Når må virksomheter som er etablert utenfor EØS-området behandle personopplysninger i overenstemmelse med GDPR?

En rettslig analyse av Forordning (EU) 2016/679 artikkel 3 andre ledd

Kandidatnummer: 101

Antall ord: 14 016

JUS399 Masteroppgave
Det juridiske fakultet

UNIVERSITETET I BERGEN

10. desember 2019

Innholdsfortegnelse

1 Innledning

1.1 Aktualitet og problemstilling

Personopplysninger er et privat anliggende. Likevel er våre navn, kontoopplysninger, personlige relasjoner og politiske preferanser i ferd med å bli en av vår tids viktigste handelsvarer.[1] Personopplysninger har blitt såpass viktige, at de omtales som «the currency of the Information Age».[2] Utviklingen skyldes særlig at teknologi og globalisering har gjort det enklere å dele personopplysninger; *muligheten* til å dele personopplysninger har blitt større. Dessuten har utviklingen sammenheng med at private personer i større grad enn tidligere gjør informasjon tilgjengelig; *viljen* til å dele personopplysninger har tiltatt.

Det er normalt profesjonelle aktører som har tilgang til våre personopplysninger. Eksempelvis har Google, Telenor og Skatteetaten god kjennskap til hvem vi er som privatpersoner. Da styrkeforholdet mellom oss som privatpersoner og de som er i besittelse av våre personopplysninger ofte er skjevt, er det hensiktsmessig at forholdet blir regulert.[3]

Som ledd i arbeidet med å sikre vern av våre personopplysninger, vedtok Europaparlamentet og Rådet for Den Europeiske Union en ny rettsakt i 2016, navnlig Forordning (EU) 2016/679 General Data Protection Regulation (heretter omtalt som GDPR eller forordningen).[4] I GDPR har EUs lovgivende organer oppstilt regler om vern av fysiske personer i forbindelse med behandling av personopplysninger, i tillegg til regler om fri utveksling av personopplysninger, jf. GDPR. art. 1 (1). GDPR regulerer dermed hvilken adgang virksomheter har til å behandle personopplysninger.

[1] Azzi, Adèle (2018). *The challenges Faced by the extraterritorial scope of the general data protection regulation*, Jipitec, s. 127.
[2] Kuner, Christopher, Cate, Fred H., Millard, Christopher, og Svantesson, Dan Jerker B. (2012). *The challenge of 'big data' for data protection*. International Data Privacy Law, 2012, Vol. 2, No. 2, side 48.
[3] Tilsvarende har lovgiver regulert forholdet mellom forbrukere og næringsdrivende, arbeidstaker og arbeidsgiver, og borgere og myndigheter.
[4] Forordning (EU) 2016/679 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [GDPR].

Dersom GDPR kommer til anvendelse, stiller forordningen krav til hvordan personopplysningene skal behandles. Det er en kjensgjerning at GDPR – sammenlignet med andre personvernregler – setter en høy standard for vern av personopplysninger.[5] Blant annet må virksomheten oppgi formålet med behandlingen, og om den har til hensikt å overføre personopplysningene til en tredjeperson, jf. GDPR art. 13. Personopplysningene skal også behandles i samsvar med fastsatte prinsipper, jf. kap. II. Videre slår GDPR fast at vi når som helst i behandlingsprosessen kan be om å få opplysningene rettet eller slettet, jf. art. 16 og 17. Dessuten forutsetter GDPR at virksomheter som holder til utenfor EØS-området skal opprette en representant i EØS-området, slik at tilsynsmyndigheter og privatpersoner enkelt kan henvende seg til virksomheten via representanten jf. art. 27.

For at GDPR skal komme til anvendelse, må virksomheten opptre innenfor forordningens *saklige* og *geografiske* virkeområde, jf. GDPR art. 2 og 3.

I denne oppgaven forutsetter jeg at virksomhetens behandling av personopplysninger ligger innenfor GDPRs saklige virkeområde.

> Jeg nevner likevel for ordens skyld at storparten av behandling av personopplysninger ligger innenfor GDPRs saklige virkeområde. Det finnes enkelte unntak, deriblant behandling som er knyttet til personlige eller familiemessige aktiviteter, i tillegg til behandling som er knyttet til myndighetenes arbeid i å forebygge, etterforske og avsløre straffbare handlinger, jf. GDPR art. 2 (2).

Det geografiske virkeområdet til GDPR er regulert i GDPR artikkel 3. Bestemmelsen slår fast *når* virksomheter opptrer innenfor det geografiske virkeområdet til GDPR, og derfor må behandle personopplysninger i overenstemmelse med forordningen. Det er tre forhold som kan føre til at en virksomhet opptrer innenfor GDPRs geografiske virkeområde. For det første kan virksomheter som er etablert i EØS-området opptre innenfor GDPRs geografiske virkeområdet, jf. art. 3 (1). Typisk vil Kiwi, Telenor og Facebook være omfattet av denne bestemmelsen. For det andre kan folkerettslige regler føre til at virksomheter opptrer innenfor GDPRs geografiske virkeområdet, jf. GDPR art. 3 (3). Dette kan for eksempel være tilfellet dersom behandlingen er knyttet til en ambassade. For det tredje kan virksomheter som er etablert *utenfor* EØS-

[5] Azzi (2018) s. 127 og Korff, Douwe (2019) *The territorial (and extra-territorial) application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service* s. 2.

området opptre innenfor GDPRs geografiske virkeområde, jf. art. 3 (2). GDPR artikkel 3 andre ledd er ofte sentral for å avgjøre om virksomheter i USA, Asia og Afrika må forholde seg til GDPR når de behandler personopplysninger. Det er derfor ikke overraskende at GDPR artikkel 3 andre ledd har blitt omtalt som «the single most important provision in the entire [...] Regulation» for virksomheter som er etablert utenfor EØS-området.[6]

Tema for denne oppgaven er GDPRs *geografiske virkeområdet*. Jeg skal særlig fokusere på virksomheter som er etablert *utenfor* EØS-området. Oppgavens problemstilling er hva som skal til for at virksomheter som er etablert utenfor EØS-området må behandle personopplysninger i overenstemmelse med GDPR.

1.2 Rettskilder og metode

Det er GDPR som er primærkilden for å besvare oppgavens problemstilling. GDPR er innlemmet i EØS-avtalen som vedlegg XI nr. 5e.[7] Norge er derfor forpliktet til å «treffe alle generelle eller særlige tiltak som er egnet til å oppfylle [GDPR]», jf. EØS-avtalen art. 3 (1), jf. art. 2 (a). Én av tiltakene, er at GDPR må gjøres «til del av [Norges] interne rettsorden», jf. EØS-avtalen art. 7. Det norske Stortinget har inkorporert GDPR til norsk lov.[8] Inkorporasjonen skjedde gjennom vedtakelse av personopplysningsloven.[9] Ved konflikt med annen lovgivning skal GDPR gis forrang, jf. personopplysningsloven § 2 (4), jf. EØS-loven § 2.[10] Et annet tiltak for å oppfylle Norges forpliktelse til EØS-samarbeidet, er at GDPR må tolkes i overenstemmelse med EU-rettslig tolkningsmetode og kilder.[11] Dette er særlig begrunnet i hensynet til homogenitet.[12] Jeg skal derfor bruke den EU-rettslige tolkningsmetoden og EU-rettslige kilder når jeg analyserer GDPR artikkel 3 andre ledd.

I det følgende skal jeg kort gjøre rede for kildene som er relevante ved tolkningen av GDPR artikkel 3 andre ledd.

---

[6] Svantesson, Dan Jerker (2013). *Extraterritoriality in Data Privacy Law.* Ex Tuto Publishing: København s. 106.
[7] Agreement on the European Economic Area, 2. May 1992 [EØS-avtalen].
[8] Inkorporasjonen skjedde i medhold av EØS-avtalen art. 7 (a).
[9] Lov 15. juni 2018 nr. 39 om behandling av personopplysninger (personopplysningsloven).
[10] Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven).
[11] Dom av 2. mars 2017, *J.D*, C-4/16, ECLI:EU:C:2017:153, avsnitt 23.
[12] Ibid.

GDPR, dens ordlyd, formål og kontekst, er viktige tolkningskilder.[13] Ved tolkningen av GDPR skal det legges vekt på begrepenes «usual meaning in everyday language», såfremt de ikke er legaldefinert.[14] GDPR har 25 offisielle språkversjoner, inkludert norsk, jf. EØS-avtalen art. 129 nr. 1. Det er ikke grunnlag for å tillegge de mest utbredte språkversjonene størst vekt.[15] I denne oppgaven skal jeg primært se hen til den norske språkversjonen, unntaksvis supplert av den danske, engelske og tyske. GDPR er et resultat av politisk forhandling, og er derfor vagt utformet. I tilfeller hvor ordlyden er vagt utformet, skal det legges desto større vekt på rettsaktens formål og kontekst.[16] Formålet med GDPR kan utledes av GDPR som sådan, og av forordningen tilblivelseshistorie.[17] Konteksten til GDPR kan utledes av EUs primær- og sekundærlovgivning, herunder EUs grunnleggende prinsipper, internasjonale forpliktelser, og GDPRs fortale.[18] Selv om fortalen har betydning som tolkningskilde, er den ikke rettslig bindene.[19]

Videre er praksis fra EU-domstolen en viktig rettskilde, da det bidrar til å sikre homogenitet innad i EØS-området, jf. EØS-avtalen art. 6. EU-domstolen har enda til gode å tolke GDPR artikkel 3 andre ledd. Mangelen på nye avgjørelser blir noe avhjulpet ved at GDPR artikkel 3 andre ledd er en delvis videreføring fra tidligere regelverk, slik at tidligere praksis fra EU-domstolen er relevant.

Videre er retningslinjer fra Det europeiske Personvernråd (heretter: Personvernrådet) en betydningsfull tolkningskilde. Personvernrådet er et uavhengig organ bestående av én representant fra tilsynsmyndighetene i hvert medlemsland, jf. GDPR art. 68 og 69. Personvernsrådet skal utstede retningslinjer, anbefalinger og beste praksis for å fremme en ensartet anvendelse av forordningen, jf. GDPR art. 70. For å sikre homogenitet innad i EØS-

[13] Fredriksen, Halvard Haukeland og Mathisen, Gjermund (2018). *EØS-rett*. 3. utgave. Fagbokforlaget: Bergen s. 296–298.
[14] Dom av 3. september 2014, *Deckmyn*, C-201/13, ECLI:EU:C:2014:2132, avsnitt 19.
[15] Fredriksen mfl. (2018) s. 297.
[16] Ibid. s. 298.
[17] Ibid. s. 308.
[18] Ibid. s. 299–308.
[19] Dom av 19. juni 2014, *Karen Millen Fashions*, C-345/13, ECLI:EU:C:2014:2013, avsnitt 31: «the preamble (...) has no binding legal force and cannot be relied on either as a ground for derogating from the actual provisions of the act in question or for interpreting those provisions in a manner clearly contrary to their wording».

området, bør uttalelsene fra Personvernsråd tillegges vekt. Ved tolkning av GDPR artikkel 3 andre ledd er det særlig Guidelines 3/2018 som er relevant. Førsteutkastet til Guidelines 3/2018 ble utgitt 16. november 2018, for offentlig gjennomlesning og tilbakemelding. Den endelige utgaven ble utgitt 12. november 2019. I denne oppgaven refererer jeg utelukkende til den endelige utgaven, såfremt annet ikke presiseres.

Før GDPR trådte i kraft var det Artikkel 29-gruppen som utformet retningslinjer. Enkelte av disse har blitt videreført av Personvernrådet, og er derfor relevante ved tolkningen av GDPR. Også de veiledere som ikke har blitt videreført kan tillegges vekt, forutsatt at de ikke strider mot GDPR eller nye retningslinjer fra Personvernrådet. I denne oppgaven skal jeg se hen til et utvalg retningslinjer fra Artikkel 29-gruppen, i tilfeller hvor de bidrar til å belyse oppgavens tema.

Forarbeidene til personopplysningsloven er primært av betydning som norsk tilpasningskilde. I denne oppgaven skal jeg derfor i liten grad legge vekt på forarbeidsuttalelser.

Forøvrig har juridisk litteratur liten vekt, men kan i tvilstilfeller bidra til argumentasjon. Jeg vil ta i betraktning både norsk og internasjonal litteratur. Litteraturen jeg bruker i denne oppgaven er eldre enn den endelige versjonen av Guidelines 3/2018. De teoretiske innvendinger tar derfor ikke høyde for de endringene som Personvernrådet har gjort.

1.3 Avgrensninger

Formålet med oppgaven er å finne ut når virksomheter som er etablert *utenfor* EØS-området må behandle personopplysninger i overenstemmelse med GDPR. Jeg skal derfor ikke skrive om GDPR artikkel 3 første og tredje ledd. Avgrensningen begrunner jeg også med at både første og tredje ledd – i det store og hele – er videreføringer fra tidligere EU-lovgivning.

I oppgaven skal jeg bare ta stilling til *når* GDPR gjelder for virksomheter i tredjestater. Virkningene av at GDPR eventuelt kommer til anvendelse, faller derfor utenfor denne oppgaven.

Jeg skal ikke behandle rettspraksis og andre relevante rettskilder som kommer etter 1. desember 2019.

1.4 Videre fremstilling

Til å begynne med, i kapittel 2.1, skal jeg skrive om den grunnleggende retten til vern av personopplysninger. Jeg skal særlig fokusere på hvordan teknologi og globalisering påvirker denne retten. Deretter, i kapittel 2.2, skal jeg se nærmere på GDPR sin tilblivelseshistorie og uttalte målsetning. Jeg skal særlig skrive om hvorfor det oppsto behov for å endre personvernlovgivningen. Formålet med denne innledende gjennomgangen er å danne en kontekst og et rammeverk for den videre oppgaven.

I oppgavens hoveddel skal jeg analysere GDPR artikkel 3 andre ledd. I kapittel 3.2 skal jeg tolke bestemmelsens inngangsvilkår, mens jeg i kapittel 3.3 og 3.4 skal tolke bestemmelsens bokstav (a) og (b). I analysen skal jeg gjøre rede for gjeldende rett. Formålet med analysen er å gi en klargjørende og systematisk gjennomgang av bestemmelsen, slik at regelens innhold blir enklere tilgjengelig og mer lettfattelig. Dessuten skal jeg i løpet av analysen belyse problemstillinger som framstår som uavklarte, og i tillegg argumentere for mine rettspolitiske meninger.

Avslutningsvis, i oppgavens del 4, skal jeg oppsummere oppgaven og gi en avsluttende refleksjon.

2 Kort om personvern og GDPR

2.1 Personvern og vern av personopplysninger

Retten til personvern er fundamental; blant annet nedfelt i Grunnloven[20] og Den Europeiske Menneskerettighetskonvensjonen[21]. I kjernen av begrepet ligger enhvers rett til integritet, autonomi, privat- og familieliv, samt respekt for sitt hjem og sin kommunikasjon, jf. Grunnloven § 102 og EMK art. 8. Retten til personvern gjelder på alle arenaer, for eksempel hjemme, på hytta, på jobb, når vi er på ferie, og når vi bruker Internett.[22]

Det finnes ingen legaldefinisjon av begrepet personvern; begrepet er dynamisk og endrer seg i takt med samfunnet forøvrig.[23] En sentral og høyst aktuell del av personvernet er retten til vern av *personopplysninger*.[24] Det økte fokuset på personopplysningsvern har, som nevnt innledningsvis, særlig sammenheng med at personopplysninger har blitt en viktig handelsvare. Det økte fokuset har også sammenheng med at personopplysninger er et privat anliggende som i verste fall kan gi et lite fordelaktig bilde av oss, eller undergrave vår autonomi.[25]

Selv om person- og personopplysningsvern er en grunnleggende rettighet, er den ikke absolutt.[26] Retten til personopplysningsvern må veies opp mot «andre grunnleggende rettigheter i samsvar med forholdsmessighetsprinsippet», jf. GDPR fortalepunkt 4. Ved vurderingen av GDPR skal det særlig ses hen til «[...] ytrings- og informasjonsfrihet, frihet til å drive næringsvirksomhet, retten til effektiv prøving og rettferdig rettergang samt kulturelt, religiøst og språklig mangfold», jf. fortalepunkt 4. Det er særlig viktig å se retten til personopplysningsvern i lys av hvor viktig personopplysninger er for samfunnsutviklingen:

[20] Lov 17. mai 1814 om Kongeriket Norges Grunnlov [Grunnloven].
[21] Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 [Den europeiske menneskerettskonvensjonen, EMK].
[22] Datatilsynet (2015) *Det Store Datakappløpet. Rapport om hvordan kommersiell bruk av personopplysninger utfordrer personvernet* s. 8.
[23] Schartum, Dag Wiese (2016). *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger.* 3. utgave. Fagbokforlaget: Bergen. s. 42.
[24] NOU 2009: 1 *Individ og integritet. Personvern i det digitale samfunnet*, punkt 4.1.5.
[25] Article 29 Data Protection Working Party. WP 251 rev.01. *Guidelines on Automated individual decision-making and Profiling for the purpose of Regulation 2016/679*. Revised and Adopted on 6 February 2018 s. 5–6.
[26] Se for eksempel EMD Sak nr. 59320/00, *Caroline von Hannover*, 24. juni 2007 avsnitt 57 flg. hvor retten til privatliv ble vurdert opp imot hensynet til ytringsfrihet.

Offentlige myndigheter må ha informasjon om borgerne for å forvalte de oppgavene de er satt til å utføre; forsknings- og utdanningsinstitusjoner er avhengig av at privatpersoner deltar i undersøkelser og forskningsprosjekter; og selskaper må ha kunnskap om hvordan dagens teknologi fungerer for å kunne utvikle ny.

2.2 Kort om GDPR

2.2.1 Historisk bakteppe

GDPR er én av mange regelsett som har blitt utformet med hensikt om å verne våre personopplysninger.

> Eksempler på andre regelsett er Forskrift 2. juli 2018 nr. 1107 om kameraovervåkning i virksomhet, Forskrift 15. mai 2013 nr. 484 om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften), Lov 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger (helseregisterloven), samt regler om taushetsplikt.

Før GDPR trådte i kraft, var det EUs Personverndirektiv som regulerte virksomheters adgang til å behandle personopplysninger.[27] Personverndirektivet ble innlemmet som norsk lov gjennom vedtakelse av personopplysningsloven av 2000.[28] Personverndirektivet regulerte – i likhet med GDPR artikkel 3 andre ledd – EUs forhold til virksomheter som var etablert utenfor EØS-området. Av Personverndirektivet artikkel 4 første ledd bokstav (c) fulgte det at virksomheter som var etablert utenfor EØS-området måtte forholde seg til nasjonale bestemmelser som var gjennomført i henhold til Personverndirektivet dersom virksomheten:

> *«[...] med henblikk på behandling av personopplysninger benytter elektroniske eller andre **hjelpemidler** som befinner seg på nevnte medlemsstats territorium, med mindre disse hjelpemidlene benyttes bare med henblikk på transitt gjennom Fellesskapets territorium. [...].»* (min utheving)

[27] Europaparlamentet og Rådets direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger [OPPHEVET].
[28] Lov 14. april 2000 nr. 31 om behandling av personopplysninger (opphevet ved lov 15. juni 2019 m.v.) [OPPHEVET].

En åpenbar utfordring var den vide ordlyden «hjelpemidler».[29] I takt med den teknologiske utviklingen fikk vilkåret «hjelpemidler» et vidt anvendelsesområde.[30] EUs lovgivende organer hadde ikke laget et «future-proof»-vilkår.[31] På grunn av vilkårets vide rekkevidde, hadde nasjonale myndigheter ikke ressurser til å håndheve bestemmelsen. Det var derfor få saker ble derfor prøvd for domstolene.[32] Da risikoen for å bli dømt var liten, var det mange virksomheter utenfor EØS-området som ikke overholdt reglene i Personverndirektivet artikkel 4 første ledd bokstav (c).[33] Bestemmelsen sikret dermed ikke en effektiv etterlevelse av regelverket.[34]

> Et eksemepl som illustrerer vilkårets vide rekkevidde, er hentet fra den polske Supreme Administrative Court.[35] Domstolen la til grunn at Google-bilen – som ble brukt til å ta bilder til Google Street View – var et *hjelpemiddel* i Personverndirektivets forstand. Tilsvarende slo Artikkel 29-gruppen fast at cookies, JavaScript, geo-lokasjonstjenester og lagring i skytjenester også skulle være omfattet av vilkåret «hjelpemidler».[36]

En annen utfordring for bestemmelsen var globaliseringen og utviklingen av ny teknologi. EUs lovgivende organer har i GDPR fortalepunkt 6 uttalt at:

> *«[...] Omfanget av innsamlingen og utvekslingen av personopplysninger har økt betraktelig. Teknologien gjør det mulig for både private selskaper og offentlige myndigheter å benytte seg av personopplysninger i sitt arbeid i et helt nytt omfang. Fysiske personer gjør i stadig større grad personopplysninger offentlig tilgjengelig, også globalt. Teknologien har endret både økonomien og det sosiale liv [...].»*

---

[29] Czerniawski, Michal (2017). *Do We Need the 'Use of Equipment' as a Factor for the Territorial Applicability of the EU Data Protection Regime?* Cambridge, Antwerp and Portland s. 227–228.
[30] Ibid. s. 232.
[31] Ibid. s. 240.
[32] Ibid. s. 234.
[33] Ibid. s. 232–233.
[34] Czerniawski (2017) s. 235, Svantesson (2013) s. 234 og de Hert, Paul og Czerniawski, Michal (2016) *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context.* International Data Privacy Law, Vol. 6, No. 3. s. 230–231.
[35] Saksnr. I OSK 2445/12, 21. februar 2014. Saken tvistepunkt var om Google måtte opprette en representant i Polen.
[36] Article 29 Data Protection Working Party, WP 56, *Working document on determining the international application of EU data protection law to personal data processing in the Internet by non-EU based web sites*, s 10–12; og Article 29 Data Protection Working Party, WP 179, *Opinion 8/2010*, s. 21–22.

Personverndirektivet artikkel 4 første ledd (c) er dermed et godt eksempel på at teknologien utviklet seg raskere enn lovverket.[37]

2.2.2 Fra direktivet til forordning

Slik gjennomgangen viser, var det mye som tilsa at Personverndirektivet var modent for endring. Den 27. april 2016 – omtrent 16 år etter at Personverndirektivet ble innlemmet som norsk lov – vedtok EU en ny rettsakt om behandling av personopplysninger. GDPR trådte i kraft den 25. mai 2018, og ble formelt innlemmet som norsk lov den 20. juli 2018.[38]

Formålet med GDPR er beskrevet i forordningens artikkel 1. Det første formålet er å «sikre[] vern av fysiske personers grunnleggende rettigheter og friheter, særlig deres rett til vern av personopplysninger», jf. art. 1 (2). Det første formålet har sammenheng med at personvern er en fundamental rettighet, og derfor viktig å beskytte, jf. fortalepunkt 1. Det andre formålet med GDPR er å sikre «[f]ri utveksling av personopplysninger i Unionen [...]», jf. art. 1 (3). Det andre formålet er ment å bidra til «økonomisk og sosial framgang, til å oppnå en styrking og tilnærming av økonomiene i det indre markedet og til fysiske personers velferd», jf. fortalepunkt 2. Ved tolkningen av GDPR artikkel 3 andre ledd må de to formålene veies opp mot hverandre, jf. fortalepunkt 4.

Videre har EUs lovgivende organer i fortalepunkt 7 uttalt at det nå er behov for:

> *«[...] en **sterk og mer sammenhengende ramme** for vern av personopplysninger i Unionen støttet av en **streng håndheving av reglene**, ettersom det er viktig å skape den nødvendige tillit som vil gjøre at den digitale økonomien kan utvikle seg i det indre marked. Fysiske personer bør ha kontroll over egne personopplysninger [...].» (mine uthevinger).*

[37] Czerniawski (2017) s. 240 og Cate, Fred H., Kuner, Christopher, Millard, Christopher, og Svantesson Dan Jerker B. (2014) «*The (data privacy) law hasn't even checked in when technology takes off»* International Data Privacy Law, Vol. 4, No. 3 s. 175.
[38] Slik nevnt i kapittel 1.2 ble GDPR innlemmelsen gjennom vedtakelse av personopplysningsloven av 2018.

EUs lovgivende organer har innført streng håndheving av reglene: Dersom en virksomhet behandler personopplysninger i strid med GDPR, kan den bli ilagt et overtredelsesgebyr på opptil 20 000 000 euro eller 4 % av den samlede globale årsomsetningen, jf. GDPR art. 83.

For å sikre et sterkere og mer sammenhengende vern, ble GDPR gjennomført som en *forordning*.[39] Forskjellen mellom direktiv og forordning er betydelig. *Direktiv* blir ikraftsatt ved at hvert land selv får «bestemme formen og midlene for gjennomføringen», jf. EØS-avtalen art. 7 bokstav (b) og TEUV art. 288 (3). Direktiver er dermed minimumskrav som gir medlemslandene et visst handlingsroms. *Forordninger* blir ikraftsatt ved at rettsakten «som sådan gjøres til del av avtalepartenes interne rettsorden», jf. EØS-avtalen art. 7 bokstav (a) og TEUV art. 288 (2). Forordninger gjelder dermed direkte og akkurat slik EUs lovgivende organer har bestemt. Fordelen med forordninger er at regelverket innad i EØS-området i større grad blir harmonisert og effektivisert. Ulempen er at hvert land får mindre handlingsrom.

> Jeg nevner for ordens skyld at GDPR gir medlemslandene et visst handlingsrom. For eksempel kan medlemslandene selv bestemme om samtykke til behandling av personopplysninger skal kunne gis av barn fra de fyller 13 eller 16 år, jf. GDPR artikkel 8 nr. 1. Videre kan det lages nasjonale særregler ved ansettelsesforhold, jf. GDPR artikkel 88. Et tredje eksempel er at medlemsstatene kan fastsette utfyllende regler der behandlingen bygger på artikkel 6 nr. 1 bokstav c eller e, jf. GDPR artikkel 6 nr. 2 og 3. Det siste handlingsrommet gir blant annet grunnlag til å fastsette visse særregler om kameraovervåkning, jf. Prop. 56 LG (2017–18) punkt 18.1.

Statenes handlingsrom fører til at regelverket blir mer komplekst, og mer ressurskrevende å forholde seg til. For virksomheter som behandler personopplysninger innebærer dette at de må ha oversikt over hvert lands ulike særregler.[40]

2.2.3 EUs utvidede jurisdiksjon

GDPR – dens formål, systematikk, terminologi, grunnprinsipper og materielle regler – er i stor grad en videreføring av Personverndirektivet.[41] Likevel førte overgangen til flere

[39] Dette til forskjell fra Personvern*direktivet*: Én av utfordringene ved Personverndirektivet var nemlig at ulik implementering i de ulike landene førte til «a fragmented legal environment which [...] created legal uncertainty and unequal protection for data subjects», jf. Svantesson (2013) s. 103.
[40] Guidelines 3/2018 s. 14.
[41] Svantesson (2013) s. 102 og Prop. 56 LS (2017-2018) Om lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen, punkt 2.

innholdsmessige endringer. Én av endringene knytter seg til EUs jurisdiksjon overfor virksomheter som er etablert utenfor EØS-området.[42] Azzi har omtalt denne endringen som «the biggest change […] of the data protection rules».[43] I juridiske kretser spås GDPR artikkel 3 andre ledd å bli mer treffsikker enn forgjengeren. Czerniawski legger vekt på at virksomheter omsider kan forutse om de må forholde seg til regelverket eller ikke.[44] De Hert skriver at bestemmelsens utvidede jurisdiksjon, sett i lys av formålet om en effektiv beskyttelse av personopplysninger, er rimelig.[45] Azzi er også positiv, og skriver at:

> «Under Article 3 of the GDPR, operators who used to be entirely out of reach of EU data protection rules, despite heavily processing of EU data, will suddenly have to comply with the highest data protection standards in the world».[46]

Overgangen fra Personverndirektivet til GDPR var – tross de positive spådommene – ikke problemfri. Både det komplekse regelverket og de høye gebyrene var medvirkende faktorer. Et eksempel som illustrerer utfordringen godt, er da en håndfull amerikanske nettaviser i tiden etter at GDPR trådte i kraft besluttet å blokkere nettavisene sine for europeiske lesere.[47] Årsaken var at nettavisene ikke visste om de måtte forholde seg til GDPR eller ikke.

Svantesson har tatt til orde for at de nevnte utfordringene vil være ekstra store for små og mellomstore bedrifter.[48] Jeg er enig med Svantesson, da det tross alt er ressurskrevende å gjøre seg godt kjent med GDPR. Det er derfor grunn til å anta at store virksomheter har bedre forutsetninger i møte med GDPR. Det er imidlertid bare tiden som kan vise som Svantessons antakelser medfører riktighet.

---

[42] Sml. det tidligere Personverndirektivet art. 4 (1) (c).
[43] Azzi (2018) s. 127 skriver at «[…] the biggest change surely lies in the new territorial scope of the data protection rules».
[44] Czerniawski (2017) s. 236.
[45] de Hert mfl. (2016) s. 231.
[46] Azzi (2018) s. 127.
[47] https://www.bbc.com/news/world-europe-44248448 (lastet ned 6. desember 2019). Blant nettavisene som ble blokkert var: New York Daily News, Chicago Tribune, LA Times, Orlando Sentinel og Baltimore Sun.
[48] Svantesson, Dan Jerker B (2015). *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation.* International Data Privacy Law, Vol. 5, No. 4. s. 230.

3 Analyse av GDPR artikkel 3 andre ledd

3.1 Presentasjon av GDPR artikkel 3 andre ledd

I det følgende skal jeg analysere GDPR artikkel 3 andre ledd, for å finne ut av *når* virksomheter som er etablert utenfor EØS-området må behandle personopplysninger i overenstemmelse med GDPR. Av GDPR artikkel 3 andre ledd følger det at:

> *«Denne forordning får anvendelse på behandling av personopplysninger om registrerte som befinner seg i Unionen, og som utføres av en behandlingsansvarlig eller databehandler som ikke er etablert i Unionen, dersom behandlingen er knyttet til*
>
> > *a) tilbud av varer eller tjenester til slike registrerte i Unionen, uavhengig av om det kreves betaling fra den registrerte eller ikke, eller*
> >
> > *b) monitorering av deres atferd, i den grad deres atferd finner sted i Unionen.»*

3.2 Inngangsvilkår

Før bokstav (a) eller (b) kan analyseres, må inngangsvilkårene være oppfylt.

For det første må det være tale om «en behandlingsansvarlig eller databehandler som ikke er etablert i Unionen». Først, i underkapittel 3.2.1, skal jeg se nærmere på forholdet mellom den behandlingsansvarlige og databehandleren. Deretter skal jeg se på vilkåret «ikke [...] etablert i Unionen» i underkapittel 3.2.2.

For det andre må det dreie seg om «behandling av personopplysninger». Dette vilkåret skal jeg behandle i underkapittel 3.2.3.

Det tredje inngangsvilkåret som må være oppfylt, er at den behandlingsansvarlige eller databehandleren behandler personopplysninger «om registrerte som befinner seg i Unionen». Dette vilkåret skal jeg behandle i underkapittel 3.2.4.

Det siste inngangsvilkår er at behandlingen må være «knyttet til» forholdene som beskrives i bokstav (a) eller (b). Bokstav (a) og (b) er alternative, jf. formuleringen «eller». Det er derfor tilstrekkelig at behandlingen er knyttet til én av de to forholdene. I underkapittel 3.2.5 skal jeg behandle tilknytningsvilkåret. Deretter, i kapittel 3.3 og 3.4, skal jeg analysere bokstav (a) og (b).

3.2.1 Forholdet mellom databehandler og behandlingsansvarlig

GDPR artikkel 3 andre ledd gjelder for «behandlingsansvarlige eller databehandlere» som ikke er etablert i Unionen.

Med *behandlingsansvarlig* menes «en fysisk eller juridisk person, en offentlig myndighet, en institusjon eller ethvert annet organ som alene eller sammen med andre bestemmer formålet med behandlingen av personopplysninger og hvilke midler som skal benyttes [...]», jf. GDPR art. 4 nr. 7. Med *databehandler* menes «en fysisk eller juridisk person, offentlig myndighet, institusjon eller ethvert annet organ som behandler personopplysninger på vegne av den behandlingsansvarlig», jf. GDPR art. 4 nr. 8. Kort oppsummert bestemmer den behandlingsansvarlige hvorfor og hvordan personopplysninger skal behandles, mens databehandleren utfører behandlingen.

Vilkårene er alternative, jf. formuleringen «eller». Det er derfor ikke tilstrekkelig å påvise en relasjon mellom behandlingsansvarlig og databehandler, og deretter slå fast at begge må forholde seg til GDPR.[49] Man må vurdere hver enhet separat.[50] At vilkårene er alternative er, slik jeg ser det, i overenstemmelse med samfunnsutviklingen. Behandlingssituasjoner er komplekse, og virksomheter er ofte differensiert.[51] Det er ikke uvanlig at virksomhetene utgjør ulike enhetene, og dessuten er etablert i ulike land.

I det følgende skal jeg gi eksempler på tilfeller hvor den behandlingsansvarlige og databehandleren utgjør ulike enheter, og hvordan dette påvirker anvendelsen av GDPR.

[49] Guidelines 3/2018 s. 10.
[50] Ibid. s. 10–11.
[51] Article 29 Data Protection Working Party. WP 169. *Opinion 1/2010 on the concepts of "controller" and "processor"* s. 2.

En forholdsvis enkel situasjon, er det tilfellet at en EØS-basert behandlingsansvarlig engasjerer en databehandler som er etablert utenfor EØS-området. Dette var tilfellet i den såkalte *Ferde*-saken, hvor et Bergensbasert bompengeselskap engasjerte et kinesisk IT-selskap for å få bistand med å utstede fakturaer til norske bilister.[52] I et slikt tilfelle må den behandlingsansvarlige, eksempelvis Ferde, forholde seg til GDPR fordi den er etablert i EØS-området, jf. GDPR art. 3 (1). Samtidig må han sørge for at databehandleren, for eksempel det kinesiske IT-selskapet, opptrer i samsvar med de krav som følger av GDPR artikkel 28 (3).[53] Databehandleren, uavhengig av hvor den er etablert, blir derfor «indirectly subject to some obligations [...]».[54]

Hva som gjelder i et motsatt tilfelle – hvor den behandlingsansvarlige er etablert utenfor EØS-området og databehandleren er etablert i EØS-området – er ikke like klart. Databehandleren må i kraft av sin etablering i EØS-området forholde seg til GDPR, jf. GDPR art. 3 (1). Hva som gjelder for den behandlingsansvarlige, er ikke eksplisitt regulert i GDPR.[55] Den behandlingsansvarlige blir ikke indirekte forpliktet, slik tilfellet er for databehandlere utenfor EØS-området.[56] Samtidig presiserer Personvernrådet at EØS-området ikke må bli en «data heaven» for virksomheter som er etablert utenfor EØS-området.[57] Hvorvidt en behandlingsansvarlig må forholde seg til GDPR, vil derfor i mange tilfeller bero på om den har opptrådt innenfor artikkel 3 andre ledd.

Slik gjennomgangen viser er det ofte er mest aktuelt å vurdere bestemmelsens andre ledd i relasjon til *behandlingsansvarlige* utenfor EØS-området. Det samme har tanketanken Centre for Information Policy Leadership (heretter CIPL) uttalt, og dessuten påpekt at «[…] all of the examples provided by the EDPB [les: Personvernrådet] under this section relate only to the application of Article 3(2) of the GDPR to controllers».[58]

---

[52] https://www.nrk.no/norge/slike-bilder-sender-bomselskap-til-kina_-na-gar-datatilsynet-inn-i-saken-1.14754918 (lastet ned 31. oktober 2019). Ferde sendte bilder av bompasseringer og bilskilt til det kinesiske selskapet, hvorpå det kinesiske selskapet manuelt leste av bilskiltene.

[53] Blant annet må databehandleren sørge for tilstrekkelig sikkerhet ved behandlingen, jf. art. 32, jf. art. 28 (3) (c), og dessuten slette eller tilbakelevere personopplysningene etter forespørsel fra den behandlingsansvarlige, jf. art. 28 (3) (g).

[54] Guidelines 3/2018 s. 11.

[55] Sml. GDPR art. 28 (3) som regulerer det motsatte tilfellet.

[56] Guidelines 3/2018 s. 12.

[57] Ibid. s. 13.

[58] Comments by Centre for Information Policy Leadership (2019). *On the European Data Protection Board's «Draft Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)»* s. 11.

Selv om behandlingsansvarlig og databehandler skal vurderes separat, har jeg i denne oppgaven valgt å behandle de samlet. Jeg behandler de samlet fordi jeg mener at forholdet mellom enhetene ikke er av betydning for oppgavens problemstilling. Hvorvidt GDPR artikkel 3 andre ledd er oppfylt avhenger ikke av om det er den behandlingsansvarlige eller databehandleren som behandler personopplysningene. Det er heller ikke avgjørende hvilket forhold de ulike enhetene har til hverandre. Jeg skal derfor vurdere når GDPR gjelder for en virksomhet som er etablert utenfor EØS-området, uavhengig av om den er samlet, eller består av ulike enheter.

3.2.2 Virksomheter som ikke er etablert i Unionen

GDPR artikkel 3 andre ledd gjelder for virksomheter som «ikke er etablert i Unionen». Ordlyden «ikke etablert i Unionen» tilsier at virksomheten er opprettet og forankret utenfor EØS-området. Selskaper som «ikke er etablert i Unionen» kan for eksempel være amerikanske IT-selskaper, eller reiseselskaper fra Asia og Sør-Amerika.

Motsatt regulerer GDPR artikkel 3 første ledd virksomheter som er etablert *i* Unionen. Slike virksomheter har «[...] en effektiv og faktisk utøvelse av aktivitet gjennom en stabil struktur [...]», jf. fortalepunkt 23, og en «inextricable link» (på norsk: uløselig tilknytning) til EØS-området.[59] En kontekstuell tolkning tilsier at det motsatte må gjelde for virksomheter som er etablert utenfor EØS-området, jf. ordlyden «ikke». De virksomhetene som reguleres av GDPR artikkel 3 andre ledd har derfor *ikke* «[...] en effektiv og faktisk utøvelse av aktivitet gjennom en stabil struktur [...]» i EØS-området, og heller ikke en uløselig tilknytning til EØS-området. En slik kontekstuell tolkning er i samsvar med ordlyden.

Formålet med GDPR artikkel 3 andre ledd er å sikre at fysiske personer ikke blir fratatt det vern de har rett til i medhold av GDPR, jf. fortalepunkt 23. Bestemmelsen utgjør dermed et sikkerhetsnett, i tilfeller hvor personopplysninger blir behandlet av en virksomhet som ikke er etablert i EØS-området.[60] Samtidig utgjør bestemmelsen en ulempe for virksomheter som er etablert utenfor EØS-området: I tillegg til at de må forholde seg til sitt hjemlands personvernlovgivning, risikerer de å også måtte forholde seg til GDPR. Selv om bestemmelsen

[59] I dom av 1. oktober 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639 la EU-domstolen blant annet vekt på at firmaet markedsførte seg mot EØS-land, mens EU-domstolen i dom av 13. mai 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317 la vekt på at Google Inc hadde en filial i Spania.
[60] Guidelines 3/2018 s. 13.

medfører visse ulemper, er den nødvendig for å sikre at retten til personopplysningsvern blir ivaretatt.[61]

Slik gjennomgangen viser gjelder GDPR artikkel 3 andre ledd for virksomheter som ikke har en stabil struktur eller uløselig tilknytning til EØS-området. I oppgaven omtaler jeg slike virksomheter som «virksomheter i tredjestater».[62]

3.2.3 Behandling av personopplysninger

En forutsetning for at GDPR skal gjelde for virksomheter i tredjestater, er at virksomheten har «behandl[et] [...] personopplysninger». Personvernrådet har presisert at det er selve behandlingen av personopplysninger, og ikke virksomheten som sådan, som kan bli omfattet av GDPR.[63] Hver behandling må derfor vurderes konkret.

«Behandling» er definert som «enhver operasjon eller rekke av operasjoner som gjøres med personopplysninger, enten automatisert eller ikke, f.eks. innsamling, registrering, organisering, strukturering, lagring, tilpasning eller endring, gjenfinning, konsultering, bruk, utlevering ved overføring, spredning eller alle andre former for tilgjengeliggjøring, sammenstilling eller samkjøring, begrensning, sletting eller tilintetgjøring», jf. artikkel 4 nr. 2. Enhver befatning med personopplysninger er dermed å anse som «behandling» i GDPRs forstand.

Med «personopplysninger» menes «enhver opplysning om en identifisert eller identifiserbar fysisk person («den registrerte»)», jf. GDPR art. 4 nr. 1. En «identifiserbar fysisk person» er en person som enten direkte eller indirekte kan identifiseres, jf. GDPR art. 4 nr. 1. Eksempler på personopplysninger er: «[...] et navn, et identifikasjonsnummer, lokaliseringsopplysninger, en nettidentifikator eller ett eller flere elementer som er spesifikke for nevnte fysiske persons fysiske, fysiologiske, genetiske, psykiske, økonomiske, kulturelle eller sosiale identitet», jf.

[61] En slik tolkning er i samsvar med «a general principle of interpretation, a Community act must be interpreted, as far as possible, in such a way as not to affect its validity […]. Likewise, where a provision of Community law is open to several interpretations, preference must be given to that interpretation which ensures that the provision retains its effectiveness [...]», jf. Forente dommer av 19. november 2009, *Air France*, C-402/07 og C-432/07, ECLI:EU:C:2009:716, avsnitt 47.

[62] Etter anbefaling fra Språkrådet. I høst sendte jeg e-post til Språkrådet med spørsmål om hvordan begrepet «non-EU-establishment» bør oversettes til norsk. Språkrådet svarte per e-post den 11. oktober 2019 at det er i samsvar med UDs oversettelsesenhets praksis å bruke begrepet «virksomheter i tredjestater».

[63] Guidelines 3/2018 s. 5 og 14.

GDPR art. 4 nr. 1. Videre følger det av fortalepunkt 30 at fysiske personer også kan identifiseres ved hjelp av radiofrekvensidentifikasjonsmerker, informasjonskapsler og IP-adresser. Majoriteten av vår atferd – særlig på Internett – kan brukes til å identifisere oss.[64] Vilkåret «personopplysninger» favner derfor vidt.

Utgangspunktet er dermed at vilkåret «behandling av personopplysninger» omfatter enhver befatning med informasjon som kan være egnet til å identifisere en person.

I denne oppgaven bruker jeg begrepet «den registrerte» som benevnelse på den fysiske personen som får sine personopplysninger behandlet.

3.2.4 Den registrerte befinner seg i Unionen

Det tredje inngangsvilkåret er at den registrerte «befinner seg i Unionen».

Ordlyden «befinner seg i Unionen» tilsier at den registrerte er i EØS-området. Ordlyden stiller ikke krav til tilhørighet eller tilknytning; også helt kortvarig tilstedeværelse er tilstrekkelig til å omfattes av ordlyden. En slik tolkning er i samsvar med fortalepunkt 14, hvor EUs lovgivende organer uttaler at «det vern som denne forordningen gir [...] bør få anvendelse på fysiske personer, uavhengig av deres statsborgerskap eller bosted [...]».[65] Dessuten er en slik tolkning i samsvar med EUs primærlovgivning, hvor blant annet EMK art. 8 nr. 1 slår fast at «enhver» har rett til respekt for sitt privatliv.

Vilkåret «befinner seg i Unionen» omfatter dermed enhver person som er i EØS-området – uavhengig av tilhørighet, formål eller varighet.

> Et eksempel som illustrerer rekkevidden av vilkåret, er konstruert av Personvernrådet:[66] En amerikansk IT-leverandør tilbyr en bykart-app for Paris og Roma. Når turistene logger seg inn på appen, sendes personopplysninger fra EØS-området til USA. Det er ikke avgjørende hvor turistene kommer fra; det avgjørende er at selskapet tilbyr en tjeneste til mennesker som befinner seg i EØS-området.

[64] Azzi (2018) s. 129.
[65] Det samme er også lagt til grunn i Guidelines 3/2018 s. 15.
[66] Eksempel nr. 9 i Guidelines 3/2018 s. 15.

Videre er det ikke tilstrekkelig at den registrerte har vært i EØS-området; det konkrete tidspunktet er også av betydning.

Personvernrådet har uttalt at vurderingen av om den registrerte «befinner seg i Unionen» skal foretas i det øyeblikket «the relevant trigger activity» finner sted.[67] «The relevant trigger activity» er, ifølge Personvernrådet, det øyeblikket hvor varen eller tjenesten tilbys, eller i det øyeblikket oppførselen blir monitorert.[68] Ved vurderingen av når den registrerte «befinner seg i Unionen», må man derfor ta utgangspunkt i tidspunktet hvor varen eller tjenesten ble tilbudt, eller i det øyeblikket oppførselen ble monitorert.

Det vil ofte være enkelt å slå fast hvor den den registrerte befinner seg. Det er for eksempel enkelt å stadfeste hvor den registrerte befinner seg når han blir tilbudt en håndverkertjeneste, eller når en informasjonskapsel overvåker hans internettsøk. Likevel kan det tenkes tilfeller hvor vurderingen vil være mer utfordrende. For eksempel kan det være vanskelig å tidfeste *når* en app har blitt tilbudt: Er det når vedkommende blir gjort kjent med appen, når appen blir lastet ned, idet vedkommende oppretter en bruker på appen, eller når vedkommende for første gang bruker appen? Konklusjonen på det ovennevnte spørsmålet vil kunne avgjøre om behandlingen av personopplysninger må gjøres i overenstemmelse med GDPR eller ikke.

Selv om problemstillingen knyttet til «the relevant trigger activity» ikke er særlig aktuell, er det etter min mening behov for en nærmere avklaring av spørsmålet. Behovet har dels bakgrunn i at spørsmålet ikke har blitt særlig drøftet i rettskildene, og dels fordi problemstillingen potensielt kan få alvorlige følger for de involverte.

3.2.5 Behandlingen må være knyttet til tilbudet eller monitoreringen

Dersom en virksomhet i tredjestat har behandlet personopplysningene til en registrert som befinner seg i EØS-området, er det siste inngangsvilkåret at den aktuelle behandlingen er «knyttet til» tilbud av varer eller tjenester, eller «knyttet til» monitorering av den registrerte.

[67] Guidelines 3/2018 s. 15.
[68] Ibid.

Ordlyden «knyttet til» tilsier at det må foreligge en sammenheng eller en forbindelse mellom databehandlingen og det aktuelle tilbudet, eller den aktuelle monitoreringen.[69] Behandling av personopplysninger på grunn av andre forhold enn de som er nevnt i bokstav (a) eller (b) er derfor ikke omfattet av GDPR artikkel 3 andre ledd.[70]

CIPL har tatt til orde for at «[…] the processing activity should be clearly linked to the initial activity […]».[71] Jeg er enig med CIPL i at tilknytningen bør være klar, da et slikt krav vil bidra til at virksomheter i større grad kan forutse når de må behandle personopplysninger i medhold av GDPR. Dette underbygges dessuten av at Personvernrådet, i de endelige retningslinjene, har fjernet uttalelsen om at indirekte tilknytning er tilstrekkelig.[72]

Behandlingen av personopplysninger må dermed ha en klar forbindelse med det aktuelle tilbudet, eller den aktuelle monitoreringen.

Det er imidlertid ikke tilstrekkelig at behandlingen er «knyttet til» tilbudet eller monitorering; det må i tillegg påvises at virksomheten hadde *hensikt* om å ramme personer i EØS-området.[73] Det er ikke unikt å basere jurisdiksjon på et krav om hensikt. Et krav om hensikt er blant annet benyttet i EUs forbrukerett.[74] I den juridiske teorien er kravet om hensikt omtalt som et «targeting criterion».[75]

Hensiktskravet har gode grunner for seg. For det første bidrar kravet til å sikre en viss grad av internasjonal regulering, hvilket er positivt da våre personopplysninger i stor utstrekning behandles utenfor EØS-området.[76] For den registrerte er derfor hensiktskravet sentralt for å sikre et effektivt personopplysningsvern. For det andre bidrar kravet til at virksomheter i tredjestater i stor grad kan forutsi når de behandler personopplysninger innenfor GDPRs

[69] Merk at behandlingen noen ganger kan være knyttet både til et tilbud og til monitorering. Se eksempelvis Eksempel nr. 9 i Guidelines 3/2018 s. 15 hvor app-utvikleren tilbyr en bykart-app, samtidig som de monitorerer forbrukerens geo-lokasjon.
[70] Eksempel på behandlingsaktivitet som faller utenfor er behandling knyttet til politietterforskning, straffeforfølgelse og sikkerhet.
[71] CIPL (2019) s. 12.
[72] I de første retningslinjene skrev Personvernrådet på side 15 at: «[…] both direct and indirect connections are relevant and to be taken into account.» Denne uttalelsen er ikke videreført i de endelige retningslinjene.
[73] Guidelines 3/2018 s. 14 og CIPL (2019) s. 12.
[74] Se denne oppgavens 3.3.5 om EU-dommen *Pammer og Alpenhof,* C-585/08 og C-144/09.
[75] de Hert mfl. (2016) s. 238 og Azzi (2018) s. 129.
[76] Fortalepunkt 6. Se også de Hert mfl. (2016) s. 230, Czerniawski (2017) s. 235, og Azzi (2018) s. 127.

geografiske virkeområde. En slik forutsigbarhet bidrar til stabilitet og sikkerhet for virksomhetene, hvilket er egnet til å ivareta hensynet til fri flyt av personopplysninger. For det tredje fører hensiktskravet til at regelverket blir mer treffsikkert; det er bare de virksomheter som har en tilstrekkelig tilknytning til EØS-området som blir rammet av GDPR.[77] Motsatt, dersom forordningen rammer vilkårlig, kan regelverket avskrekke virksomheter i tredjestater til å ta del i det europeiske markedet.

Vurderingen av om det foreligger hensikt «largely focuses on what the "processing activities" are "related to"».[78] Man må derfor vurdere om virksomheten i tredjestat har hatt hensikt om å tilby varer eller tjenester til personer i EØS-området, eller hensikt om å monitorere personer i EØS-området.[79] Jeg skal se nærmere på hensiktskravet i den følgende analysen av bokstav (a) og (b). Selv om det er alminnelig enighet om at det må påvises en hensikt om å ramme personer som befinner seg i EØS-området, er det uenighet knyttet til innholdet i kravet. Flere av disse uenighetene skal jeg belyse i den følgende analysen.

3.3 Tilbud av varer eller tjenester

3.3.1 Introduksjon

Slik allerede nevnt, er det to forhold som kan føre til at virksomheter i tredjestater må behandle personopplysninger i overenstemmelse med GDPR.[80] Det første forholdet er regulert i GDPR artikkel 3 andre ledd bokstav (a). Av bestemmelsen følger det at behandlingen må skje i overenstemmelse med GDPR dersom den aktuelle behandlingen er knyttet til:

> *«tilbud av varer eller tjenester til slike registrerte i Unionen, uavhengig av om det kreves betaling fra den registrerte eller ikke, jf. GDPR artikkel 3 andre ledd bokstav (a)».*[81]

Bestemmelsen regulerer en behandlingsaktivitet som foregår i stor utstrekning, og hvor en stor del av befolkningen i EØS-området blir rammet. For eksempel får mange europeiske studenter

[77] Czerniawski (2017) s. 236 og og de Hert mfl. (2016) s. 231.
[78] Guidelines 3/2018 s. 14.
[79] Ibid. s. 15.
[80] «[M]onitorering» i bokstav (b) utgjør det andre forholdet.
[81] Forutsatt at inngangsvilkårene er oppfylt.

tilbud om å reise til universiteter utenfor EØS-området, noe som kan resultere i at deres personopplysninger blir behandlet før avreise.[82] Dessuten reiser mange EØS-borgere til steder som Mauritius, Vietnam og Nepal, typisk ved at lokale virksomheter tilbyr pakkereiser eller lignende. Også i et slikt tilfelle vil personopplysningene til de registrerte bli behandlet før avreise. Et tredje eksempel er personer i EØS-området som handler varer på Internett, for eksempel via amerikanske eBay eller kinesiske Alibaba.

3.3.2 Vilkårene «varer eller tjenester»

Vilkårene «varer eller tjenester» er alternative, jf. «eller». Det er derfor tilstrekkelig at virksomheten i tredjestaten tilbyr én av de to.

Ordlyden «varer» tilsier et produkt, en ting eller en gjenstand. Vilkåret er innholdsmessig likt utformet på andre språk, for eksempel «varer» på dansk, «goods» på engelsk og «Waren» på tysk. I kjernen av begrepet er fysiske ting slik som mat, olje, mineraler, kjøretøy og elektroniske gjenstander. Vilkåret «varer» omfatter også teknologiske nyvinninger og utviklinger, i tråd med hensynet til teknologinøytralitet og vern av personopplysninger, jf. GDPR art. 1 (2) og fortalepunkt 6.

Begrepet «varer» er en sentral del av EUs primærlovgivning. Prinsippet om det frie varebytte er regulert i TEUV[83] artikkel 28 og 29 og tilsvarende i EØS-avtalen del II. Eksempler på ting som etter EUs primærlovgivning faller inn under begrepet «varer» er kunst, elektrisitet, gass og ikke-resirkulerbart søppel som kan selges.[84] Det samme gjelder for mynter, sedler og banksjekker som har gått ut på dato, forutsatt at de kan selges.[85] Eksempel på ting som *ikke* er omfattet av begrepet er TV-signal, samt gaver og donasjoner gitt i veldedig formål.[86]

Samlet er det klart at begrepet er vidt, og omfavner enhver gjenstand som har en viss verdi.

---

[82] I EU-retten kan utdanning anses for å være en tjeneste, jf. Dom av 9. desember 1993, *Wirth*, C-109/92, ECLI:EU:C:1993:916, avsnitt 12–18.
[83] Consolidated version of the Treaty on the Functioning of the European Union – TFEU, Roma, konsolidert 7. July 2016, OJ C 202 [Traktaten om Den europeiske unions virkemåte, TEUV] (Roma-traktaten).
[84] Europakommisjonens handbook (2010) "*Free movement of goods. Guide to the application of Treaty provisions governing the free movement of goods*". Luxembourg: Publications Office of the European Union, s. 9–10 med videre henvisning til EU-domstolens praksis.
[85] Ibid.
[86] Ibid.

Selv om man normalt forutsetter at en vare blir møtt med en motytelse, kommer GDPR til anvendelse «uavhengig av om det kreves betaling fra den registrerte eller ikke», jf. GDPR art. 3 (2). Dette er i samsvar med EUs forbrukerett og praksis fra EU-domstolen.[87]

Ordlyden «tjenester» tilsier en ytelse, handling eller arbeid, som normalt forutsetter en viss motytelse. Vilkåret er likt utformet på andre språk, for eksempel «tjenester» på dansk, «services» på engelske og «Dienstleistungen» på tysk. Ordlyden stiller ikke krav til tjenestens form: Både fysiske og elektroniske tjenester er omfattet av ordlyden. En slik tolkning er i samsvar med hensynet til teknologinøytralitet.[88] Tilsvarende har EUs lovgivende organer presisert at såkalte «informasjonssamfunnstjenester» er omfattet av vilkåret.[89]

> En «informasjonssamfunnstjeneste[]» er en tjeneste som sendes til mottakeren ved hjelp av elektroniske hjelpemidler, uten at begge parter er til stede samtidig.[90] Eksempel på en slik tjeneste er abonnement på en strømmetjenester (eksempelvis Netflix og HBO), programvarer, sosiale nettverk og bestilling av billetter via Internett og apper.

Begrepet «tjenester» er en sentral del av EUs primærlovgivning. Prinsippet om fri flyt av tjenester er regulert i TEUV artikkel 56–62 og tilsvarende i EØS-avtalen artikkel 36–39. En tjeneste er typisk en industriell virksomhet, handels- og håndverkervirksomhet og virksomheter innen de frie yrker, jf. TEUV art. 57 (2) bokstav a–d, og EØS-avtalen art. 37 (2) bokstav a–d. EUs primærlovgivning støtter dermed opp under ordlydstolkningen ovenfor.

Gjennomgangen viser at vilkåret «tjenester» er vidt utformet, og ikke stiller krav til ytelsens form. I likhet med vilkåret «varer», er det *ikke* et krav at tjenesten blir møtt med en motytelse.

---

[87] Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services, art. 3 nr. 1 (2) og fortalepunkt 24, samt *Wirth*, C-109/92 avsnitt 12–18.
[88] GDPR fortalepunkt 6.
[89] GDPR artikkel 4 nr. 25, jf. også Guidelines 3/2018 s. 16.
[90] Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 *laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services* artikkel 1 nr. 1 bokstav (b).

En ytelse som *ikke* er omfattet av vilkåret «tjenester» er, ifølge Personvernrådet, behandling av personopplysninger som er knyttet til ledelse av menneskelige ressurser (HRM).[91] Behandling som er knyttet til HRM, er oppgaver som er nødvendig for å oppfylle arbeidskontrakten eller tilsvarende plikter.[92] Behandling som ikke er nødvendig for å oppfylle arbeidskontrakten er derfor en «tjeneste» i GDPRs forstand.

> Personvernrådet har konstruert et eksempel på behandling av personopplysninger som gjøres i forbindelse med HRM:[93] Peder Ås er på jobbreise i Frankrike, og sover på hotell. Ås´ amerikanske arbeidsgiver refunderer hotellutgiftene til Ås, i tillegg til å betale ut lønn. Arbeidsgiveren må ikke behandle personopplysningene til Ås i overenstemmelse med GDPR. Personvernrådet skrivet at behandlingen: "[…] does not relate to an offer of a service to those individuals, but rather is part of the processing necessary for the employer to fulfil its contractual obligation and human resources duties related to the individual´s employment".[94] Et eksempel fra Korff er egnet til å illustrere det motsatte, altså behandling som er en tjeneste i GDPRs forstand:[95] En amerikansk arbeidsgiver tilbyr sin norske arbeidstaker Peder Ås å være med i en pensjonssparing. I forbindelse med pensjonssparingen behandler den amerikanske arbeidsgiveren personopplysningene til Ås. Behandlingen må gjøres i overenstemmelse med GDPR fordi pensjonssparingen er et separat tilbud som ikke har tilknytning til arbeidsforholdet som sådan.

3.3.3 Hensikt om å tilby varer eller tjenester

Dersom en virksomhet har «tilbud[t]» varer eller tjenester til registrerte i EØS-området, må den aktuelle behandlingen av personopplysninger gjøres i overenstemmelse med GDPR, jf. art. 3 andre ledd bokstav (a).

Den naturlige språklige forståelsen «tilbud» tilsier at en fysisk eller juridisk person forsøker å selge, overlevere eller gi noe til en annen fysisk eller juridisk person. Eksempler på «tilbud» er *salg* av matvarer eller håndverkertjenester, eller *oppfordring* om å kjøpe et rabattert produkt. Videre ligger det i tilbudets natur at virksomheten gjør et aktivt forsøk på å overbevise mottakeren; virksomheten har hensikt om å tilby en vare eller tjeneste til personer i EØS-området. Det samme har EUs lovgivende organer skrevet i fortalepunkt 23, og i tillegg presisert

[91] Guidelines 3/2018 s. 16–17.
[92] Ibid.
[93] Eksempel nr. 13 i Guidelines 3/2018 s. 16–17.
[94] Ibid.
[95] Korff (2019) s. 18.

at det må være «åpenbart» at virksomheten hadde hensikt om å tilby varer eller tjenester til personer i EØS-området.

> Personvernrådet har konstruert et eksempel hvor en virksomhet åpenbart har hensikt om å tilby en vare til personer i EØS-området:[96] En tyrkisk virksomhet redigerer, trykker og leverer fotoalbum, og sender fotoalbumene til sine kunder i Europa. Virksomhetens hjemmeside er oversatt til engelsk, fransk, tysk og nederlandsk, og kundene kan betale med Euro. Det er derfor åpenbart at virksomheten har hensikt om å tilby fotoalbum til personer i EØS-området, og behandlingen må gjøres i overenstemmelse med GDPR.
> Personvernrådet har også konstruert et eksempel hvor en virksomhet *ikke* har åpenbar hensikt om å tilby en vare til personer i EØS-området:[97] En amerikaner laster ned en amerikansk nyhets-app mens han er på ferie i EØS-området, for å holde seg oppdatert på amerikanske nyheter. Han får tilgang til nyhetsartiklene ved å betale med amerikanske dollar, og ved å registrere sitt amerikanske mobilnummer. Det framstår ikke som åpenbart at virksomheten har hatt hensikt om å tilby tjenesten til personer i EØS-området. Behandlingen av personopplysninger må derfor ikke gjøres i overenstemmelse med GDPR.

En konsekvens av hensiktskravet, er at tilfeldig og utilsiktet behandling ikke er omfattet av GDPR artikkel 3 andre ledd bokstav (a).[98] Personvernrådet skriver som eksempel at: «[…] if the processing relates to a service that is only offered to individuals outside the EU but the service is not withdrawn when such individuals enter the EU, the related processing will not be subject to the GDPR.» [99]

> Et eksempel fra Personvernrådet viser hvordan behandlingen av personopplysninger kan være tilfeldig:[100] En australsk video-app blir markedsført til personer som bor i Australia. Dersom en australier bruker appen mens han er på ferie i EØS-området, må app-utvikleren ikke behandle personopplysninger i overenstemmelse med GDPR. Personvernrådet begrunner dette med at det er tilfeldig at app-utvikleren behandler personopplysninger til en som befinner seg i EØS-området; appen har tross alt bare blitt tilbudt til folk som bor i Australia.

Slik gjennomgangen viser, innebærer vilkåret «tilbud» at virksomheten som tilbyr varen eller tjenesten, åpenbart må ha hatt hensikt om å ramme personer i EØS-området.

[96] Eksempel nr. 14 i Guidelines 3/2018 s. 18.
[97] Eksempel nr. 10 i Guidelines 3/2018 s. 16.
[98] Guidelines 3/2018 s. 15.
[99] Ibid.
[100] Ibid., Eksempel nr. 8.

3.3.4 Hvordan vurdere vilkåret «tilbud»?

Vurderingen av om en virksomhet har hatt åpenbar hensikt om å tilby en vare eller tjeneste til personer i EØS-området, må gjøres konkret. I GDPRs fortalepunkt 23 har EUs lovgivende organer oppstilt momenter som kan være av betydning ved vurderingen av om en virksomhet åpenbart har hatt en slik hensikt:

> *«[...] Selv om tilgang til den behandlingsansvarliges, databehandlerens eller en mellommanns nettsted i Unionen, til en e-postadresse eller til andre kontaktopplysninger, eller bruk av et språk som vanligvis benyttes i tredjestaten der den behandlingsansvarlige er etablert, ikke er tilstrekkelig til å fastslå en slik hensikt, kan faktorer som bruk av et språk eller en valuta som vanligvis benyttes i én eller flere medlemsstater, sammen med en mulighet til å bestille varer og tjenester på nevnte andre språk, eller omtale av kunder eller brukere som befinner seg i Unionen, gjøre det åpenbart at den behandlingsansvarlige har til hensikt å tilby varer eller tjenester til registrerte i Unionen», jf. fortalepunkt 23.*

Momentene i fortalepunkt 23 bygger på og er i samsvar med praksis fra EU-domstolen.[101] I det følgende skal jeg se nærmere på relevant praksis fra EU-domstolen, for å utpensle vurderingsmomentene ytterligere.

3.3.5 Vurderingsmomenter fra EU-dommen *Pammer og Alpenhof*

Det er særlig EU-domstolens avgjørelse i *Pammer og Alpenhof*-saken[102] som er av betydning ved tolkningen av vilkåret «tilbud» i GDPR artikkel 3 andre ledd bokstav (a); momentene i GDPR fortalepunkt 23 bygger på nettopp denne avgjørelsen.[103]

I *Pammer-saken* hadde en østerriksk mann, Herr Pammer, forhåndsbetalt en reise med et tysk cruiseskip. På grunn av skipets dårlige stand, valgte Pammer å ikke delta på reisen. Pammer fikk ikke det forhåndsbetalte beløpet refundert. Han krevde beløpet tilbakebetalt gjennom et søksmål mot det tyske rederiet. Herr Pammer anla søksmålet for en østerriksk domstol, altså i sitt hjemland. Det tyske rederiet hevdet at søksmålet bare kunne anlegges for tysk domstol, hvor

[101] Guidelines 3/2018 s. 17.
[102] Forente dommer av 7. desember 2010, *Pammer- og Alpenhof*, C-585/08 og C-144/09, ECLI:EU:C:2010:740.
[103] Guidelines 3/2018 s. 17–18.

de selv hadde tilholdssted. I *Alpenhof-saken* ferierte en tysk mann på det østerrikske hotellet Alpenhof. Mannen betalte bare deler av det avtalte beløpet. Hotellet krevde pengene tilbakebetalt gjennom et søksmål anlagt for en østerriksk domstol. Den tyske mannen anførte at søksmål bare kunne anlegges i hans eget hjemland, nemlig Tyskland.

Sentralt i begge sakene var om domstolene hadde stedlig domsmyndighet til å avgjøre søksmålene. Det rettslige grunnlaget for å avgjøre spørsmålet, var Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters. Et sentralt formål med Council Regulation (EC) No 44/2001 var at «[...] the weaker party should be protected [in relation to consumer contracts] by rules of jurisdiction more favourable to his interests than the general rules provide for», jf. fortalepunkt 13.

Reglene om stedlig domsmyndighet kom bare til anvendelse dersom den næringsdrivende «directs» (på norsk: rettet) sin næringsvirksomhet mot det aktuelle landet, jf. artikkel 15 nr. 1 (c). Forbeholdet var i samsvar med regelens formål; bare den aktivitet som er knyttet til næringsvirksomhet bør underlegges regler om forbrukervern. Det springende punktet i begge sakene var derfor om den næringsdrivende, henholdsvis det tyskeide rederiet og Hotell Alpenhof, hadde «directs» sin virksomhet mot det andre medlemslandet.

> Dersom EU-domstolen kom til at det tyske rederiet hadde «directs» sin virksomhet mot Østerrike, kunne Herr Pammer velge om han ville reise søksmål i landet hvor den næringsdrivende hadde tilholdssted (Tyskland), eller i sitt hjemland (Østerrike), jf. Council Regulation (EC) 44/2001 artikkel 16 nr. 1. For det østerrikske hotellet Alpenhof ville en slik konklusjon medføre at de bare kunne saksøke forbrukeren i hans hjemland, nemlig Tyskland, jf. art. 16 nr. 2.

Da EU-domstolen tolket vilkåret «directs», oppstilte de en rekke vurderingsmomenter. Vurderingsmomentene kan, slik allerede nevnt, tillegges vekt ved tolkning av vilkåret «tilbud» i GDPR artikkel 3 andre ledd bokstav (a).

Momenter som ifølge EU-domstolen klart tilsier at virksomheten i tredjestaten har «directs» sin virksomhet mot personer i EØS-området, er «all clear expressions of the intention to solicit the

custom of that State's consumers».[104] For det første viser EU-domstolen til eksplisitte opplysninger om at virksomheten tilbyr sine varer eller tjenester til ett eller flere medlemsstater.[105] For det andre viser EU-domstolen til eventuelle utgifter virksomheten har hatt knyttet til søke- og annonseringsytelser med formål om å nå ut til forbrukere som befinner seg i EØS-området.[106]

Momenter som etter en sammensatt og konkret vurdering kan tilsi at virksomheten i tredjestaten har «directs» sin virksomhet mot personer i EØS-området er: Virksomhetens internasjonale karakter; tilgjengeliggjøring av virksomhetens telefonnummer med internasjonal landskode; anvendelse av et toppdomenenavn som ikke er vanlig i virksomhetens etableringssted; veibeskrivelse fra ett eller flere land i EØS-området til virksomhetens tilholdssted; en presentasjon av virksomhetens internasjonale klientell; samt bruk av språk og valuta.[107] I en senere sak fra EU-domstolen, *L´Oréal v eBay*, er det i tillegg slått fast at det er av betydning om det fremgår av hjemmesiden at varen kan sendes til ett eller flere land i EØS-området.[108]

Ifølge EU-domstolen er det *ikke* av betydning at virksomheten har tilgjengeliggjort sin e-mailadresse, fysiske adresse eller telefonnummer.[109] Dette har sammenheng med at slike opplysninger er nødvendige – og i enkelte tilfeller også pålagt – for at forbruker skal kunne komme i kontakt med virksomheten.[110] Det er heller ikke av betydning at virksomhetens Internettside er tilgjengelig i EØS-området.[111] Dette fordi Internett i sin natur er tilgjengelig for enhver. Ved tolkningen av vilkåret «tilbud» i GDPR artikkel 3 andre ledd bokstav (a), skal de nevnte momentene ikke tillegges vekt.

[104] *Pammer* og *Hotel Alpenhof,* C-585/08 og C-144/09*,* avsnitt 80.
[105] Ibid. avsnitt 81.
[106] Ibid.
[107] Ibid. avsnitt 83–84.
[108] Dom av 12. juli 2011, *L´Oréal v eBay*, C-324/09, ECLI:EU:C:2011:474, avsnitt 65, og tilsvarende i Guidelines 3/2018 s. 18 siste strekpunkt.
[109] *Pammer* og *Hotel Alpenhof,* C-585/08 og C-144/09, avsnitt 76.
[110] Ibid. avsnitt 78.
[111] Ibid. avsnitt 72.

3.3.6 Teoretiske innvendinger mot vurderingsmomentene i Pammer- og Alpenhof-dommen

Svantesson mener at vektlegging av *domenenavn* kan føre til at virksomheter feilaktig blir rammet av GDPR.[112] Som eksempel viser han til at enkelte selskaper bruker domenenavn for å oppnå ordspill, for eksempel: «parti.es» eller «famili.es».[113] Etter min mening er de senarioer som Svantesson forespeiler sjeldne. Dessuten vil det normalt være enkelt å gjennomskue en slik bruk av domenenavn.

Videre mener Svatesson at vektlegging av en virksomhets bruk av *språk og valuta* ikke nødvendigvis er egnet til å gi gode resultater.[114] Herunder viser han til at rimelige e-løsninger enkelt kan oversette språk og valuta. Oversettelse er derfor ikke ensbetydende med at virksomheten har en bevisst hensikt om å tilby varer og tjenester til EØS-området.[115] Selv om jeg er enig i at oversettelse ikke er en garanti for at virksomheten har hatt hensikt, mener jeg likevel at vurderingsmomentene er egnet til å gi rimelige resultater. For den registrerte vil språk og valuta være sentrale i vurderingen av om virksomheten har et EØS-basert marked. Vurderingsmomentene er derfor viktige for at de registrerte kan forutsi sin rettsstilling.

Videre etterspør CIPL mer klargjøring av vurderingsmomentet *virksomhetens internasjonale karakter*.[116] Blant annet viser CIPL til at enkelte turistattraksjoner – tross sin popularitet – ikke nødvendigvis har hensikt om å rette sin virksomhet mot personer i EØS-området.[117] Jeg er enig med CIPL i at en virksomhet ikke nødvendigvis har hensikt om å henvende seg til personer i EØS-området, bare fordi den er populær. Likevel bidrar kriteriet til at virksomheter med et globalt marked ikke kan omgå regelverket, og dermed gi de registrerte et dårligere vern. Dessuten vil vurderingsmomentet i majoriteten av tilfeller være forutsigbart, hvilket er i tråd med hensynet til den registrerte og fri fly av personopplysninger.

---

[112] Svantesson, Dan Jerker B. (2011) *Pammer and Hotel Alpenhof - ECJ decision creates further uncertainty about when e-businesses "direct activities" to a consumer's state under the Brussels i Regulation*. Computer Law and Security Review, 27(3), punkt 4.1.
[113] Ibid.
[114] Ibid.
[115] Ibid.
[116] CIPL (2019) s. 13.
[117] Ibid.

Uansett vil alle de ovennevnte vurderingsmomentene ikke alene være nok til å konkludere med at en virksomhet har hatt hensikt om å tilby en vare eller tjeneste til personer i EØS-området; det må foretas en helhetsvurdering. Selv om hvert enkelt vurderingsmoment ikke har avgjørende betydning, er det grunn til å etterspørre mer klargjøring da dette vil bidra til at både virksomheter og de registrerte får større forutberegnelighet i møte med regelverket.

3.3.7 Kan man legge vekt på det faktiske utfallet av et tilbud?

Gjennomgangen av gjeldende rett viser at det er virksomhetens intensjon – og ikke det faktiske utfallet av tilbudet – som skal tillegges vekt ved vurderingen av om vilkåret «tilbud» er oppfylt. I den forbindelse er det særlig interessant å se hen til generaladvokat Trstenjaks forslag til avgjørelse i *Pammer- og Alpenholf*-saken.[118] Blant annet uttalte hun at «[…] these special rules of jurisdiction can only apply once it has made a conscious decision [på norsk: et bevisst valg] to direct its activities to the consumer's Member State».[119] Uttalelsen til generaladvokaten, særlig formuleringen «conscious decision», tilsier at det er virksomhetens intensjon som er avgjørende for om en virksomhet har «directs» sin næring mot EØS-området. Selv om EU-domstolen ikke tar uttrykkelig stilling til uttalelsen er den – slik jeg ser det – sentral for vurderingen av vilkåret «directs» i Regulation (EC) No 44/2001. Herunder er det avgjørende at essensen i vurderingsmomentene i *Pammer- og Alpenholf*-saken tross alt er den samme som i generaladvokatens uttalelse: Det sentrale er hva som har vært virksomhetens intensjon; ikke hva som faktisk har skjedd. Da EUs lovgivende organer og Personvernrådet har videreført de eksakt sammen vurderingsmomentene til å også gjelde for vilkåret «tilbud» i GDPR artikkel 3 andre ledd bokstav (a) må det, etter min mening, bety at innholdet i generaladvokatens uttalelse også er av betydning ved tolkningen av vilkåret «tilbud».

Til tross for at gjennomgangen viser at det er virksomhets intensjon som er avgjørende for om vilkåret «tilbud» i GDPR artikkel 3 andre ledd bokstav (a) er oppfylt, tilsier hensynet til den registrerte at man også bør kunne legge vekt på tilbudets faktiske utfall. Herunder kan det

[118] Opinion of Advocate General V. Trstenjak delivered on 18 May 2010 in joined cases C-585/08 og C-144/09, *Pammer og Alpenhof*, ECLI:EU:C:2010:273. Generaladvokatens forslag er ikke rettslig bindende, men er likevel ofte i samsvar med EU-domstolens avgjørelse. Generaladvokatens forslag er derfor en viktig del av EU-domstolens avgjørelse.
[119] Ibid. avsnitt 2.

argumenteres for at vektlegging av tilbudets faktiske utfall er nødvendig for at de registrerte sitt vern skal bli tilstrekkelig ivaretatt.[120]

> Et eksempel fra Svantesson kan illustrere problemstillingen:[121] Man kan tenke seg at en virksomhet – for eksempel en kinesisk mobilleverandør – ønsker å selge sine mobiltelefoner på det sveitsiske markedet. Den kinesiske mobilleverandøren sender derfor mobilreklame til sveitsiske husstander, både på tysk, fransk og italiensk. Som følge av en misforståelse internt hos den kinesiske mobilleverandøren, blir mobilreklamen også sendt til husstander i Tyskland, Frankrike og Italia. Som et resultat av denne feilen, blir de kinesiske mobiltelefonene kjøpt av personer som er bosatt i alle de fire landene. Den kinesiske mobilleverandøren fattet ikke «a conscious decision» om å tilby sine mobiltelefoner til personer bosatt i EØS-området; hensikten var å tilby mobiltelefonene til personer bosatt i Sveits. De registrerte, som har kjøpt mobiltelefon, har likevel en klar interesse av å nyte vern i medhold av GDPR. For de registrerte i Tyskland, Frankrike og Italia vil det oppleves som urimelig at en feil internt hos det kinesiske selskapet fører til at de mister sin grunnleggende rett til personvern.

Etter min mening er det i enkelte tilfeller formålstjenlig å legge vekt på det faktiske utfallet av tilbudet, i tillegg til virksomhetens hensikt – først da sikrer man at hensynet til den registrerte og personopplysningsvern blir tilstrekkelig ivaretatt, jf. GDPR art. 1 (2).[122] De øvrige rettskildene synes imidlertid ikke å åpne opp for en slik tolkning av vilkåret «tilbud». Selv om problemstillingen ikke er særlig aktuell er den moden til å bli nærmere avklart.

3.4 Monitorering

3.4.1 Introduksjon

Det andre forholdet som kan føre til at virksomheter i tredjestater må behandle personopplysninger i overenstemmelse med GDPR, er dersom virksomheten monitorerer atferden til personer som befinner seg i EØS-området.[123] Av GDPR artikkel 3 andre ledd (b) følger det at en virksomhet i tredjestat handler innenfor GDPRs geografiske virkeområde dersom behandlingen er knyttet til:

[120] Svantesson (2011) punkt. 4.2 og Svantesson (2015) s. 231–232.
[121] Svantesson (2011) punkt 4.2.
[122] En slik tolkning er i samsvar med prinsippet om at regelen skal aktualisere det overordnede formålet, jf. *Air France*, C-402/07 og C-432/07, avsnitt 47.
[123] «[T]ilbud av varer og tjenester» i bokstav (a) utgjør det første forholdet.

«monitorering av [den registrertes] atferd, i den grad [den registrertes] atferd finner sted i Unionen».[124]

Denne bestemmelsen regulerer – i likhet med bokstav (a) – en behandlingsaktivitet som foregår i stor utstrekning, og hvor en stor del av befolkningen i EØS-området blir rammet. Et typisk tilfelle er når den registrerte oppgir sin geo-lokasjon til en app, slik at app-utvikleren kan følge med på hvor den registrerte befinner seg til enhver tid. Monitorering kan også skje ved at en arbeidsgiver, for eksempel et busselskap, installerer bussene med GPS-sendere og tilhørende individuelt sjåførkort.[125] Et annet eksempel på monitorering av atferd er den såkalte *Ferde*-saken.[126] I Ferde-saken sendte et Bergensbasert bompengeselskap bilder av bompasseringer til en databehandler i Kina, slik at selskapet i Kina kunne lese av registreringsskiltene til bilene og deretter utstede fakturaer.[127]

3.4.2 Atferd i EØS-området

GDPR kommer bare til anvendelse dersom «atferd[en]» som monitoreres «finner sted i Unionen».

Ordlyden «atferd» tilsier hva en person gjør og tenker, og hvordan han reagerer på ytre og indre stimuli. Begrepet omfatter en persons handlingsmønster og oppførsel, for eksempel hvilken rute han går til jobb, eller hvor ofte han må løpe for å rekke bussen. Begrepet omfatter også vedkommende sin personlighet, personlige preferanser og verdisett. Det er bare informasjon som er egnet til å identifisere en person som er omfattet av vilkåret.[128] Vilkåret «atferd» favner vidt.

Ordlyden «finner sted i Unionen» tilsier at atferden – for eksempel handleturen, internettsøket, betalingen eller telefonsamtalen – har foregått innenfor EØS-området. Vilkåret er ofte enkelt å

[124] Forutsatt at inngangsvilkårene er oppfylt, se denne oppgavens kapittel 3.2.
[125] Dette var tilfellet i PVN-2017-18, *Nobina Norge AS*-saken, 20. mars 2018, hvor arbeidsgiver Nobina Norge AS installerte billettmaskiner med GPS-sender for å undersøke om sjåførene overhold rutetabellen, og dessuten om sjåførene faktisk arbeidet de overtidstimene som de fakturerte arbeidsgiveren for.
[126] Fotnote 57.
[127] Ferde-saken er for øyeblikket under behandling hos Datatilsynet. Det er derfor uklart om Ferde hadde adgang til å sende personopplysningene til Kina eller ikke.
[128] GDPR art. 4 nr. 1 og underkapittel 3.2.3.

vurdere; det vil normalt ikke by på særlige utfordringer å vurdere hvor et menneske befinner seg.

Vilkåret «atferd [som] finner sted i Unionen» omfatter dermed enhver handling som en fysisk person gjør innenfor EØS-området.

3.4.3 Monitorering av den registrertes atferd

Den andre forutsetning for at GDPR skal komme til anvendelse, er at behandlingen av personopplysninger er knyttet til «monitorering av [den registrertes] atferd».[129]

Ordlyden «monitorering» tilsier at man følger med, holder øye med eller observerer noe eller noen. I andre språkversjoner er det brukt innholdsmessige like ord, for eksempel «monitoring» på engelsk, «overvågning» på dansk og «beobachten» på tysk. Utgangspunktet er derfor at enhver atferdsovervåkningen er omfattet av vilkåret.

Det er i samsvar med hensynet til den registrerte å tolke vilkåret «monitorering» slik at enhver atferdsovervåkningen er omfattet; enhver atferdsovervåkning utgjør et inngrep i den personlige sfære, jf. GDPR art. 1 andre ledd.[130]

> Dette ble understreket av Personvernkommisjonen i NOU 2009:1, som blant annet uttalte at overvåkning i arbeidslivet er belastende, uansett om arbeidstakeren har noe å skjule eller ikke.[131] I den samme utredningen uttalte kommisjonen at overvåkning av barn og unge kan påvirke deres tanker om egen frihet og rett til privatliv, og dessuten sette uheldige begrensninger på deres hverdagslige utfoldelse.[132] Kommisjonen var også kritisk til bruk av GPS-sporing, særlig av barn.[133] Selv om Personvernkommisjonen uttalte seg om konkrete overvåkningstilfeller, er det klart at overvåkning er inngripende uavhengig av hvilket område saken gjelder.

I fortalepunkt 23 har EUs lovgivende organ uttalt at det «bør [...] bringes på det rene om det skjer sporing av fysiske personer på internett [...]». Uttalelsen i fortalepunkt 23 er ikke

[129] Forutsatt at inngangsvilkårene er oppfylt, se denne oppgavens kapittel 3.1.
[130] I henhold til prinsippet om at den mest effektive og tjenlige virkningen skal velges, se *Air France*, C-402/07 og C-432/07.
[131] NOU 2009: 1, punkt 2.4.3.
[132] Ibid. punkt 14.3.7.1.
[133] Ibid. punkt 14.3.8.

uttømmende, jf. ordlyden «bør». Også Personvernrådet og CIPL har lagt til grunn at andre overvåkningsmetoder kan være omfattet av vilkåret «monitorering».[134] Personvernrådet viser blant annet til at bærbare og smarte enheter kan brukes til å atferdsovervåke, i tillegg til kostholds- og helseanalysetjenester, kameraovervåkning, informasjonskapsler og markedsundersøkelser.[135]

Gjennomgangen av vilkåret «monitorering av [den registrertes] atferd» viser at bestemmelsen etter sin ordlyd omfatter enhver atferdsovervåkning, uavhengig av hvordan overvåkningen gjennomføres.

> Personvernrådet har konstruert eksempler som viser hvordan atferdsovervåkning kan foregå. I ett av eksemplene engasjerer et fransk kjøpesenter et konsulentselskap, som får i oppgave å gi kjøpesenterets kunder personlig markedsføring basert på hvilke butikker de handler i.[136] Da konsulentselskapet har vært i befatning med kundenes geo-lokasjon, har de *monitorert atferden* til kundene. Dessuten er det allerede nevnte eksempelet om bykart-appen egnet til å vise hvordan monitorering kan foregå:[137] Når turister sender sin geo-lokasjon til app-utvikleren i USA, i bytte mot informasjon om hvilke attraksjoner som finnes i nærheten, blir deres atferd overvåket.

CIPL er kritiske til at Personvernrådet ikke har oppstilt nærmere vurderingskriterier for hvilke overvåkningsmetoder som kan omfattes av vilkåret «monitorering».[138] Som eksempel viser CIPL til at virksomheter som driver med rutine- og sikkerhetsmessig overvåkning av ansattes e-poster vil ha interesse av å vite når slik overvåkning anses for å være monitorering i GDPRs forstand.[139] Slik jeg ser det, er kritikken fra CIPL berettiget. Uten forhåndssatte vurderingskriterier, vil det være utfordrende for virksomheter og registrerte å vite hva som faktisk er omfattet av vilkåret «monitorering». I mangel på nærmere avklaring fra Personvernrådet må man antakeligvis, på grunn av den vide ordlyden «monitorering», legge til grunn at enhver metode som kan overvåke personopplysninger er omfattet av vilkåret «monitorering».[140]

---

[134] Guidelines 3/2018 s. 19–20 og CIPL (2019) s. 14.
[135] Guidelines 3/2018 s. 20.
[136] Eksempel nr. 17 i Guidelines 3/2018 s. 20.
[137] Eksempel nr. 9 i Guidelines 3/2018 s. 15.
[138] CIPL (2019) s. 14.
[139] Ibid.
[140] En slik tolkning er i tråd med «[...] the principle that the provisions […] which constitutes one of the foundations of the Union, must be construed broadly», jf. Forente dommer av 15. desember 2016, *Depesme og Kerrou,* C-401/15 og 403/15, ECLI:EU:2016:955, avsnitt 58.

3.4.4 Hensikt om å monitorere

Selv om det ikke følger uttrykkelig av ordlyden i bokstav (b) eller fortalepunkt 24, er det klart at virksomheten må ha hatt *hensikt* om å monitorere personer i EØS-området.[141] Det ligger i begrepets natur at atferdsovervåkningen må ha et bestemt formål.[142] Også i litteraturen er det enighet om at *hensikt* om å ramme personer i EØS-området er en forutsetning for at vilkåret «monitorering» skal være oppfylt.[143]

Ordlyden «monitorering» omfatter dermed enhver atferdsovervåkning som er gjort med hensikt.

3.4.5 Profilering som en sentral del av vilkåret «monitorering»

Vurderingen av om en virksomhet har hatt hensikt om å monitorere personer som befinner seg i EØS-området, må gjøres konkret. I fortalepunkt 24 har EUs lovgivende organer skrevet at:

> *«[Det] bør [...] bringes på det rene om det skjer sporing av fysiske personer på internett, herunder en mulig påfølgende bruk av teknikker for behandling av personopplysninger som innebærer* ***profilering*** *av en fysisk person, særlig med det formål å treffe avgjørelser om vedkommende eller analysere eller forutsi vedkommendes personlige preferanser, atferd eller holdninger».*[144] (min utheving)

Det skal altså legges stor vekt på om virksomheten i tredjestaten *profilerer* personer i EØS-området. Personvernrådet har lagt til grunn en tilsvarende forståelse, og uttalt at «[…] tracking of natural persons on the Internet, including the potential subsequent use of profiling techniques, is a key consideration.»[145] Profilering utgjør altså en viktig del av vilkåret «monitorering».

---

[141] I motsetning til vilkåret «tilbud» i bokstav (a), og fortalepunkt 23 som krever at virksomheten «åpenbart [...] har til hensikt å tilby varer eller tjenester til registrerte [...]».
[142] Guidelines 3/2018 s. 20.
[143] Azzi (2018) s. 129, CIPL (2019) s. 14 og Dall, Nis Peter mfl. (2016) *Persondataforordningen - en håndbog for praktikere.* Ex Tuto Publishing: København s. 38.
[144] Fortalepunkt 24.
[145] Guidelines 3/2018 s. 20.

Profilering er definert som «enhver form for automatisert behandling av personopplysninger som innebærer å bruke personopplysninger for å vurdere visse personlige aspekter knyttet til en fysisk person, særlig for å analysere eller forutsi aspekter som gjelder nevnte fysiske persons arbeidsprestasjoner, økonomiske situasjon, helse, personlige preferanser, interesser, pålitelighet, atferd, plassering eller bevegelser».[146]

Enkelt sagt betyr profilering at man samler inn informasjon om et menneske (eller en gruppe mennesker) og evaluerer deres egenskaper eller atferdsmønster. Formålet med profileringen er å plassere enkeltindividene i en bestemt kategori eller gruppe for deretter å analysere eller forutsi vedkommende sin evne til å utføre en oppgave, interesser eller sannsynlig oppførsel.[147]

> Eksempel på profilering er når fordelsprogrammet Trumf deler sine kunder inn i grupper basert på om de er kvalitetsbevisste, prisbevisste eller tradisjonelle, og deretter sender reklame og markedsføring som passer med kundens profil.[148] Et annet eksempel på profilering er den såkalte *Cambridge Analytica*-saken, hvor personopplysninger til omlag 50 millioner Facebook-brukere ble samlet inn og analysert, med formål om å sende brukerne personlig politisk reklame i forkant av 2016-valget i USA.[149]

Selv om profilering er en sentral del av vilkåret «monitorering», er det ikke et absolutt krav, jf. formuleringene «bør» og «mulig påfølgende bruk» i fortalepunkt 24. En slik tolkning er i samsvar med hensynet til den registrerte: Behandling av personopplysninger kan – uavhengig av formål og etterfølgende bruk – oppleves som inngripende og krenkende. Dessuten gir en slik tolkning av vilkåret en enklere regel, som i mindre grad skaper rettstvister. Herunder er det nærliggende å anta at bevisføring for om profilering har funnet sted, vil være utfordrende både for den registrerte og for virksomheten i tredjestaten.

Det klare utgangspunktet er derfor at enhver formålsrettet atferdsovervåkning – uavhengig av etterfølgende bruk – er omfattet av vilkåret «monitorering».

---

[146] GDPR artikkel 4 nr. 4.
[147] WP251rev.01 s. 7.
[148] Eksempelet er hentet fra Datatilsynet (2018) *Hva vet de om deg? Bruk av innsynsretten hos fire virksomheter*, s. 10.
[149] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (lastet ned 26.11.2019).

3.4.6 Faller klassifiseringer utenfor vilkåret «monitorering»?

Klassifisering er behandling av personopplysninger som gjøres med det formål å identifisere generelle trender og korrelasjoner. Selv om klassifisering forutsetter at det samles inn personopplysninger, blir enkeltpersoner ikke vurdert og analysert. Klassifisering skiller seg dermed fra profilering.

> Det er typisk informasjonskapsler på Internett som brukes for å klassifisere personopplysninger. Eksempelvis er programvarer og IT-tjenester ofte utstyrt med logger og trackere, som sørger for å gi leverandørene og utviklerne informasjon om hvilke deler av programvaren som bør forbedres eller endres. På den måten bidrar klassifisering til å skape sømløse, intuitive og brukervennlige internettopplevelser. Informasjonskapsler kan også brukes for å overvåke nett-trafikken på en Internettside, for eksempel for å finne ut av hvilke nyhetssaker som genererer flest «klikk».[150]

Til tross for at klassifisering ikke nødvendigvis er særlig inngripende, er det formålsrettet atferdsovervåkning. Det klare utgangspunktet er derfor at slik behandling er omfattet av vilkåret «monitorering» i GDPR artikkel 3 andre ledd bokstav (b). Dette er i tråd med en uttalelse fra Personvernrådet om at «Online tracking through the use of cookies or other tracking techniques such as fingerprinting» er omfattet av GDPR.[151]

> Også et eksempel fra Personvernrådet bidrar til å underbygge at klassifisering er omfattet av vilkåret «monitorering»:[152] En app-utvikler fra Canada overvåker atferden til sine europeiske kunder. Formålet med app-utviklerens overvåkning er å optimalisere og vedlikeholde appen – altså ikke profilering. Personvernrådet legger til grunn at overvåkningen faller innenfor GDPR artikkel 3 andre ledd bokstav (b).

I motsetning til Personvernrådet mener Adèle Azzi og CIPL at klassifisering ved hjelp av informasjonskapsler bør falle utenfor vilkåret «monitorering» i GDPR artikkel 3 andre ledd bokstav (b).[153] Selv om rettstilstanden framstår som klar, er problemstillingen aktuell. Dette har særlig sammenheng med vår økende internettbruk og den stadige økende bruken av informasjonskapsler.

---

[150] CIPL (2019) s. 15.
[151] Guidelines 3/2018 s. 20.
[152] Eksempel nr. 18 i Guidelines 3/2018 s. 20.
[153] Azzi (2018) s. 130 og CIPL (2019) s. 15.

Azzi begrunner ikke sin påstand, utover å vise til Artikkel 29-gruppens gjennomgang av hva klassifisering er.[154] CIPL er på sin side kritisk til Personvernrådets angivelige overfladiske behandling av problemstillingen. Herunder er de kritiske til at Personvernrådet har lagt til grunn at enhver formålsrettet overvåkning er omfattet av vilkåret.[155] Ifølge CIPL bør «[…] tracking that is limited to aggregated analytical purposes with "no intention to target", such as analysing the frequency and use of different sections of a web page […]» falle utenfor vilkåret «monitorering».[156]

Slik jeg forstår Azzi og CIPL, er de av den oppfatning at visse former for atferdsovervåkning er såpass lite inngripende, at det ikke er grunn til å anvende GDPR. Videre er de kritiske til at Personvernrådet ikke har tatt høyde for overvåkningens kompleksitet.

Jeg er enig med CIPL i at Personvernrådet sin gjennomgang av problemstillingen er for kortfattet og lite inngående; det er tross alt snakk om svært komplekse saksforhold. Problemstillingen burde, både på grunn av sin kompleksitet og aktualitet, blitt nærmere drøftet.

Videre er jeg enig med CIPL og Azzi i at klassifisering er viktig for at virksomheter skal kunne utvikle seg, og skape gode brukeropplevelser for den registrerte. Dessuten er jeg enig i at klassifisering normalt ikke utgjør et nevneverdig inngrep i den personlige sfære. Likevel er jeg uenig med Azzi og CIPL i at klassifisering bør falle utenfor vilkåret «monitorering». Slik jeg ser det er det avgjørende at klassifisering potensielt kan utgjøre et inngrep i den registrertes personvern og private sfære, hvilket vil være i strid med formålet med GDPR.[157] For eksempel vil det være vanskelig for den registrerte å vite med sikkerhet at personopplysningene ikke skal brukes til annet enn å klassifisere.[158] Det kan også tenkes at personopplysningene blir samlet inn med formål om å klassifisere, men at opplysningene lagres etter at de har blitt klassifisert. Dessuten kan det argumenteres for at en slik tolkning – hvor klassifisering er omfattet av vilkåret «monitorering» – bidrar til at regelverket blir enklere å forholde seg til. Herunder er

[154] Azzi (2018) s. 130 med henvisning til WP251rev.01 s. 7.
[155] Personvernrådets uttalelse om at «Online tracking through the use of cookies or other tracking techniques such as fingerprinting» alltid er omfattet av vilkåret "monitorering", se footnote 151.
[156] CIPL (2019) s. 15.
[157] Article 29 Data Protection Working Party. WP 203. *Opinion 3/2013 on purpose limitation*, s. 35. For prinsippet om formålstjenlig tolkning, se fotnote 120.
[158] WP251rev.01 s. 5.

det nærliggende å anta at del vil være utfordrende å vurdere overvåkningens formål. Et enklere regelverk gir større forutberegnelighet både for de registrerte og for virksomheter.

Etter min mening er det derfor ikke adgang til å la virksomheter i tredjestater klassifisere personer i EØS-området, uten at de samtidig må forholde seg til GDPR.

3.4.7 Må monitoreringen være kontinuerlig?

I følge CIPL er det uklart om *kontinuerlig atferdsovervåkning* er en forutsetning for at GDPR artikkel 3 andre ledd (b) skal komme til anvendelse. CIPL formulerer problemstillingen slik: Må overvåkningen ha foregått «over a certain period of time» for at GDPR skal komme til anvendelse?[159]

Problemstillingen er, ifølge CIPL, særlig aktuell for virksomheter i tredjestater som benytter seg av konsulentselskaper.[160]

> For å illustrere problemstillingen, har CIPL konstruert et eksempel:[161] Et chilensk morselskap mistenker at sitt franske datterselskap begår økonomisk kriminalitet. Morselskapet ønsker derfor å granske datterselskapet. Morselskapet engasjerer et konsulentselskap. Konsulentselskapet får tilsendt kopi av PC-innholdet til de ansatte i det franske datterselskapet, og får i oppgave å analysere de digitale bevisene. Konsulentselskapet analyserer *kopier* av de registrerte sin atferd på PC-ene. Det er ikke tale om kontinuerlig atferdsovervåkning, og CIPL legger derfor til grunn at det ikke tale om «monitorering» i GDPRs forstand.

Jeg er ikke enig med CIPL i at kontinuerlig overvåkning er et krav. Etter min mening åpner ordlyden «monitorering» for at også sporadisk og unntaksvis atferdsovervåkning kan omfattes av vilkåret.[162] Etter min mening har en utvidende tolkning også støtte i hensynet til den registrerte. Sporadisk og unntaksvis atferdsovervåkning utgjør – i likhet med kontinuerlig overvåkning – et inngrep i den private sfære. Motsatt er det, slik jeg ser det, ikke grunn til at virksomhetene skal ha en særlig adgang til å sporadisk og unntaksvis monitorere registrerte, uten at de samtidig må forholde seg til GDPR. Dessuten vil en tolkning i samsvar med CIPLs

[159] CIPL (2019) s. 14–15.
[160] Ibid.
[161] Eksempelet er hentet fra CIPL (2019) s. 15.
[162] En slik forståelse er i samsvar med «[...] the principle that the provisions […] which constitutes one of the foundations of the Union, must be construed broadly», jf. *Depesme og Kerrou,* C-401/15 og 403/15.

konklusjon føre til at et vidt spekter av overvåkningstilfeller faller utenfor GDPR; en konsekvens som er stikk i strid med formålet om å verne personopplysninger.[163] Dersom det var lovgiver sin vilje å innskrenke personvernet, burde dette blitt tydelig kommunisert. Motsatt, når en slik intensjon ikke er uttrykkelig formidlet, må tausheten tolkes slik at EUs lovgivende organer ikke har forespeilet å gi bestemmelsen et snevrere virkeområde enn hva som følger av ordlyden.

Etter min mening er det derfor ikke adgang til å tolke vilkåret «monitorering» slik at kontinuerlig overvåkning skal være et absolutt krav.

[163] GDPR art. 1 (2), fortalepunkt 1 og 7, og dessuten prinsippet om at regelen skal aktualisere det overordnede formålet, jf. *Air France*, C-402/07 og C-432/07, avsnitt 47.

4 Avsluttende refleksjoner

I denne oppgaven har jeg forsøkt å svare på *når* virksomheter i tredjestater må behandle personopplysninger i overenstemmelse med GDPR. Gjennomgangen viser at virksomheter i tredjestater må behandle personopplysninger i overenstemmelse med GDPR når de har en tilstrekkelig tilknytning til EØS-området. En sentral del av vurderingen er om virksomheten har hatt hensikt om å ramme personer i EØS-området.

Etter min mening er denne vurderingen – i det store og hele – godt egnet til å gi rimelige og formålstjenlige resultater. Dersom en virksomhet har hatt hensikt om å ramme personer i EØS-området, vil det normalt være rimelig å kreve at virksomheten behandler personopplysningene i medhold av GDPR. Dessuten er hensiktskravet egnet til å gi virksomhetene økt forutberegnelighet; majoriteten av virksomheter vet hvilke personer de har hatt hensikt om å ramme. Likevel mener jeg at hensiktskravet, i visse tilfeller, ikke garanterer for rimelige resultater. Dette ble illustrert i gjennomgangen av forholdet mellom en virksomhets intensjon og det faktiske utfall. Det er også betimelig å stille spørsmål til om det er rimelig å kreve at klassifisering – som tross alt ikke utgjør et nevneverdig inngrep i den private sfære – må gjøres i overenstemmelse med GDPR.

Den foregående analysen av GDPR artikkel 3 andre ledd viser av ordlyden er vidt utformet. Selv om en vidt utformet ordlyd åpner for at det kan foretas konkrete og fleksible vurderingen, fører det også til at bestemmelsen framstår som uklar. Dette er, slik jeg ser det, en åpenbar utfordring knyttet til GDPR artikkel 3 andre ledd.

Blant annet er det grunn til å anta at mange virksomheter – særlig de med få ressurser – kan oppleve det som utfordrende å forholde seg til regelverket. Herunder er det nærliggende å anta at uklarhetene øker risikoen for at virksomheter opptrer i strid med forordningen, eksempelvis fordi de ikke vet om GDPR gjelder for den aktuelle behandlingen eller ikke. Dette er uheldig, særlig sett i lys av de store økonomiske konsekvensene feil-behandling kan få for virksomhetene. For enkelte virksomheter – typisk de med færrest ressurser – kan risikoen oppleves som såpass stor at de ikke lenger ønsker å ta del i det europeiske markedet. Dersom dette skjer, kan utvalget av næringsaktører bli mindre, og virksomheters deling av tanker, ytringer og kunnskap vil kunne skjer i mindre utstrekning enn tidligere. En forsmak på dette

fikk vi da amerikanske medieselskaper stengte sine hjemmesider i forbindelse med at GDPR trådte i kraft. Et slikt scenario er uheldig for virksomhetene, de registrerte og for samfunnet som sådan.

Etter min mening kan den vide ordlyden også slå uheldig ut for den registrerte. Selv om Personvernrådet sine retningslinjer er gode, er det grunn til å anta at majoriteten av de registrerte ikke leser denne. Derfor er det desto viktigere at de registrerte kan støtte seg til forordningens ordlyd. Den vidt utformede ordlyden kan føre til at den registrerte opplever det som utfordrende å vite hvilke rettigheter og krav han har. Dersom de registrerte opplever å ikke ha kontroll over sine personopplysninger, vil tilliten til virksomheter og myndigheter kunne blir svekket. Sett i lys av den fundamentale verdien personopplysninger har, er dette uheldig.

Den vide ordlyden og de store økonomiske sanksjonene kan bidra til at enkelte virksomheter opplever det europeiske markedet som ugunstig og risikabelt. Derfor er det, slik jeg ser det, behov for ytterligere klargjøring av bestemmelsen. Slik jeg ser det, er det et særlig behov for ytterligere klargjøring i spørsmål som har en særlig teknisk karakter, for eksempel spørsmål knyttet til klassifisering og IT-tjenester.

Jevnt over er jeg likevel av den oppfatning at GDPR artikkel 3 andre ledd er godt egnet til å ivareta hensynet til de registrertes personvern og til de aktuelle virksomhetene. Bestemmelsen sørger for at majoriteten av de som er i befatning med EØS-borgere sine personopplysninger må forholde seg til GDPR, samtidig som at virksomhetene har en relativt god visshet om de må forholde seg til regelverket eller ikke.

5 Kildehenvisning

Internasjonale traktater og konvensjoner

EMK	Convention for the Protection of Human Rights and Fundamental Freedoms, Roma, 4. november 1950 [Den europeiske menneskerettskonvensjonen].
EØS-avtalen	Agreement on the European Economic Area, 2. May 1992.
TEUV	Consolidated version of the Treaty on the Functioning of the European Union – TFEU, Roma, konsolidert 7. July 2016, OJ C 202 [Traktaten om Den europeiske unions virkemåte – TEUV] (Roma-traktaten)

EU-rettslige direktiv og forordninger

Direktiv 95/46/EF	Europaparlamentet og Rådets direktiv 95/46/EF av 24. oktober 1995 om beskyttelse av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger [OPPHEVET].
Council Regulation (EC) No 44/2001	Council Regulation (EC) No 44/2001 of 22 December 2000 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters [OPPHEVET].
Directive (EU) 2015/1535	Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services.

Forordning (EU) 2016/679	Europaparlaments- og Rådsforordning (EU) 2016/679 av 27. april 2016 om vern av fysiske personer i forbindelse med behandling av personopplysninger og om fri utveksling av slike opplysninger samt om oppheving av direktiv 95/46/EF (generell personvernforordning) [GDPR].
Directive (EU) 2019/770	Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services.

Norske autoritative kilder

Norsk lovgivning

Grunnloven	Lov 17. mai 1814 om Kongeriket Norges Grunnlov (Grunnloven).
EØS-loven	Lov 27. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v. (EØS-loven).
Personopplysnings-loven av 2000	Lov 14. april 2000 nr. 31 om behandling av personopplysninger (opphevet ved lov 15 juni 2018 nr. 38) [OPPHEVET].
Helseregisterloven	Lov 20. juni 2014 nr. 43 om helseregistre og behandling av helseopplysninger (helseregisterloven), samt regler om taushetsplikt.
Personopplysnings-loven	Lov 15. juni 2018 nr. 38 om behandling av personopplysninger (personopplysningsloven).

Norske forskrifter

Forskrift 15. mai 2013 nr. 484 om lagringsplikt for bestemte data og om tilrettelegging av disse data (datalagringsforskriften).

Forskrift 2. juli 2018 nr. 1107 om kameraovervåkning i virksomhet.

Norske forarbeider

NOU 2009: 1 Individ og integritet. Personvern i det digitale samfunnet.

Prop. 56 LS (2017-2018) Om lov om behandling av personopplysninger (personopplysningsloven) og samtykke til deltakelse i en beslutning i EØS-komiteen om innlemmelse av forordning (EU) nr. 2016/679 (generell personvernforordning) i EØS-avtalen.

Rettspraksis

Praksis fra EU-domstolen

Wirth	Dom av 9. desember 1993, *Wirth*, C-109/92, ECLI:EU:C:1993:916.
Air France	Forente dommer av 19. november 2009, *Air France*, C-402/07 og C-432/07, ECLI:EU:C:2009:716.
Pammer- og Alpenhof	Forente dommer av 7. desember 2010, *Pammer- og Alpenhof*, C-585/08 og C-144/09, ECLI:EU:C:2010:740.
L´Oréal v eBay	Dom av 12. juli 2011, *L´Oréal v eBay*, C-324/09, ECLI:EU:C:2011:474.
Google Spain	Dom av 13. mai 2014, *Google Spain*, C-131/12, ECLI:EU:C:2014:317.

Karen Millen Fashions	Dom av 19. juni 2014, *Karen Millen Fashions*, C-345/13, ECLI:EU:C:2014:2013.
Deckmyn	Dom av 3. september 2014, *Deckmyn*, C-201/13, ECLI:EU:C:2014:2132.
Weltimmo	Dom av 1. oktober 2015, *Weltimmo*, C-230/14, ECLI:EU:C:2015:639.
Depesme og Kerrou	Forente dommer av 15. desember 2016, *Depesme og Kerrou,* C-401/15 og 403/15, ECLI:EU:2016:955.
J.D.	Dom av 2. mars 2017, *J.D*, C-4/16, ECLI:EU:C:2017:153.

Opinion of Advocate General

Opinion of Advocate General V. Trstenjak delivered on 18 May 2010 in joined cases C-585/08 og C-144/09, *Pammer og Alpenhof*, ECLI:EU:C:2010:273.

Annen praksis

Den Europeiske Menneskerettighetsdomstolen, Sak nr. 59320/00, *Caroline von Hannover*, 24. juni 2007.

Polsk Supreme Administrative Court, I OSK 2445/12, *Google Street View*, 21. februar 2014.

Praksis fra Personvernsnemda, PVN-2017-18, *Nobina Norge AS*, 20. mars 2018

Veiledere og rapporter

Personvernrådet og Artikkel 29-Gruppen

WP 56	Article 29 Data Protection Working Party. 5035/01/EN/Final WP 56. Working document on determining the international application of EU data protection law to personal data processing in the Internet by non-EU based web sites.
Europakommisjonens håndbok (2010)	Europakommisjonens handbook (2010) "*Free movement of goods. Guide to the application of Treaty provisions governing the free movement of goods*". Luxembourg: Publications Office of the European Union.
WP 169	Article 29 Data Protection Working Party. WP 169. Opinion 1/2010 on the concepts of "controller" and "processor".
WP 179	Article 29 Data Protection Working Party. WP 179. *Opinion 8/2010*.
WP 203	Article 29 Data Protection Working Party. WP 203. Opinion 3/2013 on purpose limitation.
WP251rev.01	Article 29 Data Protection Working Party. WP 251 rev.01. *Guidelines on Automated individual decision-making and Profiling for the purpose of Regulation 2016/679*. Revised and Adopted on 6 February 2018.
Guidelines 3/2018	European Data Protection Board. *Guidelines 3/2018 on the territorial scope of the GDPR (Article 3*) – Version 2.0. 12. november 2019.

Rapporter fra Datatilsynet

Datatilsynet (2015) *Det Store Datakappløpet. Rapport om hvordan kommersiell bruk av personopplysninger utfordrer personvernet*.

Datatilsynet (2018) *Hva vet de om deg? Bruk av innsynsretten hos fire virksomheter*.

Juridisk litteratur

Bøker

Dall mfl. (2016)	Dall, Nis Peter mfl. (2016). *Persondataforordningen - en håndbog for praktikere.* Ex Tuto Publishing: København.
Fredriksen mfl. (2018)	Fredriksen, Halvard Haukeland og Mathisen, Gjermund (2018). *EØS-rett*. 3. utgave. Fagbokforlaget: Bergen.
Svantesson (2013)	Svantesson, Dan Jerker K. (2013). *Extraterritoriality in Data Privacy Law.* Ex Tuto Publishing: København.
Schartum (2016)	Schartum, Dag Wiese (2016). *Personvern i informasjonssamfunnet. En innføring i vern av personopplysninger.* 3. utgave. Fagbokforlaget: Bergen.

Artikler

Azzi (2018)	Azzi, Adèle (2018), *The challenges Faced by the extraterritorial scope of the general data protection regulation*, Jipitec, s. 126-137.
Cate mfl. (2014)	Cate, Fred H., Kuner, Christopher, Millard, Christopher, and Svantesson Dan Jerker B. (2014) «*The (data privacy) law hasn't even checked in when technology takes off»* . International Data Privacy Law, Vol. 4, No. 3 side 175-176.

CIPL (2019) Comments by Centre for Information Policy Leadership (2019). *On the European Data Protection Board´s «Draft Guidelines 3/2018 on the territorial scope of the GDPR (Article 3)»*.

Czerniawski (2017) Czerniawski, Michal (2017). *Do We Need the 'Use of Equipment' as a Factor for the Territorial Applicability of the EU Data Protection Regime?* Cambridge, Antwerp and Portland. pp. 221-240.

de Hert mfl. (2016) de Hert, Paul and Czerniawski, Michal (2016). *Expanding the European data protection scope beyond territory: Article 3 of the General Data Protection Regulation in its wider context.* International Data Privacy Law, Vol. 6, No. 3. s. 230-243.

Korff (2019) Korff, Douwe (2019). *The territorial (and extra-territorial) application of the GDPR With Particular Attention to Groups of Companies Including Non-EU Companies and to Companies and Groups of Companies That Offer Software-as-a-Service*.

Kuner mfl. (2012) Kuner, Christopher, Cate, Fred H., Millard, Christopher, and Svantesson, Dan Jerker B. (2012). *The challenge of 'big data' for data protection*. International Data Privacy Law, 2012, Vol. 2, No. 2. side 47-49

Svantesson (2015) Svantesson, Dan Jerker B (2015). *Extraterritoriality and targeting in EU data privacy law: the weak spot undermining the regulation.* International Data Privacy Law, Vol. 5, No. 4. side 226-234.

Svantesson (2011) Svantesson, Dan Jerker B. (2011) *Pammer and Hotel Alpenhof - ECJ decision creates further uncertainty about when e-businesses "direct activities" to a consumer's state under the Brussels i Regulation*. Computer Law and Security Review, 27(3), 298-304.

Nettsider

https://www.bbc.com/news/world-europe-44248448 (lastet ned 6. desember 2019).

https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election (lastet ned 26. november 2019).

https://www.nrk.no/norge/slike-bilder-sender-bomselskap-til-kina_-na-gar-datatilsynet-inn-i-saken-1.14754918 (lastet ned 31. oktober 2019).