POL-INTEL

er politiets behandling af personoplysninger i overensstemmelse med EU's retshåndhævelsesdirektiv?[1]

Tanja Kammersgaard Christensen, adjunkt, ph.d., Aalborg Universitet

Abstract

Since the adoption of Section 2a of the Danish Police Act in 2017, the police have been able to conduct cross-sectional information analyses in IT systems designed for this purpose, and thus process personal data for purposes other than those for which they were originally collected. This is regulated by the Executive Order on Cross-sectional Information Analyses. According to this executive order, the police shall use the POL-INTEL system to perform the analyses. The article discusses the police's use of personal data for new purposes based on the Law Enforcement Directive, the Danish Law Enforcement Act, and relevant case law from the European Court of Justice. It assesses whether the regulation of POL-INTEL in the Executive Order on Cross-sectional Information Analyses adheres to the principles of purpose limitation, data minimisation and legality, or whether there is a need for changes to the Danish regulation.

Keywords:

POL-INTEL, police cross-case analyses, law enforcement directive, purpose limitation, data minimisation, data protection

POL-INTEL, politiets tværgående analyser, retshåndhævelsesdirektivet, formålsbestemthed, dataminimering, databeskyttelse

1. Indledning

I 2017 fik dansk politi en ny analyseplatform kaldet POL-INTEL. POL-INTEL skulle gøre det nemmere for dansk politi, at søge og sammenstille alle de informationer, som politiet allerede havde i flere forskellige systemer. Med POL-INTEL blev det muligt for politiet at søge oplysninger ét sted, systemet sammenstiller flere informationer og hjælper med at skabe et overblik, hvilket blev ansat for nødvendigt i en tid, hvor politiet bliver "oversvømmet" med informationer. (Bjørnholdt, 22. december 2016) Indkøbet af POL-INTEL skete efter terrorhændelsen i København i februar 2015, hvor det blev politisk

1. Title in English: POL-INTEL - Is the police processing of personal data in accordance with the Law Enforcement Directive?

bestemt, at dansk politi skulle moderniseres og effektiviseres, herunder ved implementering af en analysebaseret politiindsats, der skulle sikre politiet bedre redskaber til at analysere, forudse, efterforske m.m. (Justitsministeriet, 25. november 2016) På den baggrund blev der igangsat et projekt til anskaffelse og implementering af analyseplatformen POL-INTEL, der giver politiet mulighed for at bearbejde og analysere store datamængder (L 171 lovforslag til ændring af politiloven, 2017, pp. 3-5). Anvendelsen af POL-INTEL blev udrullet i dansk politi i løbet af 2017 og 2018, og er i 2019 blevet vurderet af politiet til at skabe en stor merværdi for dansk politi (Digitaliseringsstyrelsen, 18. november 2019, p. 5)

I forbindelse med indkøbet af POL-INTEL udtalte den daværende Justitsminister, at: "*Den overordnede ambition for projektet er at gøre relevante datakilder så let tilgængelige som muligt for politiets medarbejdere under fuld overholdelse af de persondataretlige regler, sådan at den enkelte medarbejder populært sagt "ved, hvad politiet ved".*" (Justitsministeriet, 25. november 2016, p. 2) Det var således ambitionen, ved indkøbet af POL-INTEL, at sikre at systemerne overholdt databeskyttelsesretten. Siden anvendelsen af POL-INTEL begyndte i 2017, er der dog sket en del på området for politiets behandling af personoplysninger, idet EU's retshåndhævelsesdirektiv (Direktiv (EU) 2016/680, 2016) er trådt i kraft, hvorfor området omkring politiets anvendelse af personoplysninger er blevet mere reguleret end det var, ved indkøbet. Det betyder, at ambitionen om fuld overholdelse af de persondataretlige regler, kan blive vanskeligere for politiet at opfylde. Der er i hvert fald ingen tvivl om, at systemer som POL-INTEL, hvor der indsamles og behandles personoplysninger, kan have databeskyttelsesmæssige udfordringer. (Se også herom (Møller, 3. november 2023))

De databeskyttelsesretlige problemer med systemer som POL-INTEL er bl.a. set i Tyskland, hvor den tyske forfatningsdomstol i februar 2023, fandt at den lovgivning, der hjemlede politiets automatiske dataanalyser, er forfatningsstridig, med henvisning til retten til respekt for privatliv i den tyske forfatningslov (Grundgesetz, art. 2(1), 2023). Domstolen lagde vægt på manglende proportionalitet i lovgivningen, herunder særligt henset til indgrebets intensitet i forhold til de kriminalitetsformer, hvor politiet kunne anvende systemerne. Domstolen fandt, at systemerne kunne være værdifulde for politiet, men bestemte at systemet alene måtte anvendes under visse betingelser, herunder på grundlag af en konkret mistanke om en alvorlig strafbar handling, og at visse personoplysninger ikke måtte indgå i analysen, herunder bl.a. indhentede teletrafikdata (Grundgesetz, 2023).

Efter dommen fra den tyske forfatningsdomstol blev den danske justitsminister af folketingets retsudvalg spurgt, om dommen gav anledning til nye overvejelser vedrørende brug af POL-INTEL i Danmark. Justitsministeren svarede med henvisning til forarbejderne til politilovens § 2a, særligt

bemærkningerne i forslaget vedrørende forholdet til den Europæiske menneskerettighedskonvention (herefter EMRK) art. 8, at den tyske dom ikke giver anledning til nye overvejelser. ministeren forholdt sig ikke nærmere til dommen og eventuelle forskelle og ligheder mellem tysk og dansk ret (Retsudvalget 2022-23 (2. samling), 2023).

I Norge har politiet indkøbt et system fra samme udbyder, som det danske politi har handlet med. Et system der har fået en del kritik i medierne, både fordi systemet har været dyrt og forsinket, men også fordi der er stillet spørgsmål til systemets overholdelse af persondataretten (Østli Jakobsen, 2022).

På nuværende tidspunkt er svensk sikkerhedspoliti muligvis ved at undersøge muligheder for et nyt IT-system med lignende funktioner som i Danmark. Det er i hvert fald givet et opdrag til en udredning af, om reglerne om sikkerhedspolitiet skal ændres, bl.a. for at gøre det muligt at bearbejde og analysere information ved hjælp af tekniske hjælpemidler.[2] Og ifølge dansk politi, har Palantir allerede leveret løsninger lig POL-INTEL til svensk politi. (Bjørnholdt, 22. december 2016)

Systemer a la POL-INTEL er således udbredt i de nordiske lande, hvorfor det er centralt at undersøge, om anvendelsen af systemerne og lovgivningen (konkret den danske), der hjemler brug af systemerne er i overensstemmelse med databeskyttelsesretten.

I denne artikel analyseres, bl.a. på baggrund af ovenstående, om politiets behandling[3] af personoplysninger i POL-INTEL er i overensstemmelse med databeskyttelsesretten, herunder særligt retshåndhævelsesdirektivet. POL-INTEL og anvendelsen heraf, medfører at politiet i stort omfang håndterer personoplysninger, hvilket for politiets vedkommende er reguleret i retshåndhævelsesdirektivet, som i Danmark er implementeret i retshåndhævelsesloven.

Artiklen indledes med en analyse af indholdet af principperne for håndtering af personoplysninger ifølge retshåndhævelsesdirektivet og retshåndhævelsesloven, med fokus på formålsbestemthed og dataminimering. Principperne sammenholdes herefter med bekendtgørelsen om tværgående informationsanalyser, hvor det vurderes, om der er overensstemmelse mellem dansk ret og EU-retten.

2. POL-INTEL

Med POL-INTEL er dansk politi, som nævnt givet mulighed for at behandle personoplysninger, i et hertil indrettet IT-system, i meget stort omfang.

2. https://www.regeringen.se/rattsliga-dokument/kommittedirektiv/2023/05/dir.-202364
3. Begrebet behandling er defineret i art. (3)(nr. 2)

Det er ikke klart, konkret hvilke personoplysninger, der indsamles og behandles i POL-INTEL, ligesom det ikke er tydeligt, hvad POL-INTEL egentligt er. Nedenstående præsentation af POL-INTEL som system, bygger på offentligt tilgængelige kilder herom.

I forbindelse med et spørgsmål fra folketingets retsudvalg til justitsministeren, forklarer rigspolitiet, at der findes 2 udgaver af POL-INTEL, POL-INTEL finder og POL-INTEL analyse.

"POL-INTEL finder", er den del af systemet, som ca. 11.000 politiansatte har adgang til. Her kan søges "*på tværs af data i en række it- systemer og skabes et overblik over opmærksomhedspunkter ved en person, en adresse, et køretøj eller lignende*" (Retsudvalget - endeligt svar på spørgsmål 946, 2021, p. 2).

"POL-INTEL analyse", er en del af systemet, som ca. 800 medarbejdere har adgang til. Denne del, "*... giver mulighed for at analysere informationer og visualisere resultaterne på bl.a. kort, tidslinjer og netværksdiagrammer. Analyserne kan i relevant omfang benyttes til at understøtte operative beslutninger og prioriteringer som led i politiets arbejde.*" (Retsudvalget - endeligt svar på spørgsmål 946, 2021, p. 3) Det skal hertil bemærkes, at selvom systemet foretager automatiske analyser, kan disse ikke betragtes som "*automatiske individuelle afgørelset*" jf. direktivet art. 11, idet systemet ikke foretager afgørelser på baggrund af de analyser, der laves. Dette overlades til den enkelte politiansatte. (Se nærmere om automatiske individuelle afgørelser (Sunde, 2022))

Med "POL-INTEL finder" gives alle politiansatte, altså mulighed for at søge på tværs af flere IT-systemer. Retspraksis viser, at en simpel søgning på en nummerplade, kan give adgang til oplysninger bl.a. om personlige relationer til en person. I TFK 2023.329 blev en politiansat straffet med bøde for, uden tjenstlig anledning, at have foretaget opslag i POL-INTEL finder. Den ansatte fandt frem til en bilejer ved at søge på dennes nummerplade i POL-INTEL. Da den politiansatte nu havde cpr.nr. på bilejeren, kunne denne finde frem til bilejerens eksmand, og en ekskæreste, som hun havde haft et forhold til 12-13 år tidligere, bilejerens mor og bilejerens datter. Den tiltalte politiansatte, forklarede desuden, at man ved opslag i POL-INTEL får "*et oversigtsbillede, og man kan ikke vælge enkelte oplysninger fra i det*" samt, at "*Af oversigtsbilledet fremgår ting af særlig interesse som eksempelvis aktive og udløbne våbentilladelser, KR*[4]*-oplysninger, samt de seneste fem års sager*" (TFK 2023.329) Det er således meget private oplysninger bl.a. om relationer, der går mange år tilbage, som de politiansatte får adgang til ved opslag i POL-INTEL. I dommen anføres, at den politiansatte slår op på alle bilejerens relationers personprofiler i POL-INTEL, men dommen giver ikke svar på, hvilke oplysninger der kan findes på en sådan profil,

4. Oplysninger i det nationale kriminalregister

udover kontaktoplysninger, våbentilladelse, andre oplysninger af særlig politimæssig interesse samt relationer på tværs.

En forudsætning for, at politiet kan anvende POL-INTEL, er naturligvis, at politiet forinden har indsamlet personoplysninger[5], og at disse opbevares i politiets systemer. Der findes i dansk ret flere love og bekendtgørelser, der hjemler politiets indsamling af personoplysninger, herunder bl.a. i RPL kap. 71 om indgreb i meddelelseshemmeligheden (LBKG 2022-12-25 nr. 1655 Retsplejeloven), Bekendtgørelse om politiets anvendelse af automatisk nummerpladegenkendelse (BKG 2017-09-20 nr. 1080 (ANPG)) og Lov om indsamling, anvendelse og opbevaring af oplysninger om flypassagerer (Lov 2018-12-27 nr. 1706 (PNR-loven)). Disse love og bekendtgørelser, hjemler alle indsamling af personoplysninger i form af bl.a. telefonsamtaler, e-mail, teletrafik, overvågning, nummerpladeoplysninger, kørselsmønstre og oplysninger om rejser.

Når politiet indsamler personoplysninger f.eks. med hjemmel i RPL, sker indgrebene som overvejende hovedregel på baggrund af en retskendelse. Ved disse former for indgreb, vil domstolene tage stilling til, om indgrebet er proportionelt og nødvendigt eller om formålet med indsamlingen kan opnås med mindre indgribende midler.

For den indsamling og anvendelse af personoplysninger, der sker uden retskendelse, er det særligt lovgiver, der i forbindelse med lovgivningsarbejdet skal sikre at betingelserne for politiets indsamling af personoplysninger er nødvendig og proportionel og i øvrigt i overensstemmelse med retshåndhævelsesdirektivet.[6]

Inger Marie Sunde, professor ved Politihøjskolen i Oslo, har i en artikel om politiets indsamling af personoplysninger problematiseret, at politiet gemmer mange oplysninger i deres systemer, som efter menneskeretten og databeskyttelsesretten burde have været slettet. (Sunde, 2023) En efterfølgende brug af disse personoplysninger i POL-INTEL, vil derfor være i strid med det første princip for behandling i retshåndhævelsesdirektivet. Princippet om lovlighed i direktivet art. 4 (1)(a)), tilsiger nemlig, at behandlingen af personoplysninger skal være "lovlig og rimelig". Det må betyde, at hvis oplysningerne ikke er lovligt opbevaret, kan de heller ikke lovligt behandles. Politiet skal altså i første omgang være opmærksom på, om de oplysninger, de indsamler og gemmer i deres systemer er dataminimeret (jf. art. 4(1)(c)) og om de i så fald kan anvendes lovligt i POL-INTEL.

5. Begrebet personoplysning er defineret i GDPR art. 4, nr.1 og nærmere analyseret og defineret af Nadezhda Purtova (2018) The law of everything. Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, 10:1, 40-81
6. Der ligger udenfor rammerne af denne artikel at vurdere om direktivet er overholdt ved indsamling af personoplysninger i de øvrige af politiets systemer. For en analyse af ANPG-systemet, se Tanja Kammersgaard Christensen i Nordisk tidsskrift for Kriminalvidenskab, art. 109 nr. 2 (2022) "Automatisk Nummerpladegenkendelse (ANPG) – behandling af personoplysninger, proportionalitet og retten til privatlivets fred"

De forskellige typer af personoplysninger, som politiet indsamler, f.eks. i forbindelse med en efterforskning, kan hvis de opfylder principperne i direktivet art. 4, som udgangspunkt gemmes i politiets systemer og anvendes til nye formål i POL-INTEL. Politiet kan i Danmark bl.a. opbevare personoplysninger i det centrale kriminalregister (BKG 2021-09-23 nr. 1860 (Kriminalregisteret)) og i politiets efterforskningsstøttedatabase (PED) (BKG 2017-09-20 nr. 1079 (PED)). Både for det centrale kriminalregister og politiets efterforskningsstøttedatabase er der hjemmel til, at oplysningerne fra registrene må indgå i tværgående informationsanalyser i POL-INTEL, ligesom der for øvrige relevante bekendtgørelser vil være hjemmel til at de indsamlede personoplysninger, kan behandles i POL-INTEL, jf. f.eks. ANPG-bekendtgørelsens § 1, stk. 3.[7] POL-INTEL Bekendtgørelsen (BKG 2017-09-20 nr. 1078 om tværgående informationsanalyser) er vedtaget med hjemmel i politiloven § 2a og retshåndhævelsesloven §§ 14 og 16. Reguleringen af POL-INTEL er vedtaget i bekendtgørelsesform, hvorfor der ikke findes forarbejder mv. hertil.

Dansk politi har i 2020, 3 år efter de tog systemet i brug, vurderet at anvendelsen af POL-INTEL overordnet er "*godkendt og succesfyldt*" og at systemet har medført opklaring af flere ældre sager. Samtidig mener politiet, at POL-INTEL besidder yderligere potentiale, bl.a. ved integration af nye datakilder i systemet (Retsudvalget 2020-21, svar på spørgsmål 946, 2019). Der er således ingen tvivl om, at politiet mener, at POL-INTEL er et værdifuldt redskab, et redskab, der kan hjælpe politiet til at varetage deres opgaver mere effektivt. Politiet påpeger dog selv i forbindelse med en orientering i retsudvalget, at der er flere af politiets systemer, der har problemer med compliance, herunder databeskyttelsesmæssige udfordringer med bl.a. logning, sletteregler og håndtering af følsomme data (Retsudvalget 2022-23 (2. samling), 2023). Politiet vil derfor i forbindelse med deres re-planlægning og prioritering af it-projektporteføljen bl.a. have fokus på compliance, herunder bl.a. i POLSAS, som er en af de systemer, POL-INTEL sammenkøres med (Retsudvalget 2022-23 (2. samling)).

3. Principper for behandling af personoplysninger indenfor retshåndhævelsesdirektivet

Enhver behandling af personoplysninger, der foretages af politiet, skal være i overensstemmelse med principperne for behandling i direktivet art. 4. Principperne skal være opfyldt både ved indsamling og efterfølgende anvendelse af de indsamlede personoplysninger, (jf. definition af behandling i art. 3), hvorfor

7. Se også Henricson, Ib: "Politiloven med kommentarer", s. 41 herom

politiets anvendelse af personoplysninger i tværgående informationsanalyser skal opfylde principperne i direktivet.[8]

3.1. Formålsbestemthed, art. 4 (1)(b)

Et centralt princip for behandling af personoplysninger, også i det her omhandlede retshåndhævelsesdirektiv, er princippet om formålsbestemthed – et princip for behandling af personoplysninger, der har sin oprindelse både i EMRK art. 8 og i Chartret om grundlæggende rettigheder (Union, (2010/C 83/02)) (herefter Chartret) art. 7 og 8, hvoraf følger at et indgreb i retten til privatlivets fred, skal være til et udtrykkeligt formål, fastlagt ved lov. Behandling af personoplysninger skal, derfor, for at være i overensstemmelse både med direktivet og med de grundlæggende rettigheder, "*indsamles til udtrykkeligt angivne og legitime formål og ikke behandles på en måde, der er uforenelig med disse formål*" (art. 4 (1)(b)) Hertil kommer, at behandling til andet formål end det oplysningerne er lovligt indsamlet til, kan ske, hvis den dataansvarlige er retligt bemyndiget til at foretage behandlingen og hvis behandlingen er nødvendig og forholdsmæssig i forhold til det andet formål, jf. direktivet art. 4(2) og retshåndhævelseslovens § 5.

Ifølge direktivet art. 8 og præambelbetragtning nr. 26, må behandling af personoplysninger kun finde sted til specifikke formål fastlagt ved lov. Det betyder, at formålet med behandlingen, skal være beskrevet i den relevante lovgivning. Spørgsmålet er, hvor konkret formålet med indsamlingen skal være beskrevet i lovgivningen, idet det ikke anses for tilstrækkeligt at henvise til at indsamlingen af personoplysninger sker til de formål, der er beskrevet i art. 1(1), henholdsvis forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger (Vogiatzoglou & Marquenie, 2022, p. 34).

> Ifølge EU-Domstolen (EUD), "*... må formålene med behandlingen af biometriske og genetiske data ikke beskrives i for generelle vendinger, men kræver, at de er tilstrækkeligt præcise og konkrete til at gøre det muligt at vurdere, om den nævnte behandling er "strengt nødvendig"*. "(C-205/21 pr. 124) Selvom dommen fra EUD drejer sig om behandling af følsomme oplysninger, er formålsbegrænsningen, bestemmende for at kunne vurdere, om de øvrige principper i art. 4 er opfyldt, hvorfor dommen er relevant

8. I artiklen tages udgangspunkt i ordlyden i direktivet og retspraksis herfra. I forbindelse med implementeringen af retshåndhævelsesdirektivet i dansk ret, blev der af lovgiver lagt vægt på en korrekt implementering af direktivet. Dette bl.a. ved at affattelsen af de danske regler, skulle lægge sig tæt op ad direktivets ordlyd, for at der ikke kunne rejses tvivl om implementeringen. (retshåndhævelsesloven, 2017, p. 14) Dette taler ifølge teorien for, at der ved fortolkningen af direktivet, som Danmark kun er folkeretligt forpligtet til at følge, kan lægges vægt på nogle af de principper, vi kender fra EU-retten, herunder pligten til EU-konform fortolkning, hvilket endvidere taler for, at praksis fra EUD kan anvendes som fortolkningsbidrag ved fortolkningen af retshåndhævelsesloven. Hertil kommer, at Danmark rent folkeretligt vil anvende fortolkningsreglen ved fortolkningen af folkeretten, (Rytter, 2023, p. 59) Resultatet vil derfor formentlig være det samme, hvorfor Danmark skal fortolke direktivkonformt uanset om dette anses fra et EU-retligt eller folkeretligt perspektiv. (Sørensen, 2018, p. 323). Retshåndhævelsesloven inddrages i de tilfælde, hvor Danmark eventuelt har andre regler heri.

for beskrivelsen af formålet generelt. Dette påpeges også i direktivets præambelbetragtning 33, hvoraf det fremgår, at formålet med behandlingen skal beskrives i lovgivningen, bl.a. for at sikre mod misbrug og vilkårlighed.

I den engelske udgave af retshåndhævelsesdirektivet er betingelserne for formålets gyldighed i art. 4(1)(b): "*specified, explicit and legitimate purposes*", altså specifikke, eksplicitte og legitime formål og ikke som i den danske oversættelse "*udtrykkeligt angivne*" formål. En umiddelbar sproglig læsning af den engelske ordlyd giver en klarere forståelse af, at der kan opstilles krav til beskrivelsen af formålet med indsamlingen af personoplysninger. (Se også præambelbetragtning 26)

At indsamlingen af personoplysninger skal have et *specifikt, eksplicit og legitimt* formål betyder, at der skal være en balance mellem typen af personoplysninger, antallet af registrerede,[9] der indsamles oplysninger og det formål, der forfølges med indsamlingen, dette har EUD slået fast i flere sager, hvor EUD for at vurdere lovgivningens legitimitet netop lægger vægt på disse kriterier. (C-362/14 Schrems pr. 93, C-293/12 Digital Rights, pr. 57 og C-203/15 Tele2 Sverige, pr. 105 – se også nærmere herom i (Koning, 2020, p. 64)).

Et centralt element for vurderingen af om en behandling af personoplysninger er lovlig er ifølge EUD, om der i loven er sket en indskrænkning af indsamlingen af personoplysninger og adgangen hertil, jf. C-362/14 Schrems, vedrørende fortolkning af Chartrets art. 7 og 8, samt databeskyttelsesdirektivet, pr. 93, hvor EUD angiver, at: "*En lovgivning, der på generel vis tillader opbevaring af samtlige personoplysninger fra samtlige de personer, hvis oplysninger er blevet videregivet fra Unionen til USA, uden at der bliver foretaget nogen form for differentiering, begrænsning eller undtagelse under hensyn til det forfulgte mål, og uden at der bliver fastsat noget objektivt kriterium, som gør det muligt at afgrænse de offentlige myndigheders adgang til oplysningerne og deres senere anvendelse heraf med henblik på veldefinerede formål, der er strengt begrænsede, og som kan begrunde det indgreb, som såvel adgangen til disse oplysninger som anvendelsen heraf indebærer, er således ikke begrænset til det strengt nødvendig.*"

Derudover skal formålet være beskrevet præcist og fuldstændigt, så en almindelig registeret, kan forstå hvilken behandling, der sker med personoplysningerne, hertil kommer, at jo mere indgribende behandlingen er, jo mere specifik skal formålet være beskrevet (Koning, 2020, p. 66). Formålet skal være beskrevet så alle involverede parter, herunder den registrerede, tilsynet og øvrige 3.parter kan forstå, hvad personoplysningerne anvendes til. Formålet skal derfor være tydeligt beskrevet, forklaret og synliggjort, så alle opnår en entydig forståelse af formålet (Koning, 2020, p. 68).

9. Registrerede er defineret i GDPR art. 4, stk. 1, nr. 1, som en identificeret eller identificerbar fysisk person (»den registrerede«)

Samlet set, skal formålet være så udtrykkeligt beskrevet, at det bl.a. kan anvendes til at foretage en nødvendigheds- og proportionalitetsvurdering af indsamlingen efter direktivet art. 4 (1)(c) (Jf. generaladvokat Pikamäe's forslag til afgørelse i C-118/22 NG, præmis 53). Det er derfor ikke er nok, alene f.eks. at angive at personoplysningerne indsamles til efterforskning. (Koning, 2020, pp. 67-68).[10] Det må dermed være en fejlopfattelse, når lovgiver, angiver i forslag til Lov om retshåndhævende myndigheders behandling af personoplysninger, at: (L 168 lovforslag retshåndhævelsesloven, 2017) "*... en formålsangivelse som f.eks. "til brug for udbud af finansielle ydelser" anses for at være tilstrækkelig præcis.*" (L 168 lovforslag retshåndhævelsesloven, 2017, p. 63). Det er centralt i databeskyttelsesretten, at der skelnes mellem målet med behandlingen, som kan skrives mere overordnet og formålet med behandlingen, som skal være mere præcis og specifikt, som angivet ovenfor. (Se nærmere om forskellen mellem mål og formål bl.a. i (Christensen, 2021, p. 187), med yderligere referencer)

For at politiet kan anvende personoplysninger til andre formål, end de oprindeligt er indsamlet til, skal der være en lovhjemmel til denne nye behandling. Dette følger af direktivet art. 4.

Efter ordlyden i art. 4(2), kræver behandling af personoplysninger til et andet formål, både at den dataansvarlige[11] (her politiet) er bemyndiget til at foretage en sådan behandling efter EU-retten eller national ret og at behandlingen er nødvendig og forholdsmæssig i forhold til dette andet formål.[12] Der stilles dermed krav om, at behandlingen til et andet formål er proportionel. Hertil kommer, at de øvrige principper for behandling, fortsat skal være opfyldt ved behandling til det andet formål, hvorfor der stilles krav om, at betingelserne om formålsbestemthed i art. 4 (1)(b) er opfyldt for den nye behandling (De Hert & Sajfert, 2021, p. 12). Princippet om formålsbestemthed kan dermed ikke fraviges ved behandling til nyt formål, hvilket underbygges af, at princippet om formålsbestemthed ved behandling af personoplysninger følger af Chartrets art. 8, og at direktivet skal fortolkes i overensstemmelse hermed (Vogiatzoglou & Marquenie, 2022, p. 35). Det betyder, at hvis der sker viderebehandling af indsamlede personoplysninger, skal denne viderebehandling have et formål, der er legitimt, specifikt og eksplicit fastlagt ved lov.

Som illustreret ovenfor stilles der, med art. 4 strenge krav til beskrivelsen af formålet med både indsamlingen af personoplysninger og lige så strenge krav til beskrivelsen af formålet med en evt. efterfølgende behandling til et andet formål. For at behandlingen af personoplysninger finder sted indenfor retshåndhævelsesdirektivets rammer, bestemmer art. 8 desuden, at

10. Se i samme retning EDBP "Retningslinjer 3/2019 om brug af videoudstyr til behandling af personoplysninger" Version 2.0 Vedtaget den 29. januar 2020, s. 9, hvor det er angivet, at:" »Sikkerhed« eller »personers sikkerhed« som eneste begrundelse for videoovervågning er ikke tilstrækkelig specifikt"
11. Begrebet dataansvarlig er defineret i direktivet art. 3(8)
12. Bestemmelsen er implementeret I retshåndhævelseslovens § 5, med stort set samme ordlyd som i direktivet.

behandlingen skal være hjemlet i lov og at loven skal angive mål og formål med behandlingen, jf. nærmere nedenfor.

3.2. Formålsbestemthed og POL-INTEL

Som det fremgår af ovenstående, skal bekendtgørelsen om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser, angive et formål med behandlingen. Et formål, som skal være legitimt, specifik og eksplicit beskrevet.

I bekendtgørelse om tværgående informationsanalyser angives i §§ 4 og 5, til hvilke formål personoplysninger kan behandles i POL-INTEL. § 4 omhandler situationer med henblik på at bringe strafbar virksomhed til ophør, konkret fareafværgelse mv., mens § 5 omhandler behandling til øvrige formål, særligt forebyggelse af strafbare forhold.

Formålet i POL-INTEL bekendtgørelsens § 4, nr. 1 er "*at bringe strafbar virksomhed til ophør samt efterforske og forfølge strafbare forhold*", hvilket er enslydende med politilovens § 2, nr. 3. De øvrige formål i bekendtgørelsen er beskrevet i ligeså vide termer og kan, stort set alle, krydsrefereres direkte med de meget brede formål, der er angivet i politilovens § 2.

Når formålene i bekendtgørelsen om tværgående informationsanalyser, er beskrevet så brede som de er, gør det det svært efterfølgende at vurdere om de personoplysninger, der indgår i systemerne, er afgrænset til det nødvendige og er proportionelle med formålet. Hvilket naturligvis skal sammenholdes med politiets meget brede opgaveportefølje, hvor politiet både har til opgave at strafforfølge, sikre orden, forebygge og afværge kriminalitet.[13] Formålsbeskrivelsen skal som nævnt ovenfor, være så specifik og eksplicit, at en almindelig registeret kan, forstå hvilken behandling, der vil ske med personoplysningerne, hvilket nok ikke kan siges at være tilfældet med bekendtgørelsens formålsbeskrivelse i sin nuværende form. Hertil kommer at formålsbeskrivelsen i sin nuværende form, gør det meget svært at kunne vurdere, om behandlingen af, adgangen til og opbevaringen af personoplysninger i POL-INTEL, er begrænset til det strengt nødvendige.

Formålene i bekendtgørelsen, bør altså præciseres, så det specifikt og eksplicit angives til hvilke formål, personoplysningerne kan behandles. Både så der kan foretages en vurdering af proportionalitet og nødvendighed, men også så de registrerede, kan forstå, hvad deres oplysninger kan blive brugt til.

Det anerkendes dog, at det kan være svært at formulere et formål, der på samme tid tager hensyn til politiets brede opgaveportefølje og databeskyttelsesretten.

13. Se nærmere om politiets opgaver i Henricson, Ib: "Politiret" Jurist- og økonomforbundets forlag, 7. udgave, kap. III

3.3. Dataminimeringsprincippet, retshåndhævelsesdirektivet art. 4 (1) (c)

Det følger af art. 4 (1)(c), at personoplysninger skal: "*være tilstrækkelige, relevante og ikke omfatte mere end, hvad der kræves til at opfyldelse af de formål, hvortil de behandles*", hvilket er et centralt princip i databeskyttelsesretten.

Efter præambelbetragtning nr. 26, følger det, at: '" ... *Personoplysningerne bør være tilstrækkelige og relevante i forhold til de formål, hvortil de behandles. Det bør navnlig sikres, at de indsamlede personoplysninger ikke er for omfattende og ikke opbevares i et længere tidsrum end det, der er nødvendigt af hensyn til de formål, hvortil de behandles. Personoplysninger bør kun behandles, hvis formålet med behandlingen ikke med rimelighed kan opfyldes på anden måde ...* "

I C-118/22 NG, som omhandler lovligheden af opbevaring af personoplysninger i et politiregister, udtaler generaladvokat Pikamäe i forslaget til afgørelse i præmis 27, at der ved besvarelsen af spørgsmål angående art. 4 (1) (c), skal tages hensyn til, at princippet om dataminimering er udtryk for proportionalitetsprincippet. Dataminimeringsprincippet betyder, efter domstolens faste praksis, at: "*... undtagelser fra og begrænsninger i beskyttelsen af personoplysninger begrænses til det strengt nødvendige, hvorved det forudsættes, at hvis det er muligt at vælge mellem flere egnede foranstaltninger i forhold til de tilsigtede legitime mål, skal den mindst bebyrdende foranstaltning vælges.*"(General advokatens forslag til afgørelse i C-118/22 NG præmis 44) Der skal altså ved dataminimeringsprincippet foretages en nødvendighedsafvejning, ligesom der skal foretages en proportionalitetsafvejning.

European Data Protection Supervisor (EDPS), som er den Europæiske tilsynsførende for databeskyttelse, har i 2017 udarbejdet et toolkit[14] omkring nødvendighedsvurderingen ved indgreb i retten til beskyttelse af personoplysninger i Chartrets art. 8 (EDPS, 2017) og (EDPS, 2019). I dette toolkit findes en meget velbeskrevet fremgangsmåde for lovgiver, når de skal vurdere om et nyt tiltag, som f.eks. implementering af POL-INTEL, opfylder kravet om nødvendighed. Her skal lovgiver bl.a. tage stilling til, hvorfor netop det valgte tiltag er nødvendig for at opnår formålet, og der fremhæves af EDPS at f.eks. nemhed (convenience) eller omkostningseffektivitet ikke er nok til at tiltaget er nødvendigt. (EDPS, 2017, p. 17) Det skal af lovgiver forklares, hvorfor allerede eksisterende tiltag ikke er tilstrækkelige til at løse problemet, hvorfor alternative, mindre indgribende tiltaget ikke er tilstrækkelige og hvordan det nye tiltag kan løse problemet mere end andre tiltag. Lovgiver skal for at dataminimere overveje, hvilke oplysninger, der skal indsamles i systemer som POL-INTEL, hvem der skal gives adgang til personoplysninger og på hvilke

14. Toolkittet er tiltænkt til at hjælpe lovgiver til at foretage nødvendigheds- og proportionalitetsvurderingen, ved nye tiltag, der medfører behandling af personoplysninger. Toolkittet er udarbejdet på grundlag af EU-retten, retspraksis fra EUD og EMD.

vilkår. Der stilles dermed krav til lovgivningsprocessen og dokumentation for, at der er foretaget en nødvendighedsvurdering (EDPS, 2017, p. 18).

Efter der er foretaget en vurdering af nødvendighed, skal lovgiver foretage en proportionalitetsvurdering af det nye tiltag. Her skal lovgiver først og fremmest vurdere indgrebets intensitet på retten til privatliv op mod fordele ved det nye tiltag (EDPS, 2019, p. 28). Hvis lovgiver vurderer at indgrebet ikke er proportionelt, kan det imødekommes ved at minimere indgrebets intensitet, f.eks. ved at begrænse kategorier af personoplysninger, der indsamles eller adgangen hertil. Selvom lovgiver én gang har vurderet at tiltaget er proportionelt, skal lovgiver revurdere tiltaget løbende, ligesom der skal holdes løbende tilsyn (EDPS, 2019, p. 32).

I relation til efterfølgende behandling af personoplysninger skal dataminimeringsprincippet også være opfyldt. For at kunne foretage en nødvendigheds- og proportionalitetsvurdering af behandlingen af personoplysninger, er det derfor nødvendigt at kunne skelne mellem det oprindelige formål med behandlingen og formålet med den efterfølgende behandling af personoplysninger, idet dataminimeringsprincippet skal være opfyldt for hver af disse behandlinger på tidspunktet for indsamlingen.[15] Det betyder at man ikke kan indsamle flere oplysninger, end det er nødvendigt for at opfylde det oprindelige formål, selvom disse yderligere oplysninger eventuelt kan være nødvendige for et efterfølgende formål. (Se nærmere om dataminimering for de oprindeligt indsamlede personoplysninger i (Sunde, 2023))

Hvis personoplysninger, på tidspunktet for indsamlingen, indsamles med flere formål, må disse formål være bestemt på forhånd, og dataminimeringsprincippet må så vurderes herudfra.

I den danske implementering af retshåndhævelsesdirektivet, fremgår det af ordlyden i § 4, stk. 3, at: "*Oplysninger, som behandles, skal være relevante og tilstrækkelige og må ikke omfatte mere, end hvad der kræves til opfyldelse af de formål, hvortil oplysningerne indsamles, og de formål, hvortil oplysningerne senere behandles.*" Ifølge bemærkninger til lovforslaget, er dette blot en videreførelse af formuleringen fra den tidligere danske persondatalov, hvorfor der umiddelbart ikke er taget stilling til ordlyden. Bestemmelsen kan imidlertid læses, så den åbner op for indsamling, der er nødvendig for den senere behandling, hvilket dog, jf. ovenfor, ikke vil være i overensstemmelse med EU-retten.

3.4. Dataminimeringsprincippet og POL-INTEL

Allerede fordi formålet med behandling af personoplysninger i bekendtgørelse om tværgående informationsanalyser, som nævnt ovenfor, er beskrevet meget bredt, er det svært at tage stilling til, om dataminimeringsprincippet er opfyldt for behandlingen af personoplysninger i POL-INTEL, idet formålet bl.a. er bestemmende for nødvendigheden af personoplysninger. Som formålet

15. Jf. præambelbetragtning nr. 26, hvorefter formålet skal være fastlagt når personoplysningerne indsamles.

er formuleret i dag, vil alle personoplysninger formentlig kunne betragtes som nødvendige, hvilket også er i tråd med den nuværende indsamling af personoplysninger i POL-INTEL, samt politiets ønske om at indsamle flere oplysninger til POL-INTEL.

Et element af dataminimeringsprincippet er, som nævnt, nødvendighed. For at kunne vurdere om behandlingen af personoplysninger i POL-INTEL er begrænset til, hvad der er nødvendigt, skal lovgiver, som det fremgår ovenfor, tage stilling til, om formålet med POL-INTEL kunne opnås med andre tiltag eller allerede eksisterende tiltag. Der kan findes bidrag til lovgivers overvejelser omkring anvendelsen af POL-INTEL i "*Forslag til Lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer)*", fremsat den 29. marts. 2017. Her angiver justitsministeren flere grunde til, at de nye systemer kan være et værdifuldt værktøj for politiet, dette begrundes med effektivitet og modernisering, fordi søgning i de nuværende systemer, er en tung – og typisk manuel proces (L 171 lovforslag til ændring af politiloven, 2017, p. 4). Justitsministeren finder derfor, at: "*En forbedret dataanvendelse hos politiet og en styrkelse af den analyse- og videnbaserede tilgang til politiarbejdet vurderes at ville få væsentlig betydning for alle dele af politiets arbejde – fra den alvorligste organiserede grænseoverskridende kriminalitet til den mere borgernære kriminalitet og både i forhold til efterforskning og forebyggelse.*" (L 171 lovforslag til ændring af politiloven, 2017, p. 5) Dette følges op med flere eksempler på, hvordan de nye systemer kan være mere effektive end de tidligere (L 171 lovforslag til ændring af politiloven, 2017, p. 5). Anvendelsen af de tværgående analyser er dermed begrundet både ud fra en nødvendighed for at politiet kan effektivisere og modernisere, men også ud fra nemhed, idet de daværende systemer var tunge. Der er dermed i vidt omfang taget stilling til, hvordan de nye systemer kan løse problemerne mere effektivt, mens der ikke er taget stilling til, om de tidligere systemer ikke kunne løse samme opgave på en mindre indgribende måde. Politiet har ikke med de nye systemer fået flere opgaver, eller nye kompetencer, men de tidligere systemer understøttede ikke tværgående søgninger og analyser, da de var mere manuelle. Det kan således ikke konstateres om POL-INTEL og den omfattende behandling, der sker heri, er nødvendig for politiet i et databeskyttelsesretligt perspektiv. Altså, om det er vurderet at POL-INTEL er det mindst indgribende middel til at nå målet.

Dataminimeringsprincippet, indebærer desuden, jf. direktivet art. 4 (1) (b), at personoplysningerne skal være begrænset til, hvad der er tilstrækkeligt, relevant og ikke omfatte mere, end hvad der er nødvendigt for at opnå formålet. For at vurdere dette, må der tages stilling til, hvilke personoplysninger, der indgår i POL-INTEL, hvem der skal gives adgang hertil og på hvilke vilkår, der gives adgang.

Informationskilder i POL-INTEL

Det følger ikke specifikt af POL-INTEL bekendtgørelsen, hvilke informationskilder POL-INTEL, kan bruge til den tværgående informationsanalyse, idet der i § 8 i bekendtgørelsen blot angives, at der i systemet kan anvendes de registre og databaser mv., som politiet fører efter gældende ret, samt i de øvrige kilder, som politiet kan anvende som led i varetagelsen af deres opgaver. Det er dermed en meget bred formulering, som forudsætter kendskab til politiets faste kilder og øvrige kilder.

På politiets hjemmeside, angives det, at: "*POL-INTEL giver politiet adgang til at analysere oplysninger på tværs af POLSAS, Kriminalregistret, CRM*[16]*, Indexregistret, Nationalt Fotoregister og ANPG.*" (Politi.dk) På hjemmesiden angives altså 6 datakilder til POL-INTEL.[17]

I forbindelse med et spørgsmål til folketingets retsudvalg i oktober 2019, angiver Rigspolitiet dog, at POL-INTEL kan foretage søgning i 11 datakilder.[18]

Indholdet af politiets registre kan ikke læses ud af de nugældende udgaver af lovteksten,[19] men for det centrale kriminalregister henviser politiet selv, på deres hjemmeside (Politi.dk), til en historisk udgave af bekendtgørelsen, hvori der i bilag 1 og 2 angives, hvilke (person)oplysninger, der indgår i kriminalregistret (BKG 2021-09-23 nr. 1860 (Kriminalregisteret)). Kriminalregistret består, jf. bekendtgørelsen herom § 1, af en afgørelsesdel og en efterforskningsdel. Det følger af bilag 1 til den historiske udgave af bekendtgørelsen, at der i afgørelsesdelen findes oplysninger om domme og bødevedtagelser, som er omfattet af straffeloven, domme for overtrædelse af anden lovgivningen, hvis der er idømt frihedsstraf, herunder både betinget og ubetinget, samt en lang række andre afgørelser, dog med undtagelse af afgørelser i civil-

16. Det centrale motorkøretøjsregister
17. CRM og Indexregistret falder ind under anvendelsesområdet for GDPR og ikke retshåndhævelsesdirektivet, hvorfor anvendelsen af disse kilder til nye formål i POL-INTEL, skal være i overensstemmelse med GDPR.
18. POLSAS (politiets journaliserings- og sagsstyringssystem, hvor politirapporter oprettes mv.), CRM3 (Det Centrale Motorkøretøjsregister, hvor alle informationer om køretøjer i Danmark findes), Index2 (register indeholdende adresseoplysninger), GoAML (international database indeholdende hvidvaskindberetninger), Våbenregisteret (landsdækkende våbenregister, der indeholder oplysninger om våben, som politiet meddeler tilladelse til), EK (register indeholdende oplysninger om efterlyste køretøjer i Danmark), PED (Politiets Efterforskningsstøttedatabase til brug for politiets arbejde med de særlige kriminalitetsområder der er undergivet systematisk, politimæssig monitorering) NF (Nationalt Fotoregister, hvor alle af politiet optagne personfotografier opbevares digitalt) KR (Kriminalregisteret, hvor oplysninger om rejste sigtelser og afgørelser truffet i straffesager opbevares), INTERPOL (database indeholdende bl.a. internationalt efterlyste personer og genstande) og SIS (Schengen Informationssystemet, som indeholder internationale oplysninger om eftersøgte eller savnede personer eller stjålne køretøjer og dokumenter)." (Retsudvalget 2018-19 (2. samling), 2019)
19. En fuldstændig vurdering af om dataminimeringsprincippet er opfyldt, vil kræve kendskab til om dataminimeringsprincippet er opfyldt i de enkelte datakilder, der indgår i POL-INTEL. Idet et sådan overblik ikke haves, og for flere af kilderne ikke kan læses ud af lovteksten, forudsættes dataminimeringsprincippet opfyldt heri

retlige straffesager.[20] Indholdet af efterforskningsdelen af kriminalregistret, er beskrevet i bilag 2 til den historiske udgave af bekendtgørelsen, der er i alt 15 forskellige typer oplysninger, der kan registreres heri. Det bl.a. er identifikationsoplysninger, aktualitetsmarkeringer, som angiver, at en person er "politimæssig" aktuel, uanset om der er en verserende sag. Med denne aktualitetsmarkering, kan registreres en kode, så det fremgår hvilke type aktualitet personen her, herunder om vedkommende har været med bevæbnet, er voldsmand, farlig, i alkoholbehandling, handler med narko mv. På tidspunktet for bilaget, fandtes der 40 forskellige markeringskoder. Derudover er der i registret oplysninger om sager om vedkommende, eftersøgningsoplysninger, oplysninger om sigtelser, for udvalgte lovovertrædelser, oplysninger om eventuelle frihedsberøvelser, oplysninger om afgørelser og særlige typer af indberetninger mv. (Se nærmere bilag 2 til BEK nr. 881 af 04/07/2014 (Historisk) Bekendtgørelse om behandling af personoplysninger i Det Centrale Kriminalregister (Kriminalregisteret))

Hvilke personoplysninger, der kan indsamles i politiets efterforskningsstøttedatabase (PED), fremgår ikke af bekendtgørelsen herom. PED må alene anvendes inden for de områder, der er undergivet systematisk, politimæssig monitering. Hvad dette nærmere indebærer, fremgår ikke af bekendtgørelsen, men er ifølge rigspolitiet bl.a. narkotikakriminalitet, menneskehandel, bandekriminalitet og radikalisering (Rigspolitiet, 2016) (Retsudvalget 2009-10, 2010). PED består af en persondel og en hændelsesdel, jf. § 2. Det angives alene i § 3 vedr. persondelen, at der optages relevante oplysninger om dømte, sigtede eller mistænkte, samt om meddelere, politiagenter og personer under vidnebeskyttelse. I hændelsesdelen, kan der jf. § 4 optages relevante oplysninger om hændelser, hvilket ikke defineres yderligere. Af en orientering fra rigspolitiet til justitsministeriet i 2016 fremgår det, at politiet bl.a. gemmer oplysninger om hændelser og personer, baseret på tips og lignede informationer for politikredsene (Rigspolitiet, 2016), og i et spørgsmål til folketingets retsudvalg fortæller rigspolitiet, at der i persondelen også kan være personoplysninger om andre personer, der har en særlig tilknytning til de personer, der er undergivet monitering (Retsudvalget 2009-10, 2010). Det er derfor ikke nemt at se hvilke oplysninger, der reelt indgår i PED, hvilket gør det svært at vurdere om principperne i direktivet er overholdt for denne database, og da oplysningerne indgår i POL-INTEL videreføres denne problematik hertil.

Sammenfattende er det meget uigennemsigtigt hvilke informationskilder, der indgår i POL-INTEL, idet svaret må fremsøges via forskellige online kilder. Hertil kommer, at det er uigennemsigtigt, hvilke informationer de enkelte kilder indeholder, og dermed er det rigtigt svært samlet at vurdere, hvilke personoplysninger, der er indeholdt i POL-INTEL. Det betyder, at der ikke

20. Se nærmere bilag 1 til BEK nr. 881 af 04/07/2014 (Historisk) Bekendtgørelse om behandling af personoplysninger i Det Centrale Kriminalregister (Kriminalregisteret)

kan foretages en vurdering af, om dataminimeringsprincippet egentlig er opfyldt i POL-INTEL.

Flere kilder i POL-INTEL

I "*Forslag til Lov om ændring af lov om politiets virksomhed og toldloven (Politiets anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer)*" påpeger justitsministeren, at erfaring for andre landes anvendelse af systemer som POL-INTEL (intelligence-led policing), viser: "*at det er af afgørende betydning for realiseringen af det fulde potentiale af denne tilgang, at politiet har mulighed for at bruge så mange af de oplysninger, som politiet behandler, som muligt på tværs af opgavevaretagelsen.*" (L 171 lovforslag til ændring af politiloven, 2017, p. 5) Hvilket formentlig er grunden til, at man har valgt at sammenkøre en række af politiets centrale systemer i POL-INTEL. Dette modsiges dog i en rapport udarbejdet af det hollandske konsulentfirma Considerati, til rigspolitiet om "*Big Data for Law enforcement*", hvor det på side 49 netop påpeges, at flere data ikke nødvendigvis giver bedre resultater, hvorimod nøje udvalgte datakilder, derimod vil give bedre resultater (Considerati, 2016). På trods at dette ønsker politiet adgang til flere datakilder i POL-INTEL, herunder f.eks. adgang til teledata fra politiets indgreb i meddelelseshemmeligheden (Retsudvalget 2019-20, 2020).

Udfordringen ved adgang til f.eks. logningsdata, er at EUD har påpeget, at trafikdata og lokaliseringsdata ikke kan "*gøres til genstand for en generel og udifferentieret lagring med henblik på bekæmpelse af grov kriminalitet, og adgang til disse data kan derfor ikke begrundes i dette formål. Når disse data undtagelsesvis er blevet lagret generelt og udifferentieret med henblik på at beskytte den nationale sikkerhed mod en trussel, som må anses for at være reel og aktuel eller forudsigelig, under de betingelser, som er omhandlet i denne doms præmis 58, kan de kompetente nationale myndigheder på området for strafferetlig efterforskning ikke få adgang til disse data i forbindelse med strafferetlig forfølgning, idet forbuddet mod at foretage en sådan lagring med henblik på bekæmpelse af grov kriminalitet, jf. præmis 65 ovenfor, herved vil blive berøvet sin effektive virkning*" (C-140/20 G.D. pr. 100) EUD påpeger altså, at hvis personoplysninger indsamles og vurderes proportionelle til bekæmpelse af en trussel mod national sikkerhed, så kan disse oplysninger ikke efterfølgende anvendes til opklaring af grov kriminalitet. Se tillige C-162/22 A.G, pr. 44, hvor dette præciseres, her også med henvisning til Chartrets art. 7 og 8, hvorfor afvejningen ikke kun finder anvendelse for teleoplysninger, men for personoplysninger generelt. (C-162/22 A.G, pr. 44) Et element, som dansk lovgiver skal tage stilling til, hvis man tillader at teleoplysninger, kan indgå i POL-INTEL, er derfor på hvilket grundlag oplysningerne er indsamlet, og om oplysninger derfor kan tilgås på generelt plan i POL-INTEL, eller om oplysningerne kun er proportionelle i forhold til konkrete formål. Dette burde lovgiver, som et generelt princip, tage stilling til, ved alle datakilder, der skal indgå i POL-INTEL.

Generelt tyder det ikke på, at der er foretaget en vurdering af, om alle datakilder er nødvendige for at kunne opnå formålet med behandlingen med POL-INTEL.

Idet det må være særdeles store datamængder, der kan indgå i POL-INTEL, er der ingen tvivl om, at politiets anvendelse af POL-INTEL medfører et meget omfattende indgreb i retten til respekt for privatliv og beskyttelse af personoplysninger, og at anvendelsen af POL-INTEL derfor skal være proportionel og nødvendig.

4. Afrunding

Ovenstående gennemgang af den danske bekendtgørelse om tværgående informationsanalyser viser, at bekendtgørelsen har en del, mangler i forhold til de betingelserne, der er for behandling af personoplysninger efter EU's retshåndhævelsesdirektiv, bl.a. fordi behandlingen af personoplysningerne og betingelserne herfor ikke er så forudsigelig og gennemsigtig, som der stilles krav til fra EU. Idet hjemlen findes i bekendtgørelsesform, betyder det, at der ikke findes forarbejder hertil, hvorfor de manglende oplysninger vedrørende POL-INTEL ikke kan findes heri.

For at bekendtgørelsen skal leve op til direktivet, skal formålet med behandlingen i POL-INTEL beskrives mere specifikt og eksplicit, så det ud fra loven kan udledes, hvad personoplysningerne anvendes til. Derudover skal det i bekendtgørelsen angives, hvilke personoplysninger, der behandles, ligesom der skal foretages en nødvendigheds- og proportionalitetsvurdering af behandlingen af personoplysninger, så der konkret tages stilling til, ud fra de nye mere specifikke formål, hvilke personoplysninger, der er nødvendige og relevante for formålet.

Der er ingen tvivl om, at politiet har et ønske om, at så mange oplysninger som muligt indgår i POL-INTEL, og at oplysningerne heri ikke slettes. For at leve op til databeskyttelsesretten kunne man derfor overveje, som EDPS påpeger i sit Toolkit, om man kan begrænse adgangen til de oplysninger, der vises i POL-INTEL. I TFK 2023.329, forklarer den politiansatte i retten, at man ikke selv kan vælge, hvilke oplysninger man ser i POL-INTEL, når man slår op heri. For at imødekomme nogle af de databeskyttelsesretlige udfordringer i POL-INTEL kunne man derfor overveje, om de oplysninger, der vises i POL-INTEL skulle afhænge af det konkrete formål med opslaget. Hvis den politiansatte skal se om en bilejer tidligere er stoppet for hastighedskørsel, kunne dette formål angives, hvorefter der så kun vises oplysninger relateret hertil. Man kan forestille sig tilsvarende, når et opslag angår kontaktoplysninger, våbentilladelser, besiddelse af stoffer mv. Dette mangler, som et generelt databeskyttelsesretligt princip i bekendtgørelsen, hvorefter det skal præciseres, hvem der har adgang til personoplysningerne og på hvilke betingelser. Dette for, at der

sikres fortrolighed og integritet. Hertil kommer, at der skal være procedure for sletning, så personoplysningerne ikke opbevares længere tid, end det konkret er nødvendigt for formålet.

Kontaktoplysninger
Tanja Kammersgaard Christensen: tkc@law.aau.dk

5. Bibliografi

Bjørnholdt, K., 22. december 2016. *Ny it skal hjælpe politiet med at fange forbrydere.* [Online]
Available at: https://dansk-politi.dk/nyheder/ny-it-skal-hjaelpe-politiet-med-fange-forbrydere [Senest hentet eller vist den 24 april 2024].

BKG 2017-09-20 nr. 1078 om tværgående informationsanalyser, u.d. s.l.: s.n.

BKG 2017-09-20 nr. 1078, § 2, 2017. *om politiets behandling af oplysninger i forbindelse med tværgående informationsanalyser,* s.l.: s.n.

BKG 2017-09-20 nr. 1079 (PED), u.d. s.l.: s.n.

BKG 2017-09-20 nr. 1080 (ANPG), u.d. s.l.: s.n.

BKG 2021-09-23 nr. 1860 (Kriminalregisteret), u.d. s.l.: s.n.

Christensen, T. K., 2021. *Digital overvågning – Lovgivningens grænser i et menneskeretligt krydsfelt.* s.l.:Djøf Forlag.

Considerati, 2016. *Big data for law enforcement – Report prepared for the Danish National Police, Data Protection Unit,* s.l.: s.n.

De Hert, P. & Sajfert, J., 2021. *The fundamental right to personal data protection in criminal investigations and proceedings: framing big data policing through the purpose limitation and data minimisation principles of the Directive (EU) 2016/680,* s.l.: s.n.

Digitaliseringsstyrelsen, D. f. i.-p., 18. november 2019. *Gevinstrealiseringsrapport POLINTEL,* https://www.ft.dk/samling/20201/almdel/reu/spm/946/svar/1780435/2390656.pdf: Den fællesstatslige it-projektmodel, Digitaliseringsstyrelsen.

Direktiv (EU) 2016/680, 2016. *EUROPA-PARLAMENTETS OG RÅDETS DIREKTIV (EU) 2016/680 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger ell.* [Online]
Available at: https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:32016L0680

EDPS, 2017. *Assessing the necessity of measures that limit the fundamental right to the protection of personal data: A Toolkit.* [Online]
Available at: https://edps.europa.eu/sites/edp/files/publication/17-04-11_necessity_toolkit_en_0.pdf

EDPS, 2019. *EDPS Guidelines on assessing the proportionality of measures that limit the fundamental rights to privacy and to the protection of personal data.* [Online]
Available at: https://edps.europa.eu/data-protection/our-work/publications/guidelines/edps-guidelines-assessing-proportionality-measures_en

Europa-kommissionen, forslag til AI Act præambel 26, 2021. *Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING OM HARMONISEREDE REGLER FOR KUNSTIG INTELLIGENS (RETSAKTEN OM KUNSTIG INTELLIGENS) OG OM ÆNDRING AF VISSE AF UNIONENS LOVGIVNINGSMÆSSIGE RETSAKTER.* s.l.:s.n.

Europa-Kommissionen, forslag til AI Act, 2021. *Forslag til EUROPA-PARLAMENTETS OG RÅDETS FORORDNING OM HARMONISEREDE REGLER FOR KUNSTIG INTELLIGENS (RETSAKTEN OM KUNSTIG INTELLIGENS) OG OM ÆNDRING AF VISSE AF UNIONENS LOVGIVNINGSMÆSSIGE RETSAKTER.* [Online]

Available at: https://eur-lex.europa.eu/legal-content/DA/TXT/HTML/?uri=CELEX:52021PC0206

Europa-Kommissionen, 2012. *Kommissionen foreslår en omfattende reform af databeskyttelsesreglerne for at øge brugernes kontrol med deres oplysninger og mindske omkostningerne for erhvervslivet.* [Online]
Available at: https://ec.europa.eu/commission/presscorner/detail/da/IP_12_46

European Parliament, AI Act, 2023. *EU AI Act: first regulation on artificial intelligence.* [Online]
Available at: https://www.europarl.europa.eu/news/en/headlines/society/20230601STO93804/eu-ai-act-first-regulation-on-artificial-intelligence?&at_campaign=20226-Digital&at_medium=Google_Ads&at_platform=Search&at_creation=RSA&at_goal=TR_G&at_advertiser=Webcomm&at_audien

European Parliament, news AI Act, 2023. *AI Act: a step closer to the first rules on Artificial Intelligence.* [Online]
Available at: https://www.europarl.europa.eu/news/en/press-room/20230505IPR84904/ai-act-a-step-closer-to-the-first-rules-on-artificial-intelligence

Folketingstidende A, 2016. *Forslag til folketingsbeslutning om Danmarks tilslutning på mellemstatsligt grundlag til EU's direktiv om databeskyttelse på retshåndhævelsesområdet.* [Online]
Available at: https://www.ft.dk/ripdf/samling/20161/beslutningsforslag/b3/20161_b3_som_fremsat.pdf

Folketingstidende C, 2016. *Folketingsbeslutning om Danmarks tilslutning på mellemstatsligt grundlag til EU's direktiv om databeskyttelse på retshåndhævelsesområdet.* [Online]
Available at: https://www.ft.dk/ripdf/samling/20161/beslutningsforslag/b3/20161_b3_som_vedtaget.pdf

Grundgesetz, art. 2(1), 2023. *Legislation in Hesse and Hamburg regarding automated data analysis for the prevention of criminal acts is unconstitutional.* [Online]
Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html

Grundgesetz, 2023. *Legislation in Hesse and Hamburg regarding automated data analysis for the prevention of criminal acts is unconstitutional.* [Online]
Available at: https://www.bundesverfassungsgericht.de/SharedDocs/Pressemitteilungen/EN/2023/bvg23-018.html

Jasserand, C., 2018, august. Subsequent Use of GDPR Data for a Law Enforcement Purpose: The Forgotten Principle of Purpose Limitation?. *European Data Protection Law Review, Vol. 4, Issue 2*, August, pp. 152-167.

Jasserand, C., 2018. Law enforcement access to personal data originally collected by private parties: Missing data subjects' safeguards in directive 2016/680?. *Computer Law & Security Review, volume 34, issue 1*, Februar, pp. 154-165.

Justitsministeriet, 25. november 2016. *Besvarelse af spørgsmål nr. 52 (Alm. del).* [Online]
Available at: https://www.ft.dk/samling/20161/almdel/reu/spm/52/svar/1362234/1693008.pdf
[Senest hentet eller vist den 24 april 2024].

Koning, E. M., 2020. *The purpose and limitations of purpose limitation.* [Online]
Available at: https://merelkoning.nl/wp-content/uploads/2020/10/M.Koning_The-purpose-and-limitations-of-purpose-limitation_thesis.pdf

L 168 lovforslag retshåndhævelsesloven, 2017. s.l.: s.n.

L 171 lovforslag til ændring af politiloven, 2017. *Politiets anvendelse af databaserede analyseredskaber og adgang til oplysninger om flypassagerer,* s.l.: s.n.

LBKG 2022-12-25 nr. 1655 Retsplejeloven, u.d. s.l.: s.n.

Lov 2018-12-27 nr. 1706 (PNR-loven), u.d. s.l.: s.n.

Marquenie, T., 2017. The Police and Criminal Justice Authorities Directive: Data protection standards and impact on the legal framework. *Computer Law & Security Review*, juni, 3(33), pp. 324-340.

Møller, P. A. o. G. V., 3. november 2023. POL-INTEL: Lad os tale om de menneskeretlige og demokratiske konsekvenser af datadrevet politi. *Radar.*

Politi.dk, u.d. *Politiets brug af personoplysninger.* [Online]
Available at: https://politi.dk/hjemmesiden/politiets-brug-af-personoplysninger

Radar, 2023. *POL-INTEL: Lad os tale om de menneskeretlige og demokratiske konsekvenser af datadrevet politi.* [Online]
Available at: https://radar.dk/holdning/pol-intel-lad-os-tale-om-de-menneskeretlige-og-demokratiske-konsekvenser-af-datadrevet-politi

retshåndhævelsesloven, J. -. f. t., 2017. *L 168 Forslag til lov om retshåndhævende myndigheders behandling af personoplysninger..* [Online]
Available at: https://www.ft.dk/samling/20161/lovforslag/l168/index.htm

Retsudvalget – endeligt svar på spørgsmål 946, 2021. *REU Alm.del – endeligt svar på spørgsmål 946.* [Online]
Available at: https://www.ft.dk/samling/20201/almdel/reu/spm/946/svar/1780435/2390655.pdf

Retsudvalget 2009-10, 2010. *Svar på spørgsmål 751.* [Online]
Available at: https://www.ft.dk/samling/20091/almdel/reu/spm/751/svar/732486/877565.pdf

Retsudvalget 2018-19 (2. samling), 2019. *Besvarelse af spørgsmål nr. 459 (Alm. del).* [Online]
Available at: https://www.ft.dk/samling/20182/almdel/reu/spm/459/svar/1600396/2093978/index.htm

Retsudvalget 2019-20, 2020. *REU Alm.del – endeligt svar på spørgsmål 1182.* [Online]
Available at: https://www.ft.dk/samling/20191/almdel/reu/spm/1182/svar/1657456/2188189.pdf

Retsudvalget 2020-21, svar på spørgsmål 946, 2019. *Gevinstrealiseringsrapport POL-INTEL.* [Online]
Available at: https://www.ft.dk/samling/20201/almdel/reu/spm/946/svar/1780435/2390656.pdf

Retsudvalget 2020-21, 2021. *Besvarelse af spørgsmål nr. 948 (Alm. del) fra Folketingets Retsudvalg.* [Online]
Available at: https://www.ft.dk/samling/20201/almdel/reu/spm/948/svar/1780433/2390648.pdf

Retsudvalget 2022-23 (2. samling), 2023. *REU Alm.del – endeligt svar på spørgsmål 362.* [Online]
Available at: https://www.ft.dk/samling/20222/almdel/reu/spm/362/svar/1944601/2683792.pdf

Retsudvalget 2022-23 (2. samling), 2023. *Udfordringer på it-området i politiet og igangsatte tiltag.* [Online]
Available at: https://www.ft.dk/samling/20222/almdel/REU/bilag/184/2707465.pdf

Retsudvalget 2022-23 (2. samling), u.d. *Udfordringer på it-området i politiet og igangsatte tiltag.* [Online]
Available at: https://www.ft.dk/samling/20222/almdel/REU/bilag/184/2707466.pdf

Retsudvalg, F., 2020. REU besøg i Rigs politiet 170120_Præsentation af nye værktøjer_til ft.dk *(pdf-version).* [Online]
Available at: https://www.ft.dk/samling/20191/almdel/reu/bilag/232/index.htm
[Senest hentet eller vist den januar 2024].

Rigspolitiet, 2016. *Orientering vedrørende Politiets Efterforskningsstøtte Database (PED).* [Online]
Available at: https://www.ft.dk/samling/20151/almdel/REU/bilag/289/1626705.pdf

Rytter, J. E., 2023. *Individets grundlæggende rettigheder.* 5. udgave red. s.l.:Karnov Group.

Sørensen, K. E., 2018. Pligten til EU-konform fortolkning. I: *EU-retten i Danmark.* s.l.:Djøf forlag.

Statsministeriet, 2016. *Her er erklæringen om Danmarks fremtidige tilknytning til Europol.* [Online]
Available at: https://www.regeringen.dk/nyheder/2016/her-er-erklaeringen-om-danmarks-fremtidige-tilknytning-til-europol/
[Senest hentet eller vist den 11. oktober 2023].

Sunde, I. M., 2023. To have or have not: Limiting the data available for subsequent use by the police. *New Joornal of European Criminal Law,* Vol 0(0), pp. 1-17.

Sunde, N. & S. I., 2022. Conceptualizing anAI-based PoliceRobotforPreventingOnline-ChildSexualExploitationandAbuse:Part 2 – Legal Analysis of PrevBOT. *Nordic Journal of Studies in Policing*, december, pp. 1-15.

Union, D. E., (2010/C 83/02). *CHARTER OM GRUNDLÆGGENDE RETTIGHEDER*. s.l.:s.n.

Vogiatzoglou, P. & Marquenie, T., 2022. *Assessment of the implementation of the Law Enforcement Directive.* [Online]
Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)740209

Østli Jakobsen, H., 2022. [Online] Available at: https://www.skup.no/sites/default/files/2022-02/palantir-metoderapport.pdf