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 4

Nærmere om persondatarettens dækning

Sten Schaumburg-Müller

Som det fremgik af kapitel 3, er persondataretten i udgangspunktet meget omfattende: Persondataretten dækker al automatisk behandling af oplysninger om identificerbare, fysiske personer, og både "behandling" og "oplysning" skal forstås meget bredt. Hertil kommer en mindre del ikke-automatisk behandling, se ovenfor kapitel 3, afsnit 4.

Fra dette udgangspunkt er der en del undtagelser og modifikationer. I det følgende behandles først forskellige områder med undtagelser mv., afsnit 4.1. Dernæst behandles spørgsmålet om reglernes geografiske anvendelsesområde. Det forekommer oplagt, at f.eks. en behandling, der foregår i Kina og vedrører en kinesisk statsborger, der er bosiddende i Kina, hverken reguleres af databeskyttelsesforordningen (GDPR) eller af den danske databeskyttelseslov. Men hvordan forholder det sig med en behandling, der foregår i USA og vedrører en EU-borger, bosiddende i et EU-land? Eller en behandling i Europa af en amerikaner? Og på de områder, hvor GDPR åbner mulighed for nærmere national regulering, hvornår er det så den danske regulering, der skal anvendes? Disse spørgsmål behandles i afsnit 4.2. Endelig er der den særlige undtagelse i GDPR artikel 2, stk. 2, litra c, der undtager fysiske personers rent private eller familiemæssige behandling, i denne

fremstilling kaldet "privat"-reglen. Omfanget af denne undtagelse behandles særskilt i afsnit 4.3.

4.1. Undtagelser og modifikationer

Fra det brede udgangspunkt er der en længere række undtagelser og modifikationer, jf. databeskyttelseslovens (DBL) §§ 1-3.

4.1.1. Den korte udgave

De mange og forskelligartede undtagelser og modifikationer kan meget kort beskrives som følger:

For det første er der nogle undtagelser, der forekommer intuitivt selvfølgelige. Dette gælder det strafferetlige område, hvor det f.eks. er oplagt, at man ikke kan kræve, at politiet løbende udleverer personoplysninger om igangværende efterforskning. I så tilfælde ville interesserede kriminelle løbende kunne tjekke, hvad politiet har på dem, og indrette sig derefter. Det går selvfølgelig ikke. Det samme gælder det sikkerhedspolitiske. Også her må en stat have mulighed for at træffe de nødvendige foranstaltninger.

For det andet er der nogle undtagelser, som vi i nærværende fremstilling har valgt at gå nærmere ind på, undtagelser, som stort set alle vil komme i berøring med. Dette gælder:

1. Privat behandling, behandlet nedenfor i afsnit 4.3.
2. Generelt hensyn til ytrings- og informationsfrihed, behandlet i kapitel 7.
3. Den særlige regulering af journalistisk behandling, se nærmere kapitel 20.
4. Litterær og kunstnerisk persondatabehandling, nærmere omhandlet i kapitel 21.

Endelig er der en række specialundtagelser og -reguleringer. Disse listes op umiddelbart nedenfor i afsnit 4.1.2.

4.1.2. Den specificerede udgave

Efter DBL § 1, stk. 2, gælder loven og forordningen ikke i de tilfælde, der er omfattet af GDPR artikel 2, stk. 2, litra b-d. Disse tre undtagelser er

- De behandlinger, "som foretages af medlemsstaterne, når de udfører aktiviteter, der falder inden for rammerne af afsnit V, kapitel 2, i TEU", jf. artikel 2, stk. 2, litra b. Dette kapitel i Traktaten om Den Europæiske Union omfatter "Særlige bestemmelser om den fælles udenrigs- og sikkerhedspolitik", et område, hvor Danmark i øvrigt har forbehold. Det er i første omgang op til staterne selv at tage stilling til, hvornår et område falder under udenrigs- eller sikkerhedspolitikken.

  Teknisk set omtaler DBL § 1, stk. 2, ikke GDPR artikel 2, stk. 2, litra a, der bestemmer, at forordningen ikke gælder på områder, der ikke er berørt af EU-retten. Eftersom det i realiteten kun er sikkerhedspolitikken, der – i et eller andet omfang – falder uden for EU-retten, er reglen ikke gentaget i den danske lovgivning.
- De behandlinger, "som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter", falder udenfor. Denne undtagelse er nærmere behandlet nedenfor afsnit 4.3.
- Strafferetlig efterforskning mv. er også undtaget. De behandlinger, "som foretages af kompetente myndigheder med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner, herunder beskytte mod og forebygge trusler mod den offentlige sikkerhed", er undtaget efter GDPR artikel 2, stk. 2, litra d. Her gælder i stedet retshåndhævelsesloven[1] (RHL), der er udformet på baggrund af EU-direktiv 2016/680.[2]

1. Lov nr. 410 af 27. april 2017 om retshåndhævende myndigheders behandling af personoplysninger, retshåndhævelsesloven (RHL).
2. Europa-Parlamentets og Rådets Direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse

Det bemærkes, at undtagelsen kun angår de kompetente myndigheders behandling, herunder politi, anklagemyndighed og domstole, hvad straffesager angår, se nærmere RHL § 1. Andres behandling af strafbare forhold er reguleret i DBL § 8. Hvis en forretningsindehaver F optager en indbrudstyv på en tv-overvågning, vil F's behandling af disse data være reguleret efter DBL § 8 og tv-overvågningsloven (TVOL), se nærmere herom i kapitel 6, mens politiets håndtering af en eventuel anmeldelse reguleres af rethåndhævelsesloven.

DBL § 1, stk. 3, indeholder en særlig prioriteringsregel:

> "Regler om behandling af personoplysninger i anden lovgivning, som ligger inden for databeskyttelsesforordningens rammer for særregler om behandling af personoplysninger, går *forud* for reglerne i denne lov." (egen kursivering).
>
> Dette betyder, at hvis der er andre persondataretlige regler, der er mere specifikt rettede mod andre sektorer, skal disse regler anvendes i stedet for reglerne i databeskyttelsesloven. Som nævnt umiddelbart ovenfor er politiets behandling af persondata i straffesager undtaget DBL og GDPR, og retshåndhævelsesloven kan for så vidt siges at være et eksempel på et særområde, hvor der gælder særlige regler.
>
> Det er dog kun eventuelle særlige persondataregler, der skal anvendes forud. Andre regler, f.eks. straffelovens regler, skal anvendes uafhængigt af persondatarettens regler, eller "i sammenstød med", som jurister siger. Det betyder, at begge regelsæt kan anvendes uafhængigt af hinanden. I sådanne situationer skal man være opmærksom på, at reguleringen kan være forskellig: Hvis en person tager et billede af en anden person til eget private brug, vil situationen ikke være dækket af persondataretten, jf. GDPR artikel 2, stk. 2, litra c ("privat"-reglen omtalt nedenfor afsnit 4.3), mens det i straferetlig henseende er relevant, *om* den fotograferede befinder sig på ikke frit tilgængeligt sted, og *om* fotograferingen er uberettiget, f.eks. fordi der ikke foreligger samtykke. Er disse betingelser opfyldt, er fotograferingen strafbar efter straffelovens (STL) § 264 a[3] – men altså ikke omfattet af persondatarettens regler.

2008/977/RIA.

3. Se f.eks. Jakobsen & Schaumburg-Müller 2013, kapitel 4.

DBL § 2, stk. 1-3 *udvider* persondatarettens anvendelsesområde:

> § 2, stk. 1, udvider dækningen til al manuel persondatabehandling, der foretages af forvaltningen. Normalt vil forvaltningsmyndigheder behandle digitalt, og normalt vil oplysningen være indeholdt i eller beregnet til et register og derfor være omfattet. Men for de – formentlig ret få – tilfælde, hvor disse to betingelser ikke er opfyldt, bestemmer § 2, stk. 1, at behandlingen under alle omstændigheder er omfattet af centrale bestemmelser i persondataretten, nærmere bestemt DBL §§ 6-8, 10 og § 11, stk. 1, og GDPR artikel 5, stk. 1, litra a-c, artikel 6, artikel 7, stk. 3, nr. 1, og 2, artikel 9, artikel 10 og artikel 77, stk. 1.
>
> Bestemmelserne i § 2, stk. 2 og 3, udvider dækningen til også at omfatte oplysninger om *virksomheder mv.*, når behandling udføres af et kreditoplysningsbureau. Med "virksomheder m.v." forstås ikke blot erhvervsdrivende virksomheder, men også foreninger og institutioner.[4] GDPR gælder kun for behandling af oplysninger om fysiske personer, jf. ovenfor kapitel 3, afsnit 1, men her bestemmer DBL § 2, stk. 2, så, at loven og forordningen alligevel også gælder for behandling af oplysninger om juridiske personer, hvis denne behandling udføres for kreditoplysningsbureauer. Stk. 3 bestemmer, at hele databeskyttelseslovens kapitel 4 om videregivelse til kreditoplysningsbureauer af oplysninger om gæld til det offentlige også reguleres af persondataretten.

Persondataret og tv-overvågning:

> DBL § 2, stk. 4, regulerer forholdet til tv-overvågningsloven: Persondataretten gælder enhver form for behandling af personoplysninger i forbindelse med tv-overvågning. Tv-overvågningsloven regulerer betingelserne for, hvornår der overhovedet må foretages tv-overvågning. Hertil indeholder loven nogle regler for behandling af personoplysninger, der fremkommer i forbindelse med tv-overvågning. Det er således meget begrænset, hvem tv-overvågningsbilleder må videregives til, hvis de indeholder personoplysninger, jf. TVOL §§ 4 c (der gælder private) og 4 d (der gælder kommuner). DBL § 2, stk. 4, bestemmer så, at persondatarettens regler gælder

4. Se Waaben & Nielsen 2015, s. 98. bestemmelsen i DBL § 2, stk. 2, er en videreførelse af den tidligere persondatalov (PDL) § 1, stk. 4.

ud over disse særlige regler for behandling af personoplysninger i tv-overvågningsloven. (Se nærmere om tv-overvågning kapitel 8, afsnit 7).

Afdøde:

Som nævnt ovenfor i kapitel 3, afsnit 1, gælder GDPR kun for levende, fysiske personer. DBL § 2, stk. 5, bestemmer for dansk rets vedkommende, at loven og forordningen tillige finder anvendelse på oplysninger om afdøde personer i 10 år efter vedkommendes død. Stk. 6 giver mulighed for, at der ved bekendtgørelse kan fastsættes en kortere eller længere periode end 10 år. Ideen er, at der på særlige områder kan være behov for en anden beskyttelsesperiode, og en sådan kan så fastsættes uden at skulle ændre loven. P.t. – april 2019 – er der ikke sådanne særlige regler.

Mulighed for at udvide persondatarettens område til også at gælde juridiske personer:

Som nævnt gælder persondataretten som udgangspunkt kun for fysiske personer, mens DBL § 2, stk. 3 og 4 udvider dækningen, når der er tale om kreditoplysningsbureauer.

§ 2, stk. 7 og 8, giver mulighed for yderligere at udvide dækningen til juridiske personer, uden at dette kræver en lovændring. P.t. – april 2019 – er der ikke udstedt sådanne bekendtgørelser.

DBL § 3 indeholder en række undtagelser og modifikationer. En del af disse relaterer sig til GDPR artikel 85, der foreskriver, at medlemsstaterne ved lov nærmere skal forene hensynet til beskyttelse af personoplysninger med hensynet til informations- og ytringsfriheden. Der ligger heri en stor selvbestemmelse for staterne med hensyn til, hvordan denne "forening" nærmere skal ske. På den anden side er det et krav efter GDPR, *at* medlemsstaterne foretager nærmere overvejelser over forholdet mellem disse to hensyn, der ikke altid går i samme retning, og *at* dette kommer til udtryk i lovgivning.

Forholdet til ytrings- og informationsfriheden:

DBL § 3, stk. 1, bestemmer, at loven og forordningen ikke finder anvendelse, hvis det vil være i strid med EMRK artikel 10 og EUC, artikel 11. Denne undtagelse behandles nærmere i kapitel 7.

PET, FE og Folketingets parlamentariske arbejde:

Politiets og forsvarets efterretningstjenesters persondatabehandling er undtaget, jf. DBL § 3, stk. 2. På samme måde som ved strafferetlig behandling duer det ikke f.eks. at give forbrydere eller farlige personer indsigt i, hvilke oplysninger myndigheden ligger inde med, hvordan de er indsamlet osv. Det bemærkes, at PET og FE ikke er omfattet af retshåndhævelsesloven, der regulerer politiets, anklagemyndighedens, mfl., behandling af personoplysninger.

Folketingets *parlamentariske* arbejde er også undtaget, jf. § 3, stk. 3. Bestemmelsen skal ses i sammenhæng med GDPR artikel 85. Folketingsmedlemmer har en særligt beskyttet ytringsfrihed, jf. grundlovens § 57, og ideen er, at Folketingets Administration i dets bistand til medlemmerne er fritaget for reglerne i persondataretten.[5] Anden administration, f.eks. vedrørende løn for ansatte ved Folketinget, er omfattet af persondataretten.

Undtagelser fra persondatabehandling i journalistisk øjemed mv.:

DBL § 3, stk. 4-8, friholder på forskellig vis persondatabehandling i journalistisk øjemed. Undtagelserne knytter an til anden lovgivning og behandles nærmere i kapitel 20.

Også kunstnerisk og litterær virksomhed holdes i vidt omfang uden for persondataretten. Dette område behandles i kapitel 21.

Begrænsning i opbevaringssted:

GDPR nævner også den frie udveksling af personoplysninger inden for EU som et formål, jf. artikel 1, stk. 3, ved siden af beskyttelsen af fysiske personers oplysninger. Medlemsstaterne kan derfor ikke gyldigt træffe beslutninger om, at personoplysninger, der er omfattet af GDPR, kun må behandles nationalt, herunder f.eks. kun må opbevares nationalt. GDPR omfatter imidlertid ikke forhold, der hører under statens sikkerhed, jf. GDPR artikel 2, stk. 2, litra a og b.

5. Betænkning 1565/2017, s. 955.

> På dette område giver DBL § 3, stk. 9, mulighed for, at justitsministeren efter forhandling med den relevante minister kan bestemme, at it-systemer med personoplysninger, der behandles af den offentlig forvaltning, kun må opbevares i Danmark.[6]

Forsvarets internationale virke

> Efter DBL § 3, stk. 10 kan forsvarsministeren "fastsætte regler om, at loven og databeskyttelsesforordningen helt eller delvis ikke finder anvendelse på forsvarets behandling af personoplysninger i forbindelse med forsvarets internationale operative virke." Bemyndigelsen er udnyttet ved bkg. 594 af 29. maj 2018.

4.2. Geografisk anvendelsesområde

Jurister taler her sommetider om "jurisdiktion", som er spørgsmålet om, hvilket lands lov der skal anvendes på en situation. Hvis f.eks. en person, P, der bor i Flensborg og arbejder på en virksomhed i Aabenraa, hvis virksomheden, V, behandler persondata, og hvis P til tider arbejder hjemme, efter hvilket regelsæt skal det afgøres, om der er sket en ulovlig behandling? GDPR, selvfølgelig, den gælder for alle EU-lande, men dansk eller tysk ret? Eller bulgarsk ret, hvis behandlingen omfatter personer fra Bulgarien?

Man kan tale om flere forskellige principper for jurisdiktion:

1. **Territorialprincippet:** Her er det afgørende, hvor *handlingen* foregår. I det ovennævnte tilfælde foregår handlingen i Tyskland.
2. **Personalitetsprincippet:** Her er det afgørende, hvor den *udførende person* befinder sig eller har sin tilknytning. I ovennævnte tilfælde befinder den fysiske person sig i Tyskland, mens den juridiske person befinder sig i Danmark.
3. **Det passive personalitetsprincip:** Her er det afgørende, hvor den, det går ud over, befinder sig. Behandles data om en bulgarer, vil bulgarsk ret kunne anvendes.

6. Bestemmelsen træder i stedet for tidligere såkaldte "krigsregel" i PDL § 41, stk. 4.

4. **Universaljurisdiktion:** Loven gælder alle steder. Umiddelbart forekommer dette måske oplagt, især for grovere forbrydelser, men der viser sig hurtigt problemer: *For det første* er det politisk uacceptabelt, hvis f.eks. kinesisk ret skulle gælde i Danmark på alle mulige områder. *For det andet* er det upraktisk: Danske myndigheder har ikke gode muligheder for at efterforske i andre lande, og da slet ikke mulighed for at retsforfølge. Endelig er der hensynet til gerningsmanden. Det kan være svært nok at finde ud af, hvad der gælder efter dansk ret, men hvis man også skulle overholde alle andre landes ret samtidig, ville det være helt umuligt.

Persondataretten er væsentligst bygget på personalitetsprincippet og det passive personalitetsprincip, og det giver sammenlagt en ganske bred dækning.

4.2.1. GDPR. EU-ret

Det hedder i GDPR artikel 3, stk. 1: "Denne forordning finder anvendelse [...] på aktiviteter, der udføres for en dataansvarlig eller en databehandler, som er etableret i Unionen, uanset om behandlingen finder sted i Unionen eller ej."

Der er *ikke* noget krav om, at databehandlingen skal finde sted i EU. Territorialprincippet anvendes således ikke.

Det er tilstrækkeligt, at enten en dataansvarlig eller en databehandler er etableret i EU. En dataansvarlig er den, der bestemmer, at der skal foretages aktiviteter, der udgør persondatabehandling. Den tilsvarende engelske term "controller" er måske en bedre betegnelse.[7] (Se kapitel 10 for nærmere om databehandler mv.). En databehandler er den, der behandler persondata på den dataansvarsliges vegne. At være etableret vil i hvert fald omfatte også filialer af udenlandske virksomheder,[8] og selv blot en enkelt repræsentants tilstedeværelse i EU kan være

7. I princippet er alle sprogversioner lige gyldige, jf. EU-domstolen i C-283/81, *CILFIT*, pr. 18. Det er derfor helt relevant at inddrage termer mv. fra andre sprogversioner, da disse også er retskilder.
8. EU-domstolens afgørelse af 13. maj 2014 i sagen *Google Spain*, C-131/12.

tilstrækkelig.[9] Personalitetsprincippet er genkendt, og det fungerer her på den måde, at det knytter sig til både dataansvarlige og databehandlere, men ikke til andre. Både dataansvarlige og databehandlere vil ofte være virksomheder eller foreninger, dvs. juridiske personer, men det kan selvfølgelig også være en enkelt, fysisk person, hvis denne selvstændigt behandler persondata og ikke gør det som led i en ansættelse hos en dataansvarlig eller en databehandler.

GDPR artikel 3, stk. 1, indebærer, at hvis blot en dataansvarlig eller en databehandler er etableret i EU, finder GDPR anvendelse.[10] Det er således uden betydning, hvor selve den fysiske databehandling foregår, og hvem behandlingen retter sig mod. En dataansvarlig eller databehandler med kontor eller repræsentation i EU vil være omfattet af GDPR, også selvom hovedsædet har adresse på Bahamas, serveren står i USA, og behandlingen vedrører en congoleser.

Hertil kommer GDPR artikel 3, stk. 2, der bestemmer, at forordningen finder anvendelse på personer, "der er i Unionen", og hvis behandlingen vedrører "(a) udbud af varer eller tjenester til sådanne registrerede i Unionen, uanset om betaling fra den registrerede er påkrævet, eller (b) overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Unionen."

Det passive personalitetsprincip er genkendt: Det er afgørende, hvor den person, det går ud over – altså den person, der får sine personoplysninger behandlet = den "registrede" – befinder sig. Tilknytningskravet er beskedent. GDPR gælder ikke kun EU-borgere, eller

9. EU-domstolens afgørelse af 1. oktober 2015 i sagen *Weltimmo*, C-230/14", pr. 30: "tilstedeværelsen af en enkelt repræsentant under visse omstændigheder kan være tilstrækkeligt til at udgøre en permanent struktur, såfremt denne repræsentant optræder med en tilstrækkelig grad af stabilitet og under tilstedeværelse af de midler, der er nødvendige for at kunne levere de pågældende konkrete tjenesteydelser i den pågældende medlemsstat."

10. EU-Domstolen har netop anvendt dette princip i EU-domstolens afgørelse af 24. september 2019 i sagen *Google France*, C-507/17. Domstolen bestemmer videre, at forpligtelsen til at fjerne links kun angår links, hvad angår medlemsstater, ikke links, der knytter sig til ikke-medlemsstater, pr. 64-66. I en anden dom, EU-domstolens afgørelse af 3. oktober 2019 i sagen *Eva Glawischnig-Piesczek v Facebook Ireland*, C-17/18, fastslår EU-Domstolen, at EU-retten ikke er til hinder for, at en sletning, pålagt i én medlemsstat, pålægges gennemført i alle EU-stater, pr. 49. Men krav om sletning i alle EU-lande er ikke noget, der følger af EU-retten.

personer, der bor i et EU-land, men alle, der blot befinder sig i EU. Et colombiansk firmas overvågning af en amerikaner, der besøger Paris, vil således være omfattet af GDPR.

Dertil skal en af de to betingelser i (a) og (b) være opfyldt.

Er der tale om udbud af varer eller tjenesteydelser i EU, gælder GDPR for personer i EU. En canadier, der køber varer fra en kinesisk tjeneste under sit turistbesøg i Rom, vil således være beskyttet af GDPR. Princippet gælder også, selvom ydelsen ikke koster noget. Sociale medier, der er gratis i den forstand, at servicen ikke koster penge, vil således være omfattet af GDPR's regler, så snart ydelsen vedrører en person, der befinder sig i EU.

Det samme gælder overvågning. Hvis en fysisk person, der befinder sig i Danmark, bliver overvåget i sin færden på nettet, er denne overvågning en persondatabehandling, der er omfattet af GDPR, uanset hvor overvågningsdataene samles. En amerikansk virksomhed, der indsamler oplysninger om personers færden på nettet, vil være omfattet af GDPR's territoriale dækning, blot den overvågede befinder sig i EU (jf. betragtning 24).

Desuden gælder GDPR for den persondatabehandling, der finder sted på EU-landenes diplomatiske repræsentationer og lignende, jf. artikel 3, stk. 3.

4.2.2. Databeskyttelsesloven. Dansk ret

Et er, hvor GDPR skal anvendes, noget andet, hvornår den danske databeskyttelseslov skal anvendes. Selvom GDPR er en forordning, der uden videre gælder i alle EU-lande, overlades en del regulering i vidt omfang til medlemsstaterne. Det gælder f.eks. behandling af oplysninger om strafbare forhold, jf. GDPR artikel 10, og behandling i journalistisk øjemed, jf. GDPR artikel 85.

I det ovennævnte tilfælde med en virksomhed i Aabenraa vil virksomheden være dataansvarlig eller databehandler, og GDPR skal anvendes, jf. ovenfor om artikel 3, stk. 1. Opstår der spørgsmål om, hvilket lands ret der skal anvendes, f.eks. fordi virksomheden er et medie og behandler personoplysninger i journalistisk øjemed, må man se nærmere på de enkelte landes regler for territorial anvendelse. Den danske databeskyttelseslov er her fornuftigvis bygget op helt på samme måde som GDPR:

Hvis en dataansvarlig eller en databehandler er etableret i Danmark, skal de danske regler anvendes, jf. DBL § 4, stk. 1. Er virksomheden i Aabenraa en medievirksomhed, skal dens behandling af personoplysninger i journalistisk øjemed behandles efter dansk ret (se herom kapitel 20), virksomheden vil være dataansvarlig, og det har ingen betydning for dette spørgsmål, at en medarbejder arbejder fra hjemmeadressen Flensborg. Det er virksomheden, der er dataansvarlig, ikke medarbejderen. (Hvorvidt tysk ret også finder anvendelse, f.eks. fordi personer i Tyskland får deres personoplysninger behandlet, afgøres efter tysk ret).

Hvis en person i Danmark får sine data behandlet, vil den danske databeskyttelseslov skulle anvendes under samme betingelser som nævnt ovenfor: hvis behandlingsaktiviteterne vedrører enten "udbud af varer eller tjenester til sådanne registrerede, der befinder sig i Danmark, uanset om betaling fra den registrerede er påkrævet", *eller* "overvågning af sådanne registreredes adfærd, for så vidt deres adfærd finder sted i Danmark". Bemærk dog, at dansk ret kun skal anvendes, hvis den dataansvarlige eller databehandleren er etableret uden for EU. En tysk virksomhed, der registrerer strafbare forhold også om danske statsborgere, skal derfor *ikke* overholde reglerne herom i den danske databeskyttelseslov (her DBL § 8, behandlet nærmere nedenfor kapitel 7), men reglerne i GDPR (der ikke siger meget herom, jf. artikel 10), og formentlig tysk ret afhængig af, hvordan de tyske regler er udformet.

Og på samme måde som GDPR bestemmer DBL § 4, stk. 2, at den også gælder for den behandling, der udføres for danske diplomatiske repræsentationer.

4.3. "Privat"-reglen[11]

I en del lovgivning sættes der grænser for, hvor meget reguleringen skal gribe ind i privatlivet. Ophavsretten gælder i vidt omfang ikke for

11. Afsnit 3 er i høj grad identisk med "Nyt kapitel om Medier og persondata", supplement til henholdsvis Jakobsen & Schaumburg-Müller 2013 og Jacobsen & Schaumburg-Müller 2016.

det, der foregår ganske privat,[12] og på samme måde er der grænser for, hvor langt persondataretten rækker ind i private aktiviteter.

I persondataretten er det formuleret således: "Forordningen gælder ikke for behandling af personoplysninger, som foretages af en fysisk person som led i rent personlige eller familiemæssige aktiviteter", jf. GDPR artikel 2, stk. 2, litra c.

For at falde ind under undtagelsen skal der *for det første* være tale om fysiske personer. Virksomheder og foreninger er ikke undtaget, og firmaer, skoler, menighedsråd, foreninger og lignende vil således alle skulle opfylde persondatarettens krav. Man kan således fint have venners og families telefonnumre på sin private telefon uden at bekymre sig om persondataretten. Er der derimod tale om, at man behandler personoplysninger for en virksomhed eller en forening, kan undtagelsen ikke bruges, og persondataretten skal efterleves.

For det andet skal behandlingen være af rent personlig eller familiemæssig karakter for at kunne undtages. Hvad dette nærmere betyder, er ikke ganske klart. På den ene side må f.eks. upubliceret slægtsforskning, fotos til familiealbum, adressefortegnelser på egen mobiltelefon, private presseklip mv. falde uden for forordningen. På den anden side er alle kommercielle eller erhvervsmæssige aktiviteter ikke "personlige" i forordningens forstand og falder derfor under forordningens mange regler, også selvom aktiviteten foretages af en fysisk person. En person, der overvejer at starte egen it-virksomhed, vil således være omfattet af persondataretten f.eks. ved indsamling af oplysninger om potentielle kunder, også selvom de første kunder skulle være at finde i familie- eller vennekredsen, mens den samme persons adressefortegnelse af samme familie og venner ikke vil være omfattet.

I præamblens pkt. 18 hedder det: "[K]orrespondance og føring af en adressefortegnelse eller sociale netværksaktiviteter og onlineaktiviteter, der udøves som led i sådanne aktiviteter", og der er hermed lagt op til en udvidelse af privat-undtagelsen. Formuleringen må indebære, at i hvert fald en del aktiviteter, herunder på nettet, falder uden for persondatarettens strenge regimente. Fotografering til privat brug, også af personer i det offentlige rum, og upload af billeder på Instagram

12. Detaljerne kan være komplicerede. Der henvises til speciallitteratur, Schiønning 2016.

el.lign. af familie, venner eller folk på gaden, må derfor kunne være uden for persondatarettens rækkevidde. (Se også om personbilleder nedenfor kapitel 8). Hvor langt undtagelsen strækker sig efter de nye regler, er endnu ikke klart, men der må være et område, der nok ikke er kommercielt, men alligevel heller ikke kan siges at være en rent personlig eller familiemæssig aktivitet. Som eksempel kan nævnes den såkaldte "Viborg-mappe", hvor billeder af unge kvinder deles, helst så mange, så nøgne og så eksplicitte som muligt. Selvom aktiviteten ikke er kommerciel – der foregår muligvis en betaling, men der byttes også bare – kan den næppe siges at være "rent personlig eller familiemæssig." Det samme må gælde f.eks. politikeres Facebook-sider og Twitterkonti: Her henvender kendte personer sig til offentligheden, og de personoplysninger, der måtte forekomme, må være reguleret af persondataretten. I hvilket omfang dette også gælder for mere ukendte personers kommunikation, henstår p.t. uafklaret. Her må der lægges vægt på, hvor personlig og familiemæssig kommunikationen er. En Facebook-profil, der nok i princippet er lukket, men som i realiteten omfatter mange hundrede "venner", kan efter vores vurdering ikke opfattes som "rent personlig".

Man skal her være opmærksom på, at undtagelsen fra persondatarettens regler ikke gælder for den dataansvarlige eller for databehandlere, der "tilvejebringer midlerne" for persondatabehandlingen. Dette betyder, at aktører som Facebook og Instagram fortsat skal overholde persondatarettens regler, også når den private aktør er undtaget efter artikel 2, stk. 2, litra c.

Man skal være opmærksom på, at andre regler fortsat gælder, herunder f.eks. straffelovens regler om fotografering af personer på ikke frit tilgængeligt sted, § 264 a, og videregivelse af private oplysninger og meddelelser, § 264 d. Her skal man være opmærksom på, at reglerne ikke er sammenfaldende. F.eks. vil det være strafbart efter STL § 264 a at fotografere ind i naboens have, hvor der er børnefødselsdag, mens fotograferingen vil være undtaget persondataretten, hvis fotograferingen kun er til personlig eller familiemæssig brug. Der henvises til speciallitteraturen.[13]

13. Jakobsen & Schaumburg-Müller 2013, s. 199 f., og Baumbach 2017.