UiO : Det juridiske fakultet

Data protection by design and by default

Behandlingsansvarliges ansvar etter EUs personvernforordning artikkel 25

Kandidatnummer: 712

Leveringsfrist: 25.4.2017

Antall ord: 15 527

Innholdsfortegnelse

1 Innledning

1.1 Tema, bakgrunn og problemstilling

Den 25. mai 2018 trer EUs nye personvernforordning[1] i kraft og den erstatter med det personverndirektivet fra 1995[2]. Forordningen viderefører store deler av direktivet, men det innføres også flere nye regler. Blant disse er plikten til «data protection by design and by default» som er temaet for denne avhandlingen.

Temaet for avhandlingen er EUs nye personvernforordning artikkel 25 om «*data protection by design and by default*». Hovedformålet med avhandlingen er å gjennomføre en rettsdogmatisk analyse av artikkel 25, med særlig fokus på hvilke krav som stilles til den behandlingsansvarlige.

Artikkel 25 bygger på konseptet innebygd personvern, som går ut på at man skal ta hensyn til personvern i alle ledd av en utviklingsprosess. Det har derfor vært naturlig å også inkludere utviklingen av dette konseptet som en del av avhandlingen.

1.2 Presiseringer og avgrensninger

Avhandlingens hovedfokus vil ligge på å redegjøre for hvilke krav som stilles til den behandlingsansvarlige etter artikkel 25, ettersom det primært er den behandlingsansvarlige som er forpliktet etter denne bestemmelsen. Jeg vil også forsøke å redegjøre for hvilke andre aktører som omfattes av bestemmelsen, men det vil gå utover oppgavens rammer å gå særlig i dybden på dette punktet.

Ettersom avhandlingens tema er en bestemmelse i en EU-forordning, tar jeg utgangspunkt i EU-rettslig metodelære og tolkningsprinsipper. Jeg kommer ikke til å trekke inn norsk personvernrett eller bestemmelsens mulige anvendelse i Norge. De EU-rettslige vurderingene vil likevel være relevante for norsk rett fordi Norge etter EØS-avtalen vil komme til å være forpliktet til å implementere personvernforordningen ettersom denne er EØS-relevant, jf. EØS-loven § 1[3].

---

1 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

2 DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

3 Lov av 29. november 1992 nr. 109 om gjennomføring i norsk rett av hoveddelen i avtale om Det europeiske økonomiske samarbeidsområde (EØS) m.v.

1.3 Rettskildebildet

Siden temaet for avhandlingen baserer seg på en bestemmelse i en EU-forordning som ikke ennå er trådt i kraft, knytter det seg noen særskilte problemstillinger til rettskildebildet. Det har vært en utfordring å finne gode rettskilder under arbeidet med denne avhandlingen. Dette skyldes i hovedsak at bestemmelsen ennå ikke har trådt i kraft, og det er grunn til å regne med at rettskildebildet vil endre seg mye i årene som kommer.

Videre må besvarelsen som nevnt bygge på en EU-rettslig rettskildelære, noe som vil ha betydning for hvilke rettskilder som er relevante, hva slags vekt de har og hvilke slutninger som er skjønnsomme å trekke fra dem.

1.3.1 Bestemmelsens ordlyd

Avhandlingens primære rettskilde er bestemmelsens ordlyd. Tolkning og analyse av en EU-rettslig bestemmelse må basere seg på EU-rettslige tolkningsprinsipper. For det første må det tas hensyn til at bestemmelsen er vedtatt på 24 forskjellige språk og at disse naturlig nok vil ha visse variasjoner seg i mellom. Hovedregelen er at alle versjonene har lik vekt. Dette gjør at man i mindre grad legger vekt på den eksakte ordlyden ved å drive fintolkning av formuleringer, slik at man heller må søke å finne meningen med bestemmelsen.[4] Ved tolkning må de ulike språklige versjonene sammenlignes. Dette ble fastslått av EU-domstolen i blant annet CILFIT-saken[5] hvor retten uttalte at *«[d]et skal først og fremmest tages hensyn til den omstændighed, at de EF-retlige bestemmelser er affattet på flere forskellige sprog, og at alle sproglige versioner er autentiske. Fortolkningen av en EF-retlig bestemmelse kan derfor først ske efter en sammenligning af de sprogelige versioner.»* [6]

Avhandlingen kommer til å ta utgangspunkt i den engelske versjonen av bestemmelsen, fordi denne versjonen var arbeidsversjonen ved utarbeidelsen av forordningen og de andre versjonene er oversatt fra denne versjonen. Det er også denne versjonen det meste av kildematerialet baserer seg på.

Det har ikke foreligget noen norsk oversettelse av forordningen under arbeidet med denne avhandlingen. Av hensyn til å få best mulig flyt i teksten, har jeg derfor valgt å oversette enkelte elementer av bestemmelsen selv. I de fleste tilfeller har dette vært snakk om begreper hvor oversettelsen nærmest er gitt (e.g. *organisational* til *organisatorisk*). For de begrepene

---

4 Sejersted m.fl. (2011) s. 45

5 Case C-283/81 – Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health, judgment of 6 October 1982

6 C-283/81 CILFIT, premiss 18

hvor dette ikke er tilfellet, vil jeg legge meg tett opp mot den danskspråklige versjonen, fordi dansk er det EU-språket som er mest likt norsk.

For det annet er EU-rett gjenstand for autonom tolkning, som innebærer at man ikke kan legge til grunn at ord og uttrykk har samme innhold i EU-rettslig sammenheng som det man kjenner fra før. I CILFIT-saken ble dette formulert slik: «*Det bemærkes dernæst, at der i EF-retten – selv om de sproglige versioner er nøje overenstemmende – anvendes en særlig sprogbruk. Det skal i øverigt understreges, at indholdet af de retlige begreper ikke nødvendigvis er det samme som i de nationale retsordner*.»[7]

For det tredje innebærer EU-rettens dynamiske karakter at betydningen av bestemmelsen er i kontinuerlig utvikling og at tolkningen av bestemmelsen må reflektere dette. Dette fremgår av CILFIT-saken avsnitt 20: «*Endelig skal de enkelte EF-regler vurderes i deres rette sammenhæng og fortolkes i lyset af EF-rettens bestemmelser som helhed, den bagved liggende målsætning og EF-rettens udviklingstrin på tidspunktet for de pågældende bestemmelsers anvendelse.»* I prinsippet er dette en mindre relevant problemstilling for denne avhandlingen fordi forordningen er ny. Et helt uinteressant poeng er det likevel ikke, all den tid avhandlingen tar for seg en bestemmelse som regulerer utformingen av teknologi og teknologien er i rask endring.

1.3.2 Forarbeider

Den rettskildemessige betydningen av forarbeider i EU-retten skiller seg en del fra det vi er vant med etter norsk rett. Bakgrunnen for dette er at EU som rettssystem bygger på en lovgivningstradisjon som i langt mindre grad baserer seg på forarbeider som rettskilde.[8] Dette er noe av grunnen til at bestemmelsene i EUs lovverk er langt mer ordrike enn hva vi er vant med.

Videre er selve lovgivningsprosessen av betydning for forarbeidenes vekt; lovgivning blir til gjennom en forhandlingsprosess mellom medlemsstatene hvor den endelige lovteksten ofte må ses på som et kompromiss, slik at forarbeidene blir av mindre betydning.[9] Dette gjør at forarbeider i EU-retten vil ha mindre vekt enn i norsk rett.

Personvernforordningen har vært utsatt for intens lobbyvirksomhet under lovgivningsarbeidet.[10] Lobbyvirksomheten svekker vekten av forarbeidene ytterligere, både fordi det forsterker forordningens karakter av å være et kompromiss slik at uttalelser i forarbeidene ikke er repre-

---

7 C-283/81 CILFIT, premiss 19

8 Sejersted m.fl. (2011) s. 57

9 Sejersted m.fl. (2011) s. 57

10 https://www.digi.no/artikler/hardt-skyts-mot-skjerpet-personvern/204197

sentative for den endelige lovteksten og fordi den endelige lovteksten på flere punkter faktisk er forskjellig fra de første utkastene fra Kommisjonen og Europaparlamentet. Dette vil det komme eksempler på i det følgende.

1.3.3 Rettspraksis

1.3.3.1 EU-domstolen

Generelt er praksis fra EU-domstolen en rettskilde av tung vekt. På nåværende tidspunkt finnes det ikke rettspraksis som baserer seg på artikkel 25, i og med at forordningen ennå ikke har trådt i kraft, men slik rettspraksis vil komme til å bli en svært viktig kilde ved tolkning av bestemmelsen i fremtiden.

Jeg vil trekke inn noen avgjørelser fra EU-domstolen som er avsagt etter andre bestemmelser. Disse avgjørelsene er ikke direkte relevant for tolkningen av artikkel 25, men de illustrerer hvordan domstolen også tidligere har stilt krav til tekniske løsninger for sikring av personvernet. Jeg kommer nærmere tilbake til dette under punkt 3.2.3.

1.3.3.2 Den europeiske menneskerettsdomstolen

EU-domstolen har slått fast at Den europeiske menneskerettskonvensjonen (heretter forkortet EMK) har «*special significance*» innen EU-retten.[11] Praksis fra Den europeiske menneskerettsdomstolen (heretter forkortet EMD) vil dermed kunne være nyttig ved tolkningen av bestemmelsen og som bakgrunnsstoff. Det er likevel grunn til å være oppmerksom på at EU-domstolen ikke anser seg bundet av avgjørelser i EMD.[12]

Selv om det ikke fremgår noe prinsipp om innebygd personvern av EMK, har EMD likevel bygget på en tankegang som kan minne om dette i noen avgjørelser, blant annet i avgjørelsen I. v. Finland. Jeg kommer nærmere tilbake til dette under punkt 3.2.3.

1.3.4 Forvaltningspraksis og annen praksis

Forvaltningspraksis har i utgangspunktet ikke veldig tung vekt i EU-retten.[13] På personvernrettens område er forvaltningspraksis likevel viktig, delvis fordi forvaltningen har mulighet til å reagere kjapt på ny teknologi og derfor kan ta stilling til og veilede på nye områder hvor rettspraksis og lovgivning ikke ennå har tatt stilling.

En viktig type forvaltningspraksis er uttalelser fra The Working Party on the Protection of Individuals with regard to the Processing of Personal Data (heretter Artikkel 29-gruppen).

---

11 Opinion 2/13 avsnitt 37. Se også TFEU artikkel 6 annet ledd.

12 Se Opinion 2/13 avsnitt 183 flg.

13 Sejersted m.fl. (2011) s. 57

Artikkel 29-gruppen er et rådgivende ekspertorgan opprettet med hjemmel i personverndirektivet artikkel 29. Gruppen har uavhengig status og består av representanter fra medlemslandenes tilsynsmyndigheter, European Data Protection Supervisor (EDPS) og EU-Kommisjonen. De avgir rådgivende uttalelser om personvernrettslige spørsmål og har avgitt viktige uttalelser i forbindelse med utarbeidelsen av forordningen. Uttalelsene er ikke bindende, men de vil i praksis ha stor vekt ved tolkning av forordningen.

Ved ikrafttredelsen av forordningen vil gruppen bli erstattet av et European Data Protection Board (EDPB), jf. forordningen artikkel 68. Dette organet vil i tillegg til å opptre som rådgivende organ for Kommisjonen, også kunne avgi bindende uttalelser som de nasjonale tilsynsmyndighetene må rette seg etter.[14]

Det er altså grunn til å regne med at forvaltningspraksis vil bli en viktig rettskilde ved tolkning av bestemmelsen i tiden etter ikrafttredelsen. Særlig vil uttalelser og retningslinjer fra European Data Protection Board komme til å spille en viktig rolle. Det er også grunn til å tro at retningslinjer utviklet av bransjene selv («codes of conduct») vil få stor praktisk betydning, dette kommer jeg tilbake til under punkt 5. Det er imidlertid lite å hente her på nåværende tidspunkt.

1.3.5 Juridisk teori

Juridisk teori som rettskilde har formelt liten vekt i EU-retten. For denne avhandlingen har teorien likevel vært praktisk viktig fordi den har vært en kilde til bakgrunnsstoff. Det er skrevet en del om bestemmelsen både før og etter vedtakelsen av forordningen. En svakhet ved noen av disse artiklene er de i hovedsak har handlet om konseptet innebygd personvern generelt, og bare i mindre grad om artikkel 25. Dette gjelder for eksempel Schartum[15] og Krebs[16]. En annen svakhet er at det bare Bygrave som har skrevet om bestemmelsen i sin endelige form.[17]

1.3.6 Fortale og formålsbetraktninger

Formålsbetraktninger er generelt en svært viktig rettskilde i EU-retten. Dette har sammenheng med at man ved tolkningen av en bestemmelse ikke kan legge vekt på den nøyaktige ordlyden, men må se hen til meningen bak bestemmelsen, se punkt 1.3.1. Formålsbetraktninger kan være både lovfestet og ulovfestet. EU-retten har en rekke grunnleggende formål som ofte vil

---

14 Se artikkel 65

15 Schartum (2016)

16 Krebs (2013)

17 Bygrave (2017)

være sentrale ved lovtolkning, for eksempel integrasjonshensynet. Disse formålene har vært mindre sentrale ved fortolkningen av artikkel 25.

For å finne frem til formålene for de ulike bestemmelsene er forordningens fortale («preamble») en helt sentral kilde, fordi det er den kilden som gir best uttrykk for lovgivers hensikt med bestemmelsene, i mangel på autoritative forarbeider.[18] Personvernforordningen har en omfattende fortaletekst på 173 avsnitt. For denne avhandlingen har fortalen vært spesielt viktig fordi forordningen er ny og fordi det er mangel på rettskilder. Fortalen vil derfor ofte henvises til som kilde i det følgende.

1.4 Terminologi

I personvernretten benyttes det noen begreper som det er nødvendig å redegjøre litt nærmere for innholdet av. Begrepene «privacy by design», «data protection by design» og «innebygd personvern» er helt sentrale i denne oppgaven. Forholdet mellom dem vil redegjøres for nedenfor, men først vil jeg ta for meg forholdet mellom «privacy» og «data protection», fordi det er greit å ha klart for seg hva som skiller disse fra hverandre som bakgrunn for skillet mellom de andre begrepene.

1.4.1 Privacy og data protection

Begrepene «privacy» og «data protection» er overlappende, men ikke identiske begreper. I dagliglivet brukes de ofte om hverandre uten at dette er problematisk, men det kan være hensiktsmessig å gjøre nærmere rede for distinksjonene mellom dem for å forstå skillet mellom «privacy by design» og «data protection by design».

Til begrepet «*privacy*» knyttes det tradisjonelt konsepter som bygger på tanken om en sfære hvor individet kan være fri fra andres uønskede innblanding, ofte omtalt som «the right to be let alone».[19] I kjernen av begrepet ligger individets mulighet til informasjonskontroll, hvor individet selv kan velge om og eventuelt hva det ønsker å dele. Begrepet er ikke begrenset til å gjelde personopplysninger, men omfatter alle sider av det som kan omtales som privatlivet, inkludert de fysiske, kroppslige og psykiske aspektene.[20]

Begrepet «*data protection*» har røtter i den europeiske personvernlovgivningen og har mindre fokus på individets selvbestemmelsesrett enn hva «privacy»-begrepet har. Bygrave formulerer det som at «data protection» ofte benyttes om «*a set of norms that serve a broader range of*

[18] Sejersted m. fl. (2011) s. 57

[19] Bygrave (2014) s. 24

[20] Bygrave (2014) s. 3

interests than simply privacy protection».[21] Fokuset ligger på at behandling av personopplysninger skal skje med grunnlag i personvernprinsippene, slik som prinsippene om innsamling av minst mulig personopplysninger, formålsbegrensning og relevans. Begrepet har også sterk tilknytning til informasjonssikkerhet, fordi sistnevnte er knyttet til beskyttelse av tilgang, integritet og konfidensialitet. Informasjonssikkerhet er likevel noe annet enn «*data protection*» fordi «*data protection*» bare angår personopplysninger, mens informasjonssikkerhet knytter seg til alle typer data.[22]

1.4.2 «Data protection by design» og «Privacy by design»

I likhet med begrepene redegjort for ovenfor har også begrepene «data protection by design» og «privacy by design» i stor grad overlappende innhold. De har delvis blitt brukt om hverandre i arbeidet med utviklingen av forordningen; Kommisjonen brukte i utgangspunktet betegnelsen «*privacy by design*»,[23] men i det første utkastet til ny forordning gikk de over til betegnelsen «*data protection by design*».[24] Det ble ikke gitt noen kommentar til endringen og det har derfor ikke vært helt klart i hvilken grad Kommisjonen har ment å tillegge begrepene ulikt innhold. I en rapport fra PRIPARE-prosjektet[25] ble det spekulert i om noe av grunnen kanskje kan ligge i skillet mellom «*right to privacy*» og «*right to data protection*» i EUs Charter for grunnleggende rettigheter.[26] Det gir for så vidt mening å basere seg på et slikt skille, ettersom retten til privatliv etter Charteret omfatter noe mer og annet enn retten til beskyttelse av personopplysninger. En kan anta at det var dette skille Kommisjonen ønsket å få frem.

Bygrave har kommentert at begrepene i praksis ofte benyttes om hverandre uten at det er ment at det skal forstås som at det er en betydningsfull forskjell[27], men at rekkevidden av begrepene antagelig er noe ulik og at de derfor ikke bør benyttes som synonymer. Han henviser til at Cavoukian[28] mener at «privacy by design» utgjør noe mer enn bare juridiske normer, men han er kritisk til om det stemmer at PbD egentlig er et videre begrep enn DPbD. Han peker blant annet på rettigheter den registrerte har som del av europeisk personvernrett som vedkommende ikke har etter «privacy by design», som tilsier at «data protection by design» på visse om-

---

21 Bygrave (2014) s. 26

22 Bygrave (2014) s. 2

23 COM(2010) 609 final

24 COM/2012/011 final

25 PRIPARE-prosjektet er et personvernprosjekt i regi av EU.

26 PRIPARE (2014) side 27

27 Bygrave (2017) s. 5

28 Dr. Ann Cavoukian er hjernen bak «Privacy by design», se punkt 3.

råder går lengre enn sin motpart.[29] Det er dermed et poeng i å være oppmerksom på hvilke begrep som benyttes.

I denne avhandlingen vil jeg benytte begge begrepene. Der hvor det er snakk om kravet etter forordningen til innebygd personvern, kommer jeg til å benytte «data protection by design», og der det er snakk om innebygd personvern som generelt konsept, kommer jeg til å benytte «privacy by design».

1.4.3 Innebygd personvern

På norsk benyttes begrepet «innebygd personvern» som en oversettelse av både «privacy by design» og «data protection by design». Det er ikke gitt at «innebygd personvern» omfatter det samme som disse begrepene og det er mulig at innholdet er noe litt annet. For denne avhandlingens del vil jeg primært benytte begrepet når det er snakk om innebygd personvern som konsept eller generelle prinsipper. I noen tilfeller vil det likevel bli brukt i sammenheng med kravet etter bestemmelsen for å få best mulig flyt i teksten, men da vil dette fremgå klart av sammenhengen hva som er ment.

1.5 Fremstillingen videre

I kapittel 2 vil jeg gå gjennom bakgrunnen for personvernforordningen, samt redegjøre for noen sentrale definisjoner og trekk ved den som kan ha betydning for tolkningen av artikkel 25. Kapittel 3 handler om konseptet innebygd personvern, hva det er og utviklingen gjennom de siste to tiår, med fokus på utviklingen i EU og innebygd personvern slik det har kommet til uttrykk i eldre rettspraksis. I kapittel 4 vil jeg først ta for meg noen generelle punkter i tilknytning til artikkel 25, før jeg gjennomgår bestemmelsen ledd for ledd. Kapittel 5 omhandler bransjenormer eller såkalte «*codes of conduct*» etter artikkel 40 og deres mulige betydning for artikkel 25. Kapittel 6 handler om administrative bøter ved overtredelse av artikkel 25, inkludert de generelle vilkårene for ileggelse av overtredelsesgebyr. I kapittel 7 vil jeg gå kort gjennom noen bestemmelser i forordningen som har nær tilknytning til artikkel 25. I kapittel 8 tar jeg for meg hovedpunktene i kritikk av artikkel 25, før jeg avslutter i kapittel 9.

[29] Bygrave (2017) s. 8 flg.

2 Den nye personvernforordningen

I dette kapittelet vil jeg gjennomgå bakgrunnen for personvernforordningen, noen sentrale definisjoner, samt noen grunnleggende trekk ved forordningen som kan ha betydning for tolkning og vurdering av artikkel 25.

2.1 Bakgrunn

EU vedtok den 27. april 2016 en todelt personvernreform bestående av en generell personvernforordning og et særdirektiv for politi- og straffesektoren. Vedtakelsen markerte begynnelsen på slutten for EUs gjeldende personverndirektiv 95/46/EC (heretter personverndirektivet). Regulation (EU) 2016/679 (General Data Protection Regulation, heretter forordningen) trer i kraft den 25. mai 2018 og vil erstatte det gjeldende direktivet.[30]

Arbeidet med utviklingen av forordningen har tatt lang tid. Etter flere år med forberedelser fremmet Kommisjonen et forslag til ny personvernreform den 25. januar 2012.[31] I pressemeldingen som fulgte uttaler Kommisjonen at reformen er ment å bedre individets rett til beskyttelsen av personvernet, samt å styrke Europas digitale økonomi.[32] Det pekes på at ulik praksis har utviklet seg mellom medlemslandene og at ved å velge forordning som form for det nye regelverket, vil det være mulig å oppnå en høyere grad av harmonisering gjennom en felles europeisk løsning. En ny forordning vil dessuten bedre konkurranseforholdene for multinasjonale bedrifter, samt øke tilliten til digitale tjenester i befolkningen for øvrig.

Videre pekes det på teknologisk utvikling og globalisering som to faktorer som har endret hvordan personopplysninger samles inn og brukes. Den teknologiske utviklingen som har skjedd siden personverndirektivet ble vedtatt i 1995 har vært betydelig og det er nødvendig med et nytt regelverk for å møte dagens og fremtidens utfordringer. Globalisering har skapt behov for et regelverk som reflekterer at internett er uten landegrenser og at det derfor er sterkt behov for beskyttelse av europeiske borgeres personvern.

2.2 Fra direktiv til forordning

Når forordningen trer i kraft vil den erstatte det gjeldende personverndirektivet. Siden forordningen kommer til å gjelde direkte som lov,[33] vil medlemslandenes nasjonale lovgivning som implementerer dagens direktiv også bli erstattet. Det vil derfor ikke være nødvendig å trans-

[30] Se forordningen artikkel 94

[31] COM(2012) 11

[32] IP/12/46

[33] TFEU art. 288

formere forordningen inn i nasjonale regelverk. Ettersom forordningen er EØS-relevant,[34] vil dessuten Norge og de andre EØS-landene få begrenset spillerom til å vedta egne personvernregler.

Som en konsekvens av at forordningen vil gjelde direkte som lov er den langt mer omfattende enn sin forgjenger. Den regulerer langt mer detaljert, noe som ikke bare innebærer at den har langt flere bestemmelser,[35] men at bestemmelsene jevnt over er lengre og mer utfyllende.[36] I sum innebærer dette at forordningen er mer komplisert å forholde seg til enn sin forgjenger, noe som vil stille skjerpede krav til de som skal anvende den.

2.3 Legaldefinisjoner

I personvernforordningen artikkel 4 er det definert en rekke sentrale begreper. I dette avsnittet vil jeg gjennomgå de som er viktigst for denne avhandlingen.

2.3.1 Personopplysninger

Personopplysninger («*personal data*») er definert i artikkel 4 første ledd som «*any information relating to an identified or identifiable natural person («data subject»)*». Dette innebærer at informasjon som navn, adresse, fødselsdato, telefonnummer, e-postadresse og IP-adresse er personopplysninger, i tillegg til en rekke andre typer opplysninger. Både informasjon som er direkte og informasjon som er indirekte identifiserende kan være personopplysninger. Informasjon som gjelder juridiske personer er ikke personopplysninger og juridiske personer omfattes derfor ikke av forordningen.[37] Definisjonen er i det vesentlige den samme i forordningen som i direktivet.

2.3.2 Behandling av personopplysninger

Behandling av personopplysninger («processing») er definert i artikkel 4 annet ledd som «any operation or set of operations which is performed on personal data or on sets of personal data». Behandlingen kan bestå i «collection, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction». Definisjonen er vid og det skal mye til for at en behandlingsform ikke er omfattet av den. Også denne definisjonen er i det vesentlige den samme som i direktivet.

---

[34] Forordningen er markert som EØS-relevant i Official Journal, men er ennå ikke formelt tatt inn som en del av EØS-avtalen. Se også Regjeringens EØS-notat om Personvernforordningen.

[35] Forordningen inneholder 99 artikler og 173 avsnitt i fortalen. Til sammenligning inneholder direktivet 34 artikler og 72 avsnitt i fortalen.

[36] Forordningen med fortale består av 48245 ord. Til sammenligning består direktivet med fortale av 12531 ord.

[37] Se fortalen avsnitt 14

2.3.3 Behandlingsansvarlig

Behandlingsansvarlig («*controller*») er definert i artikkel 4 syvende ledd. Den behandlingsansvarlige kan være en «*natural or legal person, public authority, agency or other body*». Det sentrale er at den behandlingsansvarlige er den som bestemmer formål(ene) for behandling av personopplysninger og hvilke hjelpemidler som skal brukes («*determines the purposes and means of the processing*»). Behandlingsansvar kan være delt mellom flere («*alone or jointly*»). Definisjonen er i det vesentlige den samme i forordningen som under direktivet.

Etter forordningen er det primært de behandlingsansvarlige som pålegges forpliktelser. Dette bygger antagelig på en forutsetning om at det er disse som er best egnet til å utøve kontroll over behandlingsprosessen. Dette har blitt kritisert, både i forhold til artikkel 25 spesielt og forordningen generelt. Jeg kommer tilbake til denne kritikken senere i oppgaven.

2.3.4 Databehandler

Databehandlere («*processors*») er etter artikkel 4 åttende ledd definert som «*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller*». Denne definisjonen er i det vesentlige den samme i forordningen som under direktivet. Det sentrale poenget er at databehandlere behandler data på vegne av den behandlingsansvarlige. Det er med andre ord den behandlingsansvarlige som skal avgjøre formål og metode, selv om behandlingen faktisk utføres av en databehandler.[38]

2.4 Geografisk virkeområde

En av de viktigste endringene i det nye personvernregelverket er utvidelsen av det geografiske virkeområdet for forordningen. Dette reguleres i forordningen artikkel 3. I første ledd slås det fast at forordningen gjelder behandling av personopplysninger hvor behandlingsansvarlig eller databehandler er etablert i EU, uavhengig av om behandlingen finner sted i EU. I annet ledd slås det fast at forordningen i tillegg gjelder behandling av personopplysninger hvor behandlingsansvarlig eller databehandler ikke er etablert i EU, men hvor behandlingen relaterer seg til tilbud av varer og tjenester til EU-borgere, eller overvåking av deres oppførsel så langt som deres atferd finner sted innenfor unionen.

Bestemmelsene i annet ledd rammer aktører som ikke er etablert i EU og tvinge dem til å forholde seg til forordningens krav. Dette representerer en betydelig utvidelse av forordningens geografiske virkeområde, fordi aktører som ikke har vært etablert i EU ikke har vært rammet

[38] Ved bruk av databehandlere må det inngås en databehandleravtale, jf. artikkel 28 tredje ledd

av direktivet tidligere. Disse aktørene plikter i en del tilfeller å ha en representant etablert i EU, jf. artikkel 27.

Forordningen vil med andre ord ramme et stort antall nye aktører og disse vil dermed måtte forholde seg til forpliktelsene etter artikkel 25 på samme måte som EU-etablerte aktører.

2.5 Teknologinøytralitet

En viktig grunn til at personverndirektivet har overlevd så lenge på tross av den kjappe teknologiske utviklingen, har vært at den er teknologinøytralt utformet.[39] Dette trekket er videreført i forordningen. Teknologinøytral utforming er motsetningen til teknologispesifikk utforming og det innebærer at regelverket utformes på en slik måte at det ikke er knyttet opp mot noen bestemte former for teknologi. Dette fremgår for eksempel av fortalen avsnitt 15, hvor det står at forordningen skal omfatte både automatisert og manuell[40] behandling av personopplysninger.

Teknologinøytral utforming er viktig av flere grunner. For det første fordi det sikrer at forordningen holder seg effektiv og relevant i lang tid fremover. På den måten slipper man å gå inn i kompliserte og tidkrevende lovgivningsprosesser på nytt etter hvert som teknologien utvikler seg. Hildebrandt og Tielemans omtaler dette som «*the sustainability objective*».[41] Videre er teknologinøytral utforming viktig fordi det forhindrer omgåelse av lovgivningen. Dette poenget er fremhevet i fortalen avsnitt 15 hvor det står at beskyttelsen av fysiske personer må være teknologinøytral «*to prevent creating a serious risk of circumvention*».

Teknologinøytralitet var et sentralt poeng for Artikkel 29-gruppen i diskusjonen om behovet for en bestemmelse om innebygd personvern. De har blant annet uttalt at «*a principle [of data protection by design] should be defined in a technologically neutral way in order to last for a long period of time in a fast changing technological and social environment*».[42]

---

39 A29WP (2009) s. 12

40 Manuell behandling omfattes når personopplysninger er del av eller ment å være det av et filsystem.

41 Hildebrandt og Tielemans (2013) s. 511

42 A29WP (2009) s. 14

2.6 Ansvarlighetsprinsippet («accountability»)

Ansvarlighetsprinsippet fremgår direkte av artikkel 5 annet ledd. Bestemmelsen fastslår at den behandlingsansvarlige er ansvarlig for og skal kunne dokumentere etterlevelse av personvernprinsippene i artikkel 5 første ledd.

Prinsippet gjennomsyrer hele forordningen. Dette uttrykkes på flere måter; på den ene side ved at det lempes på visse krav til den behandlingsansvarlige sammenlignet med direktivet, blant annet på kravene til konsesjon for behandling av personopplysninger.[43] På den annen side balanseres dette ved at den behandlingsansvarlige pålegges mer ansvar for egen etterlevelse. Dette uttrykkes for eksempel ved at det etter artikkel 24 stilles krav om at den behandlingsansvarlige må implementere tekniske og organisatoriske tiltak for sikre og kunne dokumentere at behandling skjer i samsvar med forordningen.

De behandlingsansvarlige blir med andre ord i større grad enn tidligere holdt ansvarlig for den behandlingen de bedriver. Som jeg vil komme til senere i oppgaven er artikkel 25 et utslag av ansvarlighetsprinsippet.

[43] EØS-notat om Personvernforordningen

3 Konseptet innebygd personvern

Artikkel 25 bygger på konseptet innebygd personvern. I dette kapittelet vil jeg redegjøre for hva innebygd personvern er og den historiske utviklingen fra PETs via PbD til DPbD. I tillegg vil jeg redegjøre for hvordan innebygd personvern har kommet til uttrykk i eldre rettspraksis.

3.1 Hva er innebygd personvern?

Innebygd personvern er et konsept som går ut på at man skal ta hensyn til personvernet i alle ledd av en utviklingsprosess.[44] Ved å ta hensyn til personvernet allerede i startfasen av et prosjekt unngår man å måtte gjøre dyre, kompliserende endringer i etterkant når systemet allerede er etablert. I mange tilfeller vil slike endringer dessuten være umulig å gjennomføre. Det vil som regel være både enklere og rimeligere å ta hensyn til personvern allerede i utviklingsfasen, enn det vil være å gjøre endringer i etterkant.

Konseptet innebærer at man skal ta hensyn til personvernet både i utviklingsfasen, driftsfasen og avviklingsfasen av et produkt, system eller en tjeneste. Et helt sentralt element ved innebygd personvern er at personvernet skal utgjøre en høyt prioritert, integrert del av løsningen, ikke et tillegg eller en ettertanke. Man kan si at personvern skal være en like integrert del av en virksomhet som HMS er del av et byggefirma.

Innebygd personvern kan defineres ved hjelp av de syv grunnleggende prinsippene utarbeidet av Dr. Ann Cavoukian.[45] Prinsippene er oversatt og tilpasset til norsk av Datatilsynet og lyder som følger:

1. Vær i forkant, forebygg fremfor å reparere.
2. Gjør personvern til standardinnstilling.
3. Bygg personvern inn i designet.
4. Skap full funksjonalitet.
5. Ivareta informasjonssikkerheten fra start til slutt.
6. Vis åpenhet.
7. Respekter brukerens personvern.[46]

---

44 ENISA (2015) s. 2

45 https://www.datatilsynet.no/globalassets/global/english/7foundationalprinciples_anncavoukian.pdf

46 https://www.datatilsynet.no/Teknologi/Innebygd-personvern/

3.2 Historisk utvikling

3.2.1 Fra PETs til PbD

Konseptet innebygd personvern har sitt opphav i ideen om personvernøkende teknologier, også kjent som PETs[47]. Ideen om PETs oppstod som resultat av et samarbeid mellom nederlandske og canadiske tilsynsmyndigheter i 1995 og har lenge vært populær i personvernkretser.[48] Det finnes ikke noen autoritativ definisjon på hva personvernøkende teknologi er og begrepet kan defineres på flere måter, men det benyttes ofte om teknologiske mekanismer som er utviklet med den hensikt å styrke personvernet.[49] Et praktisk eksempel på dette kan være krypteringsteknologi.

Senere på 1990-tallet ble ideen om innebygd personvern utviklet av Cavoukian.[50] Konseptet kan ses på som en videreutvikling av PETs, men til forskjell fra PETs, som fokuserer på tekniske mekanismer, så omfatter innebygd personvern hele utviklingsprosessen til et system. Konseptet har lenge vært ansett som «best practise»[51] og ble anerkjent som en internasjonal standard for personvern i 2010.[52] Selv om det fortsatt snakkes om PETs, blir begrepet i dag ofte inkludert som en del av dialogen om innebygd personvern.

3.2.2 Innebygd personvern i EU: Fra PbD til DPbD

I EU har det i lengre tid vært oppmerksomhet rundt «privacy by design». Selv om det ikke tidligere har eksistert noen lovfestet plikt til å implementere innebygd personvern i personverndirektivet, har flere bestemmelser likevel bygget på en lignende tanke.[53]

Særlig gjelder dette personverndirektivet artikkel 17 som stiller krav til at den behandlingsansvarlige implementerer tekniske og organisatoriske tiltak for å sikre behandling av personopplysninger. Bestemmelsen kan anses som en variant av «security by design»[54]. Etter direktivets fortale avsnitt 46 skal implementering av tiltak etter artikkel 17 skje både på tidspunktet for utarbeidelsen av et behandlingssystem, og under selve behandlingen. Men denne bestemmelsen har ikke gitt tilstrekkelig beskyttelse for individene og i 2009 etterspurte Artikkel 29-gruppen «*a broader and consistent principle of privacy by design*». De argumenterte med at det var nødvendig for å balansere den risiko den teknologiske utviklingen førte med seg og la

---

47 Privacy Enhancing Technologies

48 Koops and Leenes (2014) s. 167

49 Bygrave (2017) s. 3

50 Cavoukian (2013)

51 Krebs (2013) s. 3

52 På den 32. International Conference of Data Protection and Privacy Commissioners i Jerusalem, se Cavoukian (2012)

53 A29WP (2009) s. 12-13

54 Direktivet artikkel 17 har blitt videreført i forordningen artikkel 32.

til grunn at prinsippet måtte være bindende for behandlingsansvarlige, produsenter og designere.[55] Også Kommisjonen har vært inne på denne tankegangen og de gikk i 2010 inn for å implementere PbD inn i personvernlovgivningen.[56]

Når første utkast til ny personvernforordning endelig ble publisert, var prinsippet om «privacy by design» blitt byttet med et prinsipp om «data protection by design and by default». Som jeg var inne på under punkt 1.4.2, kan det antas at dette var på grunn av skillet mellom retten til privatliv og retten til beskyttelse av personopplysninger som følger av EUs Charter for grunnleggende rettigheter, men de to begrepene har likevel i stor grad overlappende innhold.

3.2.3 Innebygd personvern i eldre rettspraksis

I og med at forordningen ennå ikke har trådt i kraft, finnes det ikke rettspraksis som direkte bygger på artikkel 25. Det er likevel slik at både EU-domstolen og Den europeiske menneskerettsdomstolen tidligere har avsagt dommer som kan være av interesse. Selv om det vil være noe unaturlig å anse det som at disse avgjørelsene angår innebygd personvern, kan de i hvert fall si noe om hvordan det implisitt har blitt stilt krav til utvikling av tekniske løsninger.

Det er særlig avgjørelsen I v. FINLAND[57] som ble avsagt av Den Europeiske Menneskerettsdomstolen i 2008 som er interessant. I denne saken kom EMD til at Finland hadde krenket Den Europeiske Menneskerettighetskonvensjonen artikkel 8 som gjelder retten til respekt for privatlivet. Bakgrunnen for avgjørelsen var at et finsk sykehus ikke hadde gjort tilstrekkelig for å beskytte personopplysninger til en HIV-positiv kvinne, som i tillegg til å bli behandlet ved sykehuset også var ansatt der. Staten sviktet sin positive forpliktelse etter konvensjonen og ble dømt for brudd på artikkel 8, jf. dommen avsnitt 48 og 49.

Dommen angår ikke direkte en plikt til å sørge for innebygd personvern, men kan ses på som et uttrykk for en tendens hvor det stilles krav til tekniske løsninger for å oppfylle en rettslig plikt om beskyttelse av individets rett til privatliv.

Retten uttaler i avsnitt 36 at *«[a]lthough the object of Article 8 is essentially that of protecting the individual against arbitrary interference by the public authorities, it does not merely compel the State to abstain from such interference: in addition to this primarily negative undertaking, there may be positive obligations inherent in an effective respect for private or family life*». Selv om formålet med artikkel 8 første ledd i hovedsak er å beskytte borgerne mot vil-

---

55 A29WP (2009) s. 12

56 COM(2010) 609 final pkt. 4.4

57 Case of I v. FINLAND (Judgement Application no. 20511/03)

kårlig innblanding fra det offentlige, har bestemmelsen et virkeområde utover dette. Statene har også en positiv forpliktelse til å sikre respekt for privatlivet.

Videre uttaler retten at «*these obligations may involve the adoption of measures designed to secure respect for private life even in the sphere of relations of individuals between themselves*". Dette kan tolkes som et indirekte krav om innebygd personvern.

Retten konkluderer med at «*the mere fact that the domestic legislation provided the applicant with an opportunity to claim compensation (...) was not sufficient to protect her private life. What is required in this connection is practical and effective protection to exclude any possibility of unauthorized access occurring in the first place»*. Det er med andre ord ikke tilstrekkelig med rettslig adgang til å kreve erstatning for krenkelser av personvernet. Bestemmelsen gir også krav på en praktisk og effektiv beskyttelse som forhindrer krenkelsen i utgangspunktet. Tankegangen bak denne avgjørelsen bygger på mye av den samme tankegangen som ligger bak artikkel 25, ved at det legges vekt på faktisk og effektiv beskyttelsen av personvernet, på den måten at det må finnes løsninger som i praksis sikrer personopplysninger.

De andre sakene er avgjørelser avsagt av EU-domstolen selv. De har en noe mer perifer tilknytning til problemstillingen, men jeg har likevel tatt dem med siden jeg mener de kan illustrere at EU-domstolen i visse tilfeller har stilt krav til tekniske løsninger.

Google Spain-saken[58] kan være illustrerende for hvordan EU-domstolen har stilt krav til tekniske løsninger. En spansk statsborger gikk til sak mot en spansk avis, Google Inc. og datterselskapet Google Spain i et forsøk på å få fjernet en sak om et tvangssalg fra flere år tilbake som lå åpent på avisens nettside og som kom opp i søkeresultatet ved søk på mannens navn. Mannens krav mot avisen ble avvist av det spanske datatilsynet, men saken mot Google gikk videre til spansk høyesterett som bad om prejudisiell avklaring fra EU-domstolen.

Resultatet ble at Google ble pålagt å fjerne lenker knyttet til tvangssalget fra sin søkemotor («retten til å bli avindeksert»). Dommen innebar at Google måtte gjøre endringer i sine systemer for å muliggjøre slik avindeksering. Bygrave bruker avgjørelsen som et eksempel på hvordan EU-domstolen indirekte nører opp under PbD og DPbD-tankegang.[59]

---

[58] Case C-131/12 – Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014.

[59] Bygrave (2017) s. 18

De siste to sakene illustrerer hvordan EU-domstolen har gått inn og forhindrer personvern-inngripende teknologi. [60] Begge sakene angår Den belgiske sammenslutningen for forfattere, komponister og utgivere (forkortet SABAM).

I den første saken, C-70/10, gikk SABAM til sak mot internettleverandøren Scarlet Extended SA med krav om at selskapet skulle treffe tiltak for å bringe til opphør opphavsrettskrenkelsene begått av Scarlets kunder ved nedlastning av opphavsrettslig beskyttet innhold gjennom et peer-to-peer nettverk.[61] I den andre saken, C-360/10, gikk SABAM til sak mot Netlog NV., en sosial nettverkstjeneste hvor brukerne kan opprette profiler med informasjon om seg selv.[62] SABAM hevdet her at tjenesten tilrettela for at brukerne kunne dele opphavsrettslig beskyttet materiale seg i mellom og krevde blant annet at Netlog satte i verk tiltak for å forhindre dette.

SABAM fikk ikke medhold i noen av sakene. Avgjørelsene ble begrunnet blant annet i personvernhensyn, fordi det ville krev overvåkning av all internettrafikk fra alle brukere av Scarlet og Netlogs tjenester, dersom SABAM hadde fått medhold. Dette ville krev implementering av sterkt personverninngripende teknologi, og dette ble ikke akseptert av domstolen.

De overnevnte dommene fra EU-domstolen viser at domstolen ikke viker tilbake for å ta stilling til og stille krav til tekniske løsninger. Det er derfor all grunn til å regne med at domstolen vil fortsette å ta aktivt stilling til om de behandlingsansvarlige oppfyller sine forpliktelser til å implementere tekniske og organisatoriske tiltak slik de fremgår av artikkel 25.

---

60 Bygrave (2016)

61 Case C-70/10 Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), Judgment of 24 November 2011

62 Case C-360/10 Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (Sabam) v Netlog NV, judgment of the Court (Third Chamber) of 16 February 2012

4 Artikkel 25 «Data protection by design and by default»

I dette kapittelet vil jeg først gjennomgå noen generelle punkter i tilknytning til artikkel 25, før jeg tar for meg de ulike leddene i bestemmelsen hver for seg.

4.1 Generelt om bestemmelsen

4.1.1 Plassering i forordningen

Artikkel 25 er plassert i kapittel IV av forordningen som gjelder «*Controller and processor*», under Section 1 «*General obligations*». Denne delen av forordningen inneholder generelle regler om hvilke forpliktelser den behandlingsansvarlige har, og regler som regulerer forholdet mellom behandlingsansvarlig og databehandler. I tillegg til bestemmelsen om «*data protection by design and by default*» er det blant annet regler om delt behandlingsansvar, om krav til representant hvor aktørene ikke er etablert i EU og om samarbeid med tilsynsmyndigheter.

4.1.2 Formålet med bestemmelsen

Hovedformålet med artikkel 25 er at den behandlingsansvarlige skal tilfredsstille kravene etter forordningen og beskytte rettighetene til de registrerte. Formålet fremgår av siste del av første ledd i bestemmelsen, hvor det står at implementering av tiltak skal skje «*in order to meet the requirements of this Regulation and protect the rights of data subjects*». Dette innebærer at det etter forordningen ikke er tilstrekkelig å anse personvernbeskyttelse som en sjekkliste med forpliktelser som kan krysses av og arkiveres. Dette poenget fremgår også av fortalen avsnitt 78 hvor det står følgende: «*in order to be able to demonstrate compliance with this Regulation, the controller should (…) implement measures which meet in particular the principles of data protection by design and data protection by default*».

Videre fremgår det av første ledd at effektivitet er et sentralt formål. Den behandlingsansvarlige skal implementere tiltak som «*in an effective manner*» oppfyller kravene etter forordningen. Dette understreker poenget jeg var inne på i avsnittet over; for å oppfylle forpliktelsen i artikkel 25 er det ikke tilstrekkelig å implementere tiltak bare for å kunne dokumentere etterlevelse, de implementerte tiltakene må ha en faktisk effekt.

4.1.3 Behandlingsansvarliges ansvar

Det er i utgangspunktet bare den behandlingsansvarlige som er forpliktet etter bestemmelsen («*the controller shall*»). Dette er i tråd med resten av forordningen; den behandlingsansvarlige er det primære pliktsubjektet. Hvem som er behandlingsansvarlig er definert i artikkel 4 syvende ledd som den som avgjør formålet med behandlingen av personopplysninger og hvilke hjelpemidler som skal benyttes, se punkt 2.3.3. Forpliktelsen bygger på en slags forutsetning om at den behandlingsansvarlige er den som har best kontroll over behandlingen.

Hildebrandt og Tielemans legger til grunn at tanken bak at den behandlingsansvarlige er pliktsubjektet ser ut til å være at de behandlingsansvarlige skal legge press på produsenter til å utvikle den teknologi de har behov for.[63] Man kan i så fall stille spørsmål ved hvorvidt dette er en fornuftig lovgivningsmetodikk. Valget av behandlingsansvarlig som det primære pliktsubjektet har blitt kritisert i litteraturen fordi den behandlingsansvarlige i mange tilfeller ikke vil ha den kontrollen, verken over behandlingen eller over produsenter, som er forutsatt i bestemmelsen. Jeg kommer nærmere inn på denne kritikken under punkt 8.

Selv om bestemmelsen ikke direkte stiller krav til andre aktører, vil de likevel kunne rammes av bestemmelsen. Dette gjelder særlig databehandlere etter artikkel 28, men produsenter og offentlige virksomheter kan også tenkes omfattet etter fortalen avsnitt 78.

4.1.3.1 Valg av databehandlere

I det første utkastet fra Europaparlamentet var databehandlere direkte inkludert som pliktsubjekt etter bestemmelsen.[64] Dette ble fjernet i senere utkast og databehandlere omfattes ikke direkte av bestemmelsen slik den er vedtatt. Helt unntatt er de likevel ikke: Etter artikkel 28 første ledd plikter behandlingsansvarlig å benytte «*processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject*». Bestemmelsen stiller ikke direkte krav til databehandlere, men den krever at den behandlingsansvarlige velger databehandlere som oppfyller kravene etter forordningen ved å implementere tekniske og organisatoriske løsninger. Dette innebærer indirekte at databehandler må oppfylle kravet etter artikkel 25.

Databehandlere må kunne stille tilstrekkelige garantier for at de oppfyller kravene etter forordningen. Hva som ligger i kravet til tilstrekkelig garantier utdypes i fortalen artikkel 81 hvor det fremgår at garantiene særlig skal gjelde «*expert knowledge, reliability and resources*». Videre kan tilslutning til godkjente sertifiseringsmekanismer[65] eller codes of conduct[66] benyttes for å vise at databehandler overholder forordningens krav.

Artikkel 28 stiller altså ikke direkte krav til databehandler, men bygger på en antagelse om at de vil rette seg etter den fordi databehandlere som oppfyller kravene vil bli foretrukket av de behandlingsansvarlige. Behandlingsansvarlige som ikke oppfyller kravet etter artikkel 28, vil

---

63 Hildebrandt og Tielemans (2013) s. 517

64 Europaparlamentet (2014) artikkel 23 1.

65 Artikkel 25 tredje ledd, se punkt 4.4

66 Artikkel 40, se punkt 5

kunne sanksjoneres med administrative bøter etter artikkel 83 fjerde ledd bokstav a.[67] Det foreligger derfor sterke økonomiske incentiver for behandlingsansvarlig til å velge databehandlere som oppfyller kravene, og derved også sterke konkurransemessige incentiver for databehandlerne til å følge opp. Bygrave har uttalt at «*[i]n essence, the Regulation is relying on controllers to shape the market and technology foundations for information systems development in a privacy-friendly direction*»[68]. Tiden vil vise om dette fungerer i praksis.

4.1.3.2 Oppfordring til produsenter

Produsenter rammes som utgangspunkt ikke av forordningen, til tross for at de i mange tilfeller vil ha den største innflytelsen på hvordan et produkt ender opp med å fungere.[69] Likevel er heller ikke de helt unntatt. Av fortalen avsnitt 78 fremgår det at produsenter «*should be encouraged to take into account the right to data protection when developing and designing such products, services and applications and with due regard to the state of the art, to make sure that controllers and processors are able to fulfil their data protection obligations*». Produsenter skal oppfordres til å ta hensyn til personvernforpliktelsene til behandlingsansvarlig og databehandler. Det stilles ingen lovkrav til produsenter utover denne oppfordringen og plasseringen midt i et ordrikt avsnitt i fortalen er ikke egnet til å rette søkelyset på den.[70] Det er med andre ord grunn til å anta at betydningen av denne uttalelsen utover en viss symbolsk effekt sannsynligvis vil være liten.

På dette området strider bestemmelsen mot Artikkel 29-gruppens anbefaling slik de uttrykte den i rapporten «The Future of Privacy» i 2009. De mente at innebygd personvern måtte være et bindende prinsipp for produsenter, designere og behandlingsansvarlige i fremtidig lovgivning.[71] Dette ble ikke fulgt opp og det har heller ikke blitt kommentert i forarbeidene.

I likhet med tilstanden for databehandlere som redegjort for over, kan det derimot antas at markeds- og konkurransemessige forhold vil ha stor innvirkning på hvordan denne gruppen kommer til å handle. Behandlingsansvarlige vil forhåpentligvis foretrekke produsenter som kan tilby løsninger som gjør at de kan oppfylle sine forpliktelser etter forordningen. Dette er dermed nok et eksempel på at forordningen baserer seg på at det er de behandlingsansvarlige som skal forme markedet.

---

67 Se punkt 6

68 Bygrave (2017) s. 19

69 Tsormpatzoudi m. fl. (2015) s. 207

70 Bygrave (2017) s. 19

71 A29WP (2009) s. 13

4.1.3.3 Betydning ved offentlige anbud

Etter fortalen avsnitt 78 bør «*the principles of data protection by design and by default (…) also be taken into consideration in the context of public tenders*». Det innebærer at bestemmelsen også er av interesse for offentlige virksomheter, ettersom de har en oppfordring til å ta med i betraktning hvorvidt prinsippene for innebygd personvern er fulgt. I det første forslaget fra Europaparlementet var offentlige anbud inkludert direkte i bestemmelsen, men det ble senere tatt ut, omformulert og flyttet til fortalen. Av Europaparlamentets lovforslag fremgikk det at man inkluderte offentlige anbud fordi det ville fremme omfattende bruk av prinsippene i ulike økonomiske sektorer.[72] Begrunnelsen er antagelig den samme, selv om teksten om offentlige anbud er flyttet til fortalen.

Inkluderingen av offentlige anbud er et tredje eksempel på hvordan EU benytter markedskreftene som incentiv for databehandlere og produsenter. Avsnitt 78 sier likevel bare at innebygd personvern *bør* tas i betraktning og stiller ingen krav om at det *må* tas i betraktning. Her skiller forordningen seg betydelig fra Europaparlamentets første utkast hvor innebygd personvern ble foreslått å være en forutsetning for offentlige anskaffelser.[73] Den videre utviklingen vil derfor i stor grad skje på grunnlag av hvordan offentlige virksomheter selv velger å vektlegge oppfordringen i praksis.

[72] Europaparlamentet (2014) artikkel 23 1a.

[73] Europaparlamentet (2014) artikkel 23 1a.

4.2 Artikkel 25 første ledd – «Data protection by design»

Artikkel 25 første ledd gjelder «data protection by design» og lyder som følger:

«Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.»

Bestemmelsen stiller krav til at behandlingsansvarlig skal innføre tekniske og organisatoriske tiltak for å implementere personvernprinsippene. Formålet med bestemmelsen er å sikre at personvern er en integrert del av design- og utviklingsprosesser fra start av, slik at behandling av personopplysninger samsvarer med kravene etter forordningen og rettighetene til de registrerte.

4.2.1 «Designed to implement data-protection principles»

De tekniske og organisatoriske tiltakene skal være utformet på en slik måte at de implementerer personvernprinsippene. Bestemmelsen peker konkret på prinsippet om å samle inn minst mulig personopplysninger («*data minimisation*»), men også de andre personvernprinsippene er omfattet. Prinsippene fremgår av forordningen artikkel 5. I det følgende vil jeg gjennomgå noen av de prinsippene som er særlige relevante for artikkel 25.

Prinsippet om å samle inn minst mulig personopplysninger er definert i artikkel 5 første ledd bokstav c som sier at personopplysninger skal være «*adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed*». Prinsippet retter seg primært mot innsamlingsfasen av behandlingen, slik at mengden personopplysninger som samles inn skal begrenses til det som er nødvendig, men prinsippet gjelder også for etterfølgende behandling. Dette innebærer at personopplysninger som ikke lenger er nødvendig for formålet skal slettes eller anonymiseres[74].

Implementering av prinsippet innebærer at de behandlingsansvarlige faktisk må ta standpunkt til hva slags personopplysninger som er nødvendige. Prinsippet kan for eksempel gjennomfø-

[74] Se punkt 4.2.3.4.1

res organisatorisk ved at de behandlingsansvarlige etter interne rutiner eller retningslinjer må kartlegge hvilke behov de har for personopplysninger før behandlingen starter.

Et annet prinsipp av særlig interesse er prinsippet om formålsbegrensning («*purpose limitation*»). Dette prinsippet er interessant både fordi det er et viktig prinsipp i seg selv, men også fordi det er nært knyttet til prinsippet om minst mulig innsamling av personopplysninger.

Prinsippet om formålsbegrensning er definert i artikkel 5 første ledd bokstav b som sier at personopplysninger skal være «*collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes*». Kjernen av dette prinsippet er at personopplysninger kun skal samles inn for bestemte, legitime formål. Disse formålene må være klarlagt før innsamling av personopplysninger gjennomføres og når formålet er oppfylt skal opplysningene slettes eller anonymiseres[75]. Det er med andre ord ikke anledning til å behandle personopplysninger ut fra et «kjekt å ha»-perspektiv. Bakgrunnen for dette er knyttet til den registrertes forventning om hva den innsamlede informasjonen skal benyttes til, samt at personopplysninger bare skal benyttes til de formål som de er egnet til å benyttes til. Det er med andre ord også et element av å sikre tilstrekkelig informasjonskvalitet.

Det er mulig at implementering av dette prinsippet best kan gjennomføres ved bruk av organisatoriske tiltak. For eksempel kan klarlegging av formålene inngår som del av interne rutiner eller retningslinjer for utviklingsprosesser. Dette kan gjøres som en del av konsekvensanalyser for personvern, i de tilfeller det er krav om dette.[76]

4.2.2 «Both at the time of the determination of the means for processing and at the time of the processing itself»

Behandlingsansvarlig må ha implementert tekniske og organisatoriske tiltak «*both at the time of the determination of the means for processing and at the time of the processing itself*». Dette innebærer at tiltak må være på plass senest på det tidspunkt formålet for behandlingen fastsettes, samt all den tid behandling av personopplysninger pågår. Bestemmelsen setter en livsløpsstandard for behandling av personopplysninger som gjelder fra behandlingen settes i gang og helt frem til den avsluttes, i samsvar med Cavoukians femte prinsipp for innebygd personvern.[77]

At implementering skal skje senest på tidspunktet for avgjørelsen av formålet for behandlingen har vært et viktig poeng for Artikkel 29-gruppen. Begrunnelsen for dette har vært at im-

[75] Se punkt 4.2.3.4.1

[76] Se punkt 7.2 og artikkel 35

[77] Se Cavoukian (2013) og punkt 3.1

plementering på senere tidspunkt vil være «*inconsistent and insufficient as regards the requirements of an effective protection of the rights and freedoms of the data subjects*». [78] De legger med andre ord til grunn at implementeringen må skje tidligst mulig for å sikre et tilstrekkelig beskyttelsesnivå for de registrerte.

Ordlyden tilsier at den behandlingsansvarlige plikter å implementere passende tiltak *både* på tidspunktet for fastsettelsen av formålet for behandlingen *og* mens behandlingen foregår, jf. bruken av «*and*». Dette innebærer at den behandlingsansvarlige må ta stilling til hva som er passende tiltak på begge tidspunktene. Situasjonen vil ikke nødvendigvis være den samme for begge alternativene. Det kan tenkes at det på tidspunktet for fastsettelsen av formålet ikke forelå noen passende tiltak, men at det senere under selve behandlingen foreligger. Hildebrandt og Tielemans argumenterer for at den behandlingsansvarlige i slike tilfeller plikter å implementere tiltak på det tidspunkt hvor passende tiltak foreligger.[79] Den behandlingsansvarlige slipper dermed ikke unna med å foreta vurderingen bare på det førstnevnte tidspunktet og deretter si seg fornøyd med at det ikke finnes noen passende tiltak. Etter mitt syn har denne forståelsen støtte også i ordlyden. Den behandlingsansvarliges forpliktelse til å foreta dobbel vurdering kan ses på som et utslag av ansvarlighetsprinsippet, ved at det stilles krav til faktisk og effektiv etterlevelse av forordningen, jf. punkt 2.6.

Hildebrandt og Tielemans trekker en linje mellom innovasjon og forpliktelser etter forordningen, og understreker at behandlingsansvarlige som ønsker å drive rask innovasjon, må følge opp med tilsvarende raske oppdateringer for personvernbeskyttelsen.[80] Dette følger i prinsippet direkte av at den behandlingsansvarlige er forpliktet til å ha implementert tiltak på tidspunktet for behandlingen.

4.2.3 «Technical and organisational measures»

Den behandlingsansvarlige plikter å implementere passende tekniske og organisatoriske tiltak («*technical and organisational measures*»). Tiltakene må være utformet slik at de implementerer personvernprinsippene «*in an effective manner*» og integrerer de nødvendige sikkerhetstiltak inn i behandlingen, slik at kravene i forordningen blir oppfylt.

4.2.3.1 «Measure»

Spørsmålet er hva som ligger i at den behandlingsansvarlige må implementere *tiltak*. Rent språklig stiller ikke begrepet «*measure*» særlig strenge krav til hva slags handling som må foretas. Begrepet er teknologinøytralt og i prinsippet stiller det bare krav til at den behand-

[78] A29WP (2009) s. 14

[79] Hildebrandt og Tielemans (2013) s. 517

[80] Hildebrandt og Tielemans (2013) s. 517

lingsansvarlige har en plikt til å foreta seg *noe*. Dette fremgår tydelig ved en sammenligning av ulike språkversjoner av bestemmelsen. I den danske versjonen benyttes for eksempel begrepet «*foranstaltninger*» og i den svenske versjonen benyttes «*åtgärder*». Disse begrepene har det til felles at de innebærer krav til handling, men denne handlingen kan ha nesten hvilken som helst form. Det skal med andre ord lite til for at en handling den behandlingsansvarlige implementerer tilfredsstiller kravet til «*measure*».

Noe av grunnen til at bestemmelsen ikke har en mer konkret ordlyd på dette punktet, er fordi den er ment å være en generell forpliktelse. Dette fremgår blant annet av plasseringen i forordningen under kapittelet «*General obligations*», se punkt 4.1.1. Bestemmelsen er ment å ramme et bredt spekter av virksomheter i ulike bransjer og av ulik størrelse, som kan ha svært forskjellige formål og behov. For å treffe bredt er den derfor vagt utformet. Bestemmelsen har vært gjenstand for en del kritikk på grunn av dette. Denne kritikken kommer jeg tilbake til under punkt 8.

4.2.3.2 «Technical and organisational»

Videre er det et krav at disse tiltakene er *tekniske og organisatoriske*. Heller ikke dette stiller strenge krav til hva slags type tiltak som kan tenkes. Dette er delvis fordi begrepene er vanskelig å definere presist. Mange typer tiltak kan falle inn under betegnelsene teknisk og organisatorisk. Det enkleste er å definere begrepene ved hjelp av eksempler. Organisatoriske tiltak kan tenkes å være internkontrollsystemer, opplæringsprogrammer, rutiner eller retningslinjer i en virksomhet. Tekniske tiltak kan være alt fra programmering til fysisk utforming. Artikkel 29-gruppen har brukt som eksempel på tiltak at helseforetak lagrer pasientnavn og andre identifikatorer adskilt fra opplysninger om helsetilstand og medisinering, eller at videoovervåking på offentlig transport blir utformet på en slik måte at ansiktene på sporede individer ikke kan gjenkjennes.[81]

Skillet mellom hva som er et teknisk tiltak og hva som er et organisatorisk tiltak er neppe av særlig betydning, fordi det i mange tilfeller vil være både vanskelig og kunstig å si om en type tiltak er det ene eller det andre. Mange tiltak vil kunne ha både tekniske og organisatoriske karaktertrekk og mange tiltak vil kunne implementeres enten teknisk eller organisatorisk, avhengig av hva som er mest hensiktsmessig i den enkelte virksomhet. Dette gjelder for eksempel for tilgangskontroll. Tilgangskontroll kan karakteriseres som et teknisk *og* organisatorisk tiltak fordi det både inkluderer organisatoriske prosesser i tilknytning til for eksempel rolle- og ansvarsfordeling, samtidig som det krever teknisk implementering.

---

[81] A29WP (2009) s. 14

Et spørsmål er om man plikter å innføre både tekniske *og* organisatoriske tiltak. Etter en naturlig språklig forståelse bør bestemmelsen forstås som at begge typer tiltak må implementeres, sett i lys av at bestemmelsen benytter begrepet «technical *and* organisational measures». Dersom lovgiver hadde ment at de to tiltakstypene er alternative, kunne dette enkelt fremgått av bestemmelsen med annen ordbruk. Det er også en viss sikkerhet i å implementere tiltak av begge typer, fordi de kan fange opp ulike situasjoner. Etter mitt syn burde bestemmelsen likevel ikke tolkes strengt på dette punktet, fordi det som nevnt over i flere tilfeller er både vanskelig og kunstig å definere hva slags type tiltak et tiltak er. Det avgjørende bør være at tiltak, i tråd med formålet for bestemmelsen, er implementert på en *effektiv* måte som gjør at den behandlingsansvarlige overholder sine forpliktelser etter forordningen, ikke om man har implementert begge typer tiltak.

I fortalen avsnitt 78 er det listet opp noen eksempler på tekniske og organisatoriske tiltak. De som er nevnt er minimering av mengden innsamlede opplysninger, pseudonymisering av personopplysninger på tidligst mulig tidspunkt, åpenhet om formålet for og behandlingen av personopplysninger, mulighet for den registrerte til å overvåke behandlingsprosessen og mulighet for behandlingsansvarlig til å lage og forbedre sikkerhetsfunksjoner. Listen er bare ment som eksempler på mulige tiltak og er ikke uttømmende. Tsormpatzoudi m.fl. peker på at denne listen i hvert fall delvis bidrar til å klargjøre hvilke krav som stilles etter bestemmelsen.[82] Det er grunn til å regne med at ytterligere klargjøring på dette punktet vil komme fra Artikkel 29-gruppen, EDPB og nasjonale tilsynsmyndigheter etter hvert.

4.2.3.3 «Appropriate»

Pseudonymisering («*pseudonymisation*») nevnes som et konkret eksempel på et mulig tiltak, men prinsipielt kan alle slags tekniske og organisatoriske tiltak være aktuelle. Forutsetningen er at tiltaket er passende («*appropriate*»).[83] Begrepet «*appropriate*» har ikke et konkret innhold, men viser til en skjønnsmessig helhetsvurdering som vil kunne endre karakter etter hvert som forordningen utvikler seg.[84]

På den ene side innebærer kravet om at et tiltak skal være passende at det har en faktisk effekt på personvernbeskyttelsen. Dette fremgår direkte av bestemmelsen ved at det stilles krav om at tiltak må være utformet på en slik måte at de implementerer personvernprinsippene «*in an effective manner*». På den annen side innebærer begrepet ikke et krav om at behandlingsansvarlig trenger å gjennomføre hvilke som helst tenkelige tekniske og organisatoriske tiltak

---

82 Tsormpatzoudi m. fl. (2015) s. 204

83 Jeg velger å bruke begrepet «passende» fordi dette blir brukt i den danske versjonen av bestemmelsen.

84 Se også punkt 1.3.1 om EU-rettens dynamiske tolkningsstil

som kan ha effekt. Det er i stor grad rom for den behandlingsansvarliges eget skjønn i vurderingen av hvilke tiltak som bør implementeres.

Bestemmelsen lister opp flere vurderingsmomenter som er relevante ved vurderingen av hvilke tiltak som er passende. For det første skal det tas hensyn til det tekniske nivået («*state of the art*»). I dette ligger det at man må ta stilling til hvilke tiltak som faktisk er mulig å implementere. Hildebrandt og Tielemans omtaler dette som «*technical feasibility*»[85]. I utgangspunktet har ikke behandlingsansvarlig plikt til å implementere tekniske tiltak som ennå ikke er utviklet. Dette er mulig at dette er en sannhet med modifikasjoner. Dersom det vil være relativt enkelt å utvikle et passende tiltak, kan det likevel være at en slik plikt vil foreligge.

Videre skal det tas hensyn til kostnadene ved implementering («*the cost of implementation*»). Den behandlingsansvarlige plikter ikke å implementere tiltak dersom det ikke er økonomisk gjennomførbart. Motsatt vil den behandlingsansvarlige ha plikt til å implementere tiltak hvor kostnadene ikke er et hinder. Hildebrandt og Tielemans omtaler dette som «*economic feasibility*».[86] Hva slags implementeringskostnader som kan pålegges behandlingsansvarlig ved implementering av tiltak, må antas å variere med flere faktorer. Blant annet vil størrelsen på virksomheten, omfanget av behandlingen og hvilke type personopplysninger som behandles kunne være av betydning. For små virksomheter hvor behandling av personopplysninger bare skjer i liten skala, er det ikke rimelig at de skal pålegges store kostnader ved implementering av tiltak. For globale virksomheter som driver behandling av personopplysninger i stor skala eller hvor dette er kjernevirksomheten, vil store implementeringskostnader sannsynligvis være både rimelig og nødvendig.

Det er en svakhet ved bestemmelsen at den ikke sier noe mer om på hvilken måte implementeringskostnader skal vurderes. Det er forståelig at det er utfordrende å si noe generelt om dette, med tanke på hvor bredt bestemmelsen skal treffe, men slik bestemmelsen er utformet nå står den behandlingsansvarlige i utgangspunktet fritt i sin vurdering. Da er det grunn til å regne med at implementeringskostnader vil kunne komme til å bli det sentrale momentet for mange behandlingsansvarlige på bekostning av de andre vurderingsmomentene. Dette vil i så fall være uheldig.

For det tredje skal det tas hensyn til behandlingens karakter, omfang, sammenheng og formål. Det skal foretas en konkret helhetsvurdering av behandlingen som skal gjennomføres. I denne helhetsvurderingen skal det også legges vekt på hvilke risiki behandlingen innebærer, sann-

[85] Hildebrandt og Tielemans (2013) s. 517

[86] Hildebrandt og Tielemans (2013) s. 517

synligheten for disse og hvor alvorlig det er. Det vil for eksempel i tilfeller hvor det behandles små mengder personopplysninger og hvor sannsynligheten for krenkelser av personvernet er liten, stilles mindre strenge krav til implementering av tiltak enn hvor det behandles store mengder personopplysninger og sannsynligheten for krenkelser er stor.

Det stilles med andre ord ingen klare krav til hvilke tekniske og organisatoriske tiltak behandlingsansvarlig må implementere, men spørsmålet må avgjøres på grunnlag av en konkret helhetsvurdering av momentene nevnt ovenfor. Et hovedelement i vurderingen må være at kostnader og byrder står i forhold til personvernrisikoen. I tilfeller hvor det finnes tiltak som ikke er urimelig kostbare å implementere, må det antas at behandlingsansvarlig har en plikt til å implementere dem, med mindre andre forhold taler mot. Denne vurderingen må i første omgang foretas av behandlingsansvarlig selv og behandlingsansvarlig bør kunne dokumentere at dette gjøres, for eksempel ved å vise til interne retningslinjer.[87]

Dette er i tråd med synspunktet Artikkel 29-gruppen hadde i en uttalelse i forbindelse med utarbeidelsen av forordningen. De gikk inn for at det burde være opp til behandlingsansvarlig å velge passende tiltak og henviste til ansvarlighetsprinsippet i artikkel 24. Videre uttalte de at vurderingen av hvorvidt den behandlingsansvarlige har implementert passende tiltak må avgjøres fra sak til sak. Gruppen anså det ikke som nødvendig med ytterligere lovgivning, men regnet med at veiledning fra EDPB vil kunne være nyttig.[88]

Bestemmelsen gir som nevnt ingen veiledning med tanke på hvordan de ulike vurderingsmomentene skal vektes mot hverandre. I det første utkastet til ny forordning hadde Kommisjonen mulighet til å vedta delegerte rettsakter og stadfeste tekniske standarder etter tredje og fjerde ledd.[89] Dette ble ikke inkludert i den endelige versjonen, muligens fordi det ville vært problematisk å gi Kommisjonen slik myndighet av hensyn til subsidiaritetsprinsippet.[90] Frem til en eventuell avklaring fra domstolen eller EDPB vil det derfor i stor grad være opp til den behandlingsansvarlige selv hvordan avveiingen mellom vurderingsmomentene skjer.

4.2.3.4 «Pseudonymisation»

Pseudonymisering nevnes som et konkret eksempel på en type teknisk tiltak i artikkel 25 første ledd. Pseudonymisering innføres som et nytt begrep i forordningen. Pseudonymiserte personopplysninger i utgangspunktet fortsatt personopplysninger[91], men bruk av pseudonymise-

87 Se fortalen avsnitt 78 og avsnitt 82.

88 A29WP (2012) s. 25

89 COM/2012/011 final

90 Koops og Leenes (2014) s. 161

91 Se fortalen avsnitt 26

ring kan lempe på kravene som stilles til den behandlingsansvarlige. Begrepet er definert i artikkel 4 femte ledd:

«'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person;"

Det sentrale er at behandling av personopplysninger skal skje på en slik måte at opplysningene ikke lenger kan knyttes til en spesifikk person uten bruk av tilleggsinformasjon. Slik tilleggsinformasjon må oppbevares separat. Alle identifiserende personopplysninger erstattes med informasjon som ikke er identifiserbar. Dette kan for eksempel gjøres ved bruk av «hashing»[92]. På den måten kan man beholde informasjon uten å beholde koblingen til den registrerte. Dette kan være nyttig hvor personopplysninger samles inn for formål hvor koblingen til individet i prinsippet er uinteressant. Pseudonymisering er dermed et nyttig teknisk tiltak fordi det kan ivareta legitime behov, samtidig som personvernet ivaretas ved at det blir vanskelig å identifisere individet. Av fortalen avsnitt 78 fremgår det at pseudonymisering bør skje tidligst mulig.

Som nevnt kan bruk av pseudonymisering myke opp andre krav i forordningen. Begrunnelsen for dette er at pseudonymisering kan redusere risikoen for de registrerte og gjøre det lettere for behandlingsansvarlig og databehandler å oppfylle sine personvernforpliktelser fordi beskyttelsesnivået ikke trenger å være like høyt, se fortalen avsnitt 28. For eksempel stilles det mindre strenge krav til kompatibilitet mellom primære og sekundære behandlingsformål ved gjenbruk av personopplysninger, jf. artikkel 6 fjerde ledd. Dette innebærer at den behandlingsansvarlige vil kunne ha større rom for å gjenbruke data til andre formål enn det opprinnelige formålet, når opplysningene er pseudonymisert. Pseudonymisering vil i tillegg kunne ha betydning ved fastsettelse av nivået på administrative bøter etter artikkel 83 annet ledd bokstav d. Jeg kommer tilbake til dette under punkt 6.

4.2.3.4.1 Forholdet til anonymisering

Anonymisert opplysninger er opplysninger som ikke relaterer seg til en identifisert eller identifiserbar fysisk person, jf. fortalen avsnitt 26. Anonymiserte opplysninger er ikke personopplysninger og omfattes ikke av forordningen, jf. fortalen avsnitt 26 siste setning. Det er viktig å

[92] «Hashing» er navnet på en mulig fremgangsmåte for å pseudonymisere data ved å benytte en hashfunksjon. Det gjøres ved å omforme data ved hjelp av en logaritme slik at den opprinnelige informasjonen ikke kan utledes fra dataen direkte.

skille mellom pseudonymisering og anonymisering, fordi anonymisering innebærer at en behandlingsansvarlig som benytter dette som tiltak ikke behøver å forholde seg til kravene etter artikkel 25.

Det er grunn til å være oppmerksom på at det i praksis ofte viser seg at det svært vanskelig å anonymisere personopplysninger. Netflix-casen illustrerer dette. Strømmetjenesten Netflix offentliggjorde et (antatt) anonymisert datasett bestående av rangeringene til en halv million abonnenter som en del av Netflix Prize Contest. To forskere ved University of Texas klarte deretter å identifisere nesten hele datasettet ved å sammenføye det med offentlig tilgjengelig informasjon fra blant annet Internet Movie Data Base (IMBD).[93] Saken illustrerer hvor vanskelig det er å anonymisere opplysninger, i hvert fall i de tilfeller hvor det er snakk om store, granulerte datasett som det var i dette tilfellet.

En nylig avgjørelse fra EU-domstolen kan dessuten komme til å få indirekte betydning for hva som skal regnes som anonymisering. I Breyer-saken[94] tok retten stilling til hvorvidt dynamiske IP-adresser skal regnes som personopplysninger. Dynamiske IP-adresser er IP-adresse som, i motsetning til statiske IP-adresser, endres hver gang det skjer en ny tilkobling til internett.[95] Disse har tidligere ikke blitt regnet for å være personopplysninger.

Domstolen kom frem til at i de tilfeller hvor behandlingsansvarlig ikke selv sitter på tilleggsinformasjon, men likevel har «*legal means*» til å skaffe seg denne tilleggsinformasjon, så skal ikke informasjonen den behandlingsansvarlige sitter med regnes for å være anonymisert. Dette innebærer at dynamiske IP-adresser nå skal regnes som personopplysninger hvor behandlingsansvarlig har «legal means».[96] Selv om avgjørelsen ble avsagt etter direktivet og derfor ikke gjelder forordningen direkte, er det grunn til å anta at domstolen vil opprettholde dette standpunkt også i forordningen, fordi definisjonen av hva som er personopplysninger i det store og hele er tilsvarende for direktivet og forordningen. Dette kan bety at det i praksis vil bli enda vanskeligere å faktisk anonymisere personopplysninger.

---

93 Narayanan og Shmatikov (2006)

94 Case C-582/14 Bundesrepublik Deutschland v Patrick Breyer, judgment of 19 October 2016.

95 Dommen avsnitt 16

96 Dommen avsnitt 49

4.3 Artikkel 25 annet ledd – «Data protection by default»

Artikkel 25 andre ledd gjelder «data protection by default» og lyder som følger:

«*The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.* »

Behandlingsansvarlig har plikt til å sikre at, som standard, bare personopplysninger som er nødvendig for formålene med behandlingen blir behandlet. Dette skal gjøres ved å implementere passende tekniske og organisatoriske tiltak[97]. Konkret gjelder denne plikten omfanget av opplysninger som samles inn («*amount of personal data collected*»), omfanget av behandlingen av disse opplysningene («*the extent of their processing*»), lagringstid («*the period of their storage*») og tilgang («*their accessibility*»). Det skal særlig fattes tiltak for å forhindre at personopplysninger spres til et ubestemt antall fysiske personer uten den registrerte sitt samtykke. Annet ledd utgjør en spesifisering av første ledd på den måten at annet ledd stiller krav til *hvilken effekt* tiltak som den behandlingsansvarlige implementerer *skal* ha.

4.3.1 Bakgrunn

Artikkel 25 annet ledd springer ut fra Cavoukians andre prinsipp for innebygd personvern, som går ut på å gjøre personvern til standardinnstilling.[98] Artikkel 29-gruppen argumenterte for behovet for en slik forpliktelse allerede i 2009 i rapporten «The Future of Privacy». De la til grunn at brukere av IKT-systemer ikke har tilstrekkelig mulighet for kontroll over sine egne personopplysninger ved bruk av disse tjenestene, og at slike tjenester derfor burde utformes med «privacy by default»-innstillinger.[99]

4.3.2 «By default»

Den behandlingsansvarlige må sikre at bare nødvendig personopplysninger blir behandlet som standard. Dette innebærer i prinsippet ikke at det er forbudt for den behandlingsansvarlige å behandle mer personopplysninger enn nødvendig, men dersom den behandlingsansvarlige ønsker å gjøre dette, så krever det at den registrerte gir sitt samtykke. Slikt samtykke vil den registrerte for eksempel kunne gi gjennom å gjøre endringer i standardinnstillingene til et produkt eller tjeneste. Standardinnstillingenes rolle fremheves i formuleringen av både den dans-

---

97 Se punkt 4.2.4

98 Cavoukian (2013)

99 A29WP (2009) s. 13

ke og den tyske versjonen av bestemmelsen. Overskriften av den tyske versjonen er for eksempel nettopp «personvernvennlige innstillinger» («*datenschutzfreundliche Voreinstellungen*»). Av den danske versjonen fremgår det at personopplysninger skal sikres «gennem standardinnstillinger».

Forpliktelsen innebærer at det i utgangspunktet ikke skal være nødvendig å måtte gjøre endringer i innstillinger for å forhindre at den behandlingsansvarlige behandler mer personopplysninger enn nødvendig. Dette kan for eksempel innebære at en innstilling som regulerer tredjepartsaktørers mulighet til å lagre informasjonskapsler eller en innstilling som regulerer GPS-sporing er satt til nei som standard.[100]

Annet ledd bygger på en tankegang om at produkter og tjenester stort sett vil bli brukt på den måten standardinnstillingene legger opp til. Av den grunn vil de innstillingene som settes som standard faktisk ha en innvirkning på graden av beskyttelse for de registrerte.

4.3.3 "Only personal data which are necessary for each specific purpose"

De tekniske og organisatoriske tiltakene skal sikre at bare personopplysninger som er nødvendige for hvert enkelt formål for behandlingen blir behandlet. Dette innebærer at den behandlingsansvarlig må ta aktivt stilling til hvilke personopplysninger det er nødvendig å behandle. Dersom det viser seg at det ikke er nødvendig å behandle personopplysninger i det hele tatt, så må dette være standardnivået. Bestemmelsen er et uttrykk for prinsippet om innsamling av minst mulig personopplysninger og prinsippet om formålsbegrensning, som det ble redegjort for under punkt 4.2.2.

I utgangspunktet vil vurderingen av hvilke personopplysninger som er nødvendig å behandle for hvert formål måtte gjennomføres av den behandlingsansvarlige selv. Den behandlingsansvarlig bør kunne dokumentere at dette gjennomføres, for eksempel ved å vise til interne retningslinjer.[101]

Forpliktelsen gjelder som nevnt både mengden personopplysninger, omfanget av behandling av disse personopplysningene, lagringsperiode og tilgjengelighet. Dette innebærer at den behandlingsansvarlige ikke bare må ta stilling til hva slags type personopplysninger som er nødvendig å behandle for hvert formål. Den behandlingsansvarlige må i tillegg ta stilling til hva som er nødvendig i tilknytning til mengde, omfang, lagring og tilgjengelighet. For eksempel

[100] Schartum (2016) s. 155

[101] Se fortalen avsnitt 78 og avsnitt 82.

kan det innebære at en behandlingsansvarlig som bruker IP-adresser for å forhindre svindel, uten å krenke sin forpliktelse etter bestemmelsen kan lagre disse i 30 dager, men ikke i tre år. Et annet eksempel er at en behandlingsansvarlig som tilbyr værvarseltjenester til den registrerte kanskje må nøye seg med å bruke IP-adresser, og ikke lokasjonsdata, fordi lokasjonsdata vil innebære mer informasjon enn det som er nødvendig for å levere tjenesten.[102]

4.3.4 «Not made accessible to an indefinite number of natural persons»

Etter artikkel 25 annet ledd siste punktum skal tiltak særlig sikre at personopplysninger som standard ikke gjøres tilgjengelig for et ubestemt antall fysiske personer.

At personopplysninger ikke skal gjøres *tilgjengelig* («*not made accessible*») innebærer at den behandlingsansvarlige plikter å ha kontroll over hvilke fysiske personer som har adgang til personopplysninger. Dette innebærer at den behandlingsansvarlige må sikre begrenset teknisk, organisatorisk og fysisk tilgjengelighet. Teknisk tilgjengelighet kan for eksempel være tilgang til databaser. Det er naturlig å anse dette kravet som en konfidensialitetsforpliktelse. De behandlingsansvarlige kan sikre denne kontrollen enten ved tekniske eller organisatoriske tiltak, for eksempel i form av administratorsperrer eller ved retningslinjer og internkontroll. Tekniske og organisatoriske tiltak er redegjort for under punkt 4.2.4.

Et spørsmål er hva det innebærer at personopplysninger ikke skal være tilgjengelig *for et ubestemt antall personer* («*to an indefinite number of natural persons*»). Bruken av uttrykket «*indefinite number*» innebærer prinsipielt sett ikke at ikke personopplysninger kan gjøres tilgjengelig for et stort antall personer, så lenge dette er avgrenset. Bestemmelsen stiller derfor ikke krav til at tilgjengelighet for fysiske personer skal være begrenset til det som er nødvendig eller hensiktsmessig. Det er med andre ord ikke et krav til streng kontroll, utover at den behandlingsansvarlige faktisk må ha kontroll.

I det første forslaget fra Europaparlamentet var det også inkludert i annet ledd siste punktum et krav om at de registrerte skulle ha mulighet til å kontrollere spredningen av sine personopplysninger, men dette ble ikke inkludert i den endelige versjonen.[103] Et slikt krav ville i tilfelle ha innebåret en strengere plikt for den behandlingsansvarlige enn det som nå er tilfellet.

---

[102] Forbrukerrådet (2016) s. 34

[103] Europaparlamentet (2014) artikkel 23 annet ledd

4.3.5 Forholdet mellom første og annet ledd i artikkel 25

Første ledd innebærer en generell plikt til innebygd personvern ved implementering av tekniske og organisatoriske tiltak. Annet ledd utgjør en spesifisering av denne plikten, ettersom annet ledd setter opp et minstekrav til hvilken *effekt* tiltak som den behandlingsansvarlige implementerer *skal* ha. På mange måter utgjør annet ledd en klarere plikt enn første ledd, fordi annet ledd stiller opp en konkret standard. Bygrave er inne på denne tankegangen og omtaler annet ledd som en «*seemingly unqualified duty*», i motsetning til første ledd som er «*qualified by a long list of contextual factors*».[104]

På bakgrunn av dette er det ikke helt usannsynlig at tilsynsmyndigheter i større grad vil pålegge behandlingsansvarlige overtredelsesgebyr for brudd på annet ledd enn for brudd på første ledd, fordi det er lettere å sanksjonere behandlingsansvarlige for brudd på konkrete krav enn for brudd på generelle forpliktelser.

4.3.6 Eksempel: «Do not track»

«Do not track»-innstillinger i nettleseren er et eksempel på teknisk tiltak som sikrer at bare nødvendige personopplysninger blir behandlet som standard. «Do not track» er et signal nettleseren kan sende til et nettsted med anmodning om ikke å spore brukeren. I utgangspunktet vil det være opp til nettstedet om det vil respektere denne anmodningen. I de fleste nettlesere må brukeren selv gå inn i personverninnstillingene og endre disse for at nettleseren skal sende et slikt signal. Det har imidlertid blitt gjort forsøk på å sette standardinnstillingene til at sporing som utgangspunkt ikke skal skje, men dette forsøket møtte sterk motstand fra store aktører og ble avsluttet.[105]

---

[104] Bygrave (2017) s. 18

[105] https://blogs.microsoft.com/on-the-issues/2015/04/03/an-update-on-microsofts-approach-to-do-not-track/#sm.0000scnjk01b1sdlrxktk11v6nprv

4.4 Artikkel 25 tredje ledd – Sertifiseringsmekanismer

Artikkel 25 tredje ledd gjelder sertifiseringsmekanismer og lyder som følger: «*An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements set out in paragraphs 1 and 2 of this Article*».

Bestemmelsen går ut på at den behandlingsansvarlige kan benytte godkjente sertifiseringsmekanismer som et element for å dokumentere etterlevelse av første og annet ledd under henvisning til artikkel 42. At sertifiseringsmekanismer kan benyttes som et element, innebærer at bruk av slike ikke alene kan oppfylle kravet etter første og annet ledd. Den behandlingsansvarlige må i tillegg kunne vise til andre tiltak som nevnt i første og andre ledd.

Tredje ledd henviser til artikkel 42. Artikkel 42 gjelder sertifisering og etter første ledd er det medlemsstatene, tilsynsmyndigheter, EDPB og Kommisjonen som skal oppfordre til etablering av sertifiseringsmekanismer. Det fremgår av tredje ledd at sertifisering skal være frivillig og tilgjengelig gjennom en åpen prosess. Sertifisering i seg selv vil ikke redusere den behandlingsansvarliges forpliktelser etter forordningen, jf. artikkel 42 fjerde ledd. Dette harmoniserer med ordlyden i artikkel 25 tredje ledd om at sertifiseringsmekanismer kan være et «element».

På dette tidspunktet foreligger det ingen sertifiseringsmekanismer for artikkel 25. Det er derfor vanskelig å si noe om hvilken betydning slike vil ha i fremtiden.

5 Bransjenormers betydning for artikkel 25

Artikkel 40 åpner for at bransjenormer kan benyttes for å klargjøre forpliktelsene etter blant annet artikkel 25. Artikkel 40 lyder slik: «*Associations and other bodies representing categories of controllers or processors may prepare codes of conduct (…) for the purpose of specifying the application of this Regulation, such as with regard to (…) the measures and procedures referred to in (…) Article 25*».

Bestemmelsen legger til grunn at bransjeorganisasjoner og andre organer som representerer grupper av behandlingsansvarlige eller databehandlere kan utarbeide bransjenormer («*codes of conduct*») for å klargjøre forpliktelsene etter artikkel 25. Bransjenormer kan være nyttige verktøy fordi de er tilpasset til den enkelte bransje, slik at de kan angi mer spesifiserte krav enn det som fremgår av bestemmelsen. Dette vil i stor grad kunne avhjelpe problemene med at bestemmelsen er vagt utformet, se punkt 4.2.4.1. På grunnlag av dette er det grunn til å håpe på utvikling av bransjenormer for artikkel 25 i løpet av de nærmeste årene.

Bransjenormer er omtalt på flere punkter i fortalen. I fortalen avsnitt 77 oppfordres det blant annet til at bransjeorganisasjoner skal utforme normer for implementering av tiltak og dokumentering av etterlevelse til hjelp for behandlingsansvarlige og databehandlere. Bransjenormene bør særlig gjelde identifisering og vurdering av risiko knyttet til behandling av personopplysninger, samt identifisering av hva som er «best practise» for å redusere denne risikoen.

I fortalen avsnitt 98 oppfordres det til at bransjeorganisasjoner vedtar bransjenormer for å legge til rette for en effektiv anvendelse av forordningen. Videre fremgår det av fortalen avsnitt 99 at bransjeorganisasjonene skal sørge for å få innspill fra berørte parter ved utarbeidelsen av bransjenormer. Dette inkluderer innspill fra de registrerte i de tilfeller hvor dette er gjennomførbart. Bransjeorganisasjonene bør ta hensyn til disse innspillene.

Av artikkel 41 første ledd, jf. artikkel 40 fjerde ledd fremgår det at et uavhengig organ kan utnevnes til å overvåke og håndheve bransjenormer hvor dette organet har tilstrekkelig ekspertise på området. Tanken bak dette er at man ser for seg at bransjene selv er bedre egnet til å håndheve bransjenormer enn det tilsynsmyndighetene er. Denne kompetansetildelingen er ny av forordningen. Etter direktivet var det bare tilsynsmyndighetene og i noen tilfeller Artikkel 29-gruppen som hadde myndighet til å håndheve bransjenormer.[106]

[106] Personverndirektivet artikkel 27 annet og tredje ledd

Noen bransjeorganisasjoner har allerede startet arbeidet med utvikling av disse bransjenormene. Dette gjelder for eksempel CISPE, som er den europeiske sammenslutningen av skytjenesteleverandører.[107]

[107] Pressemelding fra CISPE, 14. februar 2017.

6 Administrative bøter ved overtredelser av artikkel 25

Overtredelse av forpliktelser etter forordningen kan straffes med bøter etter artikkel 83. I personverndirektivet har det vært opp til den enkelte medlemsstat å fastsette maksimalt bøtenivå, noe som har ført til ujevnt nivå og ujevn praksis mellom medlemsstatene.[108] I forordningen harmoniseres bøtenivået, samtidig som det åpnes for mye strengere sanksjoner ved at bøtenivå heves.[109]

6.1 Generelle vilkår for ileggelse av overtredelsesgebyr

Etter artikkel 83 første ledd skal tilsynsmyndighetene i det enkelte land sikre at ileggelsen av bøter er effektiv, står i rimelig forhold til overtredelsen og har preventiv virkning. Bøter kan gis ved overtredelse av bestemmelsene som nevnt i artikkel 83 fjerde og femte ledd. Ved brudd på flere bestemmelser, skal det totale bøtenivået ikke overstige det maksimale bøtenivået for den groveste overtredelsen, jf. artikkel 83 tredje ledd.

Det fremgår av artikkel 83 annet ledd hvilke hensyn som kan tas ved avgjørelsen av om det skal ilegges bøter og eventuelt hvor store disse bøtene skal være. Blant annet skal det tas hensyn til overtredelsens karakter, alvor og varighet, hvorvidt overtredelsen ble begått forsettlig eller uaktsomt og den behandlingsansvarliges eller databehandlers grad av ansvar med hensyn til tekniske og organisatoriske tiltak som er gjennomført i henhold til artikkel 25 og 32. Forordningen opererer med to maksnivåer for bøter på henholdsvis 20 000 000 EUR og 10 000 000 EUR. For virksomheter kan overtredelse straffes med henholdsvis 4 % eller 2 % av årlig global omsetning, hvis dette beløpet er høyere.

6.2 Overtredelse av artikkel 25

Overtredelse av behandlingsansvarliges forpliktelser etter artikkel 25 kan sanksjoneres etter artikkel 83 fjerde ledd bokstav a. Overtredelse kan straffes med administrative bøter på opp til 10 000 000 EUR, eller 2 % av årlig global omsetning for virksomheter, hvis dette beløpet er høyere. Det er med andre ord snakk om at det kan ilegges svært strenge økonomiske sanksjoner ved overtredelse, noe som burde virke som et sterkt økonomisk incentiv for behandlingsansvarlig til å overholde sine forpliktelser. Hvorvidt dette vil være tilfellet i praksis vil bare tiden kunne vise.

---

[108] Blume (2015), pkt. 8.4

[109] Se blant annet fortalen avsnitt 11

7 Andre bestemmelser som kan ses i sammenheng med artikkel 25

Flere bestemmelser i personvernforordningen har likhetstrekk med, eller på annet vis en form for tilknytning til, artikkel 25. I dette kapittelet vil jeg kort gjennomgå noen av disse, samt se på hvordan innebygd personvern er kommet til utrykk i forslaget til ny kommunikasjonsvernforordning.

7.1 Artikkel 32 – Behandlingssikkerhet

Artikkel 32 gjelder behandlingsansvarlig og databehandlers ansvar for å implementere tekniske og organisatoriske tiltak for sikkerhet ved behandlingen av personopplysninger *(«security of processing»).* Bestemmelsen viderefører artikkel 17 i personverndirektivet.[110]

Det er nær sammenheng mellom artikkel 25 og artikkel 32. For eksempel har ordlyden i artikkel 32 store likhetstrekk med ordlyden i artikkel 25. Flere av de sentrale elementene i begge bestemmelser er de samme, herunder kravet til implementering av tekniske og organisatoriske tiltak og de vurderingsmomentene som skal legges til grunn. Av hensyn til intern sammenheng i forordningen bør man kunne legge til grunn at innholdet av begrepet «tekniske og organisatoriske tiltak» er det samme for begge bestemmelsene. Praksis og uttalelser i tilknytning til artikkel 32 vil derfor for disse begrepene kunne være relevant ved tolkningen av artikkel 25.

Ettersom kjernen i artikkel 32 er kjent fra personverndirektivet, er det mulig at de behandlingsansvarlige raskere vil tilpasse seg denne. I så fall kan man håpe på at likhetene mellom artikkel 25 og artikkel 32 vil gjøre at artikkel 25 også blir dratt med på lasset.

7.2 Artikkel 35 – Konsekvensanalyser for personvern

Etter artikkel 35 skal behandlingsansvarlig i visse tilfeller[111] gjennomføre konsekvensanalyser for beskyttelse av personopplysninger, en såkalt «*data protection impact analysis*».

Konsekvensanalysen skal gjennomføres før behandling settes i gang, jf. første ledd, og eventuelle mulige brudd på forordningen vil derfor kunne oppdages før behandlingen i det hele tatt har startet. I tillegg inneholder artikkel 35 rimelig klare krav til hva en konsekvensanalyse skal inneholde. Disse to forholdene gjør at konsekvensanalyser kan være et effektivt organisatorisk tiltak som del av oppfyllelse av forpliktelsen etter artikkel 25.

---

[110] Se punkt 3.2.2

[111] Ved ny behandling hvor denne utgjør en høy risiko, og særlig ved bruk av ny teknologi, jf. artikkel 35 første ledd.

I praksis blir konsekvensanalyser ofte knyttet tett opp til kravet om innebygd personvern etter artikkel 25. For eksempel viser Datatilsynet til konsekvensanalyser som første steg i sin sjekkliste for innebygd personvern.[112]

7.3 Innebygd personvern i Draft E-privacy Regulation

Den 10. januar 2017 ble forslaget til ny kommunikasjonsvernforordning (e-Privacy regulation) publisert.[113] Forslaget inneholder ikke noe generelt krav til innebygd personvern slik personvernforordningen gjør, men man finner spor av en slik tankegang også der.

Det fremgår blant annet av den foreslåtte artikkel 10 at tilbydere av programvare som tillater elektronisk kommunikasjon, som for eksempel nettlesere, må hjelpe sluttbrukere med å gjøre effektive valg av personverninnstillinger.[114] Dette skal gjøres blant annet ved å tilby muligheten for å hindre tredjeparter fra å lagre informasjon på brukerens utstyr. Den foreslåtte bestemmelsen stiller krav til hvilke tekniske løsninger tilbydere må sørge for å ha implementert i sitt produkt og kan på den måten anses som en mildere variant av forpliktelsen etter artikkel 25 i personvernforordningen.

På samme måte som under arbeidet med personvernforordningen er store lobbyorganisasjoner allerede på banen og de stiller seg kritiske til behovet for en ny kommunikasjonsvernforordning generelt og artikkel 10 i forslaget spesielt. Blant annet har bransjeorganisasjonen News Media Europe argumentert for at en opt in-funksjon i nettleseren ikke vil være i brukernes interesse.[115] Det blir derfor interessant å se hvordan den endelige versjonen av forordningen eventuelt ender opp med å se ut.

---

112 https://www.datatilsynet.no/globalassets/global/04_skjema_maler/sjekkliste-for-innebygd-personvern.pdf

113 COM (2017) 10 final

114 COM (2017) 10 final punkt 5.2.

115 http://www.newsmediaeurope.eu/issues/position-paper-regulation-on-privacy-and-electronic-communications-eprivacy-regulation/

8 Kritikk av artikkel 25

Artikkel 25 har vært gjenstand for en god del kritikk i litteraturen siden det første forslaget fra Kommisjonen ble offentliggjort i 2012. I dette kapittelet vil jeg ta for meg hovedpunktene i denne kritikken.

8.1 Kritikk av ordlyden

Når det gjelder kritikken av ordlyden i artikkel 25, må det skilles mellom de ulike leddene i bestemmelsen. Det er primært artikkel 25 første ledd som er gjenstand for kritikk. Dette skyldes i hovedsak at det er første ledd det har blitt skrevet mest om. Første ledd skiller seg likevel markant fra de øvrige leddene ved at den rent faktisk er mer komplisert å forholde seg til, både på grunn av hvordan selve bestemmelsen er bygget opp og fordi den generelt er vag og uklar.[116]

Det første forholdet som gjør at artikkel 25 fremstår som uklar er den språklige *vagheten*. Vagheten i første ledd skyldes i stor grad at bestemmelsen er generelt utformet, fordi den er ment å treffe et stort antall virksomheter av ulike størrelse i ulike bransjer. Utformingen innebærer på den ene side at bestemmelsen vil være effektiv og relevant i lang tid, men på den annen side fører det til at bestemmelsen mister presisjon og klarhet.

Det andre forholdet som gjør at første ledd fremstår som uklar er selve *setningsoppbygningen*.[117] Første ledd består av én lang og fragmentert setning. For det første gjør lengden at bestemmelsen er vanskelig å skjønne uten flere gjennomlesninger. Dette er likevel bare et pedagogisk problem. Et større problem er at det er uklart hvilke deler av bestemmelsen som forholder seg til hverandre. Det er for eksempel ikke gitt hvilken del av bestemmelsen «*in an effective manner*» peker tilbake på, ettersom dette både kan gjelde implementering av tiltak og implementering av personvernprinsippene. Muligens peker det på begge, men dette kunne med fordel vært klarer formulert. Dersom første ledd hadde vært delt opp i flere setninger, ville det gjort bestemmelsen mye klarere, både fra en juridisk og en pedagogisk synsvinkel.

Et tredje forhold som blir kritisert er vurderingsmomentene og mangelen på veiledning knyttet til hvordan de ulike vurderingsmomentene skal tolkes og prioriteres i forhold til hverandre. Det er i hovedsak Tsormpatzoudi m.fl. som har fremmet denne kritikken. Kritikken gjaldt forslaget til artikkel 25 slik den lød opprinnelig, men den problematikken de peker på er den samme i den endelige lovteksten. De mener at vurderingsmomentene i bestemmelsen roter til

---

[116] Bygrave (2017) s. 19

[117] Etter hva jeg har sett har dette forholdet ikke blitt tatt opp i litteraturen, men jeg mener at det er et sentralt problem med artikkel 25 og velger derfor å inkludere det her.

og gjør den mindre håndgripelig, særlig på grunn av mangel på veiledning i forhold til hvordan de ulike vurderingsmomentene skal prioriteres i forhold til hverandre. De konkluderer deretter med at dette vil kunne komme til å bli et problem for implementering av bestemmelsen i praksis.[118]

8.1.1 Hvorfor er dette et problem?

Kritikken mot uklarheten i artikkel 25 er særlig problematisk av to grunner: for det første fordi de behandlingsansvarlige som forpliktes etter bestemmelsen ikke primært er personer med juridisk kompetanse som er vant til å forholde seg til lovtekst. Dette punktet blir fremhevet av Bygrave som uttaler at «*the legislative decree falls short of communicating clearly and directly with the engineering community*». Videre påpeker han at «*[t]he complexity and vagueness of its legalese ends up being akin to a form of encryption vis- à-vis persons who are without formal legal qualifications and expertise in data privacy law*».[119] Tsormpatzoudi m.fl. er også inne på dette. De poengterer at forskjellige fagdisipliner opererer med ulikt vokabular og ulike verdisett, og at uklarhet kan føre til det de omtaler som «*lack of cross-disciplinary understanding*».[120]

For det annet er uklarheten problematisk fordi bestemmelsen på grunn av den generelle utvidelsen av det geografiske virkeområdet for forordningen vil omfatte et stort antall aktører utenfor EU/EØS. Disse vil i utgangspunktet ikke nødvendigvis har noe forhold til den europeiske personverntradisjonen- eller lovgivningen. Da er det ekstra problematisk at bestemmelsen er vag og komplisert, fordi dette gjør innføringen enda vanskeligere.

Helt kritisk er den overnevnte problematikken likevel ikke. De forhold det er redegjort for under punkt 8.1 kan i stor grad avhjelpes med retningslinjer fra Artikkel 29-gruppen, EDPB, nasjonale tilsynsmyndigheter og bransjenormer, men å få på plass dette vil sannsynligvis ta lang tid og det er neppe på plass innen 25. mai 2018. Dessuten er det et prinsipielt problem at lovtekst er vag og komplisert, særlig når den er ment å ramme bredt og særlig når overtredelse av den kan sanksjoneres så hardt som overtredelser av artikkel 25 kan sanksjoneres.

---

118 Tsormpatzoudi m. fl. (2015) s. 203-204.

119 Bygrave (2017) s. 20

120 Tsormpatzoudi m. fl.(2015) s. 205

8.2 Kritikk av valget av den behandlingsansvarlige som det primære pliktsubjekt

Artikkel 25 har videre blitt kritisert fra flere hold for at den bare direkte forplikter den behandlingsansvarlige. Denne kritikken har jeg så vidt vært inne på flere steder i avhandlingen. Kritikken går primært ut på at den behandlingsansvarlige i mange tilfeller ikke vil være den som er i best posisjon til å ta avgjørelser om utforming av behandlingssystemer, selv om dette ser ut til å være forutsatt i artikkel 25.

Bygrave er blant de som har vært kritiske og han har blant annet uttalt at «*the traction of GDPR Article 25 on information systems development might well be hindered by its limited reach. Article 25 measures are primarily imposed on data controllers only (…)we cannot assume that basic design decisions in information systems development will be exclusively or predominantly taken by entities acting in a controller capacity*».[121] Han peker videre på at det tidspunktet som artikkel 25 stiller opp som tidspunktet når implementering av tiltak må ha funnet sted, forsterker problematikken i tilknytning til behandlingsansvarlig, fordi dette tidspunktet ikke nødvendigvis er det tidspunktet hvor behandlingsinnretningen faktisk blir utformet og produsert. Dette undergraver målet om å integrere personvern inn i behandlingen.

Schartum er også kritisk til at bestemmelsen bare omfatter de behandlingsansvarlige og uttaler at «*[i]n a perfect world including willingness among controllers to attain full compliance with privacy regulation supported by privacy-designed systems, there is little need for other perspectives. However, because the world of privacy law compliance is far from perfect, and because there is little reason to believe that it will ever be perfect, privacy by design efforts should encompass more than controllers' systems*».[122]

Man kan altså for det første ikke anta at den behandlingsansvarlige er inkludert på tidspunktet hvor sentrale avgjørelser i tilknytning til behandlingen blir tatt og man kan heller ikke anta at den behandlingsansvarlige nødvendigvis er i posisjon til å ta slike avgjørelser uansett. Av den grunn burde også andre aktører vært forpliktet etter bestemmelsen.

Som jeg var inne på under punkt 4.1.3 blir problematikken i tilknytning til behandlingsansvarlig noe avhjulpet ved at fortalen avsnitt 78 inneholder en oppfordring til produsenter om å ta hensyn til personvernforpliktelsene til de behandlingsansvarlige. Spørsmålet er om denne strategien vil ha gjennomslag i praksis. Bygrave på sin side er i hvert fall skeptisk til dette og ut-

[121] Bygrave (2017) s. 18-19

[122] Schartum (2016) s. 170

taler at *«[t]he efficacy of this strategy is, at the very least, questionable»*.[123] I tilknytning til dette kan erfaringene med DNT og forslaget i draft e-Privacy regulation illustrere ett av de potensielle problemene for artikkel 25; dersom store og mektige produsenter, som for eksempel Google, setter seg på bakbeina og nekter å følge opp bestemmelsen fordi den strider mot deres interesser, kan artikkel 25 komme til å slite med å få det momentum som er nødvendig for at den skal få gjennomslag.[124]

[123] Bygrave (2017) s. 18-19

[124] Bygrave (2017) s. 11

9 Avsluttende bemerkninger

Regelen i artikkel 25 er ny i europeisk personvernlovgivning og har ennå ikke trådt i kraft. På nåværende tidspunkt kan man derfor ikke gjøre annet enn å spekulere i hvordan den kommer til å utvikle seg i fremtiden. Basert på kritikken som er fremsatt mot bestemmelsen, er det grunn til å håpe på at Artikkel 29-gruppen, European Data Protection Board og de ulike tilsynsmyndighetene raskt kommer på banen med uttalelser og retningslinjer om hvordan artikkel 25 skal tolkes og implementeres. Tilsvarende er det grunn til å håpe at bransjene selv utvikler klare bransjenormer som forenkler implementeringen av bestemmelsen for den enkelte virksomhet. Dessverre er det ikke gitt at artikkel 25 er blant de bestemmelsene i forordningen hvor avklaring prioriteres av disse aktørene frem mot 25. mai 2018. Andre viktige bestemmelser i forordningen ser ut til å stille foran i køen, i hvert fall fra Artikkel 29-gruppen sin side.[125]

Et annet spørsmål er om incentivene for implementering av artikkel 25 er gode nok til at de behandlingsansvarlige vil prioritere oppgaven. Bygrave er ikke overbevist om det.[126] For mange behandlingsansvarlige vil det kreve et omfattende arbeid å få på plass de nødvendige strukturer for å oppfylle forpliktelsene etter bestemmelsen. Det vil blant annet kunne kreve omlegging av interne prosesser, noe som er både tid- og kostnadskrevende. Det er ikke gitt at de økonomiske incentivene i form av muligheten for sanksjoner mot behandlingsansvarlige som ikke oppfyller bestemmelsen er tilstrekkelig, selv om det potensielt er snakk om store summer.

Artikkel 25 har potensiale til å være en av de viktigste bestemmelsene i personvernforordningen, men spørsmålet er om den er for vag og for generelt til å ha noen praktisk effekt i det hele tatt. Hvorvidt artikkel 25 i fremtiden vil få gjennomslag etter lovgivers intensjon eller bli en harmløs papirtiger, vil bare tiden kunne vise.

---

125 https://www.datatilsynet.no/Regelverk/Internasjonalt/Uttalelser-fra-Artikkel-29-gruppen/nar-far-vi-vite-med-om-nye-regler-fra-eu/

126 Bygrave (2017) s. 19

LITTERATURLISTE

Lover

- REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

- DIRECTIVE 95/46/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

- Convention for the Protection of Human Rights and Fundamental Freedoms

- Charter of Fundamental Rights of the European Union

Rettspraksis

European Court of Human Rights

- Case of I v. FINLAND (Judgement Application no. 20511/03)

Court of Justice of the European Union

- Case C-283/81 – Srl CILFIT and Lanificio di Gavardo SpA v Ministry of Health, judgment of 6 October 1982

- Case C-70/10 – Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM), judgment of 24 November 2011

- Case C-360/10 – Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (Sabam) v Netlog NV, judgment of the Court (Third Chamber) of 16 February 2012

- Case C-131/12 – Google Spain v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, judgment of 13 May 2014.

- C-582/14 – Patrick Breyer v Bundesrepublik Deutschland, judgment of the Court (Second Chamber) of 19 October 2016

Bøker

Bygrave, Lee A.

- Data privacy law: An international perspective.
  Oxford: Oxford University Press, 2014

Sejersted, Fredrik, Finn Arnesen, Ole-Andreas Rognstad og Olav Kolstad

- EØS-rett
  Universitetsforlaget, 2011

Artikler

Blume, Peter

- «Persondatabeskyttelse i stormfyldt hav» (2015)
  Tidsskrift for Rettsvitenskap 02/2015 s. 222-246

Bygrave, Lee A.

- «Hardwiring Privacy» (2017)
  University of Oslo Faculty of Law Research Paper No. 2017-02 (tilgjengelig på SSRN)

Cavoukian, Ann

- «Privacy by design [leading edge]» (2012a)
  IEEE Technology and Society Magazine 31.4 18-19

- «A Regulator's Perspective on Privacy By Design» (2012b)
  http://www.futureofprivacy.org/privacy-papers-2012. (sist lastet ned 16.4.2017)

- «Privacy by Design - The 7 Foundational Principles» (2013)
  https://www.datatilsynet.no/globalassets/global/english/7foundationalprinciples_anncavoukian.pdf (sist lastet ned 14.4.2017)

Hildebrandt, Mireille, and Laura Tielemans

- «Data protection by design and technology neutral law» (2013)
  Computer Law & Security Review 29.5 509-521

Krebs, David

- «'Privacy by Design': Nice-to-Have or a Necessary Principle of Data Protection Law?» *JIPITEC, Vol. 4*, 2013 (2013)

Koops, Bert-Jaap and Ronald Leenes

- «Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law» (2014)
  International Review of Law, Computers & Technology 28.2 159-171

Kosta, Eleni, and Kees Stuurman

- «Technical Standards and the Draft General Data Protection Regulation» (2016)
  P. Delimatsis (ed), The Law, Economics and Politics of International Standardization, Cambridge University Press, Forthcoming (tilgjengelig på SSRN)

Narayanan, Arvind, and Vitaly Shmatikov

- «How to break anonymity of the netflix prize dataset» (2006)
  2008 IEEE Symposium on Security and Privacy
  arXiv preprint cs/0610105

Schartum, Dag Wiese

- «Making privacy by design operative» (2016)
  International Journal of Law and Information Technology 24.2 151-175

Tsormpatzoudi, Pagona, Bettina Berendt and Fanny Coudert

- «Privacy by Design: From Research and Policy to Practice–the Challenge of Multi-disciplinarity» (2015)
  Annual Privacy Forum. Springer International Publishing

Dokumenter

The European Commission

- IP/12/46 - Commission proposes a comprehensive reform of data protection rules to increase users' control of their data and to cut costs for businesses

- Procedure 2012/0011/COD - Proposal for a regulation of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)

- SEC(2012) 72 final - Impact assessment

- COM/2007/0228 final - Communication from the Commission to the European Parliament and the Council on Promoting Data Protection by Privacy Enhancing Technologies (PETs)

- COM(2010) 609 final - Communication from the commission to the European parliament, the council, the economic and social committee and the committee of the regions, A comprehensive approach on personal data protection in the European Union

- COM (2017) 10 final - Proposal for a regulation of the european parliament and of the council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)

Court of Justice of the European Union

- Opinion 2/13 - Accession of the European Union to the European Convention for the Protection of Human Rights and Fundamental Freedoms — Compatibility of the draft agreement with the EU and FEU Treaties

The European Parliament

- European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)
  (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) (Ordinary legislative procedure: first reading)

Article 29 Data Protection Working Party

- 02356/09/EN, WP 168, The Future of Privacy, Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data, adopted on 1 December 2009

- Opinion 08/2012 providing further input on the data protection reform discussions

European Union Agency for Network and Information Security (ENISA)

- Privacy and Data Protection by Design – from policy to engineering, 2015

PReparing Industry to Privacy-by-design by supporting its Application in REsearch (PRIPARE)

- Deliverable D5.1 State-of-play: Current Practices and Solutions, 2014

Regjeringen

- EØS-notat om Personvernforordningen av 23.4.2017 https://www.regjeringen.no/no/sub/eos-notatbasen/notatene/2014/aug/forslag-til-personvernforordning/id2433856/ (sist lastet ned 20.4.2017)

Forbrukerrådet

- Appfail – Threats to consumers in mobile apps (2016)

Nettsider

Europalov.no

- http://europalov.no/rettsakt/personvernforordningen-om-behandling-av-persondata/id-5275

Datatilsynet

- https://www.datatilsynet.no/Teknologi/Innebygd-personvern/

- https://www.datatilsynet.no/Regelverk/Internasjonalt/Uttalelser-fra-Artikkel-29-gruppen/nar-far-vi-vite-med-om-nye-regler-fra-eu/

CISPE

- Pressemelding fra 14. februar 2017 https://cispe.cloud/wp-content/uploads/2017/02/CISPE-PR3-FINAL.pdf

Digi.no

- https://www.digi.no/artikler/hardt-skyts-mot-skjerpet-personvern/204197

WC3

- https://www.w3.org/TR/tracking-dnt/

Annet

Bygrave, Lee A.

- «*Person(opplysnings)vernforordningens bestemmelser om innebygget person(opplysnings)vern*» Personvernkonferansen 2016 http://www.jus.uio.no/ifp/om/organisasjon/seri/arrangementer/2016/bygrave_pvkonferanse_021216.pdf

Olsen, Thomas

- «*Sanksjoner ved overtredelse av personvernforordningen*» Personvernkonferansen 2016. http://www.jus.uio.no/ifp/om/organisasjon/seri/arrangementer/2016/thomas-olsen---sanksjoner-gdpr.pdf

News Media Europe

- http://www.newsmediaeurope.eu/issues/position-paper-regulation-on-privacy-and-electronic-communications-eprivacy-regulation/