomme oplysninger. Det at være kærester, indebærer normalt et seksuelt forhold, og en sådan oplysning er derfor særligt følsom. Det samme gælder det at være gift, mens det at indgå ægteskab er en offentlig handling, jf. igen reglen i artikel 9, stk. 2, litra e. Også sex med sig selv er et seksuelt forhold, og oplysninger herom falder under

5. Om profilering og afledte oplysninger, se kapitel 3, afsnit 3.

artikel 9. Sex med dyr er nu kriminaliseret,[6] og oplysninger herom falder derfor under kategorien strafbare forhold (behandlet nedenfor afsnit 6.3.2). Oplysninger om en bestemt persons seksuelle orientering er en følsom oplysning, og det gælder, uanset om der er tale om almindeligt forekommende orienteringer som heteroseksualitet eller om mere specielle præferencer. En offentlig diskussion af mere eller mindre kendte personers formodede seksualitet skal derfor leve op til de særlige behandlingsbetingelser i artikel 9, hvad de formentlig jævnligt har svært ved.

Behandlingsbetingelserne for de følsomme oplysninger gennemgås nærmere nedenfor afsnit 6.5.

6.3.2. Almindelige oplysninger

Hvis en personoplysning ikke er særligt følsom, dvs. ikke omfattet af opregningen i GDPR artikel 9, stk. 1, hører de principielt til i restkategorien: almindelige personoplysninger, der skal behandles efter GDPR artikel 6. Eftersom oplysninger om strafbare forhold er særskilt reguleret både i forordningen og i databeskyttelsesloven, medtages de i denne fremstilling som en særskilt kategori, jf. afsnit 6.3.3 og mere detaljeret i afsnit 6.6. Endvidere er der nogle særlige kategorier og områder, omtalt kort i afsnittene 6.3.4 og 5.7.

Behandlingsbetingelserne for almindelige personoplysninger gennemgås nærmere nedenfor afsnit 6.4.

6.3.3. Oplysninger om strafbare forhold

GDPR artikel 10 overlader i vidt omfang til de enkelte medlemsstater at regulere behandlingen af straffedomme og lovovertrædelser. Reguleringen i dansk ret findes i databeskyttelsesloven (DBL) § 8, der taler om "oplysninger om strafbare forhold". Den danske term dækker bredt og omfatter både selve gerningen eller mistanke herom, den eventuelle straffesag, og efterfølgende oplysninger om afsoning og om den tidligere straffedom.

Behandlingsbetingelserne for oplysninger om strafbare forhold gennemgås nærmere nedenfor afsnit 6.6.

---

6. Dyreværnslovens § 3 a, indført ved lov nr. 533 af 29. april 2015.

6.3.4. Særlige kategorier og særlige områder

Ud over den overordnede inddeling i almindelige oplysninger, særligt følsomme oplysninger og oplysninger om strafbare forhold, er der to særlige kategorier: CPR-numre og oplysninger om gæld til det offentlige.

Ifølge GDPR artikel 87 kan "medlemsstaterne [...] nærmere fastsætte de specifikke betingelser for behandling af et nationalt identifikationsnummer [...]".

Denne mulighed har Danmark udnyttet i DBL § 9. Der er ingen problemer forbundet med at identificere et CPR-nummer, der består af ti cifre, hvoraf de første seks angiver fødselsdato og år og de sidste fire i hvert fald køn.

Oplysninger om gæld til det offentlige kan videregives til kreditoplysningsbureauer, når betingelserne i DBL §§ 15-18 er opfyldt. Det er ikke forbundet med vanskeligheder at identificere, hvornår der er tale om videregivelse af oplysninger om gæld til det offentlige.

Udover de forskellige kategorier af personoplysninger indeholder databeskyttelsesloven særlige regler på nogle særlige områder. Her er således ikke tale om særlige kategorier af oplysninger, men om, hvorvidt særlige områder har en særlig regulering ud over den, der allerede gælder.

De særlige områder er:

- Behandling med henblik på at føre retsinformationssystemer, DBL § 9;
- Behandling til videnskabelige og statistiske formål, DBL § 10;
- Behandling i forbindelse med ansættelsesforhold, DBL § 12;
- Virksomheders videregivelse af oplysninger til andre virksomheder i markedsføringsøjemed, DBL § 13;[7] og
- Videregivelse til arkiv, DBL § 14.

Disse særlige kategorier og særlige områder gennemgås kort nedenfor i afsnit 6.7.

7. Se herom i denne bogs kapitel 22.

6.4. Behandlingsbetingelser. Almindelige personoplysninger

GDPR artikel 6, stk. 1, litra a-f, opstiller de betingelser, der gælder, hvis man ønsker at behandle almindelige personoplysninger, dvs. de oplysninger, der ikke er særligt følsomme eller vedrører strafbare forhold. Betingelserne er ikke kumulative. Hvis blot én af betingelserne er opfyldt, vil en persondatabehandling være lovlig.

6.4.1. Samtykke

En behandling er lovlig, hvis "den registrerede har givet samtykke til behandling af sine personoplysninger til et eller flere specifikke formål", jf. GDPR artikel 6, stk. 1, litra a.

Bestemmelsen giver god mening. Persondataretten er ikke beregnet på at umuliggøre behandling af personoplysninger, men på at beskytte personer, hvis data behandles – og i øvrigt at sikre en fri udveksling af persondata inden for EU, jf. GDPR artikel 1.

Man skal være opmærksom på følgende:

For det første stiller persondataretten specificerede krav til et samtykke: der skal være frivilligt, specifikt, informeret og utvetydigt og skal foreligge som en egentlig erklæring eller en klar bekræftelse, jf. GDPR artikel 4, nr. 11. Dette betyder, at ikke ethvert klik eller nik kan udgøre et samtykke, når vi er inden for persondatarettens område. For en nærmere forklaring på disse særlige krav til samtykke, se kapitel 8, afsnit 8.4.1. Dette kapitel omhandler personbilleder, men der gælder selvfølgelig de samme krav til samtykke, uanset om personoplysningen foreligger som et billede eller i en anden form, f.eks. som tekst.

For det andet skal man være opmærksom på, at den, der afgiver et samtykke, retligt set skal være i stand til at afgive et samtykke. Det forekommer umiddelbart oplagt, at hverken et nyfødt barn eller en bevidstløs person kan afgive et samtykke. Men hvor går grænsen? Hvor gammel skal man være for at kunne afgive et gyldigt samtykke, hvor ædru skal man være, og kan andre afgive samtykke på en andens vegne i de tilfælde, hvor den pågældende ikke selv er i stand til det? Disse spørgsmål løses i høj grad *uden for* persondataretten, jf. nedenfor afsnit 6.4.1.1.-6.4.1.4.

Endelig *for det tredje* kan et samtykke tilbagekaldes. Dette spørgsmål behandles nedenfor afsnit 6.4.1.5.

6.4.1.1. Alder

Er man over 18 år, kan man normalt afgive et gyldigt samtykke, også inden for persondataretten. Der kan dog opstå problemer, f.eks. hvis man er sanseløst beruset, er ramt af demens og lignende. Dette behandles nedenfor afsnit 6.4.1.3. Er man under 18 år, er man som udgangspunkt undergivet forældremyndighed,[8] men det er ikke helt klart, hvad det indebærer i forhold til samtykke efter persondataloven. Nogle love sætter en 15-årsgrænse: Efter straffeloven[9] er det ikke muligt at give et retligt gyldigt samtykke til sex, når man er under 15, og – mere relevant for persondataretten – efter sundhedslovens § 17 kan "en patient, der er fyldt 15 år […] give samtykke til videregivelse af helbredsoplysninger […]".[10] Andre love kræver samtykke fra børn over 12 år, typisk på områder med vigtige, personlige beslutninger.[11] Selvom disse forskellige regler ikke er udformet med henblik på samtykke inden for persondataretten, kan man tage dem til indtægt for, at lovgiver ikke har ønsket at operere med ét skarpt skel ved 18 år. Man kan formentlig sige det sådan, at i hvert fald 15-17-årige har en mulighed for at give selvstændigt samtykke inden for persondataretten, mens samtykke fra børn ned til 12 år kan kræves i mange situationer, når andre ønsker at behandle deres personoplysninger. Forældre, bedsteforældre, tanter, onkler og venner, der ønsker at lægge billeder på åbne internetsider af en 12-årig, må indhente dennes samtykke i de situationer, hvor et samtykke er fornødent. Under alle omstændigheder gælder, at vurderingen af, hvor-

8. Forældreansvarsloven § 1, lovbekendtgørelse nr. 1417 af 1. december 2017 med senere ændringer.
9. Straffeloven, lovbekendtgørelse nr. 1156 af 20. september 2018 med senere ændringer.
10. Sundhedsloven, lovbekendtgørelse nr. 1286 af 2. november 2018 med senere ændringer. Se også værgemålslovens § 1, hvorefter ugifte under 18 år ikke kan forpligte sig ved retshandler eller råde over deres formue, mens §§ 42 og 43 giver særlige regler for personer over 15 år (værgemålsloven, lovbekendtgørelse nr. 1015 af 20. august 2008 med senere ændringer).
11. Adoptionsloven (lov nr. 775 af 7. aug. 2019) § 6, lov om voksenansvar for anbragte børn og unge (lovbekendtgørelse nr. 764 1. aug. 2019) § 5 og navneloven (lovbekendtgørelse 767 af 7. aug. 2019) § 4, stk. 5.

vidt der foreligger et "frivilligt, specifikt, informeret og utvetydigt" samtykke, jf. GDPR artikel 4, nr. 11, må underlægges en særlig skrap vurdering, når der er tale om børn og unge. Præamblens betragtning 38 taler netop om, at "børn bør nyde særlig beskyttelse af deres personoplysninger", og det fremhæves, at "en sådan særlig beskyttelse bør navnlig gælde for brug af børns personoplysninger med henblik på markedsføring eller til at oprette personligheds- eller brugerprofiler og indsamling af personoplysninger vedrørende børn, når de anvender tjenester, der tilbydes direkte til et barn."

Hvis barnet/den unge ikke selv kan give samtykke, er det forældrenes ansvar. Den nærmere regulering af, hvem der har forældreansvaret, er reguleret i forældreansvarsloven og værgemålsloven.[12] Hvis to forældre har fælles forældremyndighed, må udgangspunktet være, at én kan give gyldigt samtykke, medmindre der er grund til at antage, at der er uenighed mellem forældrene.[13] I nogle tilfælde skal forældrene informeres om barnets beslutning, jf. sundhedslovens § 17.

I særlige situationer er forældresamtykke ikke nødvendigt, nemlig når det drejer sig om forebyggende eller rådgivende tjenester, der tilbydes direkte til børn, jf. præamblens pkt. 38. En sådan rådgivning, der nødvendigvis vil indebære behandling af personoplysninger og typisk de følsomme af slagsen, kan altså foregå uden samtykke fra forældre, også selvom barnet er yngre end 15 år. Men rådgivningstjenesten skal selvfølgelig sikre, at persondatarettens øvrige regler overholdes, herunder dataminimering, sikkerhed, mv., jf. GDPR artikel 5 (nærmere behandlet i denne bogs kapitel 5, afsnit 5.3).

6.4.1.2. Efter dødsfald

Efter DBL § 2, stk. 5, gælder persondatabeskyttelsen indtil 10 år efter den pågældende persons død, hvilket giver anledning til at stille spørgsmålet, hvem der så kan give gyldigt samtykke. Udgangspunktet må her være, at den afdødes gyldige samtykke fortsat gælder. Hvis den afdøde ikke selv har givet samtykke, må nærmeste pårørende kunne

12. Se for detaljer f.eks. Pedersen & Pedersen 2018.
13. Se f.eks. UfR 1999.1154 Ø (Farvel far), hvor faren havde optaget et overvåget samvær under en løbende forældremyndighedssag. Her krævedes også morens samtykke. Sagen angår straffeloven, men det samme må gælde i persondataretten, når det drejer sig om, hvem der på barnets vegne kan give gyldigt samtykke.

gøre det: ægtefælle, forældre (især hvis afdøde er et barn), børn (især hvis afdøde er ældre) og søskende.[14] Pårørende må også kunne tilbagekalde et samtykke fra en afdød. (se nedenfor afsnit 6.4.1.5 om tilbagekaldelse).

6.4.1.3. Samtykke i forbindelse med udbud af informationssamfundstjenester

GDPR artikel 8 bestemmer, at samtykke til behandling af personoplysninger i forbindelse med udbud af informationssamfundstjenester kun kan være gyldigt, hvis barnet er over 16 år, dog således at medlemsstaterne kan sætte mindstealderen til 13 år. Danmark har udnyttet denne mulighed, jf. DBL § 6, stk. 2, således at børn over 13 år kan give samtykke til behandling af deres persondata i forbindelse med udbud af informationssamfundstjenester.

Men hvad betyder dette? Det er vigtigt at forstå, at der ikke er tale om nogen generel regel for alder i forbindelse med samtykke efter persondataretten (som er behandlet ovenfor afsnit 6.4.1.1). Der er derimod tale om en særlig regel, der muliggør udbydere af de såkaldte "informationssamfundstjenester" at udbyde til børn ned til 13 år, uden at der skal lægges særlige spærringer ind og uden krav om forældres godkendelse. Hvad er en "informationssamfundstjeneste" så? Det er et særligt EU-retligt begreb, der defineres i EU-direktiv 2017/1535:[15] "enhver tjeneste i informationssamfundet, dvs. enhver tjeneste, der normalt ydes mod betaling, og som teleformidles ad elektronisk vej på individuel anmodning fra en tjenestemodtager". Afgørende er, at selve ydelsen (fjern)leveres elektronisk, og termen omfatter således både sociale medier som Facebook og Instagram og mere traditionelle medier, hvis disse leveres online og on demand som f.eks. dr.dk.

---

14. Disse fire grupper er nævnt i retsplejelovens § 725 om retten til privat påtale, hvis den forurettede er død. Reglen er ikke direkte anvendelig på samtykke til behandling af afdødes personoplysninger, men kan tjene som inspiration.
15. EU-Parlamentets og Rådets Direktiv (EU) 2015/1535 af 9. september 2015 om en informationsprocedure med hensyn til tekniske forskrifter samt forskrifter for informationssamfundets tjenester (kodifikation). GDPR henviser i artikel 4, nr. 25, om definitionen af "informationssamfundstjeneste" netop til dette direktivs artikel 1, stk. 1, litra b. Man kan sige, at det er smart, at de forskellige EU-regler benytter samme definition, men definitionen er ikke let at forstå, og man skal have fat i flere EU-regler for nærmere at få fat i, hvad der tales om.

De ikke-elektroniske ydelser falder udenfor, selvom salget er formidlet elektronisk via internettet. Hvis man f.eks. køber en rejse på nettet, er det kun salget, der formidles elektronisk, mens selve ydelsen, rejsen, ikke er elektronisk (der er ikke meget ved at tage på virtuel ferie), og der er ikke tale om nogen "informationssamfundstjeneste". Hvis *formidlingen* af salget foregår via et særligt site, vil formidlingen udgøre en informationssamfundstjeneste.

Ideen bag GDPR artikel 8 er, at rigtigt mange børn og unge gør brug af sociale medier, og derfor er aldersgrænsen sat lavere. I Danmark er den sat til 13 år, og reglen indebærer, at den unge kan samtykke til tjenestens behandling af personoplysninger uden at skulle involvere forældrene.

Det er vigtigt at holde sig for øje, at bestemmelsen kun siger noget om samtykke til behandling af personoplysninger. Hvis der indgår andre aftaler, f.eks. om betaling, vil gyldigheden afhænge af andre regler, f.eks. værgemålslovens § 42, hvorefter personer over 15 år kan råde over penge, som de selv har tjent.

Det er også vigtigt at holde sig for øje, at bestemmelsen ikke i øvrigt siger noget om gyldigheden af samtykket. Efter nærværende forfatters vurdering forekommer det nærliggende, at Facebooks betingelser *ikke* lever op til persondatarettens krav om, at et samtykke skal være frivilligt, specifikt, informeret og utvetydigt.

6.4.1.4. Sindslidelse, demens, beruselse mv.

Et samtykke skal være afgivet af en person, der retligt set er i stand til at give samtykke. I juridisk sprogbrug kaldes dette *habilitet*.[16] Stærkt demente, berusede eller psykotiske personer kan ikke give samtykke, og det må komme an på en konkret vurdering i det enkelte tilfælde, hvorvidt personen er så beruset mv., at den pågældende ikke er i stand til at give et retligt bindende samtykke. Medmindre der er etableret et egentligt værgemål, eller der er udstedt en fuldmagt, mens den pågældende var ved sine fulde fem, kan andre ikke give samtykke på den inhabiles vegne.

16. Se om habilitet, når det drejer sig om videregivelse af private oplysninger: Jakobsen & Schaumburg-Müller 2013, s. 167-170.

6.4.1.5. Tilbagekaldelse af samtykke

Den samtykkende (eller den, der handler på dennes vegne, jf. ovenfor) kan trække sit samtykke tilbage jf. GDPR artikel 7, stk. 3. Den, der indhenter samtykket, og det vil typisk være den dataansvarlige, skal oplyse om denne mulighed, allerede inden samtykket gives. Tilbagekaldelsen skal kunne gives lige så let som samtykket. Det vil således ikke være lovligt, hvis man skal igennem alle mulige procedurer for at kunne tilbagekalde samtykket, hvis dette blev givet ved en simplere fremgangsmåde, f.eks. via afkrydsning.

Tilbagekaldelsen gælder fremadrettet. Den persondatabehandling, der er foretaget på baggrund af samtykket, har haft et lovligt behandlingsgrundlag. Men fremadrettet kan der ikke ske persondatabehandling på baggrund af et samtykke, der er tilbagekaldt. Dette kan være alvorligt nok. Hvis en dataansvarlig har baseret sine aktiviteter på de registreredes samtykker, kan det være ødelæggende for forretningen eller aktiviteten, hvis samtykket trækkes tilbage. Derfor kan det være relevant at se på andre mulige behandlingsgrundlag, jf. umiddelbart nedenfor.

6.4.2. Kontrakt

Efter GDPR artikel 6, stk. 1, litra b, kan en behandling af personoplysninger lovligt foretages, hvis "behandling er nødvendig af hensyn til opfyldelse af en kontrakt, som den registrerede er part i, eller af hensyn til gennemførelse af foranstaltninger, der træffes på den registreredes anmodning forud for indgåelse af en kontrakt."

Ideen er, at en aftalepartner – f.eks. et firma, der leverer varer til en kunde, eller en arbejdsgiver, der påtænker ansættelse af en person – skal kunne behandle de personoplysninger, der er nødvendige for at gennemføre aftalen. Det giver ingen mening, at et firma, der skal levere en vare til en kunde, ikke må behandle kundens navn og adresse, og bestemmelsen gør det muligt for firmaet at behandle de nødvendige oplysninger, også uden et egentligt samtykke. På samme måde må en arbejdsgiver behandle relevante oplysninger om en ansat, f.eks. navn og adresse, CPR-nummer, bankkonto, navn mv. på pårørende. Grundlaget skal være en kontrakt – eller en påtænkt kontrakt – mellem den

dataansvarlige og den registrerede. Aftaler med tredjepart er selvfølgelig ikke tilstrækkelige.

Man skal være opmærksom på, at bestemmelsen kun giver grundlag for behandling af almindelige personoplysninger. Er der tale om følsomme oplysninger eller oplysninger om strafbare forhold, skal hjemmelen findes i henholdsvis GDPR artikel 9 og DBL § 8. En vareleverandør vil normalt ikke have brug for den slags oplysninger, mens en arbejdsgiver kan have brug for at indhente – og i nogle tilfælde skal indhente – oplysninger om strafbare forhold og i et vist omfang visse følsomme oplysninger.

Bestemmelsen giver mulighed for at behandle oplysninger allerede inden en aftale er indgået. En arbejdsgiver, der påtænker en nyansættelse, må behandle de fornødne personoplysninger om ansøgere, også selvom det ikke resulterer i en aftale.[17]

Bestemmelsen giver, som de øvrige bestemmelser i artikel 6, stk. 1, et lovligt behandlingsgrundlag. Hvis man ikke kan finde et sådant grundlag, (og hvis man er inden for persondatarettens område), må behandling af persondata slet ikke finde sted. Bestemmelsen siger derimod ikke noget om, *hvordan* oplysningerne skal behandles. Dette følger af de generelle regler især i GDPR artikel 5.

I nogle situationer kan det være vanskeligt at afgøre, om behandlingsgrundlaget skal findes i reglerne om samtykke eller i reglerne om kontrakts-indgåelse. Dette er især tilfældet, hvis kontrakten går ud på at levere personoplysninger, f.eks. i form af personbilleder (modelfoto). Dette spørgsmål er særskilt behandlet i kapitel 8, afsnit 8.4.2.

6.4.3. Retlig forpligtelse

Efter GDPR artikel 6, stk. 1, litra c, er behandling af persondata lovlig, hvis den "er nødvendig for at overholde en retlig forpligtelse, som påhviler den dataansvarlige". For at bestemmelsen kan finde anvendelse, skal der være tale om en *forpligtelse*, og ikke bare noget, den dataansvarlig må gøre, heller ikke selvom det kan være smart og praktisk. I sådanne tilfælde kan afvejningsbestemmelsen i litra f muligvis anvendes (se nedenfor afsnit 6.4.6). En retlig forpligtelse foreligger, f.eks. når

17. Om det arbejdsretlige, se kapitel 28.

en arbejdsgiver er forpligtet til at indberette en ansats A-skat, og når en bank er forpligtet til at indberette mistanke om hvidvask.[18]

Bestemmelsen har ikke den store praktiske betydning, idet litra e om opgaver i samfundets interesse og offentlig myndighedsudøvelse typisk vil dække de relevante situationer.[19]

En retlig forpligtelse sættes typisk af en lov, men det er oplagt, at et land ikke kan indføre en lov, der kræver, at alle personoplysninger skal videregives til staten, og derefter henvise til artikel 6, stk. 1, litra c, som behandlingsgrundlag.

Det er også klart, at en aftaleretlig forpligtelse ikke kan udgøre det fornødne behandlingsgrundlag i litra c. Hvis en dataansvarlig indgår aftale med tredjepart om at levere personoplysninger om en person, vil dette selvfølgelig ikke være tilstrækkelig hjemmel til videregivelsen. Den dataansvarlige har måske nok påtaget sig en forpligtelse, men den er ikke relevant i persondataretlig henseende.

Reglen gælder kun undtagelsesvis, den er ikke retvisende efter sin ordlyd, og synes i det hele taget overflødig.

6.4.4. Vitale interesser

Behandling af persondata kan endvidere foretages, hvis den "er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser", jf. GDPR artikel 6, stk. 1, litra d. Ideen er, at persondataretten ikke skal være til hinder for at redde liv, helbred eller betydelig formue. Man kan f.eks. videregive navn mv. på en tilskadekommen, hvis denne ikke selv er i stand hertil.[20] Og på samme måde kan en

18. Eksemplerne er fra Artikel 29-Gruppen WP 217, s. 19. Arbejdspapiret vedrører det gamle direktiv, men ordlyden i forordningen er identisk. Man kan overveje, om ikke videregivelse af mistænkelige oplysninger om fysiske personers pengetransaktioner retteligt vedrører strafbare forhold og dermed hører under DBL § 8, jf. nedenfor afsnit 6.3. Se Hvidvaskloven eller Lov om forebyggende foranstaltninger mod hvidvask og finansiering af terrorisme, lov nr. 930 af 6. september 2019 med senere ændringer, § 26.
19. I EU-domstolens afgørelse af 30. maj 2013 i sagen *Worten*, C-342/12, fandt EU-Domstolen, at videregivelse af personoplysninger i forbindelse med kontrol af overholdelse af arbejdstider havde hjemmel i hvad der nu svarer til GDPR artikel 6, stk. 1, litra c og litra e.
20. Videregivelse af sundhedsoplysninger hører under følsomme oplysninger, GDPR artikel 9, behandlet nedenfor afsnit 6.5.8.

nabo kontakte et forsikringsselskab og videregive relevante personoplysninger på naboen, når dennes hus er oversvømmet.

Bestemmelsen finder kun anvendelse, når *vitale* interesser er truet. I mindre presserende tilfælde kan afvejningsbestemmelsen i litra f eventuelt bruges. Desuden er bestemmelsen kun beregnet på konkrete, individuelle interesser. Behandling af personoplysninger til brug for mere omfattende tiltag f.eks. i forbindelse med naturkatastrofer eller lignende må finde et andet grundlag, jf. præambelbetragtning nr. 46

6.4.5. Opgaver i samfundets interesser og pålagte opgaver

GDPR artikel 6, stk. 1, litra e, dækker to situationer: *For det første* de situationer, hvor persondatabehandling er nødvendig af hensyn til udførelse af en opgave i samfundets interesse, og *for det andet* offentlig myndighedsudøvelse.

Som eksempel på opgaver i samfundets interesse kan nævnes behandling i statistisk, historiske eller videnskabeligt øjemed. Her skal man være opmærksom på, at artikel 6, stk. 2 og 3, giver mulighed for og anvisning på nærmere national regulering, en mulighed, Danmark har udnyttet i DBL § 10. Det samme gælder retsinformationssystemer, databaser, hvor man kan søge oplysninger om gældende ret, herunder afsagte domme, der meget ofte vil indeholde oplysninger om fysiske personer. Sådanne informationssystemer er åbenlyst i samfundets interesse, og også her har Danmark udnyttet muligheden for nærmere regulering, jf. DBL § 9. Lidt polemisk kan man dog bemærke, at man i Danmark endnu ikke har formået at skabe en offentligt tilgængelig domsdatabase. Kun Sø- og Handelsretten og Højesteret offentliggør alle sine domme.

Offentliggørelse af medarbejderoplysninger kan formentlig og i et vist omfang siges at være i samfundets interesse, f.eks. oplysning om navn og arbejdstelefon og lignende. Til højere embeder kan også offentliggørelse af visse cv-oplysninger være i samfundets interesse, så offentligheden kan se det dokumenteret, at den pågældende har de fornødne kvalifikationer.

Også andre aktiviteter kan falde ind under bestemmelsen. Datatilsynet har i en tidligere sag[21] fundet det naturligt, at Undervisningsministeriet løste opgaven vedrørende digital tilmelding til og ansøgning om optagelse på uddannelser. Der var ikke udtrykkelig lovhjemmel, og hjemlen kunne derfor ikke findes i litra c, der kræver en retlig forpligtelse. Men hjemlen kunne findes i den bestemmelse, der nu findes i GDPR artikel 6, stk. 1, litra e.

Det er ikke noget krav, at opgaven skal udføres af eller for en offentlig myndighed. Også private kan bedrive forskning og udarbejde statistik mv.

I forarbejderne nævnes det, at videregivelse af oplysninger til politiet om muligt ulovlige aktiviteter kan udgøre en behandling i samfundets interesse.[22] Det er rigtigt, forstået på den måde, at videregivelse til politi om mulige strafbare forhold oplagt er i samfundets interesse. En sådan oplysning relaterer sig imidlertid til strafbare forhold og er derfor ikke blot er en "almindelig" personoplysning. Om behandling af oplysninger om strafbare forhold, se nedenfor afsnit 6.6.

Som eksempel på offentlig myndighedsudøvelse kan nævnes skattevæsnet, der behandler personoplysninger med henblik på at beregne skatten, og kommuner, der driver skoler og biblioteker og også her behandler personoplysninger.[23] Bestemmelsen kan også anvendes, selvom myndighedsudøvelsen er henlagt til private.[24]

Som nævnt kræver brug af denne bestemmelse ikke, at der foreligger en retlig forpligtelse. Der skal blot være tale om enten en opgave i samfundets interesse eller om myndighedsudøvelse. Det er, som ovenfor nævnt, vanskeligt at forestille sig, at en retlig forpligtelse, der ikke er i samfundets interesse og ikke sker som led i myndighedsøvelse, selvstændigt kan danne hjemmel for persondatabehandling. Eller sagt på en anden måde: Alle relevante tilfælde under litra c dækkes af litra e.

---

21. Datatilsynets afgørelse af 13. juni 2004 vedrørende Digital tilmelding til og ansøgning om optagelse på videregående uddannelser, j.nr. 2004-54-1396.
22. Betænkning 1565/2017, s. 131-132.
23. Ibid., s. 119-120.
24. Ibid., s. 131. I hvilket omfang myndighedsudøvelse kan udlægges til private, er et andet spørgsmål. Se nærmere herom Fenger m.fl. 2018, s. 143-154.

6.4.6. Afvejningsreglen

GDPR artikel 6, stk. 1, litra f, indeholder en generel afvejningsregel, der ikke som en del af de foregående bestemmelser har et afgrænset og specifikt sigte, men kan betragtes som en form for opsamlingsbestemmelse, der kan anvendes i mange forskellige situationer.

Bemærk dog, at afvejningsreglen i litra f *ikke* kan anvendes af offentlige myndigheder, jf. artikel 6, stk. 1, sidste sætning. Offentlige myndigheder må finde anden hjemmel som f.eks. i litra e, omtalt ovenfor. Dette skærper kravene til offentlige myndigheders behandling i den mere uforpligtende ende af skalaen. Offentliggørelse af medarbejderoplysninger kan således ikke længere foretages blot ud fra en afvejning af legitime interesser,[25] men må være i samfundets interesse eller pålagt, litra e (eller en anden behandlingshjemmel må foreligge, som f.eks. samtykke i litra a).

EU-Domstolen har slået fast, at reglen indeholder en tretrinstest.[26] *For det første* skal der være en legitim interesse, for andet skal persondatabehandlingen være nødvendig for at forfølge denne interesse, og for det tredje må den registreredes rettigheder ikke gå forud.

Den konkrete sag, C-13/16, angik spørgsmålet om, hvorvidt et taxaselskab måtte udlevere navn og adresse på en passager, der ved udstigningen havde åbnet døren på en måde, så der skete skade på en trolleybus.

EU-Domstolen siger hertil for det første, at det helt åbenlyst er en legitim interesse at kunne gøre krav gældende mod en person, der har gjort skade på ejendom. Det samme må gælde ved personskade.

For det andet var det i sagen nødvendigt nærmere at kunne identificere den pågældende passager i taxaen. Uden denne oplysning kunne busselskabet ikke komme videre med sagen.

Endelig siger Domstolen, at afvejningen over for den registreredes rettigheder skal afgøres konkret og netop ud fra tyngden af de involverede interesser og rettigheder. Her kan det indgå, hvorvidt den (eller de) oplysninger, der videregives, i forvejen er offentliggjorte. Der skal

25. Betænkning 1565/2017, s. 136.

26. Sag C-13/16, *Valsts policijas Rigas*, dom af 4. maj 2017, pr. 22-33. Også denne dom vedrører det tidligere direktiv, men da ordlyden af de relevante bestemmelser er stort set identiske, har dommen også betydning for forordningen.

også tages hensyn til, om den registrerede er et barn, jf. formuleringen i slutningen af bestemmelsen: "navnlig hvis den registrerede er et barn". Domstolen bemærker dog, at i den konkrete sag, hvor det er et spørgsmål om at kunne rejse et lovligt krav mod en person, spiller alderen ikke ind.

Domstolen konkluderer i sagen, at tretrinstesten gør det legitimt at videregive de personoplysninger, således at den pågældende kan identificeres. Domstolen understreger, at der ikke er nogen *pligt* til en sådan udlevering. Men i den konkrete sag gav afvejningsbestemmelsen tilstrækkeligt grundlag for den behandling af persondata, der består i at udlevere oplysninger, der kan identificere den pågældende.

I et arbejdspapir udarbejdet af det, der nu er Det Europæiske Databeskyttelsesråd,[27] anbefales det, at den dataansvarlige redegør for sin afvejning. Dette kan indebære forskellige fordele: *For det første* får den dataansvarlige situationen tænkt igennem og derved mulighed for nærmere at overveje, om det fornødne behandlingsgrundlag er til stede. *For det andet* har den dataansvarlige mulighed for at dokumentere sine overvejelser ved en eventuel tvist, og *sidst*, men ikke mindst, kan den registrerede se, om der er foretaget en overbevisende afvejning eller ikke.

Som eksempler på legitime interesser kan nævnes forebyggelse af svig,[28] kundeforhold og ansættelse[29] (som dog jævnligt kan behandles efter litra b om kontraktforhold), intern videregivelse af oplysninger internt i en koncern[30] og sikkerhedsforhold.[31] Disse interesser er som nævnt ovenfor ikke i sig selv nok, der skal en afvejning til, men kun *legitime* interesser kan overhovedet komme i spil ved en afvejning.

Datatilsynet har i det hele taget en omfattende praksis efter de tidligere regler, herunder om personbilleder (se nærmere herom kapitel 8). Man skal her være opmærksom på, at forordningen stiller krav om en

27. Artikel 29-Gruppen WP 217. Rådet består af medlemmer fra medlemslandenes datatilsyn. Tidligere hed det Artikel 29-Gruppen, nu efter GDPR Det Europæiske Databeskyttelsesråd, på engelsk: *European Data Protection Board*, ofte forkortet EDPB.
28. Betænkning 1565/2017, s. 133.
29. Betænkning 1565/2017, s. 132.
30. GDPR præambelbetragtning nr. 48.
31. GDPR præambelbetragtning nr. 49.

ensartet fortolkningspraksis, hvilket indebærer en forpligtelse for de enkelte landes tilsyn til at koordinere med hinanden.[32]

6.5. Behandlingsbetingelser. Følsomme oplysninger

Er der tale om de særlige personoplysninger, der er nævnt i GDPR artikel 9 – ofte kaldet følsomme eller særligt følsomme oplysninger – skal man først ind i artikel 9, stk. 2, for at se, om der er en undtagelser fra forbuddet i artikel 9, stk. 1. Er der en brugbar relevant undtagelse efter stk. 2, skal man tilbage i artikel 6 for at finde et lovligt behandlingsgrundlag. Det vil normalt ikke være noget problem. Hvis der ikke er et forbud mod behandling af de særlige oplysninger, vil der som regel også være et behandlingsgrundlag i artikel 6. Som eksempel kan nævnes, at hvis der foreligger et "udtrykkeligt samtykke" efter artikel 9, stk. 2, litra a, vil der også foreligge et "samtykke" efter artikel 6, stk. 2, litra a.

> Tidligere ansås artikel 9, stk. 2, for selvstændigt behandlingsgrundlag, således at man skulle finde et behandlingsgrundlag enten i artikel 6 eller i artikel 9. Pr. 7. november 2019 har Datatilsynet imidlertid annonceret, artikel 9 ikke udgør et behandlingsgrundlag, men alene et forbud mod undtagelser. Opfattelsen er nærmere begrundet i Datatilsynets baggrundsnotat af samme dato.

I nogle af undtagelserne efter artikel 9, stk. 2, kræves der så at sige dobbelt tilladelse, forstået på den måde, at nogle af bestemmelserne, nemlig litra b, g, h i og j, forudsætter, at der er relevante bestemmelser i medlemsstaternes lovgivning eller i EU-retten, og for litra b's vedkommende tillige i kollektiv overenskomst. Denne lidt kringlede måde at lovgive på er et eksempel på, at GDPR nok er en forordning, der principielt gælder umiddelbart i alle medlemslande, men at GDPR sommetider opfører sig mere som et direktiv, hvorefter de enkelte lande selv skal gennemføre en lovgivning inden for EU-rettens rammer. I Danmark er det væsentligst løst på den simple måde, at databeskyttelsesloven giver de specifikke undtagelser ved at henvise til forordningen.

32. Præambelbetragtning nr. 10, også understreget i betænkning 1565/2017, s. 134.

6.5.1. Samtykke

Ligesom ved de almindelige oplysninger er det en mulighed for lovlig persondatabehandling, at den, hvis data behandles, har givet samtykke. Der gælder de samme regler, herunder ikke mindst at samtykket skal være frivilligt, specifikt, informeret og utvetydigt, jf. artikel 4, nr. 11 (behandlet nærmere overfor afsnit 6.4.1 og i kapitel 8 om personbilleder afsnit 8.4.1). Ved de særligt følsomme oplysninger, skal samtykket endda være "udtrykkeligt", jf. artikel 9, stk. 2, litra a, hvilket skærper kravet til den måde, på hvilken samtykket kan anses for givet.[33] Det kan være ved underskrift, og ved digitalt samtykke, at der etableres en totrinsmodel med klik og efterfølgende bekræftelse pr. mail eller sms. Et udtrykkeligt samtykke kan i princippet også foreligge mundtligt, men man skal være opmærksom på, at det altid er den dataansvarliges ansvar at kunne påvise samtykket, jf. artikel 7, stk. 1, herunder også at det foreligger udtrykkeligt.

Den afgørende forskel på krav til samtykke ved almindelige oplysninger (samt oplysninger om strafbare forhold) og til samtykke ved følsomme oplysninger er netop kravet til udtrykkelighed. Ved almindelige oplysninger (og oplysninger om strafbare forhold) kan et gyldigt samtykke været indforstået – det forudsætter fortsat, at samtykket er frivilligt, specifikt, informeret og utvetydigt – men ved viderebehandling af følsomme oplysninger skal samtykket tillige være udtrykkeligt, dvs. det skal være ekspliciteret og ikke bare ligge som en indforstået selvfølgelighed.[34] Se mere indgående om samtykke ved personbilleder kapitel 8, afsnit 8.5.1.

6.5.2. Arbejdsretlige forpligtelser

Litra b undtager fra forbuddet mod behandling af følsomme oplysninger, når

33. Artikel 29-Gruppen WP 259 rev.01, afsnit 4, "Obtaining explicit consent".

34. I forarbejderne angives det, at kravet til udtrykkelighed ikke giver nogen særlig forskel ud over at skærpe opmærksomheden på samtykket, jf. betænkning 1565, s. 208. Efter nærværende forfatters vurdering holder betragtningen ikke i detaljen. Der er forskel på et samtykke, der er udtrykkeligt ("explicit" som det hedder i den engelske udgave), og et stiltiende (eller underforstået) samtykke, også selvom de øvrige betingelser er opfyldt (frivillig, specifik, informeret og utvetydig).

> "behandling er nødvendig for at overholde den dataansvarliges eller den registreredes arbejds-, sundheds- og socialretlige forpligtelser og specifikke rettigheder, for så vidt den har hjemmel i EU-retten eller medlemsstaternes nationale ret eller en kollektiv overenskomst i medfør af medlemsstaternes nationale ret, som giver fornødne garantier for den registreredes grundlæggende rettigheder og interesser."

Reglen er skruet sådan sammen, at der skal foreligge et yderligere grundlag, enten i EU-retten, i national ret eller i kollektive overenskomster. I dansk ret har man valgt kun at benytte muligheden for de *arbejdsretlige* forpligtelser og rettigheder, jf. DBL §§ 7, stk. 2, og 12.

Dette betyder ikke, at der ikke er undtagelser fra behandlingsforbuddet inden for sundheds- eller socialretten, men blot, at persondatabehandlingen ikke kan ske udelukkende med reference til forordningen og databeskyttelsesforordningen.

For at litra b og DBL § 7, stk. 2, kan finde anvendelse skal behandlingen ligge inden for arbejdsretten. Der kan være tale om en arbejdsgivers behandling af relevante følsomme oplysninger f.eks. i forbindelse med sygefravær. Desuden skal der være tale om den dataansvarlige eller den registreredes rettigheder og forpligtelser. Hensyn til tredjeperson er ikke tilstrækkeligt. Endelig er det en betingelse, at den relevante hjemmel indeholder de fornødne garantier. Se nærmere om persondatabehandling i arbejdsforhold: Datatilsynets Vejledning om databeskyttelse i forbindelse med ansættelsesforhold af november 2018 og nærværende bogs kapitel 28.

6.5.3. Vitale interesser

GDPR artikel 9, stk. 2, litra c, lyder således: "Behandling er nødvendig for at beskytte den registreredes eller en anden fysisk persons vitale interesser i tilfælde, hvor den registrerede fysisk eller juridisk ikke er i stand til at give samtykke."

Bestemmelsen svarer til artikel 6, stk. 1, litra d, se ovenfor afsnit 6.4.4, dog således at kravet til behandling af følsomme oplysninger tillige kræver, at den registrerede ikke er i stand til at give samtykke. Er en person bevidstløs efter en trafikulykke og har akut brug for blod, kan oplysning om blodtype – en følsom oplysning – behandles efter

denne bestemmelse. Det samme gælder, hvis der er behov for behandling af stærkt berusede, stærkt demente eller psykotiske personer, og behandlingen kræver behandling af personoplysninger, hvad den typisk vil gøre.

Igen skal det understreges, at bestemmelsen selvfølgelig kun drejer sig om behandling af personoplysninger. Selve retten (og pligten) til fysisk at foretage en lægelig behandling følger af andre regler som f.eks. sundhedslovens § 19.

6.5.4. Organisationers behandling

Mange organisationer vil behandle følsomme oplysninger, fordi man via sit medlemskab og eventuelt via aktiviteter netop involverer følsomme oplysninger i form af "politisk, religiøs eller filosofisk overbevisning". Det ville ikke give mening, hvis f.eks. en partiorganisation ikke måtte behandle oplysninger om medlemskab eller om medlemmernes aktiviteter i foreningen.

Artikel 9, stk. 2, litra d, bestemmer, at forbuddet mod behandling af følsomme oplysninger ikke gælder, hvis "behandling foretages af en stiftelse, en sammenslutning eller et andet organ, som ikke arbejder med gevinst for øje, og hvis sigte er af politisk, filosofisk, religiøs eller fagforeningsmæssig art, som led i organets legitime aktiviteter og med de fornødne garantier, og på betingelse af at behandlingen alene vedrører organets medlemmer, tidligere medlemmer eller personer, der på grund af organets formål er i regelmæssig kontakt hermed, og at personoplysningerne ikke videregives uden for organet uden den registreredes samtykke."

Bestemmelsen indeholder nogle nærmere betingelser:

Der skal være tale om organisationer, der ikke arbejder med gevinst for øje. Kommercielle aktiviteter falder ikke under undtagelsen. En forening af private erhvervsdrivende inden for en bestemt branche vil dog typisk være omfattet af undtagelsen, eftersom selve foreningen ikke er kommerciel, men ideel i den forstand, at den søger at fremme medlemmernes interesser. Det er heller ikke afgørende, om organisationen har en betydelig økonomi. Mange større organisationer som Kræftens Bekæmpelse og Folkekirkens Nødhjælp har en stor økonomi med betydelige indtægter fra donationer mv., men de vil være omfattet af bestemmelsen, fordi de ikke arbejder med gevinst for øje.

Den personkreds, hvis oplysninger kan behandles er: medlemmer, tidligere medlemmer og andre med hvem organisationen på grund af sit formål er i regelmæssig kontakt. Især hvad de tidligere medlemmer angår, skal man være opmærksom på kravet om dataminimering efter GDPR artikel 5. Det kan være legitimt fortsat at have oplysninger om tidligere medlemmer f.eks. med henblik på at genhverve dem som betalende medlemmer, men der er grænser for, hvor længe dette hensyn kan bære. Med hensyn til ikke-medlemmer skal to betingelser være opfyldt: Kontakten skal være knyttet til organisationens formål, og kontakten skal være regelmæssig. Er der kun tale om sporadisk kontakt, eller er der tale om andre former for kontakter som f.eks. med personer på et reklamebureau, kan undtagelsen ikke anvendes. Bemærk her, at bestemmelsen vedrører mulighed for behandling af de særligt følsomme oplysninger. Ved kontakt til f.eks. en person på et reklamebureau har organisationen ikke nogen legitim interesse i at behandle den pågældendes politiske, religiøse eller filosofiske overbevisning, men skal blot have de relevante kontaktoplysninger, dvs. almindelige personoplysninger, og her er man henvist til bestemmelserne i GDPR artikel 6, hvor afvejningsreglen i litra f er relevant.

Andre personer end disse tre grupper er ikke relevante for undtagelsen i artikel 9, stk. 2, litra d. Undtagelsen strækker sig ikke til f.eks. at registrere politiske modstandere. Hvis persondatabehandlingen består i en sådan registrering, må der findes en anden undtagelse i artikel 9 – det kunne være selvoffentliggørelse efter stk. 2, litra e – og en behandlingshjemmel i artikel 6. Her kunne afvejningsreglen overvejes, jf. artikel 6, stk. 1, litra f, men den hjemler ikke nødvendigvis en sådan registrering.

Undtagelsen gælder endvidere kun for den (nødvendige) interne behandling, medlemsfortegnelse (der på grund af organisationens art typisk i sig selv vil indeholde oplysninger om politisk, religiøs eller filosofisk overbevisning), medlemsaktiviteter mv. Der må ikke ske videregivelse af de følsomme oplysninger, medmindre den pågældende giver samtykke, jf. litra a, behandlet ovenfor afsnit 6.5.1.

Behandling af de følsomme oplysninger skal selvfølgelig leve op til persondatarettens krav om sikkerhed mv. (se herom kapitel 14), og de almindelige krav til behandling (lovlighed, rimelighed, gennemsigtighed, dataminimering mv., jf. artikel 5, behandlet i kapitel 5). Desu-

den skal man være opmærksom på, om behandlingen overhovedet falder under persondataretten. Er der tale om journalistisk virksomhed, er denne i meget vidt omfang undtaget fra persondatarettens mange regler (behandlet nærmere i kapitel 20).

6.5.5. Selvoffentliggørelse

Efter litra e er behandling af følsomme oplysninger ikke forbudt, hvis disse "tydeligvis er offentliggjort af den registrerede". Bestemmelsen er praktisk vigtig: Det giver ikke mening, at man ikke må omtale eller på anden måde behandle f.eks. folketingspolitikeres politiske opfattelser, præster eller imamers religiøse opfattelse eller samfundsdebattørers filosofiske overbevisninger. Derfor denne undtagelse fra forbuddet, og artikel 6, stk. 1, litra f, vil jævnligt kunne bruges som relevant behandlingsgrundlag.

For nærmere detaljer henvises til kapitel 8, afsnit 8.5.2. Afsnittet handler om personbilleder, men spørgsmålet om selvoffentliggørelse behandles indgående.

Bemærk – som altid – de øvrige regler i persondataretten, såsom dataminimering, krav om oplysningers korrekthed mv. Se GDPR artikel 5, og nærværende bogs kapitel 5, afsnit 5.3.

6.5.6. Fastlæggelse af retskrav

I de tilfælde, hvor "behandling er nødvendig, for at retskrav kan fastlægges, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol", gælder forbuddet mod behandling af følsomme data ikke, jf. artikel 9, stk. 2, litra f.[35] Det kan være situationer, hvor offentlige myndigheder skal vurdere sager om incest, forsikringsselskaber skal vurdere erstatning for invaliditet, eller skattemyndigheder skal tage stilling til betaling af kirkeskat.[36] Spørgsmålet om, hvor-

35. Se om den tilsvarende bestemmelse, når der er tale om almindelige personoplysninger, artikel 6, stk. 1, litra d.

36. Se evt. UfR 2017.1294 H (Offentligt ansattes almindelige tavshedspligt), hvor Højesteret fandt, at videregivelse af sundhedsoplysninger fra en kommune til en arbejdsgiver var lovlig. Dommen angår den tidligere persondatalov, der havde en bestemmelse svarende til GDPR artikel 9, stk. 2, litra f.

når domstolene handler i egenskab af domstole, er behandlet i kapitel 19 i denne bog.

Som ved mange andre bestemmelser i artikel 9, stk. 2, forudsætter undtagelsen, at behandlingen er nødvendig, og de almindelige krav om dataminimering, sikkerhed mv. gælder naturligvis under alle omstændigheder. Det relevante behandlingsgrundlag vil her kunne være artikel 6, stk. 1, litra b, e eller f.

6.5.7. Væsentlige samfundsinteresser

Ifølge GDPR artikel 9, stk. 2, litra g, er der ikke forbud mod behandling af særligt følsomme personoplysninger behandles under følgende betingelser:

1. **"Behandling er nødvendig af hensyn til væsentlige samfundsinteresser […]"**
   Som eksempel på en sådan væsentlig samfundsinteresse kan nævnes tilladelse til en privat organisation, der rådgiver børn og unge i forbindelse med forældres sygdom og dødsfald. Datatilsynet accepterede, at det er nødvendigt at have en til tider detaljeret viden om den pågældende forælders sygdom og/eller død for at kunne yde den rette rådgivning.[37] Det forekommer oplagt, at en sådan form for rådgivning er en væsentlig samfundsinteresse.

2. **"[…] på grundlag af EU-retten eller medlemsstaternes nationale ret […]"**
   Forordningens bestemmelse kræver tillige hjemmel i EU- eller national ret, og for Danmarks vedkommende er det gennemført i databeskyttelseslovens § 7, stk. 4. Denne bestemmelse åbner for, at offentlige myndigheder at behandle følsomme personoplysninger af hensyn til væsentlige samfundsinteresser, men er der tale om privates persondatabehandling, kræver dette en godkendelse.[38] Ideen er, at private ikke bør stå med vurderingen

37. Datatilsynet 2012, s. 25.
38. Anden del af stk. 4 er formuleret således: "Tilsynsmyndigheden giver tilladelse hertil, hvis behandlingen efter 1. pkt. ikke foretages for en offentlig myndighed. Der

af, om en nærmere bestemt persondatabehandling er af væsentlig samfundsinteresse. Vurderingen må foretages af en kompetent offentlig myndighed.

3. **"[…] står i rimeligt forhold til det mål, der forfølges […]"**
   Kravet er en understregning af det almindeligt gældende princip om proportionalitet. I forhold til det ovennævnte eksempel med rådgivning til børn og unge med forældre, der er syge eller afgået ved døden, kan der være behov for behandling af endda mange og detaljerede oplysninger om forældrene og den nærmeste familie.

4. **"[…] respekterer det væsentligste indhold af retten til databeskyttelse […]"**
   Også en understregning af et almindeligt persondataretligt princip.

5. **"[…] og sikrer passende og specifikke foranstaltninger til beskyttelse af den registreredes grundlæggende rettigheder og interesser."**
   Hvad angår det nævnte eksempel med rådgivning til børn og unge med forældre med alvorligt syge eller afdøde forældre kan der være behov for endda meget detaljerede oplysninger om den pågældende forælder og de nærmeste familiemedlemmer. Disse oplysninger må imidlertid kun bruges til rådgivning af den unge og ikke til alt muligt andet. (Hvis en sådan organisation ønsker at samle oplysninger til mere generel viden på området, kan oplysningerne anonymiseres). Det almindelige persondataretlige princip om fornødne garantier er her skærpet til "specifikke foranstaltninger". Dette kan f.eks. være særlige krav om tavshedspligt og begrænset adgang kun for få behandlere[39] – begge dele oplagt i eksemplet med rådgivning af børn og unge.

---

kan i en tilladelse efter 2. pkt. fastsættes nærmere vilkår for behandlingen."

39. Som anført i betænkning 1565/2017, s. 216.

6.5.8. Patientbehandling mv.

GDPR artikel 9, stk. 2, litra h, åbner for behandling af følsomme data inden for et bredt spektrum af områder: "forebyggende medicin […] arbejdsmedicin til vurdering af arbejdstagerens erhvervsevne, medicinsk diagnose, ydelse af social- og sundhedsomsorg, […] eller -behandling, […] forvaltning af social- og sundhedsomsorg og -tjenester […]", og stk. 3 forudsætter, at de pågældende persondatabehandlere har tavshedspligt.

Den danske bestemmelse dækker imidlertid kun det sundhedsfaglige område: Behandling af følsomme oplysninger – og det vil der være inden for sundhedsvæsenet – "kan ske, hvis behandling af oplysninger er nødvendige med henblik på forebyggende sygdomsbekæmpelse, medicinsk diagnose, sygepleje eller patientbehandling eller forvaltning af læge- og sundhedstjenester og behandlingen af oplysningerne foretages af en person inden for sundhedssektoren, der efter lovgivningen er undergivet tavshedspligt […]", jf. DBL § 7, stk. 3. Behandlingsgrundlaget i artikel 6 kan findes i dennes stk. 1, litra e.

Det bemærkes, at databeskyttelsesloven kun regulerer behandling af persondata, ikke den medicinske behandling af patienter. Reglerne for denne behandling må findes andre steder, f.eks. i sundhedsloven. Der er tavshedspligt for sundhedspersonale efter sundhedslovens § 40 og straf for brud på tavshedspligt efter straffelovens §§ 152-152 f.

6.5.9. Folkesundhed

I GDPR artikel 9, stk. 2, litra i, er der en særlig undtagelser fra forbuddet mod at behandle følsomme personoplysninger, nærmere bestemt i det omfang, det er nødvendigt af hensyn til samfundsinteresser på folkesundhedsområdet. Eftersom forordningen allerede har en bestemmelse, som muliggør behandling, der er nødvendig af hensyn til "væsentlige samfundsinteresser", jf. litra g og ovenfor afsnit 6.5.7, synes bestemmelsen i litra i at være overflødig. Folkesundhed må siges at være en væsentlig samfundsinteresse. Der er heller ikke medtaget en særlig hjemmel i den danske databeskyttelseslov. Der er til gengæld relevante bestemmelser i sundhedslovgivningen såsom § 20, stk. 2, om

lægemiddelstyrelsens adgang til patientjournaliser i lov om kliniske forsøg med lægemidler,[40] og § 22 om udenlandske myndigheders adgang.

6.5.10. Arkiv, videnskab, historie og statistik

Som ovenfor nævnt er ideen med persondataforordningen ikke at hindre eller begrænse behandling af personoplysninger. Ideen er på én gang at muliggøre den fri udveksling af personoplysninger især inden for EU *og* at beskytte den enkeltes rettigheder, jf. GDPR artikel 1. Til tider vil disse to formål være i modstrid med hinanden, men det er bestemt ikke altid tilfældet. En statistiker, der er med til at frembringe brugbar viden til gavn for samfundet, er ikke det mindste interesseret i, hvilken konkret person der har en bestemt sygdom, men er interesseret i at kunne påvise, f.eks. hvor mange der har sygdommen, hvilke faktorer der statistisk påvirker risikoen for at få sygdommen etc. Det praktiske problem er, at oplysningerne i første omgang må relatere sig til enkelte, konkrete personer, idet den statistiske viden ikke ellers er mulig.

Regulering af dette brede og vigtige område er noget kringlet, og her trækkes blot hovedtrækkene op. Skal man beskæftige sig nærmere med området, må man konsultere mere specialiseret litteratur.[41] GDPR artikel 89 giver medlemslandene mulighed for nærmere regulering af området på nærmere angivne betingelser, artikel 9, stk. 2, litra j, giver undtagelser fra forbuddet mod at behandle følsomme oplysninger til den slags formål – dvs. arkiv, forskning, historie og statistik, den danske databeskyttelseslov § 10 regulerer persondatabehandling i forbindelse med forskning og statistik, og § 14 regulerer arkivformål. Udtrykket "historiske forskningsformål" er ikke medtaget i den danske tekst, men det må antages, at historieforskning (normalt) er videnskabelig, så det giver næppe den store praktiske forskel. Hvad angår oplysninger om strafbare forhold (til arkiv, videnskab og statistik), er disse medtaget i den danske databeskyttelseslov § 10. Behandlingsgrundlaget i forordningen kan findes i GDPR artikel 6, stk. 1, litra e, om opgaver i samfundets interesse (se herom ovenfor afsnit 6.4.5).

40. Lov nr. 620 af 8. juni 2016 med senere ændringer.
41. Som f.eks. Kristensen 2014.

I GDPR artikel 89, stk. 1, første sætning, hedder det: "Behandling til arkivformål i samfundets interesse, til videnskabelige eller historiske forskningsformål eller til statistiske formål skal være underlagt fornødne garantier for registreredes rettigheder og frihedsrettigheder i overensstemmelse med denne forordning." Det overlades således til medlemsstaterne nærmere at regulere, men selvfølgelig med skyldig hensyntagen til forordningens mange beskyttelsesregler, f.eks. i artikel 5 (bl.a. dataminimering) og artikel 32 (sikkerhed).

Bemærk, at artikel 89 kun omtaler arkivformål i samfundets interesse. Dette betyder selvsagt ikke, at arkiver, der ikke er i samfundets interesse, ikke skal leve op til forordningens regler, men at man må finde en anden hjemmel, hvis arkiver med personoplysninger ikke føres i samfundets interesse. Her er især privat-reglen relevant, GDPR artikel 2, stk. 2, litra c (omtalt i kapitel 4, afsnit 4.3). Et arkiv over familiemedlemmer mv. kan meget vel være privat, men kun i det omfang det ikke offentliggøres.

Det hedder videre i artikel 89: "Disse garantier skal sikre, at der er truffet tekniske og organisatoriske foranstaltninger, især for at sikre overholdelse af princippet om dataminimering." De sikkerhedsmæssige foranstaltninger skal som altid være på plads, jf. især artikel 32, men netop spørgsmålet om dataminimering trænger sig på. Et omfattende statistisk materiale, som i Danmark i høj grad er muliggjort med den omfattende brug af CPR-numre, kan give anledning til nye søgninger, altså udtræk af statistisk viden, uden at nogen havde tænkt på det, da oplysningerne blev indsamlet. Efter de tidligere regler måtte man kun bruge personoplysninger til de indsamlede formål, men dette er nu udvidet. Efter artikel 5, stk. 1, litra b, må man ikke bruge de indsamlede personoplysninger på en måde, der er *uforenelig* med det oprindelig formål, men viderebehandling til arkiv, forskning, historie og statistik anses *ikke som uforenelig* med det oprindelig formål. Eller sagt på en anden måde: Oplysninger kan behandles til arkiv-, forsknings-, historie- og statistiske formål, uanset hvordan de i øvrigt er indsamlet. Det omvendte er ikke tilfældet. Databeskyttelsesloven bestemmer i § 10, stk. 2, at oplysninger, der behandles (herunder indsamles) til videnskabeligt eller statistisk formål, ikke senere må behandles til andet formål – men altså nok til ny videnskabelig eller statistisk behandling.

Som modvægt hertil indskærper artikel 89 vigtigheden af dataminimering, herunder muligheden for pseudonymisering, og hvis det er muligt, bør oplysningerne helt anonymiseres. Kan der ske anonymisering, falder behandlingen helt uden for persondataretten.

Artikel 89, stk. 2, 3 og 4, giver medlemsstaterne mulighed for at begrænse retten til indsigt, berigtigelse, behandlingsbegræsning og indsigelse (efter artiklerne 15, 16, 18 og 21) og ved arkivformål tillige retten til dataportabitet (efter artikel 20). Ideen er, at det skal være muligt at forske og udarbejde statistik på baggrund af indsamlede personoplysninger, uden at den enkelte kan modsætte sig. Til gengæld er der (ind)skærpede krav til dataminimering, og efter dansk ret kræves der en egentlig tilladelse, hvis oplysningerne ønskes videregivet til tredjelande, hvis de vedrører biologisk materiale, eller hvis der ønskes videregivelse i videnskabelige tidsskrifter, jf. DBL § 10, stk. 3.

6.6. Oplysninger om strafbare forhold

Termen "strafbare forhold" dækker bredt og omfatter både selve gerningen eller mistanke herom, den eventuelle straffesag, og efterfølgende oplysninger om afsoning og om den tidligere straffedom. Under "strafbare forhold" hører også rettighedsfrakendelse. Hvis en person er frakendt retten til at være advokat, er dette en oplysning om strafbart forhold i persondatarettens forstand.

Man kan overveje, om også forkerte oplysninger om strafbare forhold hører under bestemmelsen. Hvis en person udsættes for en chikanøs politianmeldelse, der intet har på sig, har den pågældende ikke begået noget strafbart (mens anmelderen eventuelt kan pådrage sig straf, jf. straffelovens § 165), og det kan derfor virke søgt at tale om strafbare forhold.[42] På den anden side er urigtige personoplysninger også omfattet af persondataretten – med ret til korrektion eller sletning, jf. GDPR artikel 5 og artikel 16 – og en urigtig oplysning om strafbare forhold synes derfor bedst at skulle behandles efter reglerne for denne type oplysninger: Der er ingen grund til, at en urigtig oplysning om strafbare forhold kun skal vurderes efter artikel 6 med dennes mere omfattende hjemmelsgrundlag.

42. Betænkning 1565/2017, s. 233-234 afviser, at sådanne forkerte oplysninger kan falde under kategorien "strafbare forhold".

Lovteknisk er det skruet sådan sammen, at GDPR artikel 10 kategoriserer oplysning om strafbare forhold under almindelige oplysninger.[43] Dog overlades den nærmere regulering til national ret med krav om, at den offentlige myndighed enten skal føre kontrol, eller også skal den nationale (eller EU-) lovgivning give et behandlingsgrundlag med de fornødne sikkerheder. Et omfattende straffedomsregister må dog kun føres under en offentlig myndigheds kontrol.

Den danske regulering i databeskyttelseslovens § 8 er bygget op på den måde, at offentlige myndigheders behandling reguleres i stk. 1 (behandling generelt) og stk. 2 (særligt om videregivelse), og privates behandling af oplysninger om personers strafbare forhold er reguleret i stk. 3 (behandling generelt) og stk. 4 (særskilt om videregivelse). Endelig refererer stk. 5 til behandling af følsomme oplysninger.

Man skal – selvfølgelig – være opmærksom på andre regler i persondataretten. Sker omtalen af strafbare forhold i personlig venne- eller familiekreds, falder situationen helt uden for persondataretten, jf. GDPR artikel 2, stk. 2, litra c, og sker behandlingen i journalistisk øjemed, gælder særlige regler (se kapitel 20).

Efter Datatilsynets praksis bliver mere løse beskyldninger kategoriseret som "meningstilkendegivelser", der helt er undtaget persondataretten efter DBL § 3, stk. 1, om ytrings- og informationsfrihed. Hvis beskyldningerne derimod er specificerede og velbegrundede, skal § 8 anvendes. Det giver den ejendommelige situation, at ubegrundede beskyldninger om strafbare forhold frit kan behandles, mens begrundede beskyldninger kun må behandles efter de strammere krav i databeskyttelseslovens § 8. Datatilsynets praksis er nok praktisk på den måde, at tilsynet slipper for at behandle sager om ubegrundede beskyldninger, men den er ikke i god overensstemmelse med ytrings- og informationsfriheden, hvor netop de velbegrundede og sande beskyldninger nyder en langt større beskyttelse end ubegrundede beskyldninger.[44]

---

43. Jf. referencen i artikel 10 til artikel 6, stk. 1.

44. Se f.eks. EMD-domstolens afgørelse af 7. juni 2017 i sagen *Medzlis Islamske Zajednice Brcko v Bosnien-Herzegovina*, hvor en national dom med sanktioner for æreskrænkende udtalelser imod en navngiven person fandtes at være overensstemmende med ytrings- og informationsfriheden, fordi beskyldningerne ikke var velbegrundede.

6.6.1. Offentlige myndigheder. Generelt krav til behandling

I udgangspunktet "må der ikke behandles oplysninger om strafbare forhold, medmindre det er nødvendigt for varetagelsen af myndighedens opgaver". Reglen siger således på den ene side, at hvis behandling af en oplysning om en persons strafbare forhold er nødvendig for myndighedens opgave, så er den tilladt. Det er oplagt, at politiet må behandle oplysninger om strafbare forhold, men også for andre myndigheder kan det være relevant, f.eks. forskellige tilsynsmyndigheder inden for skat, miljø, arbejdsmiljø osv. Er rene straffeattester[45] eller børneattester[46] en forudsætning for en autorisation, kan myndigheden naturligvis behandle sådanne oplysninger. På den anden side skal det netop være "nødvendigt". Hvis strafbare forhold ikke er relevante for den pågældende myndighedsudøvelse, må sådanne oplysninger ikke behandles. Et hospital vil typisk ikke skulle bruge oplysninger om strafbare forhold for at kunne behandle en patient, oplysningerne er typisk ikke nødvendige, og behandling derfor typisk ikke tilladt.

Endelig skal man være opmærksom på, at "nødvendighed" er den eneste mulighed for behandling, når der ikke er tale om videregivelse (herom nedenfor afsnit 6.6.2). Det indebærer, at en myndighed ikke kan behandle oplysninger om strafbare forhold (bortset fra videregivelse), selvom den registrerede har samtykket. Ideen er den for så vidt selvfølgelige, at myndigheden ikke skal andet end at udføre sin opgave.

6.6.2. Offentlige myndigheder. Videregivelse

For den behandling, der består i videregivelse af strafbare oplysninger, er der flere muligheder end kravet om nødvendighed.

For det første kan den registrerede efter § 8, stk. 2, nr. 1, give samtykke til videregivelse (men altså ikke til anden behandling).

45. Efter bekendtgørelse om behandling af personoplysninger i Det Centrale Kriminalregister (nr. 881 af 4. juli 2014 med senere ændringer) kan oplysninger om afgørelser – også kaldet straffeattesten – videregives til private under samme betingelser som nævnt i databeskyttelseslovens § 8, stk. 2.

46. Efter børneattestloven (lovbekendtgørelse af 362 af 2. april 2014 med senere ændringer) skal der indhentes børneattest i forbindelse med ansættelse o.a. i job med kontakt til børn under 15 år.

Samtykket skal være udtrykkeligt og i øvrigt leve op persondatarettens krav om samtykke, jf. ovenfor afsnit 6.4.1.

For det andet kan der efter § 8, stk. 2, nr. 2, ske videregivelse, hvis det sker "til varetagelse af private eller offentlige interesser, der klart overstiger hensynet til de interesser, der begrunder hemmeligholdelse, herunder hensynet til den, oplysningen angår". Der er tale om vægtet afvejning (se tilsvarende for private nedenfor afsnit 6.6.4), hensynet til den modgående interesse skal "klart" overstige hensynet til den registrerede. Forarbejderne nævner, at væsentlige hensyn som forbrugerbeskyttelse, folkesundhed eller miljøbeskyttelse i forbindelse med offentliggørelse af kontrolresultater kunne falde under bestemmelsen i nr. 2, ligesom f.eks. tilsynsmyndigheders videregivelse af oplysninger om sundhedspersonales strafbare forhold til regionerne eller til udenlandske sundhedsmyndigheder. [47]

Det er dog det problem, at forordningen ikke giver mulighed for, at offentlige myndigheder kan benytte en afvejningsbestemmelse som hjemmel. Afvejningsreglen i artikel 6, stk. 1, litra f, om almindelige personoplysninger gælder ikke for offentlige myndigheder, og der er ikke nogen afvejningsbestemmelse i artikel 9 om de følsomme oplysninger. Forordningen opererer ganske vist med et vist råderum for den nationale lovgivning, jf. artikel 6, stk. 2, men denne angår ikke afvejningsbestemmelsen, men kun bestemmelserne i artikel 6, stk. 1, litra c (retlig forpligtelse) og litra e (opgave i samfundets interesse, herunder myndighedsudøvelse). Der synes således ikke at være nogen retlig mulighed for national lovgivning, der muliggør en afvejningsbestemmelse for offentlige myndigheder ved behandling af personoplysninger, heller ikke når oplysningerne drejer sig om strafbare forhold.

Dette er dog mere et teknisk-retligt problem end et reelt. Bestemmelsen i § 8, stk. 2, nr. 2, har ikke dækning i forordningen, men de eksempler, der nævnes i forarbejderne, kan finde lovligt behandlingsgrundlag i andre bestemmelser, især artikel 6, stk. 1, litra e.

For det tredje kan der ske videregivelse, når den er "nødvendig for udførelsen af en myndigheds virksomhed eller påkrævet for en afgørelse, som myndigheden skal træffe", jf. § 8, stk. 2, nr. 3. Myndighed 1 kan altså videre oplysninger om strafbare forhold til myndighed 2, hvis

47. Betænkning 1565/2017, s. 236.

det er nødvendigt for, at myndighed 2 kan udføre sin opgave, herunder træffe en afgørelse. Således må f.eks. en tilsynsmyndighed videregive oplysninger om strafbare forhold til politiet – og der kan være en forpligtelse hertil i andre bestemmelser – og politiet må videregive oplysninger om strafbare forhold til en myndighed, der skal træffe beslutning om autorisation, hvis autorisation er afhængig af en ren straffeattest.[48]

Endelig *for det fjerde* kan videregivelse ske, hvis den er "nødvendig for udførelsen af en persons eller virksomheds opgaver for det offentlige." En virksomhed, der leverer ydelser til det offentlige, må således kunne få oplysninger om strafbare forhold fra det centrale kriminalregister.[49]

6.6.3. Privates behandling og videregivelse

Privates behandling er reguleret i DBL § 8, stk. 3 og 4. Stk. 3 handler om behandling af oplysninger om strafbare forhold generelt, mens stk. 4 handler om videregivelse. Imidlertid er der ingen reel forskel på de to bestemmelser, og der er ikke i forarbejderne angivet nogen begrundelse for opdelingen.

Der er to muligheder for privates behandling af oplysninger om personers strafbare forhold, nemlig udtrykkeligt samtykke og en vægtet afvejning.

Hvad *samtykke* angår, skal dette være udtrykkeligt, ligesom ved behandling af følsomme oplysninger. Hertil skal samtykket opfylde de almindelige persondataretlige krav: Samtykket skal være frivilligt, specifikt, informeret og utvetydigt. Der henvises til nærmere behandling heraf ovenfor afsnit 6.4.1.

Om den *vægtede afvejning* siger § 8, stk. 3: "behandling (kan) ske, hvis det er nødvendigt til varetagelse af en berettiget interesse og denne interesse klart overstiger hensynet til den registrerede." Der stilles således skærpede krav til afvejningen i forhold til artikel 6, stk. 1, litra f. Dette giver god mening, da oplysninger om strafbare forhold kan være mere følsomme end almindelige oplysninger som navn og telefonnum-

48. Betænkning 1565/2017, s. 239.

49. Se tilsvarende formulering i kriminalregisterbekendtgørelsens § 17.

mer – uden dog at strafbare oplysninger behandles som en følsom oplysning efter GDPR artikel 9.

Forarbejder lægger op til, at bestemmelsen kun undtagelsesvist kan anvendes. Det kunne f.eks. være registrering af strafbare forhold med henblik på at indgive politianmeldelse og eventuelt senere vidneforklaring i retten. Og af hensyn til den registrerede nævnes, at en organisation som Amnesty International må behandle oplysninger, f.eks. fordi den pågældende person ikke kan findes eller ikke kan kontaktes på grund af fængsling.[50]

Den tilsvarende formulering i stk. 4 er en smule anderledes, men forskellen til formuleringen i stk. 3 er blot, at det i stk. 4 er specificeret, at der både kan være tale om private og offentlige interesser, og at interessen kan ligge hos den registrerede (som eksemplet med Amnesty International viser). Dette vil også være tilfældet efter stk. 3.

Et tilsyneladende udbredt fænomen på internettet går ud på at omtale eller advare imod personer, der menes at have begået noget strafbart eller i hvert fald noget dadelværdigt eller irriterende.

Retsstillingen kan skitseres som følger:

Efter *straffeloven* kan det være strafbart at beskylde andre for noget kriminelt eller andet, der kan være alvorligt f.eks. i forhold til erhverv, job mv. En sådan beskyldning er selvfølgelig straffri, hvis den er sand: Man må gerne kalde en morder for en morder. Men selvom den ikke helt præcist er sand, kan det være straffrit, hvis der er et faktuelt grundlag for vurderingen, og hvis vurderingen har en "anerkendelsesværdig interesse".[51] Ubegrundede beskyldninger og formodninger (om lidt grovere forhold) kan derfor være strafbare, og det samme gælder udbredelse og videregivelse af rygter (fortsat af grovere karakter), der kun har til hensigt at genere ekskærester eller andre, man ikke bryder sig om.[52]

Efter *persondataretten* ser det noget anderledes ud. Hvis der ikke er samtykke – og det vil der i praksis sjældent være – så kan oplysninger

50. Betænkning 1565/2017, s. 238-239.

51. Straffelovens §§ 267 og 269.

52. Der henvises til litteratur, der mere indgående behandler dette emne, f.eks. Jakobsen & Schaumburg-Müller 2013 og Baumbach 2017. Man skal her være opmærksom på, at straffelovens bestemmelser blev ændret pr. 1. januar 2019.

om strafbare forhold kun undtagelsesvist behandles. Interessen i behandlingen, her i form af omtale på nettet, skal veje markant tungere end den registreredes interesse i ikke at få sine (mulige) strafbare forhold offentlig omtalt. Og det vil sjældent være tilfældet. Heller ikke i tilfælde, hvor den pågældende tages på fersk gerning f.eks. via tv-overvågning, må det strafbare forhold videregives til offentligheden, men gerne til politiet.[53] Som ovenfor nævnt vil mere løse beskyldninger blive kategoriseret som meningstilkendegivelser, hvorfor de efter Datatilsynets praksis ikke er omfattet af persondataretten. Hertil skal man være opmærksom på, at beskyldninger mod firmaer kun er omfattet af persondataretten, hvis beskyldningen er rettet mod en fysisk person. Virksomheder er ikke beskyttet efter *person*dataretten.

Fremadrettet burde det overvejes, om § 8 kunne formuleres mere heldigt, og om den måske er helt overflødig. Afvejningsreglen i § 8, stk. 2, nr. 2, har ikke nogen hjemmel i forordningen, og som nævnt er indholdet af § 8, stk. 3 og 4, i realiteten identisk, hvorfor der ikke synes at være nogen grund til at foretage en opdeling i behandling og videregivelse. Endvidere synes de situationer, hvor oplysninger om strafbare forhold lovligt kan behandles, dækket af bestemmelserne om følsomme oplysninger (se umiddelbart nedenfor om § 8, stk. 5). Man kunne derfor formentlig nøjes med denne ene bestemmelse i § 8. Og endelig er der det problem, at løse ubegrundede beskyldninger om strafbare forhold er lovlige, mens mere detaljerede og begrundede beskyldninger ikke er. Det virker ikke overbevisende, og det er i modsætning til retsstillingen både efter straffeloven og efter Den Europæiske Menneskerettighedskonvention.[54]

6.6.4. Behandling efter reglerne for følsomme oplysninger

Efter § 8, stk. 5, kan oplysninger om strafbare forhold også behandles, hvis betingelserne for behandling af følsomme oplysninger er opfyldt.

53. Lovteknisk er videregivelse til politiet en tungtvejende interesse efter databeskyttelseslovens § 8, stk. 4, og i tv-overvågningsloven er det præciseret, at der kan ske videregivelse til politiet, jf. § 4 c, stk. 3.

54. Se bl.a. EMD-domstolens afgørelse af 7. juni 2017 i sagen *Medzlis Islamske Zajednice Brcko v Bosnien-Herzegovina* med systematisk gennemgang og analyse af afvejningen mellem privatlivsbeskyttelse i form af æreskrænkelser og ytrings- og informationsfriheden.

Bestemmelsen er formuleret ud fra den opfattelse, der var fremherskende før november 2019, dvs., at bestemmelserne i artikel 9, stk. 2, danner et behandlingsgrundlag. Eftersom denne opfattelse nu er forladt, fremstår henvisningen i § 8, stk. 5, i bedste fald som overflødig; i værste fald misvisende.

Der er dog ikke noget i vejen for, at man overvejer de situationer, der er undtaget fra forbuddet mod at behandle følsomme oplysninger, hvilket gøres i det efterfølgende.

Hvis oplysningen "tydeligvis er offentliggjort af den registrerede", kan oplysningen viderebehandles af andre.[55] En person, der selv fortæller om sine strafbare forhold, må tåle, at disse oplysninger også behandles af andre. Man skal dog være sikker på, at det er personen selv, der har offentliggjort oplysningerne. Hvis en person, P, til en journalist, fortæller om sin afsoning, vil P have offentliggjort, at han/hun er dømt for strafbare forhold, og andre må behandle den oplysning. Hvis der i artiklen eller udsendelsen tilføjes oplysninger om, hvilken form for kriminalitet P har begået, er det ikke sikkert, at P har samtykket til disse mere detaljerede oplysninger, og betingelsen for viderebehandling heraf er ikke opfyldt.

Oplysninger om strafbare forhold kan også lovligt behandles, hvis "*behandling er nødvendig, for at retskrav kan fastlægges*, gøres gældende eller forsvares, eller når domstole handler i deres egenskab af domstol", jf. litra f i GDPR's artikel 9, stk. 2. Behandlingsgrundlaget må findes i artikel 6, stk. 1, litra e. Det er oplagt, at politiet kan behandle oplysninger om eventuelle strafbare forhold for at kunne tage stilling til eventuel retsforfølgning, og det er lige så oplagt, at private kan behandle oplysninger om (eventuelt) strafbare forhold med henblik på at foretage en anmeldelse eller selv anlægge sag (hvilket er muligt, hvis der er tale om privatlivskrænkelser, æreskrænkelser og ophavsretskrænkelser). Det er selvfølgelig også oplagt, at en domstol kan behandle oplysnin-

55. Referencen er noget omstændelig: det følger af DBL § 8, stk. 5, at oplysninger om strafbare forhold kan behandles, hvis betingelserne i § 7 om følsomme oplysninger er opfyldt. Herefter følger det af § 7, stk. 1, at behandlinger efter GDPR artikel 9, stk. 2, litra a, c, d, e og f, også efter dansk ret er lovlige, og det følger så af GDPR artikel 9, stk. 2, litra e, at der ikke er forbud mod at behandle følsomme oplysninger. For et egentligt behandlingsgrundlag skal man tilbage til artikel 6, stk. 1, hvor litra f er oplagt.

ger om strafbare forhold. Ellers ville domstole slet ikke kunne fungere i straffesager.

Efter litra g er der ikke forbud mod behandling af følsomme oplysninger, hvis behandlingen "er *nødvendig af hensyn til væsentlige samfundsinteresser* [...]". I den danske bestemmelse kræves, at tilsynsmyndigheden, hvilket vil sige Datatilsynet, skal give tilladelse, hvis private vil persondatabehandle efter denne bestemmelse, jf. DBL § 7, stk. 4. Omfattende registre over straffedomme må kun føres under myndighedskontrol, jf. GDPR artikel 10. Bemærk her, at er registrene tilstrækkeligt anonymiserede, vil de falde helt uden for persondataretten (nærmere om anonymisering afsnit kapitel 3, afsnit 3.2).

6.7. Særlige kategorier og særlige områder

Som nævnt ovenfor i afsnit 6.3 er der ud over de centrale kategorier af personoplysninger nogle særlige kategorier og nogle særlige områder. De undergives ikke her nogen indgående omtale, men tages med for oversigtens skyld. Vil man vide mere, må man søge til speciallitteratur, herunder nogle af denne bogs øvrige kapitler.

CPR-numre: GDPR artikel 87 giver medlemsstaterne mulighed for at fastsætte regler for et nationalt identifikationsnummer, dog med det sædvanlige krav, at der gives "de fornødne garantier for den registreredes rettigheder og frihedsrettigheder i henhold til denne forordning". I Danmark har vi haft CPR-numre siden 1968, hvilket på den ene side er praktisk for at kunne identificere hver borger og giver mulighed for stor, statistisk viden.[56] På den anden side bliver CPR-nummeret brugt til mange forskellige funktioner fra bibliotekslån, sundhedsjournaler, sociale ydelser mv., og det giver derved mulighed for en omfattende, centraliseret viden om hver enkelt borger.

Databeskyttelseslovens § 11 giver offentlige myndigheder ret til at behandle oplysninger om personnummer med henblik på en entydig identifikation eller som journalnummer. Privates brug er tilladt i en række nærmere specificerede tilfælde, der ikke her nærmere bliver omtalt. De detaljerede regler findes i CPR-loven.[57]

---

56. Se om folkeregistreringsloven og forgængeren i kapitel 1, afsnit 1.6.
57. Lovbekendtgørelse nr. 646 af 2. juni 2017 med senere ændringer. Hovedlovene er fra år 2000 og synes at være ændret mindst en gang hvert år siden da.

Oplysninger om gæld til det offentlige: I den danske databeskyttelseslov er der særlige regler om videregivelse af oplysninger om gæld til det offentlige til kreditoplysningsbureauer, jf. DBL §§ 15-18. En sådan videregivelse og behandling antages at have hjemmel i GDPR artikel 6, stk. 1, litra e, om nødvendig behandling i samfundets interesse.[58] De særlige regler angår ikke de følsomme oplysninger eller oplysninger om strafbare forhold, jf. DBL § 15, stk. 2. Dette betyder, at det kun er selve gældsforpligtelsen, der må videregives, men ikke at denne f.eks. hidrører fra bøder, betaling for fængselsophold el.lign.

Reglerne i forordningen om oplysningspligt, indsigelsesret, ret til berigtigelse mv. gælder også i forbindelse med behandlingen af denne særlige type personoplysninger

Retsinformationssystemer: GDPR artikel 10 kræver, at en offentlig myndighed har kontrol med "omfattende" registre over straffedomme. Ideen må være, at mindre domssamlinger, f.eks. til brug i undervisning, ikke er undergivet kravet om kontrol. Sådanne domssamlinger skal selvfølgelig overholde de øvrige regler i persondataretten. Hensynet til dataminimering mv. må indebære, at der skal foretages anonymisering af de omhandlede personer, jf. hertil GDPR artikel 89 om behandling til videnskabeligt formål, hvor der kræves anonymisering, hvis dette er muligt.

DBL § 9 omfatter ikke kun straffedomme, men retsinformationssystemer i det hele taget, og herunder falder både lov-, doms- og afgørelsesregistre. Love er generelle og indeholder ikke personoplysninger,[59] mens både domme og administrative afgørelser netop indeholder oplysninger om personer, både de personer, som der træffes afgørelse om, og andre personer, der måtte optræde i afgørelsen. Sådanne doms- og afgørelsesregistre har stor betydning for retsudøvelsen og retssikkerheden: Uden kendskab til, hvordan love og regler fortolkes i praksis, kan det være svært eller helt umuligt at kende retstilstanden, hvilket er uacceptabelt både for borgere, der gerne vil indrette sig efter loven i bred forstand, og for myndigheder, der skal træffe afgørelser i

58. Justitsministeriets forslag til databeskyttelseslov (L68/2017), s. 203.
59. Se UfR 1999.841 H (Tvind-dommen) om forbuddet mod såkaldt singulær lovgivning, hvilket vil sige en lov, der direkte regulerer forholdet for en navngiven borger.

lignende sager. Heroverfor står hensynet til de personer, hvis oplysninger behandles i de enkelte domme og afgørelser. En væsentlig del af løsningen går ud på, at der foretages en anonymisering, se også Justitsministeriets cirkulære om indlæggelse af afgørelser i Retsinformation.[60]

Behandling til videnskabelige og statistiske formål er reguleret i bl.a. DBL § 10 og er nærmere omtalt ovenfor afsnit 6.5.10.

Behandling i forbindelse med ansættelsesforhold er reguleret i bl.a. DBL § 12. Forordningen åbner mulighed for, at medlemsstaterne opstiller nærmere regler for behandling af personoplysninger i arbejdsforhold, jf. GDPR artikel 88, stk. 1, og stk. 2 skærper kravene hertil, særligt krav i stk. 2 om, at den registreredes værdighed, legitime interesser og rettigheder respekteres. GDPR artikel 9, stk. 2, litra b, indeholder en tilsvarende bestemmelse om, at følsomme oplysninger kan behandles i det omfang, det er nødvendigt og følger af en arbejdsretlig forpligtelse. Baggrunden er, at en arbejdsgiver uvægerligt vil få kendskab til en række personoplysninger om ansatte (og herunder også både tidligere og eventuelt kommende ansatte) og har et legitimt krav på at kunne behandle relevante oplysninger om løn, skat, CPR-nummer, sygdom under ansættelse, oplysninger om strafbare forhold i forbindelse med fremvisning af straffeattest ved ansættelse mv. Se nærmere om persondatabehandling i arbejdsretlig sammenhæng i kapitel 28.

Virksomheders videregivelse af oplysninger til andre virksomheder i markedsføringsøjemed er reguleret i DBL § 13. Der henvises til kapitel 22.

Endelig bestemmer DBL § 14, at videregivelse af personoplysninger *til arkiv* følger af arkivlovgivningen.[61]

60. Cirkulære nr. 85 af 8. juli 1988.

61. Se arkivloven, nu lovbekendtgørelse nr. 1206 af 1201 af 28. september 2016 med senere ændringer.