EUROPA-
KOMMISSIONEN

Bruxelles, den 10.1.2017
COM(2017) 7 final

MEDDELELSE FRA KOMMISSIONEN TIL EUROPA-PARLAMENTET OG RÅDET

om udveksling og beskyttelse af personoplysninger i en globaliseret verden

1. INDLEDNING

Beskyttelsen af personoplysninger indgår i Europas fælles konstitutionelle opbygning og er forankret i artikel 8 i EU's charter om grundlæggende rettigheder. Denne beskyttelse har været et centralt aspekt i EU-retten i over 20 år lige fra databeskyttelsesdirektivet i 1995[1] ("1995-direktivet") til vedtagelsen af den generelle forordning om databeskyttelse (GDPR)[2] og politidirektivet[3] i 2016.

Som kommissionsformand Jean-Claude Juncker understregede i sin tale om Unionens tilstand den 14. september 2016: "*At være europæer betyder, at du har ret til at få dine personoplysninger beskyttet af stærk europæisk lovgivning. […] For privatlivets fred betyder noget i Europa. Det er et spørgsmål om menneskelig værdighed*."

Behovet for beskyttelse af personoplysninger er imidlertid ikke begrænset til Europa. Forbrugere i hele verden sætter i stigende grad pris på deres privatliv. Virksomhederne anerkender i denne forbindelse, at en stærk beskyttelse af privatlivets fred giver dem en konkurrencefordel, da tilliden til deres tjenester styrkes. Mange virksomheder, navnlig globalt orienterede virksomheder, tilpasser deres privatlivspolitikker til GDPR, både fordi de ønsker at gøre forretninger i EU, og fordi de betragter forordningen som en model, der bør følges.

En række lande og regionale organisationer uden for EU i vores umiddelbare nabolande til Asien, Latinamerika og Afrika vedtager ligeledes nye eller ajourfører eksisterende databeskyttelsesregler for at udnytte de muligheder, der knytter sig til den globale digitale økonomi, og imødegår den voksende efterspørgsel efter en stærkere beskyttelse af data og privatlivets fred. Selv om der forskelle mellem landene med hensyn til deres tilgang og lovgivningsmæssige udvikling, er der tegn på større konvergens i retning af vigtige databeskyttelsesprincipper, navnlig i visse regioner i verden[4]. Større forenelighed mellem forskellige databeskyttelsessystemer vil fremme internationale strømme af personoplysninger, både i kommercielt øjemed eller med henblik på samarbejde mellem offentlige myndigheder (f.eks. om retshåndhævelse). EU bør gribe denne mulighed for at fremme sine databeskyttelsesværdier og fremme datastrømme ved at tilskynde til konvergens mellem retssystemer. Som bebudet i Kommissionens arbejdsprogram[5] redegøres der i nærværende

---

1 Europa-Parlamentets og Rådets direktiv 95/46/EF af 24. oktober 1995 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger (EFT L 281 af 23.11.1995).

2 Europa-Parlamentets og Rådets forordning (EU) 2016/679 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med behandling af personoplysninger og om fri udveksling af sådanne oplysninger og om ophævelse af direktiv 95/46/EF (generel forordning om databeskyttelse) (EUT L 119 af 4.5.2016, s. 1-188). Den trådte i kraft den 24. maj 2016 og finder anvendelse fra den 25. maj 2018.

3 Europa-Parlamentets og Rådets direktiv (EU) 2016/680 af 27. april 2016 om beskyttelse af fysiske personer i forbindelse med kompetente myndigheders behandling af personoplysninger med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger eller fuldbyrde strafferetlige sanktioner og om fri udveksling af sådanne oplysninger og om ophævelse af Rådets rammeafgørelse 2008/977/RIA (EUT L 119 af 4.5.2016, s. 89-131). Det trådte i kraft den 5. maj 2016. EU-medlemsstaterne skal gennemføre direktivet i national lovgivning senest den 6. maj 2018.

4 Jf. "Data protection regulations and international data flows: Implications for trade and development", UNCTAD (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf

5 Kommissionens arbejdsprogram 2017 – Realisering af et Europa, der beskytter, styrker og forsvarer, COM(2016) 710 final af 25.10.2016, s. 12, og bilag 1.

meddelelse for Kommissionens strategiske ramme for "afgørelser om tilstrækkeligheden af beskyttelsesniveauet" samt for andre redskaber til videregivelse af oplysninger og internationale instrumenter på databeskyttelsesområdet.

2. EU'S DATABESKYTTELSESREFORMPAKKE – EN MODERNE LOVGIVNINGSRAMME TIL FREMME AF INTERNATIONALE DATASTRØMME MED ET HØJT BESKYTTELSESNIVEAU

Med reformen af databeskyttelseslovgivningen, der blev vedtaget i april 2016, indføres et system, der både sikrer et højt beskyttelsesniveau og er åbent for mulighederne i det globale informationssamfund. Reformen sikrer enkeltpersoner større kontrol over deres personoplysninger og styrker således forbrugernes tillid til den digitale økonomi. En harmonisering og forenkling af lovgivningen gør det nemmere og mindre byrdefuldt for både indenlandske og udenlandske virksomheder at udøve deres virksomhed i EU, herunder gennem international udveksling af oplysninger. I dag kombinerer EU åbenhed over for internationale datastrømme med det højeste beskyttelsesniveau for fysiske personer. EU har potentiale til at blive et center for datatjenester, hvilket både forudsætter frie strømme og tillid.

2.1 En omfattende og forenklet fælles EU-ramme for databeskyttelse

I EU-reformen fastlægges en omfattende ramme for beskyttelse af personoplysninger i både den private og offentlige sektor og inden for både handel og retshåndhævelse (henholdsvis GDPR og politidirektivet).

I henhold til GDPR vil der fra maj 2018 være ét enkelt paneuropæisk regelsæt i stedet for de nuværende 28 nationale lovgivninger. Den nyligt etablerede one-stop-shop-mekanisme vil sikre, at en enkelt databeskyttelsesmyndighed vil være ansvarlig for overvågningen af en EU-virksomheds grænseoverskridende databehandlingsaktiviteter. Det sikres således, at de ny regler fortolkes ensartet. I grænseoverskridende sager med inddragelse af flere nationale databeskyttelsesmyndigheder, vil der navnlig blive truffet en enkelt afgørelse for at sikre fælles løsninger på fælles problemer. GDPR sikrer desuden lige konkurrencevilkår mellem EU-virksomheder og udenlandske virksomheder, da virksomheder, som er baseret uden for EU, skal anvende de samme regler som europæiske virksomheder, hvis de udbyder varer og tjenesteydelser eller overvåger enkeltpersoners adfærd i EU. En større forbrugertillid vil både være til gavn for EU og eksterne kommercielle operatører.

Politidirektivet indeholder fælles regler om behandling af personoplysninger om enkeltpersoner, der er involveret i straffesager som mistænkte, ofre eller vidner, under hensyntagen til den særlige karakter af politisamarbejdet og det retlige samarbejde i straffesager. En harmonisering af databeskyttelsesreglerne inden for retshåndhævelse, herunder reglerne om internationale overførsler, vil fremme det grænseoverskridende politisamarbejde og retlige samarbejde mellem myndighederne, både i EU og med

internationale partnere, og således skabe de rette betingelser for en mere effektiv bekæmpelse af kriminalitet. Dette er et vigtigt bidrag til den europæiske dagsorden om sikkerhed[6].

2.2 En ny og diversificeret værktøjskasse til internationale overførsler

EU-databeskyttelsesreglerne har lige fra starten omfattet en række mekanismer til brug for international videregivelse af oplysninger. Det primære formål med disse regler er at sikre beskyttelsen af europæiske borgeres personoplysninger ved videregivelse til andre lande. Disse regler har gennem årene sat standarden for internationale datastrømme i mange jurisdiktioner. Selv om arkitekturen i bund og grund er den samme som i 1995-direktivet, præciserer og forenkler reformen af reglerne om internationale overførsler deres anvendelse, og der indføres nye redskaber til videregivelse.

I henhold til EU-retten kan personoplysninger bl.a. overføres til andre lande på grundlag af Kommissionens afgørelse om "tilstrækkeligheden af beskyttelsesniveauet", hvori det fastslås, at et tredjeland skal sikre et databeskyttelsesniveau, "som i det væsentlige svarer"[7] til det, der sikres i EU. Formålet med denne afgørelse er at sikre fri udveksling af personoplysninger med det pågældende tredjeland, uden at dataeksportøren skal stille yderligere garantier eller opnå godkendelse. Et nøjagtigt og detaljeret katalog over elementer, der skal tages i betragtning ved vurderingen af tilstrækkeligheden af beskyttelsesniveauet i et udenlandsk system, er tilgængeligt for interesserede lande eller internationale organisationer[8]. Kommissionen kan nu også vedtage afgørelser om tilstrækkeligheden af beskyttelsesniveauet på håndhævelsesområdet[9]. Med udgangspunkt i praksis i henhold til 1995-direktivet giver reformen desuden mulighed for at vurdere tilstrækkeligheden af beskyttelsesniveauet i et specifikt område i et tredjeland eller en specifik sektor eller industri i et tredjeland (såkaldt "delvis" tilstrækkelighed)[10].

Hvis der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, kan internationale overførsler foretages ved brug af en række alternative redskaber til videregivelse, som sikrer de fornødne databeskyttelsesgarantier[11]. Reformen formaliserer og

---

6 Meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget, Den europæiske dagsorden om sikkerhed (COM(2015) 185 final af 28.4.2015).

7 Domstolens dom af 6. oktober 2015 i sag C-362/14, Maximillian Schrems mod Data Protection Commissioner, præmis 73, 74 og 96. Se også betragtning 104 i GDPR og betragtning 67 i politidirektivet, hvor der henvises til standarden om et "i det væsentlige" tilsvarende niveau.

8 Jf. artikel 45 i GDPR. Som fastsat i artikel 45, stk. 2, skal Kommissionen ved sin vurdering bl.a. tage højde for retsstatsprincippet, respekt for menneskerettighederne og de grundlæggende frihedsrettigheder og relevant lovgivning, herunder inden for databeskyttelse, offentlig sikkerhed, forsvar, statens sikkerhed og strafferet og offentlige myndigheders adgang til personoplysninger. Disse elementer skal understøttes af effektive rettigheder, som kan håndhæves, herunder adgang til effektiv administrativ og retslig prøvelse for enkeltpersoner og en velfungerende uafhængig tilsynsmyndighed, der skal sikre og håndhæve, at databeskyttelsesreglerne overholdes. Der vil ligeledes blive taget hensyn til retligt bindende konventioner, navnlig Europarådets konvention nr. 108, og deltagelse i multilaterale eller regionale systemer på databeskyttelsesområdet.

9 De specifikke elementer i vurderingen af beskyttelsesniveauets tilstrækkelighed er fastsat i artikel 36, stk. 2, i politidirektivet.

10 Jf. artikel 45, stk. 1, i GDPR, og artikel 36, stk. 1, i politidirektivet.

11 Jf. f.eks. meddelelse fra Kommissionen til Europa-Parlamentet og Rådet om videregivelse af personoplysninger fra EU til USA i henhold til direktiv 95/46/EF efter Domstolens dom i sag C-362/14 (Schrems) (COM(2015) 566 final af 6.11.2015).

øger mulighederne for at anvende eksisterende instrumenter såsom standardkontraktbestemmelser[12] og bindende virksomhedsregler[13]. Nu kan standardkontraktbestemmelser f.eks. inkluderes i en kontrakt mellem EU-baserede databehandlere og databehandlere i et tredjeland (såkaldte "databehandler-til-databehandler"-standardbestemmelser)[14]. Med hensyn til bindende virksomhedsregler, der indtil videre har været begrænset til enheder i samme koncern, kan de nu anvendes af en gruppe af foretagender, der udøver en fælles økonomisk aktivitet, men ikke nødvendigvis indgår i samme koncern[15]. Reformen mindsker ligeledes bureaukratiet ved at fjerne generelle krav om forudgående anmeldelse til og godkendelse fra databeskyttelsesmyndighederne af videregivelse af oplysninger til et tredjeland baseret på standardkontraktbestemmelser og bindende virksomhedsregler[16]. Dette er en vigtig forenkling af EU-systemet for international videregivelse af oplysninger, da disse krav, der i øjeblikket er forskellige i medlemsstaterne, ofte betragtes som en væsentlig hindring for datastrømme, navnlig for mindre virksomheder[17].

Derudover indfører reformen nye instrumenter vedrørende internationale overførsler[18]. Dataansvarlige og databehandlere vil på visse betingelser[19] få mulighed for at anvende godkendte adfærdskodekser eller certificeringsmekanismer (f.eks. privatlivsmærkninger eller -mærker) for at sikre "fornødne garantier". Dette burde gøre det muligt at udvikle mere skræddersyede løsninger vedrørende internationale overførsler, der f.eks. afspejler en specifik sektors eller industris eller specifikke datastrømmes særlige karakter. Det gør det ligeledes muligt at sikre de fornødne garantier for overførsel af oplysninger mellem offentlige myndigheder eller organer på grundlag af internationale aftaler eller administrative ordninger[20]. Endelig præciserer GDPR anvendelsen af de såkaldte "undtagelser"[21] (samtykke, opfyldelse af en kontrakt eller vigtige samfundsinteresser), som enheder i specifikke situationer kan basere deres dataoverførsler på, hvis der ikke er vedtaget en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, og uanset om et af ovennævnte instrumenter anvendes. Forordningen indeholder navnlig en ny, om end begrænset undtagelse om overførsler, der kan foretages i forbindelse med en virksomheds forfølgelse af legitime interesser[22].

---

12 I standardkontraktbestemmelserne fastlægges EU-eksportørens og det importerende tredjelands databeskyttelsesforpligtelser.

13 Bindende virksomhedsregler er interne regler vedtaget af en multinational koncern vedrørende videregivelse af oplysninger inden for samme koncern til enheder beliggende i lande, som ikke sikrer et tilstrækkeligt beskyttelsesniveau. 1995-direktivet indeholder allerede bestemmelser om bindende virksomhedsregler, men disse kodificeres og deres rolle som et redskab til videregivelse af oplysninger formaliseres i GDPR.

14 Jf. artikel 46, stk. 2, litra c) og d), og betragtning 168 i GDPR.

15 Jf. artikel 46, stk. 2, litra b), artikel 47 og betragtning 110 i GDPR.

16 Jf. artikel 46, stk. 2, i GDPR.

17 Disse registreringskrav udgør en handelshindring for mange virksomheder, navnlig SMV'er, hvilket bl.a. blev fremhævet i UNCTAD-rapporten, s. 34.

18 Jf. artikel 46, stk. 2, litra e) og f), i GDPR.

19 Ingen dataansvarlige uden for EU vil kunne overholde en EU-adfærdskodeks eller certificeringsmekanisme ved gennem kontrakter eller andre retligt bindende instrumenter at afgive bindende tilsagn, som kan håndhæves, om at anvende databeskyttelsesgarantierne i disse instrumenter, jf. artikel 42, stk. 2, i GDPR.

20 Jf. artikel 46, stk. 2, litra a), og artikel 46, stk. 3, litra b), i GDPR.

21 Jf. artikel 49 i GDPR.

22 Jf. artikel 49, stk. 1, andet afsnit.

Endelig tillægger reformen Kommissionen beføjelser til at udvikle mekanismer for internationalt samarbejde for at lette håndhævelsen af databeskyttelsesreglerne, herunder gennem ordninger for gensidig bistand[23]. Dette er en anerkendelse af, at et tættere samarbejde mellem myndighederne på internationalt plan både kan sikre en mere effektiv beskyttelse af den enkeltes rettigheder og større retssikkerhed for virksomhederne.

3. INTERNATIONAL VIDEREGIVELSE AF OPLYSNINGER INDEN FOR HANDEL: FREMME AF HANDEL GENNEM BESKYTTELSE AF PRIVATLIVETS FRED

Beskyttelse af privatlivets fred er en forudsætning for stabile, sikre og konkurrencedygtige globale handelsstrømme. Privatlivets fred er ikke en handelsvare[24]. Internettet og digitalisering af varer og tjenesteydelser har ændret den globale økonomi, og grænseoverskridende overførsel af oplysninger, herunder personoplysninger, er et led i europæiske virksomheders daglige drift, uanset størrelse og sektor. Da samhandel i stigende grad afhænger af udveksling af personoplysninger, er beskyttelsen af privatlivets fred og datasikkerheden i denne forbindelse blevet en central faktor for forbrugertilliden. To tredjedele af europæerne anfører f.eks., at de er bekymret over, at de ikke har kontrol over de oplysninger, de giver online, og halvdelen af respondenterne er bange for at blive ofre for svig[25]. Europæiske virksomheder, der opererer i visse tredjelande, pålægges samtidig i stigende grad protektionistiske restriktioner, der ikke kan begrundes i legitime hensyn til privatlivets fred.

I den digitale tidsalder skal fremme af høje databeskyttelsesstandarder og af international handel nødvendigvis gå hånd i hånd. Selv om beskyttelsen af personoplysninger ikke er til forhandling[26] i handelsaftaler, er EU-systemet for international videregivelse af oplysninger som ovenfor beskrevet en bred og varieret værktøjskasse, der gør det muligt at videregive oplysninger i forskellige situationer og samtidig sikre et højt beskyttelsesniveau.

3.1 Afgørelser om tilstrækkeligheden af beskyttelsesniveauet

En afgørelse om tilstrækkeligheden af beskyttelsesniveauet sikrer fri udveksling af personoplysninger fra EU, uden at EU-dataeksportøren skal gennemføre yderligere garantier eller pålægges yderligere betingelser. Ved at konkludere, at retsordenen sikrer et tilstrækkeligt beskyttelsesniveau, anerkendes det i afgørelsen, at det pågældende lands system svarer til EU-medlemsstaternes system. Overførsler til det pågældende land vil således blive sidestillet med dataoverførsler inden for EU og således give privilegeret adgang til EU's indre marked, og EU-operatører vil få adgang til nye kommercielle kanaler. Som forklaret ovenfor forudsætter denne anerkendelse nødvendigvis et beskyttelsesniveau, som svarer til (eller "i det væsentlige svarer til")[27] det, der sikres i Unionen. Dette indebærer en omfattende vurdering af

---

23 Jf. artikel 50 i GDPR.

24 Jf. f.eks. meddelelse fra Kommissionen til Europa-Parlamentet, Rådet, Det Europæiske Økonomiske og Sociale Udvalg og Regionsudvalget – Handel for alle – En mere ansvarlig handels- og investeringspolitik, COM(2015) 497 final af 14.10.2015, s. 7.

25 Special Eurobarometer 431 – Data protection, juni 2015.

26 Kommissionsformand Jean-Claude Junckers politiske retningslinjer: *En ny start for Europa: Min dagsorden for job, vækst, retfærdighed og demokratisk forandring.*

27 Jf. fodnote 7.

tredjelandets system, herunder landets regler for de offentlige myndigheders adgang til personoplysninger med henblik på beskyttelsen af den nationale sikkerhed, retshåndhævelse og andre offentlige interesser.

Som bekræftet i 2015 af Domstolen i Schremsafgørelsen forudsætter kravet om tilstrækkelig beskyttelse samtidig ikke, at alle EU-regler duplikeres fuldt ud[28]. Testen består nærmere i, om det pågældende udenlandske system som helhed sikrer det krævede høje beskyttelsesniveau gennem kerneindholdet i retten til privatlivets fred og den effektive gennemførelse, håndhævelse og overvågning heraf. Som det fremgår af de afgørelser om tilstrækkeligheden af beskyttelsesniveauet, der er vedtaget indtil videre, kan Kommissionen anerkende en række forskellige systemer til beskyttelse af privatlivets fred, der repræsenterer forskellige retstraditioner, som tilstrækkelige. Disse afgørelser vedrører lande, der er nært integreret med EU og medlemsstaterne (Schweiz, Andorra, Færøerne, Guernsey, Jersey, Isle of Man), vigtige handelspartnere (Argentina, Canada, Israel, USA) og lande, der har en pionerrolle i udviklingen af databeskyttelsesregler i deres region (New Zealand, Uruguay).

Afgørelserne om Canada og USA er afgørelser om "delvis" tilstrækkelighed. Afgørelsen om Canada finder kun anvendelse på private enheder, der er omfattet af Canadas lov om beskyttelse af personoplysninger og elektroniske dokumenter. Den nyligt vedtagne afgørelse om EU's og USA's værn om privatlivets fred[29] er en særlig ordning, der i mangel af en generel databeskyttelseslovgivning i USA[30] er baseret på de deltagende virksomheders forpligtelser til at anvende de høje databeskyttelsesstandarder, som er fastlagt i denne ordning, der efterfølgende kan kræves opfyldt i henhold til amerikansk ret. Værnet om privatlivets fred er desuden baseret på den amerikanske regerings specifikke udredninger og garantier vedrørende adgang til nationale sikkerhedsformål[31], som understøtter afgørelsen om tilstrækkeligheden af beskyttelsesniveauet. Opfyldelsen af disse forpligtelser vil blive tæt overvåget af Kommissionen og vil indgå i den årlige gennemgang af lovrammens virkning.

Igennem de senere år har flere og flere lande verden over vedtaget ny lovgivning om databeskyttelse og beskyttelse af privatlivets fred eller er i færd med at gøre det. I 2015 havde 109 lande vedtaget lovgivning om databeskyttelse og beskyttelse af privatlivets fred, hvilket er en betydelig stigning fra 76 lande i midten af 2011[32]. Derudover er 35 lande i færd med at udarbejde forslag til databeskyttelsesregler[33]. Disse nye eller moderniserede love er ofte baseret på en række centrale principper, herunder bl.a. anerkendelsen af databeskyttelse som en grundlæggende ret, vedtagelsen af rammelovgivning på dette område, indførelsen af

---

28 Jf. Schremsafgørelsens præmis 74.

29 Kommissionens gennemførelsesafgørelse (EU) 2016/1250 af 12. juli 2016.

30 Kommissionen opfordrer USA til at bestræbe sig på at skabe et omfattende system for beskyttelse af privatlivets fred og databeskyttelse, således at der på langt sigt kan opnås konvergens mellem de to systemer. Jf. meddelelse fra Kommissionen til Europa-Parlamentet og Rådet, Transatlantiske datastrømme: genoprettelse af tilliden via stærke garantier (COM(2016) 117 final af 29.2.2016).

31 Dette omfatter navnlig anvendelsen af præsidentielt politisk direktiv 28 (PPD-28), der pålægger en række begrænsninger for "signalefterretningsaktiviteter" og udpegning af en særlig ombudsmand, som skal behandle klager fra EU-borgere på dette område.

32 G. Greenleaf, "Global data privacy laws 2015: 109 countries, with European laws now in a minority", (2015) 133 Privacy Laws & Business International Report, s. 14-17.

33 UNCTAD-undersøgelse, s. 8 og 42 (fodnote 4 ovenfor).

individuelle rettigheder, der kan håndhæves, og oprettelsen af en uafhængig tilsynsmyndighed. Dette giver nye muligheder, navnlig gennem afgørelser om tilstrækkeligheden af beskyttelsesniveauet, for at fremme datastrømme og samtidig garantere et fortsat højt niveau for beskyttelse af personoplysninger.

I henhold til EU-retten forudsætter en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, at der findes databeskyttelsesregler, som svarer til reglerne i EU[34]. Dette vedrører både de materielle regler om beskyttelse af personoplysninger og de relevante tilgængelige tilsyns- og klagemekanismer i tredjelandet.

Inden for rammerne for afgørelser om tilstrækkeligheden af beskyttelsesniveauet mener Kommissionen, at der skal tages hensyn til følgende kriterier ved vurderingen af, med hvilke lande der bør indledes en dialog om tilstrækkeligheden[35]:

i) omfanget af EU's (faktiske eller potentielle) handelsforbindelser med et bestemt tredjeland, herunder eksistensen af en frihandelsaftale eller igangværende forhandlinger

ii) omfanget af strømmene af personoplysninger fra EU, der afspejler geografiske og/eller kulturelle bånd

iii) tredjelandets pionerrolle inden for beskyttelse af privatlivets fred og databeskyttelse, der kunne tjene som model for andre lande i regionen[36]

iv) de overordnede politiske forbindelser med det pågældende tredjeland, navnlig i forbindelse med fremme af fælles værdier og fælles mål på internationalt plan.

Ud fra disse betragtninger vil Kommissionen aktivt gå i dialog med centrale handelspartnere i Øst- og Sydøstasien, i første omgang med Japan og Korea i 2017[37], og – afhængigt af fremskridt i moderniseringen af sine databeskyttelsesregler – med Indien, men også med lande i Latinamerika, navnlig Mercosur, og det europæiske naboskabsområde, der har udtrykt interesse i at få en "afgørelse af tilstrækkeligheden af beskyttelsesniveauet". Derudover glæder Kommissionen sig over interessetilkendegivelserne fra andre tredjelande, som er villige til at samarbejde på disse områder. Drøftelserne om en mulig afgørelse af tilstrækkeligheden af beskyttelsesniveauet er en tovejsdialog, som indebærer, at der skal tilvejebringes nødvendige præciseringer af EU-databeskyttelsesreglerne og findes metoder, der øger konvergensen af tredjelandenes lovgivning og praksis.

---

[34] I denne forbindelse tager Kommissionen ligeledes hensyn til tredjelandets forpligtelser, der følger af retligt bindende konventioner, navnlig tredjelandets tiltrædelse af konvention nr. 108 og tillægsprotokollen hertil, ved vurderingen af tilstrækkeligheden, jf. artikel 45, stk. 2, litra c), og betragtning 105 i GDPR.

[35] For så vidt angår lande, med hvilke det er relevant at samarbejde om intern sikkerhed og retshåndhævelse, vil Kommissionen undersøge mulighederne for specifikke afgørelser om tilstrækkeligheden af beskyttelsesniveauet i henhold til politidirektivet, jf. afsnit 4.

[36] Dette kan navnlig være relevant for udviklings- og overgangslande, da beskyttelsen af personoplysninger både er et afgørende element i retsstatsprincippet og en vigtig faktor for økonomisk konkurrenceevne.

[37] Japan og Korea har for nylig vedtaget eller moderniseret deres lovgivning med henblik på indførelse af omfattende databeskyttelsesordninger.

I visse situationer kan det i stedet for at anvende en landsdækkende tilgang være mere hensigtsmæssigt at gøre brug af andre muligheder såsom delvis eller sektorspecifik tilstrækkelighed (f.eks. inden for finansielle tjenester eller IT), som kan vedrøre geografiske områder eller industrier, der udgør en vigtig del af et bestemt tredjelands økonomi. Der skal i denne forbindelse tages hensyn til elementer såsom karakteren af ordningen til beskyttelse af privatlivets fred, herunder udviklingsstadiet (selvstændig lov, flere love eller særlove osv.), tredjelandets forfatningsopbygning, eller om visse erhvervssektorer er særligt eksponeret for datastrømme fra EU.

Vedtagelsen af en afgørelse om tilstrækkeligheden af beskyttelsesniveauet indebærer etablering af en specifik dialog og et tæt samarbejde med det pågældende tredjeland. Afgørelser om tilstrækkeligheden af beskyttelsesniveauet er "levende" dokumenter, som skal overvåges tæt af Kommissionen og tilpasses i tilfælde af en udvikling, der påvirker det beskyttelsesniveau, der sikres af det pågældende tredjeland[38]. Der vil i denne forbindelse blive foretaget periodiske revisioner mindst hvert fjerde år for at tackle nye aspekter og udveksle bedste praksis mellem tætte partnere[39]. Denne dynamiske tilgang finder ligeledes anvendelse på allerede eksisterende afgørelser om tilstrækkeligheden af beskyttelsesniveauet vedtaget i henhold til 1995-direktivet, der skal revideres, hvis de ikke længere opfylder den gældende standard[40]. De pågældende tredjelande opfordres derfor til at underrette Kommissionen om eventuelle relevante ændringer af lovgivning og praksis siden vedtagelsen af afgørelsen om tilstrækkeligheden af beskyttelsesniveauet vedrørende dem. Det er afgørende at sikre disse afgørelsers kontinuitet i henhold til de nye regler i reformen[41].

EU's databeskyttelsesregler er ikke til forhandling i en frihandelsaftale[42]. Selv om dialogen om databeskyttelse og handelsforhandlinger med tredjelande nødvendigvis skal føres særskilt, er en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, herunder en delvis eller sektorspecifik dialog, den bedste tilgang til at opbygge gensidig tillid og sikre en gnidningsløs overførsel af personoplysninger og således fremme handelssamkvem, der involverer overførsel af personoplysninger til det pågældende tredjeland. Sådanne afgørelser kan derfor lette handelsforhandlingerne eller supplere eksisterende handelsaftaler, således at de bliver

---

38 I henhold til artikel 45, stk. 4 og 5, i GDPR skal Kommissionen løbende overvåge udviklingen i tredjelande og have beføjelse til at ophæve, ændre eller suspendere en afgørelse om tilstrækkeligheden af beskyttelsesniveauet, hvis den finder, at det pågældende land ikke længere sikrer et tilstrækkeligt beskyttelsesniveau.

39 Artikel 45, stk. 3, i GDPR.

40 I henhold til artikel 97, stk. 2, litra a), i GDPR skal Kommissionen forelægge Europa-Parlamentet og Rådet en evalueringsrapport senest i 2020.

41 Som opfølgning på Schremsafgørelsen, i hvilken Domstolen fastslog, at Kommissionen havde overskredet sin kompetence ved at begrænse databeskyttelsesmyndighedernes beføjelser til at suspendere eller forbyde dataoverførsel i safe harbor-beslutningen, vedtog Kommissionen den 16. december 2016 en "omnibusafgørelse", hvori tilsvarende bestemmelser i gældende afgørelser om tilstrækkeligheden af beskyttelsesniveauet blev erstattet med bestemmelser, hvori der blot stilles krav om underretning mellem medlemsstaterne og Kommissionen, hvis en databeskyttelsesmyndighed suspenderer eller forbyder overførsler til et tredjeland. I omnibusafgørelsen pålægges Kommissionen ligeledes at overvåge enhver relevant udvikling i tredjelande, jf. EUT L 355 af 17.12.2016, s. 83.

42 En afgørelse om tilstrækkeligheden af beskyttelsesniveauet er navnlig en unilateral gennemførelsesafgørelse truffet af Kommissionen i overensstemmelse med EU's databeskyttelsesregler på grundlag af kriterierne fastlagt i disse regler.

mere fordelagtige. Ved at fremme konvergensen mellem beskyttelsesniveauet i EU og tredjelandet reducerer en afgørelse om tilstrækkeligheden af beskyttelsesniveauet samtidig risikoen for, at det pågældende land gør grunde relateret til beskyttelsen af personoplysninger gældende med det formål at stille uberettigede datalokaliserings- og datalagringskrav. Som anført i meddelelsen om handel for alle vil Kommissionen desuden tilstræbe at anvende EU til at fastsætte regler for e-handel og grænseoverskridende datastrømme og bekæmpe nye former for digital protektionisme, i fuld overholdelse af og uden at det berører EU's databeskyttelsesregler[43].

Kommissionen vil:

- prioritere drøftelser om mulige afgørelser om tilstrækkeligheden af beskyttelsesniveauet med centrale handelspartnere i Øst- og Sydøstasien, i første omgang med Japan og Korea i 2017, men ligeledes overveje andre strategiske partnere såsom Indien, og med lande i Latinamerika, navnlig Mercosur, og det europæiske naboskabsområde

- nøje overvåge virkningen af eksisterende afgørelser om tilstrækkeligheden af beskyttelsesniveauet. Dette omfatter navnlig gennemførelsen af ordningen for EU's og USA's værn om privatlivets fred, især gennem den årlige fælles evalueringsmekanisme

- samarbejde med og bistå lande, der er interesseret i at vedtage stærke databeskyttelseslove, og understøtte deres konvergens med EU's databeskyttelsesprincipper.

3.2 Alternative dataoverførselsmekanismer

I EU's databeskyttelsesregler er det altid blevet anerkendt, at der ikke findes en "én for alle"-tilgang til international videregivelse af oplysninger. Dette gælder endnu mere for reglerne i reformen. Selv om der kun vil blive truffet afgørelser om tilstrækkeligheden af beskyttelsesniveauet for de tredjelande, der opfylder de relevante kriterier, indføres der med GDPR en række forskellige mekanismer, som er så fleksible, at de kan tilpasses en række forskellige videregivelsesscenarier. Der kan udvikles instrumenter, hvor der tages højde for specifikke industriers, forretningsmodellers og/eller operatørers særlige behov eller betingelser. Disse kunne f.eks. være standardkontraktbestemmelser tilpasset en bestemt sektors behov, f.eks. specifikke garantier ved behandling af følsomme oplysninger i sundhedssektoren, eller en bestemt type behandlingsaktiviteter, der er udbredt i visse tredjelande, f.eks. outsourcing af tjenester, der udføres på vegne af europæiske virksomheder. Dette kan enten ske ved at vedtage nye standardbestemmelser eller ved at supplere eksisterende bestemmelser med yderligere garantier, lige fra tekniske eller organisatoriske til erhvervsrelaterede tilgange[44]. Nogle specifikke sektorbehov kan også imødekommes gennem bindende virksomhedsregler for grupper af foretagender, der udøver en fælles økonomisk

[43] Jf. meddelelsen om handel for alle, s. 12 (fodnote 24 ovenfor).

[44] Jf. artikel 46, stk. 2, litra c) og d), og betragtning 109 i GDPR, hvori det præciseres, at det er muligt at foretage en tilpasning til godkendte standardbestemmelser, såfremt bestemmelserne hverken direkte eller indirekte er i strid med disse standardbestemmelser eller berører den enkeltes grundlæggende rettigheder eller frihedsrettigheder.

aktivitet, f.eks. i rejsebranchen. I forbindelse med internationale overførsler mellem databehandlere kan der drages fordel af udviklingen af databehandler-til-databehandler-standardkontraktbestemmelser og/eller bindende virksomhedsregler for databehandlere. Endelig giver nye overførselsmekanismer såsom godkendte adfærdskodekser og akkrediterede tredjepartscertificeringer industrien mulighed for at indføre skræddersyede løsninger vedrørende internationale overførsler og samtidig nyde godt af den konkurrencefordel, der f.eks. er knyttet til datasikkerhedsmærkninger eller mærker til beskyttelse af privatlivets fred. Nogle af disse instrumenter kan udvikles som overførselsspecifikke mekanismer eller indgå i mere generelle redskaber til påvisning af overholdelsen af alle bestemmelserne i GDPR såsom en godkendt adfærdskodeks.

Kommissionen vil samarbejde med industrien, civilsamfundet og databeskyttelsesmyndighederne for at udnytte GDPR-værktøjskassens fulde potentiale i forbindelse med internationale overførsler. Den løbende dialog med interessenter i forbindelse med gennemførelsen af reformen vil gøre det nemmere at identificere prioriterede områder i denne henseende. Dette kan omfatte afslutningen af arbejde, der allerede er blevet påbegyndt, f.eks. udarbejdelsen af databehandler-til-databehandler-standardkontraktbestemmelser[45] i samarbejde med Artikel 29-Gruppen (der erstattes af Det Europæiske Databeskyttelsesråd i 2018). Dette kan involvere udvikling af nye komponenter i EU's overholdelsesinfrastruktur, f.eks. ved at Kommissionen definerer krav og tekniske standarder for oprettelse af certificeringsmekanismer og deres funktion, herunder vedrørende aspekter relateret til internationale overførsler[46]. Nogle af disse aspekter kan suppleres af internationale tiltag, navnlig i samarbejde med organisationer, som har udviklet tilsvarende overførselsmekanismer. Man kunne f.eks. undersøge mulighederne for at fremme konvergensen mellem bindende virksomhedsregler i EU-retten og de regler om grænseoverskridende databeskyttelse, som er vedtaget af det økonomiske samarbejde i Asien-Stillehavsområdet (APEC)[47], både vedrørende gældende standarder og ansøgningsproceduren i de enkelte systemer. Dette bør bidrage til at fremme høje databeskyttelsesstandarder på verdensplan og samtidig bygge bro mellem tilgangene til beskyttelse af privatlivets fred og databeskyttelse og gøre det nemmere for kommercielle operatører at navigere mellem forskellige systemer og udforme politikker, der er i overensstemmelse hermed.

Kommissionen vil:

- samarbejde med interessenter om at udvikle alternative mekanismer til overførsel af personoplysninger, der er tilpasset specifikke industriers, forretningsmodellers og/eller operatørers særlige behov eller betingelser.

[45] Der findes på nuværende tidspunkt ingen standardkontraktbestemmelser for dataoverførsler fra databehandlere fra EU til databehandlere fra tredjelande.

[46] Artikel 43, stk. 8 og 9, i GDPR.

[47] Jf. referencedokumentet om APEC/EU Common Referential for the Structure of the EU Binding Corporate Rules og APEC Cross Border Privacy Rules System (CBPR) fra 2014, hvor begge systemers overholdelses- og certificeringskrav sammenlignes: http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf

3.3 Internationalt samarbejde om beskyttelse af personoplysninger

3.3.1. Fremme af databeskyttelsesstandarder gennem multilaterale instrumenter og fora

EU's retlige rammer for databeskyttelse har ofte været referencepunkt på tredjelande, som udarbejder lovgivning på dette område. EU vil fortsat aktivt gå i dialog med sine internationale partnere på både bilateralt og multilateralt plan for at fremme konvergens ved at udvikle høje og interoperable standarder for beskyttelses af personoplysninger på verdensplan. Dette bidrager til en mere effektiv beskyttelse af den enkeltes rettigheder og reducerer samtidig hindringerne for grænseoverskridende datastrømme som et vigtigt element i frihandel.

Kommissionen opfordrer navnlig tredjelande til at tiltræde Europarådets konvention nr. 108 og tillægsprotokollen hertil[48]. Konventionen, der kan tiltrædes af lande, som ikke er medlemmer af Europarådet, og som allerede et blevet ratificeret af 50 lande, herunder af afrikanske og sydamerikanske stater[49], er det eneste bindende multilaterale databeskyttelsesinstrument. Konventionen revideres i øjeblikket, og Kommissionen vil aktivt fremme en hurtig vedtagelse af den moderniserede tekst, således at EU kan tiltræde. Den vil afspejle de principper, der er forankret i EU's nye databeskyttelsesregler, og således bidrage til konvergensen i retning af høje databeskyttelsesstandarder.

G20-mødet i 2017 vil give EU en yderligere mulighed for at arbejde hen imod af konvergens omkring princippet om, at høje databeskyttelsesstandarder er en afgørende komponent i videreudviklingen af et globalt informationssamfund, der kan fremme innovation, vækst og social fremgang[50].

Kommissionen ser ligeledes frem til at samarbejde med vigtige nye aktører såsom FN's særlige rapportør om retten til privatlivets fred[51] og til at videreudvikle sit samarbejde med regionale organisationer såsom APEC for at fremme en global kultur, hvor retten til privatlivets fred og databeskyttelse respekteres.

Som led i sin bredere indsats for at øje bevidstheden om privatlivets fred og styrke databeskyttelsesgarantierne på internationalt plan vedtog Kommissionen den 15. november 2016 et projekt under partnerskabsinstrumentet for at styrke samarbejdet med partnerlande på dette område[52]. Dette vil omfatte finansiering af aktiviteter såsom uddannelse og bevidstgørelse. I forbindelse med gennemførelsen af reformen kan EU drage fordel af

---

48 Europarådets konvention af 28. januar 1981 til beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger (ETS nr. 180) og tillægsprotokollen til konvention om beskyttelse af det enkelte menneske i forbindelse med elektronisk databehandling af personoplysninger vedrørende tilsynsmyndigheder og grænseoverskridende videregivelse af personoplysninger (ETS nr. 181) fra 2001.

49 Mauritius, Senegal og Uruguay har ratificeret konventionen. Kap Verde, Marokko og Tunesien er desuden blevet opfordret til at tiltræde.

50 Se også OECD's ministererklæring "Digital Economy: Innovation, Growth and Social Prosperity" ("Cancun-erklæringen") af 23. juni 2016.

51 Se også: http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

52 Kommissionens gennemførelsesafgørelse C(2016)7198 om godkendelse af anden fase i det årlige handlingsprogram for 2016 (AAP 2016) under partnerskabsinstrumentet.

udvekslingen af bedste praksis og af andre systemers erfaringer med nye udfordringer vedrørende beskyttelsen af privatlivets fred og nye retlige eller tekniske løsninger, herunder inden for håndhævelse, overholdelsesfremmende værktøjer (f.eks. certificeringsmekanismer, vurderinger af indvirkningen på privatlivets fred) eller beskyttelsen af visse specifikke datasæt (f.eks. oplysninger om børn).

3.3.2. Samarbejde om håndhævelse

Det er i stigende grad nødvendigt at styrke samarbejdet med relevante håndhævelses- og tilsynsmyndigheder i tredjelande i lyset af det globale omfang af multinationale virksomheder, der behandler store mængder personoplysninger i et stort antal lande. Problemer med manglende overholdelse af databeskyttelsesreglerne eller brud på datasikkerheden berører ofte mennesker i flere jurisdiktioner samtidig. I disse tilfælde kan beskyttelsen af den enkelte gøres mere effektiv gennem fælles tiltag. Erhvervsdrivende ville samtidig drage fordel af en klarere lovgivning, hvor der udvikles fælles fortolkningsinstrumenter og håndhævelsespraksis på verdensplan.

I en forbundet verden af datastrømme uden grænser er tiden således inde til at styrke samarbejdet mellem retshåndhævende myndigheder[53]. EU er rede til at spille sin rolle. Som anført ovenfor giver GDPR Kommissionen beføjelser til at udvikle mekanismer for internationalt samarbejde for at lette den effektive håndhævelse af databeskyttelsesreglerne, herunder gennem ordninger for gensidig bistand. I denne forbindelse bør muligheden for at udvikle en rammeaftale for samarbejde mellem EU-databeskyttelsesmyndighederne og håndhævelsesmyndighederne i visse tredjelande udforskes, også på grundlag af de erfaringer som Kommissionen har fået på andre håndhævelsesområder såsom konkurrence og forbrugerbeskyttelse.

Kommissionen vil:

- fremme en hurtig vedtagelse af den moderniserede tekst i Europarådets konvention nr. 108, således at EU kan tiltræde, og for at opfordre tredjelande til at tiltræde
- anvende multilaterale fora såsom G20 og APEC for at fremme en global kultur, hvor databeskyttelsesrettighederne respekteres
- udvikle internationale samarbejdsmekanismer sammen med centrale internationale partnere for at fremme en effektiv håndhævelse.

[53] Eksisterende netværk omfatter Global Privacy Enforcement Network (GPEN), der blev oprettet i 2010 i OECD's regi. Det er et uformelt netværk af databeskyttelsesmyndigheder, herunder EU's databeskyttelsesmyndigheder, der bl.a. har til opgave at samarbejde om retshåndhævelse, udveksle bedste praksis for tackling af grænseoverskridende udfordringer og støtte fælles håndhævelsesinitiativer og oplysningskampagner. Netværket skaber ingen retligt bindende forpligtelser for deltagerne og har primært fokus på at fremme samarbejdet om håndhævelse af de regler om privatlivets fred, der gælder for den private sektor. https://privacyenforcement.net/

4. ET MERE EFFEKTIVT SAMARBEJDE OM RETSHÅNDHÆVELSE MED STÆRKE GARANTIER FOR DATABESKYTTELSE

Udveksling af personoplysninger er en integrerende del af forebyggelsen, efterforskningen og retsforfølgningen af strafbare handlinger. I en forbundet verden, hvor kriminalitet sjældent stopper ved de nationale grænser, er en hurtig udveksling af personoplysninger af afgørende betydning for et vellykket samarbejde om retshåndhævelse og en effektiv bekæmpelse af kriminalitet. Denne udveksling skal understøttes af stærke databeskyttelsesgarantier. Denne bidrager ligeledes til at opbygge tillid mellem de retshåndhævende myndigheder og styrke retssikkerheden i forbindelse med indsamling og/eller udveksling af oplysninger.

Reglerne om internationale overførsler i politidirektivet vedrører dataudveksling mellem retshåndhævende myndigheder i og uden for EU samt i særlige tilfælde overførsler fra retshåndhævende myndigheder til andre enheder. Med direktivet indføres mulighed for at træffe afgørelser om tilstrækkeligheden af beskyttelsesniveauet på det strafferetlige håndhævelsesområde. Kommissionen vil fremme muligheden for sådanne afgørelser om tilstrækkeligheden af beskyttelsesniveauet i samarbejde med berettigede tredjelande, navnlig de lande, hvor der er behov for et tæt og hurtigt samarbejde om bekæmpelsen af kriminalitet og terrorisme, og hvor der allerede udveksles store mængder personoplysninger. Kommissionen vil prioritere drøftelser om afgørelser om tilstrækkeligheden af beskyttelsesniveauet med tredjelande, som er centrale partnere på dette område.

Paraplyaftalen om databeskyttelse mellem EU og USA[54], der blev indgået i december 2016, er et vellykket eksempel på, hvordan et samarbejde om retshåndhævelse med en vigtig international partner kan styrkes ved at forhandle et sæt stærke databeskyttelsesgarantier. Ved automatisk at supplere eksisterende retsakter, der danner grundlag for udveksling af oplysninger (navnlig bilaterale aftaler på både EU-plan og medlemsstatsplan), giver paraplyaftalen den enkelte øjeblikkelige og direkte fordele og styrker samarbejdet om retshåndhævelse ved at fremme informationsudvekslingen. Ved at fastsætte et referencepunkt for fremtidige ordninger for overførsel af oplysninger med USA fjerner paraplyaftalen behovet for at forhandle de samme garantier gentagne gange. Paraplyaftalen er den første bilaterale internationale aftale med et omfattende katalog over databeskyttelsesrettigheder og -forpligtelser i overensstemmelse med EU-retten. Den kan derfor danne grundlag for forhandlinger om tilsvarende aftaler med tredjelande, ikke kun inden for retligt samarbejde og politisamarbejde, men også på andre offentlige håndhævelsesområder (f.eks. konkurrencepolitik, forbrugerbeskyttelse). Dette dækker både udveksling af oplysninger mellem regeringer og overførsler af oplysninger mellem private virksomheder og retshåndhævende myndigheder. Det kunne ligeledes fremme Unionens indgåelse af aftaler om udvekslingen af oplysninger mellem relevante EU-agenturer (navnlig Europol og Eurojust) og

[54] Aftale mellem EU og USA om beskyttelse af personoplysninger, der overføres og behandles med henblik på at forebygge, efterforske, afsløre eller retsforfølge strafbare handlinger, herunder terrorisme, i forbindelse med politisamarbejde og retligt samarbejde i straffesager: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf ("paraplyaftalen").

tredjelande[55]. Kommissionen vil således undersøge mulighederne for at indgå tilsvarende rammeaftaler med sine vigtige retshåndhævende partnere.

Politidirektivet giver desuden de retshåndhævende myndigheder i EU mulighed for at anmode en privat virksomhed i et tredjeland direkte om oplysninger og for at videregive personoplysninger (typisk et navn og en IP-adresse) i den pågældende anmodning under anvendelse af strenge garantier og under særlige omstændigheder[56]. I GDPR er der derimod særlig fokus på sager, hvor private enheder i EU overfører personoplysninger til de retshåndhævende myndigheder i et tredjeland på baggrund af en anmodning. Sådanne overførsler uden for EU kan kun tillades på særlige betingelser, f.eks. hvis de er baseret på en international aftale, eller hvis videregivelse er nødvendig af hensyn til vigtige samfundsinteresser, der anerkendes i EU-retten eller medlemsstaternes nationale ret[57].

Dette samarbejde, der er blevet af central betydning for den vellykket efterforskning og retsforfølgning af kriminalitet og terrorisme, understreges i Rådets konklusioner om styrkelse af strafferetten i cyberspace. Rådet har opfordret Kommissionen til at træffe konkrete foranstaltninger baseret på en fælles EU-tilgang, til at forbedre samarbejdet med tjenesteydere, til at gøre den gensidige retshjælp mere effektiv og til at foreslå løsninger på problemerne med at fastlægge og håndhæve kompetence i cyberspace[58]. Disse foranstaltninger omfatter både udveksling mellem retshåndhævende myndigheder og tjenesteydere etableret i EU og udveksling med myndigheder og virksomheder uden for EU. Kommissionen vil redegøre for mulighederne for adgang til elektroniske beviser i juni 2017 under hensyntagen til behovet for et hurtigt og pålideligt samarbejde, der er understøttet af de stærke databeskyttelsesstandarder i politidirektivet og GDPR, både i forbindelse med overførsler internt i EU og internationale overførsler.

Endelig vil Kommissionen i overensstemmelse med det nye retsgrundlag for Europol vurdere bestemmelserne i disse operationelle samarbejdsaftaler mellem Europol og tredjeparter indgået i henhold til Rådets afgørelse 2009/371/RIA, herunder databeskyttelsesbestemmelserne[59]. Som anført i den europæiske dagsorden om sikkerhed fra 2015 vil der i forbindelse med EU's fremtidige strategi for udveksling af PNR-oplysninger med ikke-EU-lande blive taget hensyn til behovet for at anvende ensartede standarder og særlige foranstaltninger for at beskytte de grundlæggende rettigheder. Kommissionen vil arbejde med at finde retligt forsvarlige og bæredygtige løsninger for udvekslingen af PNR-

---

55 Indgåelsen af operationelle aftaler med Europol og Eurojust har ligeledes været en benchmark i dialogen med visse tredjelande om visumliberalisering, herunder f.eks. i forbindelse med den løbende dialog med Tyrkiet.

56 Jf. artikel 39 og betragtning 73 i politidirektivet.

57 Jf. artikel 48 og betragtning 115 i GDPR.

58 Rådets konklusioner om styrkelse af strafferetten i cyberspace af 9. juni 2016: www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. Kommissionen er blevet anmodet om at fremlægge resultater vedrørende disse områder for Rådet inden juni 2017 på baggrund af sin statusrapport til Rådet fra december 2016.

59 Jf. artikel 25, stk. 4, i Europa-Parlamentets og Rådets forordning (EU) 2016/794 af 11. maj 2016 om Den Europæiske Unions Agentur for Retshåndhævelsessamarbejde (Europol) og om erstatning og ophævelse af Rådets afgørelse 2009/371/RIA, 2009/934/RIA, 2009/935/RIA, 2009/936/RIA og 2009/968/RIA (EUT L 135 af 24.5.2016, s. 53-114). Kommissionen skal senest den 14. juni 2021 forelægge en vurderingsrapport om Europols samarbejdsaftaler indgået før den 1. maj 2017.

oplysninger med andre tredjelande, herunder ved at overveje, hvordan der kan udformes en standardaftale vedrørende PNR-oplysninger, der indeholder de krav, som tredjelande skal opfylde for at modtage PNR-oplysninger fra EU. Enhver fremtidig politik på dette områder afhænger imidlertid navnlig af Domstolens kommende udtalelse om den påtænkte PNR-aftale mellem EU og Canada[60].

ET MERE EFFEKTIVT SAMARBEJDE OM RETSHÅNDHÆVELSE MED STÆRKE GARANTIER FOR DATABESKYTTELSE

Kommissionen vil:

- fremme muligheden for afgørelser om tilstrækkeligheden af beskyttelsesniveauet i henhold til politidirektivet i samarbejde med berettigede tredjelande
- fremme forhandlingerne om aftaler på retshåndhævelsesområdet med vigtige internationale partnere i overensstemmelse med den model, der er anført i paraplyaftalen med USA
- følge op på Rådets konklusioner om styrkelse af strafferetten i cyberspace for at lette den grænseoverskridende udveksling af elektroniske beviser i overensstemmelse med databeskyttelsesreglerne.

5. KONKLUSION

Beskyttelse og udveksling af personoplysninger udelukker ikke gensidigt hinanden. Et stærkt databeskyttelsessystem fremmer datastrømme ved at opbygge forbrugernes tillid til de virksomheder, der har fokus på håndteringen af deres kunders personoplysninger. Høje databeskyttelsesstandarder bliver således en fordel i den globale digitale økonomi. Det samme gælder for samarbejde om retshåndhævelse, idet garantier for beskyttelse af privatlivets fred er en integrerende del af en effektiv og hurtig udveksling af oplysninger i bekæmpelsen af kriminalitet baseret på gensidig tillid og retssikkerhed.

Da EU har afsluttet reformen af EU's databeskyttelsesregler, bør EU proaktivt gå i dialog med tredjelande om dette spørgsmål. EU bør bestræbe sig på at sikre større konvergens i opadgående retning mellem databeskyttelsesprincipper internationalt på både bilateralt og multilateralt plan. Dette er både i borgernes og virksomhedernes interesse. Den nye lovgivningsramme for databeskyttelse sikrer EU de nødvendige og relevante redskaber til at nå disse mål. På grundlag af den strategiske tilgang, der er redegjort for i denne meddelelse, vil Kommissionen aktivt gå i dialog med centrale tredjelande for at undersøge mulighederne for at vedtage afgørelser om tilstrækkeligheden af beskyttelsesniveauet, i første omgang med Japan og Korea i 2017, med henblik på at fremme den reguleringsmæssige konvergens i

[60] Domstolens udtalelse om udkastet til aftale fra 2014 om PNR-aftalen mellem EU og Canada, som Europa-Parlamentet havde henvist til Domstolen (udtalelse 1/15). Domstolen blev anmodet om at vurdere foreneligheden af udkastet til aftale med EU's charter om grundlæggende rettigheder.

retning af EU-standarderne og fremme handelsforbindelserne. EU vil samtidig gøre fuld brug af de forskellige alternative redskaber til videregivelse for at beskytte databeskyttelsesrettigheder og støtte erhvervsdrivende, når data overføres til lande, hvor den nationale ret ikke sikrer til tilstrækkeligt databeskyttelsesniveau. Sådanne redskaber bør ligeledes anvendes til yderligere at fremme samarbejdet mellem EU's tilsynsmyndigheder og retshåndhævende myndigheder og deres internationale partnere. Kommissionen vil sikre sammenhængen mellem den interne og eksterne dimension af EU's databeskyttelsespolitik og fremme en stærk databeskyttelse på internationalt plan for at forbedre samarbejdet om retshåndhævelse, bidrage til frihandel og udvikle høje standarder for beskyttelse af personoplysninger på verdensplan.