EUROPEISKA
KOMMISSIONEN

Bryssel den 10.1.2017
COM(2017) 7 final

MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH RÅDET

Utbyte och skydd av personuppgifter i en globaliserad värld

1. INLEDNING

Skydd av personuppgifter är en del av Europas gemensamma konstitutionella system. Detta är förankrat i artikel 8 i Europeiska unionens stadga om de grundläggande rättigheterna. Skyddet av personuppgifter har varit av central betydelse för EU-lagstiftningen i mer än 20 år, från dataskyddsdirektivet 1995[1] till antagandet av allmänna dataskyddsförordningen[2] och polisdirektivet[3] år 2016.

Kommissionens ordförande Jean-Claude Juncker betonade följande i sitt tal om tillståndet i Europeiska unionen den 14 september 2016: ”Att vara europé innebär rätten att få sina personuppgifter skyddade av kraftfulla lagar som gäller i hela EU. *[…] För i EU har privatlivet betydelse.* Det är fråga om den mänskliga värdigheten.”

Behovet av skydd av personuppgifter är dock inte begränsat till Europa. Konsumenter i hela världen håller i allt högre grad fast vid sin integritet och värdesätter den. Företag i sin tur konstaterar att ett starkt integritetsskydd ger dem en konkurrensfördel, eftersom förtroendet för deras tjänster ökar. Många av dem, särskilt de som arbetar på globalt plan, anpassar sin integritetsskyddspolicy till den allmänna dataskyddsförordningen, både för att de vill göra affärer i EU och för att de ser den som en modell som är värd att följa.

Dessutom finns det flera länder och regionala organisationer utanför EU, allt från vår omedelbara närhet och ända till Asien, Latinamerika och Afrika, som antar ny eller uppdaterar befintlig dataskyddslagstiftning i syfte att utnyttja de möjligheter som erbjuds inom den globala digitala ekonomin, samtidigt som de möter den växande efterfrågan på större datasäkerhet och integritetsskydd. Även om det förekommer olikheter mellan länderna i fråga om deras strategi och rättsliga utveckling, finns det tecken på ökande enhetlighet kring viktiga principer för dataskydd, särskilt i vissa regioner i världen[4]. Större kompatibilitet mellan olika system för dataskydd skulle kunna underlätta gränsöverskridande överföring av personuppgifter, oavsett om det sker i kommersiellt syfte eller om det är frågan om samarbete mellan offentliga myndigheter (t.ex. brottsbekämpande myndigheter). EU bör utnyttja denna möjlighet att främja sina principer om skydd av personuppgifter, samtidigt som unionen underlättar dataflöden genom att främja konvergens av rättssystem. Såsom anges i kommissionens arbetsprogram[5], fastställer detta meddelande därför kommissionens

---

1 Europaparlamentets och rådets direktiv 95/46/EG av den 24 oktober 1995 om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (EGT L 281, 23.11.1995, s. 31).

2 Europaparlamentets och rådets förordning (EU) 2016/679 av den 27 april 2016 om skydd för fysiska personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter och om upphävande av direktiv 95/46/EG (allmänna dataskyddsförordningen), (EUT L 119, 4.5.2016, s. 1). Den trädde i kraft den 24 maj 2016 och ska tillämpas från och med den 25 maj 2018.

3 Europaparlamentets och rådets direktiv (EU) 2016/680 av den 27 april 2016 om skydd för fysiska personer med avseende på behöriga myndigheters behandling av personuppgifter för att förebygga, förhindra, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, och det fria flödet av sådana uppgifter och om upphävande av rådets rambeslut 2008/977/RIF (EUT L 119, 4.5.2016, s. 89). Det trädde i kraft den 5 maj 2016. EU:s medlemsstater ska införliva det i sin nationella lagstiftning senast den 6 maj 2018.

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

5 Kommissionens arbetsprogram 2017 – Ett EU som skyddar, försvarar och sätter medborgarna i centrum, COM(2016) 710 final, 25.10.2016, s. 12 och bilaga 1.

strategiska ramar för "beslut om adekvat skyddsnivå" samt andra verktyg för dataöverföring och internationella instrument för dataskydd.

2. EU:S REFORMPAKET OM DATASKYDD – EN MODERN RÄTTSLIG RAM SOM STÖDER INTERNATIONELLA DATAFLÖDEN GENOM HÖGA SKYDDSNIVÅER

Reformen av EU:s dataskyddslagstiftning antogs i april 2016. Där införs ett system som dels säkerställer en stark skyddsnivå, dels är öppen för möjligheterna inom det globala informationssamhället. I och med att enskilda personer får mer kontroll över sina personuppgifter, stärker reformen konsumenternas förtroende för den digitala ekonomin. Genom reformen harmoniseras och förenklas det rättsliga regelverket, vilket gör det enklare och mindre betungande för både inhemska och utländska företag att bedriva affärsverksamhet i EU, inbegripet genom gränsöverskridande utbyte av uppgifter. EU kombinerar idag öppenhet för internationella dataflöden med högsta möjliga skydd för enskilda personer. Unionen kan bli ett nav för datatjänster som kräver både fria dataflöden och förtroende.

2.1 En övergripande, enhetlig och förenklad EU-ram för dataskydd

EU:s reform inför en övergripande ram som reglerar behandling av personuppgifter såväl i den privata som i den offentliga sektorn, samt för såväl den kommersiella som den brottsbekämpande sektorn (allmänna dataskyddsförordningen och polisdirektivet).

Enligt allmänna dataskyddsförordningen kommer det att finnas en enda alleuropeisk uppsättning bestämmelser efter maj 2018, istället för 28 nationella lagar idag. Den nyskapade mekanismen med en enda kontaktpunkt kommer att säkerställa att en enda dataskyddsmyndighet kommer att ansvara för tillsynen av gränsöverskridande databehandling som hanteras av företagen i EU. Enhetlig tolkning av de nya reglerna kommer att garanteras. Framför allt i gränsöverskridande fall där flera nationella dataskyddsmyndigheter berörs, kommer ett enda beslut att antas för att säkerställa att gemensamma problem får gemensamma lösningar. Dessutom skapar den allmänna dataskyddsförordningen lika villkor mellan EU och utländska företag, eftersom företag med säte utanför EU ska tillämpa samma bestämmelser som de europeiska företagen om de erbjuder varor eller tjänster eller övervakar beteendet hos enskilda personer inom EU. Ett ökat konsumentförtroende kommer att gynna både EU och externa kommersiella aktörer.

I polisdirektivet fastställs gemensamma regler för behandling av personuppgifter för sådana personer som deltar i straffrättsliga förfaranden i egenskap av misstänkta, offer eller vittnen, samtidigt som hänsyn tas till särdragen inom det polisiära och straffrättsliga området. Gränsöverskridande samarbete mellan polisen och rättsliga myndigheter, såväl i EU som med internationella partner, kommer att underlättas genom harmonisering av dataskyddsbestämmelserna inom sektorn för brottsbekämpning, inklusive bestämmelserna om gränsöverskridande dataöverföring. Därmed skapas förutsättningar för en effektivare brottsbekämpning. Detta är ett viktigt bidrag till den europeiska säkerhetsagendan[6].

[6] Meddelande från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: Europeiska säkerhetsagendan, COM(2015) 185 final, 28.4.2015.

2.2 En förnyad och diversifierad verktygslåda för gränsöverskridande dataöverföringar

Ända från början har EU:s dataskyddslagstiftning omfattat flera olika mekanismer som möjliggör gränsöverskridande dataöverföringar. Det primära syftet med dessa bestämmelser är att säkerställa att sådana personuppgifter om européer som överförs utomlands omfattas av ett åtföljande skydd. Under årens lopp har dessa bestämmelser fastställt standarden för internationella dataflöden i många jurisdiktioner. Medan strukturen i huvudsak förblir densamma som enligt dataskyddsdirektivet från 1995, förtydligas och förenklas tillämpningen av bestämmelserna genom reformen av reglerna för gränsöverskridande dataöverföringar, samtidigt som nya verktyg för dataöverföringar införs.

Enligt EU-rätten kan personuppgifter överföras till utlandet till exempel på grundval av ett "beslut om adekvat skyddsnivå" av kommissionen, där det fastställs att ett land utanför EU tillhandahåller en skyddsnivå för uppgifterna som är ”väsentligen likvärdig”[7] med den som garanteras i unionen. Konsekvenserna av ett sådant beslut är att personuppgifter fritt får sändas till berört tredjeland utan att uppgiftsutföraren behöver vidta ytterligare skyddsåtgärder eller erhålla tillstånd. En exakt och detaljerad förteckning över uppgifter som kommissionen måste ta hänsyn till vid bedömningen av huruvida skyddet i ett utländskt system ligger på adekvat nivå är tillgänglig för de berörda länderna eller internationella organisationerna[8]. Kommissionen kan nu fatta beslut om adekvata skyddsnivåer även inom sektorn för brottsbekämpning[9]. Dessutom bygger reformen på praxis enligt dataskyddsdirektivet av 1995, och medger uttryckligen att en bedömning om adekvat skyddsnivå ska göras med hänsyn till ett visst område i tredjeland eller en viss sektor eller bransch i tredjeland (så kallad ”partiellt adekvat skyddsnivå”)[10].

I avsaknad av ett beslut om adekvat skyddsnivå kan gränsöverskridande dataöverföringar ske på grundval av ett antal alternativa överföringsverktyg som inbegriper lämpliga dataskyddsåtgärder[11]. Denna reform formaliserar och utökar möjligheterna att använda gällande instrument såsom standardavtalsklausuler[12] och bindande företagsbestämmelser[13].

---

7 Domstolens dom av den 6 oktober 2015 i mål C-362/14, Maximillian Schrems/Data Protection Commissioner, ECLI:EU:C:2015:650, punkterna 73, 74 och 96. Se även skäl 104 i allmänna dataskyddsförordningen och skäl 67 i polisdirektivet som behandlar de grundläggande bestämmelserna om likvärdighet.

8 Se artikel 45 i allmänna dataskyddsförordningen. Enligt artikel 45.2 ska kommissionen i sin bedömning ta hänsyn till bland annat rättsstatsprincipen, respekten för de mänskliga rättigheterna och de grundläggande friheterna, relevant lagstiftning, inklusive avseende området för dataskydd, allmän säkerhet, försvar, nationell säkerhet och straffrätt och offentliga myndigheters tillgång till personuppgifter. Dessa måste stödjas av effektiva och genomförbara rättigheter, inbegripet administrativ och rättslig prövning för enskilda personer samt en effektivt fungerande oberoende tillsynsmyndighet för att kontrollera och säkerställa efterlevnaden av dataskyddsbestämmelserna. Därvid ska man också beakta tillämpningen av rättsligt bindande konventioner, särskilt Europarådets konvention 108 och deltagande i multilaterala eller regionala system som har anknytning till dataskydd.

9 Se artikel 36.2 i polisdirektivet för de punkter som särskilt ska beaktas vid bedömningen.

10 Se artikel 45.1 i allmänna dataskyddsförordningen och artikel 36.1 i polisdirektivet.

11 Se t.ex. meddelandet från kommissionen till Europaparlamentet och rådet om överföring av personuppgifter från EU till Amerikas förenta stater enligt direktiv 95/46/EG med anledning av domstolens dom i mål C-362/14 (*Schrems*), COM(2015) 566 final, 6.11.2015.

12 Standardavtalsklausuler fastställer de respektive dataskyddskraven mellan uppgiftsutföraren i EU och uppgiftsinföraren i tredjeland.

Standardavtalsklausuler kan till exempel nu inbegripas i ett avtal mellan personuppgiftsbiträden som är EU-baserade och personuppgiftsbiträden i ett land utanför EU (s.k. förlagor till bestämmelser för dataöverföringar mellan personuppgiftsbiträden)[14]. Bindande företagsbestämmelser, som hittills har begränsats till överenskommelser mellan företag i samma koncern, kan nu tillämpas av en grupp företag som deltar i en gemensam ekonomisk verksamhet, men inte nödvändigtvis tillhör samma koncern[15]. Reformen minskar också på byråkratin genom att avskaffa allmänna krav på förhandsanmälan till och godkännande av dataskyddsmyndigheterna i fråga om dataöverföringar till tredjeland på grundval av standardavtalsklausuler eller bindande företagsbestämmelser[16]. Detta är en viktig förenkling av EU:s system för gränsöverskridande dataöverföringar, eftersom sådana krav, som för närvarande varierar från medlemsstat till en annan, ofta uppfattas som ett betydande hinder för dataflöden, särskilt för mindre företag[17].

Dessutom införs nya instrument för gränsöverskridande dataöverföringar i samband med denna reform[18]. Personuppgiftsansvariga och personuppgiftsbiträden kommer på vissa villkor[19] att kunna använda godkända uppförandekoder eller certifieringsmekanismer (så som integritetsmärkning eller motsvarande) för att fastställa ”lämpliga skyddsåtgärder". På detta sätt bör det bli möjligt att utveckla mer skräddarsydda lösningar för gränsöverskridande dataöverföringar, för att exempelvis beakta särdragen och behoven i en viss sektor eller bransch, eller hos särskilda dataflöden. Dessutom medför reformen en möjlighet att föreskriva lämpliga skyddsåtgärder för överföring av data mellan offentliga myndigheter eller organ på grundval av internationella avtal eller administrativa överenskommelser[20]. I allmänna dataskyddsförordningen klargörs slutligen tillämpningen av så kallade "undantag"[21] (t.ex. samtycke, fullgörande av ett avtal eller viktiga skäl som rör allmänintresset) med stöd av vilka de berörda enheterna i vissa situationer kan göra dataöverföringar, i brist på beslut om adekvat skyddsnivå och oberoende av huruvida något av dessa instrument tillämpas. I synnerhet innehåller förordningen ett nytt, men begränsade undantag som avser sådana överföringar som kan genomföras för att tillgodose ett företags berättigade intressen[22].

---

13 Bindande företagsbestämmelser är interna regler som en multinationell företagskoncern tillämpar för att hantera dataöverföringar inom samma koncern till enheter som är belägna i sådana länder som inte har en adekvat skyddsnivå. Medan bindande företagsbestämmelser redan tillämpas enligt dataskyddsdirektivet från 1995, kodifieras och formaliseras deras roll som ett överföringsverktyg genom den allmänna dataskyddsförordningen.

14 Se artikel 46.2 c och d och skäl 168 i allmänna dataskyddsförordningen.

15 Se artiklarna 46.2 b och 47 samt skäl 110 i allmänna dataskyddsförordningen.

16 Se artikel 46.2 a i allmänna dataskyddsförordningen.

17 Att registreringskrav utgör ett hinder för handeln i många företag, särskilt i små och medelstora företag, framhölls t.ex. i Unctad-rapporten, s. 34.

18 Se artikel 46.2 e och f i allmänna dataskyddsförordningen.

19 Personuppgiftsansvariga som inte kommer från EU kommer att kunna ansluta sig till EU:s uppförandekod eller certifieringsmekanismer genom att göra bindande och verkställbara åtaganden, genom avtal eller andra rättsligt bindande åtaganden, om att tillämpa de dataskyddsåtgärder som anges i dessa instrument. Se artikel 42.2 i allmänna dataskyddsförordningen.

20 Se artikel 46.2 a och artikel 46.3 b i allmänna dataskyddsförordningen.

21 Se artikel 49 i allmänna dataskyddsförordningen.

22 Se artikel 49.1 andra stycket.

Genom denna reform får kommissionen slutligen befogenheter att utarbeta mekanismer för internationellt samarbete i syfte att underlätta efterlevnaden av dataskyddsbestämmelserna, inklusive genom överenskommelser om ömsesidigt bistånd[23]. Här framhävs vikten av närmare former av samarbete mellan tillsynsmyndigheter på internationell nivå, vilket kan bidra till att säkerställa både ett effektivare skydd av individuella rättigheter och mer rättslig säkerhet för företagen.

3. GRÄNSÖVERSKRIDANDE DATAÖVERFÖRINGAR INOM DEN KOMMERSIELLA SEKTORN: ATT UNDERLÄTTA HANDELN GENOM ATT SKYDDA PRIVATLIVET

Respekt för privatlivet är en förutsättning för stabila, säkra och konkurrenskraftiga globala handelsflöden. Integritet är inte en råvara som saluförs[24]. Internet och digitaliseringen av varor och tjänster har förändrat den globala ekonomin, samtidigt som gränsöverskridande överföringar av data, inbegripet personuppgifter, är en del av den dagliga driften vid europeiska företag av alla storlekar och inom alla sektorer. Eftersom handeln i allt högre grad förlitar sig på flöden av personuppgifter, har integriteten och säkerheten för sådana uppgifter blivit en viktig faktor för konsumenternas förtroende. Som exempel kan nämnas att två tredjedelar av européerna säger att de är bekymrade över att de inte har någon kontroll över den information de tillhandahåller på nätet, medan hälften av uppgiftslämnarna i fråga var oroade för att bli utsatta för bedrägerier[25]. Samtidigt konfronteras de europeiska företagen som är verksamma i vissa tredjeländer allt oftare med protektionistiska begränsningar som inte kan motiveras med legitima integritetsöverväganden.

I den digitala tidsåldern behöver således främjandet av strikta standarder för dataskydd och underlättande av den internationella handeln absolut gå hand i hand. Samtidigt som skyddet av personuppgifter är icke-förhandlingsbart[26] i handelsavtal, utgör EU:s system för gränsöverskridande dataöverföringar enligt vad som beskrivs ovan en omfattande och varierad verktygslåda som möjliggör flöden av personuppgifter i olika situationer och samtidigt säkerställer en hög skyddsnivå.

3.1 Beslut om adekvat skyddsnivå

En adekvat skyddsnivå tillåter fritt flöde av personuppgifter från EU utan att uppgiftsutföraren i EU behöver vidta några ytterligare skyddsåtgärder eller följa ytterligare villkor. I beslutet konstateras att lagstiftningen i ett visst land ger en adekvat skyddsnivå, och samtidigt erkänns att landets system i stort sett överensstämmer med systemet i EU:s medlemsstater. Följaktligen kommer dataöverföringar till det berörda landet att jämföras med dataöverföringar inom EU, vilket möjliggör privilegierad tillgång till EU:s inre marknad, samtidigt som handelskanaler öppnas för EU-aktörer. Såsom förklaras ovan kräver detta

[23] Se artikel 50 i allmänna dataskyddsförordningen.

[24] Se t.ex. meddelandet från kommissionen till Europaparlamentet, rådet, Europeiska ekonomiska och sociala kommittén samt Regionkommittén: Handel för alla – Mot en mer ansvarsfull handels- och investeringspolitik, COM(2015) 497 final, 14.10.2015, s. 7.

[25] *Special Eurobarometer 431 - Data protection* (särskild Eurobarometer 431 om dataskydd), juni 2015.

[26] Jean-Claude Junckers politiska riktlinjer: *En ny start för EU: Mitt program för sysselsättning, tillväxt, rättvisa och demokratisk förändring.*

erkännande absolut en skyddsnivå som är jämförbar (eller ”väsentligen likvärdig”)[27] med den som garanteras i unionen. Detta medför en omfattande bedömning av tredjelands system, vilket även inbegriper landets bestämmelser om myndigheters tillgång till personuppgifter i brottsbekämpningssyfte eller alternativt för att garantera den nationella säkerheten eller andra allmänna intressen.

Samtidigt kräver inte standarden om en adekvat skyddsnivå att EU:s regler följs till punkt och pricka, vilket bekräftades av domstolens avgörande 2015 i målet Schrems[28]. I stället handlar testet om huruvida det berörda utländska systemet som helhet ger den höga skyddsnivå som krävs genom själva innehållet i integritetsrättigheterna och genom att effektivt genomföra, verkställa och övervaka genomförandet av dessa rättigheter. Ur de beslut om adekvat skyddsnivå som utfärdats hittills framgår också att det är möjligt för kommissionen att betrakta en rad olika system för integritetsskydd som lämpliga, även om de representerar olika rättsliga traditioner. Dessa beslut berör länder som är nära integrerade med Europeiska unionen och dess medlemsstater (Schweiz, Andorra, Färöarna, Guernsey, Jersey, Isle of Man), EU:s viktigaste handelspartner (Argentina, Kanada, Israel, USA), och länder som visar vägen då de utvecklar dataskyddslagar i sin egen region (Nya Zeeland, Uruguay).

Besluten om Kanada och Förenta staterna är konstateranden om "partiellt adekvat skyddsnivå”. Beslutet om Kanada är endast tillämpligt på privata företag som omfattas av den kanadensiska lagen om skydd av personuppgifter och elektroniska dokument (*Personal Information Protection and Electronic Documents Act*). Det nyligen antagna beslutet om skölden för skydd av privatlivet i EU och USA[29] är ett specialfall såtillvida att detta beslut, i avsaknad av allmän dataskyddslagstiftning i USA,[30] istället bygger på åtaganden från de deltagande företagen om att tillämpa de höga standarder för dataskydd som fastställs genom denna överenskommelse. Dessa åtaganden är i sin tur är verkställbara enligt amerikansk lag. Dessutom bygger beslutet om skölden för skydd av privatlivet på de särskilda intyganden och garantier som givits av den amerikanska statsförvaltningen i fråga om åtkomst på grund av sådana nationella säkerhetsändamål[31] som stödjer konstaterandet om adekvat skyddsnivå. Kommissionen kommer noggrant att övervaka att dessa åtaganden följs. Efterlevnaden kommer också att inbegripas i den årliga översynen av hur dessa ramar fungerar.

Under senare år har allt fler länder i världen antagit ny lagstiftning inom området för dataskydd och personlig integritet eller är i färd med att göra detta. Under 2015 uppgick antalet länder som hade infört lagar om integritetsskydd till 109, vilket var en kraftig ökning

---

27 Se fotnot 7.

28 Se punkt 74 i domen om Schrems.

29 Genomförandebeslut EU(2016) 1260 av den 12 juli 2016.

30 Kommissionen uppmanar Förenta staterna att arbeta för att skapa ett omfattande system för integritetsskydd och dataskydd, så att dessa två system kan bli enhetliga på längre sikt. Se meddelandet från kommissionen till Europaparlamentet och rådet: Transatlantiska dataflöden – Återställande av förtroendet genom starka skyddsåtgärder, COM(2016) 117 final, 29.2.2016.

31 Detta omfattar i synnerhet tillämpningen av *Presidential Policy Directive 28* (PPD-28), där det föreskrivs ett antal begränsningar och skyddsåtgärder för signalspaningsverksamhet, och att det ska utnämnas en särskild ombudsman som hanterar klagomål i detta avseende från enskilda personer i EU.

jämfört med 76 länder i mitten av 2011[32]. Dessutom finns det cirka 35 länder som för närvarande utarbetar dataskyddslagar[33]. Dessa nya eller moderniserade lagar är i allmänhet baserade på ett antal gemensamma principer, inbegripet bland annat erkännandet av dataskydd som en grundläggande rättighet, antagande av övergripande lagstiftning på detta område, förekomsten av verkställbara rättigheter om enskilda personers privatliv, och inrättande av en oberoende tillsynsmyndighet. Detta medför nya möjligheter att ytterligare underlätta dataflöden, särskilt genom konstateranden om adekvat skyddsnivå, samtidigt som man säkerställer en fortsatt hög nivå på skyddet av personuppgifter.

Enligt EU-rätten kräver ett konstaterande om adekvat skyddsnivå att det finns bestämmelser om dataskydd som är jämförbara med dem i EU[34]. Detta gäller inte bara materiellt skydd av personuppgifter, utan även de relevanta tillsyns-och tvistlösningsmekanismerna som finns tillgängliga i berört tredjeland.

I sina slutsatser om adekvata skyddsnivåer anser kommissionen att följande kriterier ska beaktas vid bedömningen av vilka tredjeländer som ska inbegripas i en dialog om adekvata skyddsnivåer[35]:

i) Omfattningen av EU:s (faktiska eller potentiella) affärsförbindelser med ett visst tredjeland, vilket även inbegriper frihandelsavtal eller pågående förhandlingar.

ii) Omfattningen av flödet av personuppgifter från EU, vilket även avspeglar de geografiska och/eller kulturella banden.

iii) Den pionjärroll som tredjelandet spelar i fråga om integritetsskydd och dataskydd, vilket skulle kunna tjäna som modell för andra länder i samma region[36].

iv) De allmänna politiska förbindelserna med tredjelandet i fråga, i synnerhet när det gäller främjandet av delade värderingar och gemensamma mål på internationell nivå.

Mot denna bakgrund avser kommissionen att bedriva ett aktivt samarbete med de viktigaste handelspartnerna i östra och sydöstra Asien, med början från Japan och Korea under 2017[37], och med Indien, beroende på landets utveckling i riktning mot att modernisera sin dataskyddslagstiftning. Dessutom samarbetar kommissionen också med länder i Latinamerika, särskilt Mercosur, och i det europeiska grannskapet, där man har uttryckt

---

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-studien, s. 8 och 42 (fotnot 4 ovan).

34 När kommissionen utför en bedömning tar den i detta sammanhang också hänsyn till tredjelands skyldigheter som härrör från rättsligt bindande konventioner, särskilt landets anslutning till konvention 108 och dess tilläggsprotokoll. Se artikel 45.2 c och skäl 105 i allmänna dataskyddsförordningen.

35 I fråga om länder med vilka det finns ett relevant intresse att samarbeta inom området för inre säkerhet och brottsbekämpning, kommer kommissionen att undersöka möjligheten till särskilda konstateranden om adekvata skyddsnivåer enligt polisdirektivet, se avsnitt 4.

36 Detta kan vara särskilt relevant för utvecklingsländer och övergångsekonomier eftersom skydd av personuppgifter är en avgörande faktor för rättsstatsprincipen och en viktig faktor för den ekonomiska konkurrenskraften.

37 Japan och Sydkorea har nyligen antagit eller moderniserat sin lagstiftning för att införa omfattande system för dataskydd.

intresse för att få ett ”konstaterande om adekvat skyddsnivå”. Kommissionen välkomnar dessutom intresseanmälningar från andra tredjeländer som är villiga att delta i detta arbete. Diskussioner om ett eventuellt konstaterande av adekvata skyddsnivåer är en dubbelriktad dialog som inbegriper nödvändiga förtydliganden av EU:s dataskyddsbestämmelser och utforskning av möjligheter att öka enhetligheten i tredjeländers lagstiftning och praxis.

Istället för en landsomfattande strategi kan det i vissa situationer vara lämpligare att använda sig av andra alternativ såsom beslut om partiellt eller sektorsspecifikt adekvat skyddsnivå (t.ex. för finansiella tjänster eller IT-sektorn) för vissa geografiska områden eller branscher som utgör en viktig del av ekonomin i ett visst tredjeland. Detta måste ses mot bakgrund av sådana faktorer som exempelvis typen av system för integritetsskydd (en fristående lag, en uppsättning lagar eller sektorsspecifik lagstiftning osv.) och systemets utvecklingsstadium, samt den konstitutionella strukturen i tredjeland. Därvid bör också beaktas huruvida dataflödena från EU särskilt berör vissa ekonomiska sektorer.

Antagandet av ett beslut om adekvat skyddsnivå inbegriper inledande av en särskild dialog och ett nära samarbete med berört tredjeland. Beslut om adekvat skyddsnivå är ”levande” dokument som måste övervakas noggrant av kommissionen och anpassas om det händer något som påverkar den skyddsnivå som berört tredjeland garanterar[38]. I detta syfte kommer översyner att genomföras regelbundet, minst vart fjärde år, för att hantera problem som uppstår och utbyta bästa praxis mellan nära samarbetspartner[39]. Denna dynamiska metod tillämpas redan på sådana befintliga beslut om adekvat skyddsnivå som antagits enligt dataskyddsdirektivet från 1995 och som kommer att behöva ses över om de inte längre uppfyller den tillämpliga standarden[40]. De berörda tredjeländerna har därför uppmanats att meddela kommissionen om alla relevanta förändringar i lagstiftning och praxis efter att besluten om adekvat skyddsnivå antogs i just dessa länder. Detta är nödvändigt för att säkerställa kontinuiteten i dessa beslut i enlighet med de nya bestämmelserna inom ramen för reformen[41].

EU:s regler om dataskydd kan inte bli föremål för förhandlingar i ett frihandelsavtal[42]. Medan dialoger om dataskydd och handelspolitiska förhandlingar med tredjeländer måste följa separata spår, är ett beslut om adekvat skyddsnivå, inbegripet ett partiellt eller sektorsspecifikt

---

38 Artikel 45.4 och 45.5 i allmänna dataskyddsförordningen kräver att kommissionen övervakar utvecklingen i tredjeländer fortlöpande och ge dem befogenhet att upphäva, ändra eller upphäva ett beslut om huruvida den anser att det berörda landet inte längre har en adekvat skyddsnivå.

39 Artikel 45.3 i allmänna dataskyddsförordningen.

40 Artikel 97.2 a i allmänna dataskyddsförordningen kräver också att kommissionen senast 2020 lägger fram en utvärderingsrapport inför Europaparlamentet och rådet.

41 I *Schrems*-domen konstaterades att kommissionen hade överskridit sina befogenheter då den begränsat dataskyddsmyndigheternas befogenheter att stänga av eller förbjuda dataflöden i *Safe Harbour*-beslutet. Som en konsekvens av detta antog kommissionen den 16 december 2016 ett övergripande ändringsbeslut om att liknande bestämmelser i befintliga beslut om adekvat skyddsnivå raderas och ersätts med bestämmelser som endast uppfyller informationskraven mellan medlemsstaterna och kommissionen i sådana fall där dataskyddsmyndigheter tillfälligt upphäver eller förbjuder dataöverföringar till ett tredjeland. Det övergripande beslutet inför också en skyldighet för kommissionen att övervaka den relevanta utvecklingen i berört tredjeland. Se EUT L 355, 17.12.2016, s. 83.

42 I synnerhet är ett konstaterande om adekvata skyddsnivåer ett ensidigt genomförandebeslut av kommissionen i enlighet med EU:s dataskyddslagstiftning, på grundval av kriterierna i bilagan.

beslut, det bästa sättet för att skapa ömsesidigt förtroende. Skälet är att det garanterar ett obegränsat flöde av personuppgifter, och därmed underlättar ett handelsutbyte som inbegriper överföring av personuppgifter till tredjelandet i fråga. Sådana beslut kan därför underlätta handelsförhandlingar eller komplettera befintliga handelsavtal, vilket gör det möjligt för länderna att få ännu fler fördelar. Genom att främja konvergens av skyddsnivån inom EU och tredjelandet kan ett konstaterande om adekvata skyddsnivåer samtidigt minska risken för att landet ifråga åberopar skyddet av personuppgifter som skäl för att införa omotiverade krav på lokalisering eller lagring av data. Såsom det anges i meddelandet ”Handel för alla” kommer kommissionen utöver detta att försöka använda EU:s handelsavtal för att fastställa regler för e-handel och gränsöverskridande dataflöden och ta itu med nya former av digital protektionism, i fullständig överensstämmelse med och utan att det påverkar EU:s regler om dataskydd[43].

Kommissionen ska göra följande:

- Prioritera diskussionerna om eventuella beslut om adekvat skyddsnivå med viktiga handelspartner i östra och sydöstra Asien, med början från Japan och Korea under 2017, men även beakta andra strategiska partner, såsom Indien. Kommissionen prioriterar också diskussioner med länderna i Latinamerika, i synnerhet Mercosur, och i det europeiska grannskapet.

- Noga följa upp hur de nuvarande besluten om adekvat skyddsnivå fungerar. Detta omfattar bland annat genomförandet av beslutet om skölden för skydd av privatlivet i EU och USA, särskilt med hjälp av mekanismen för årliga gemensamma översyner.

- Arbeta med intresserade länder och hjälpa dem att anta kraftfulla lagar om dataskydd samt stöda lagarnas förenlighet med EU: s principer för dataskydd.

3.2 Alternativa mekanismer för dataöverföring

EU:s dataskyddsbestämmelser har alltid erkänt att det inte finns en enda strategi som passar alla då det gäller gränsöverskridande dataöverföringar. Detta gäller i ännu högre grad för de regler som följer av reformen. Medan konstateranden om adekvata skyddsnivåer kommer att vara tillgängliga endast för de tredjeländer som uppfyller de relevanta kriterierna, omfattar den allmänna dataskyddsförordningen en bred uppsättning mekanismer som är tillräckligt flexibla för att anpassas till en mängd olika överföringssituationer. Olika instrument kan utvecklas för att ta hänsyn till särskilda behov eller särskilda villkor som gäller för vissa branscher, affärsmodeller och/eller aktörer. Sådana instrument kan exempelvis omfatta standardavtalsklausuler som riktar sig till kraven i en viss sektor, t.ex. särskilda skyddsåtgärder vid behandling av känsliga uppgifter inom hälsosektorn, eller en särskild typ av bearbetning som är utbredd i vissa tredjeländer, t.ex. utkontrakterade tjänster som utförs för europeiska företag. Detta kan göras antingen genom att anta en ny uppsättning standardklausuler eller genom att komplettera de befintliga skyddsåtgärderna med ytterligare skyddsåtgärder som kan variera från tekniska till organisatoriska lösningar eller lösningar med

[43] Se meddelandet ”Handel för alla”, s. 12 (fotnot 24).

anknytning till den berörda affärsmodellen[44]. Vissa sektorsspecifika behov kan tillgodoses genom att tillämpa bindande företagsbestämmelser på grupper av företag som deltar i en gemensam ekonomisk verksamhet, till exempel inom resebranschen. Vid gränsöverskridande dataöverföringar mellan personuppgiftsbiträden skulle man kunna dra nytta de standardavtalsklausuler som utvecklats för dataöverföringar mellan personuppgiftsbiträden och/eller bindande företagsbestämmelser för personuppgiftsbiträdena. Nya mekanismer för dataöverföring såsom godkända uppförandekoder och godkända certifieringar av tredje part skapar dessutom möjligheter för denna bransch att införa skräddarsydda lösningar för gränsöverskridande dataöverföringar, samtidigt som man utnyttjar de konkurrensfördelar som är förknippade med exempelvis integritetsmärkning eller motsvarande. Vissa av instrumenten kan utformas som överföringsspecifika mekanismer eller som en del av mer allmängiltiga verktyg i syfte att intyga att alla bestämmelser i den allmänna dataskyddsförordningen uppfylls, som t.ex. då det gäller godkända uppförandekodexar.

Kommissionen kommer att arbeta tillsammans med denna sektor, civilsamhället och dataskyddsmyndigheterna för att den uppsättning av verktyg för gränsöverskridande överföringar som inbegrips i den allmänna dataskyddsförordningen ska kunna utnyttjas till sin fulla potential. I samband med att reformen genomförs kommer den pågående dialogen med intressenterna att bidra till att fastställa prioriterade åtgärder i detta avseende. Åtgärderna kan inbegripa slutförande av det arbete som redan har inletts, exempelvis om utarbetande av standardavtalsklausuler för dataöverföringar mellan personuppgiftsbiträden, tillsammans med Artikel 29-arbetsgruppen (som under 2018 kommer att ersättas av Europeiska dataskyddsstyrelsen)[45]. Det kan handla om att utveckla nya delar av EU:s infrastruktur gällande efterlevnaden, till exempel genom att kommissionen fastställer krav och tekniska standarder för att upprätta certifieringsmekanismer och för deras funktion, vilket även inbegriper aspekter som rör gränsöverskridande dataöverföring[46]. En del av dessa åtgärder kan kompletteras av arbete på internationell nivå, särskilt med organisationer som har utvecklat liknande mekanismer för dataöverföring. Till exempel kunde man undersöka sätt att främja enhetlighet mellan bindande företagsbestämmelser enligt gemenskapslagstiftningen och enligt de gränsöverskridande regler om integritetsskydd som utarbetats av länderna som ingår i det ekonomiska samarbetet i Asien och Stillahavsområdet (APEC)[47] när det gäller de tillämpliga standarderna och ansökningsförfarandet inom ramen för bägge systemen. Detta bör bidra till att främja strikta standarder för dataskydd globalt, samtidigt som skillnaderna i fråga om hantering av integritetsskydd och dataskydd överbryggs, vilket hjälper de kommersiella aktörerna att navigera mellan olika system och utforma en policy som är förenlig med dessa.

---

[44] Se artikel 46.2 c och d och skäl 109 i den allmänna dataskyddsförordningen, där det förtydligas att anpassningar av godkända förlagor till klausuler är möjliga, under förutsättning att de inte direkt eller indirekt står i strid med dessa förlagor eller påverkar enskilda personers grundläggande rättigheter och friheter.

[45] För närvarande finns inga standardavtalsklausuler för dataöverföringar från personuppgiftsbiträden inom EU till personuppgiftsbiträden utanför EU.

[46] Artikel 43.8 och 43.9 i allmänna dataskyddsförordningen.

[47] Se 2014 års gemensamma referensram för APEC-länderna och EU avseende strukturen för EU:s bindande företagsbestämmelser och APEC:s system med gränsöverskridande regler om integritetsskydd (CBPR), där det finns en jämförelse av överensstämmelse och certifieringskrav inom båda systemen: http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

Kommissionen ska göra följande:

- Arbeta tillsammans med intressenter för att utveckla sådana alternativa mekanismer för överföring av personuppgifter som är anpassade till de särskilda behoven eller villkoren som gäller för vissa branscher, affärsmodeller och/eller aktörer.

3.3 Internationellt samarbete för skydd av personuppgifter

3.3.1 Främjande av standarder för dataskydd genom multilaterala instrument och forum

EU:s regelverk för dataskydd har ofta fungerat som en referenspunkt för tredjeländer som utvecklar sin lagstiftning på detta område. EU kommer att fortsätta sin aktiva dialog med de internationella partnerna, både på bilateral och på multilateral nivå, för att främja konvergens genom att utveckla strikta och samverkande globala standarder för skydd av personuppgifter. Detta bidrar till ett mer effektivt skydd av enskilda personers rättigheter och minskar samtidigt hindren för ett gränsöverskridande dataflöde som en viktig del av frihandeln.

Kommissionen uppmanar särskilt tredjeländer att ansluta sig till Europarådets konvention 108 och dess tilläggsprotokoll[48]. Konventionen, som är öppen för icke-medlemmar av Europarådet och redan har ratificerats av 50 länder, däribland vissa afrikanska och sydamerikanska länder[49], är det enda bindande multilaterala instrumentet inom området för dataskydd. Konventionen håller på att ses över för närvarande och kommissionen kommer aktivt att främja ett snabbt antagande av den reviderade texten för att EU ska kunna bli konventionspart. Texten kommer att återspegla samma principer som erkänns i EU:s nya dataskyddsbestämmelser och därigenom bidra till förenlighet med en uppsättning strikta standarder för dataskydd.

G20-mötet år 2017 kommer att utgöra ytterligare en möjlighet för EU att sträva efter samsyn kring principen om att de strikta standarderna för dataskydd är en viktig del av den fortsatta utvecklingen av ett globalt informationssamhälle som kan främja innovation, tillväxt och social välfärd[50].

Kommissionen ser även fram emot att arbeta med viktiga nya aktörer, såsom FN:s särskilda rapportör för rätten till privatliv[51], och ytterligare utveckla sitt samarbete med regionala organisationer såsom APEC, i syfte att främja en världsomspännande-kultur med respekt för rätten till personlig integritet och skydd av personuppgifter.

---

48 Europarådets konvention av den 28 januari 1981 om skydd för enskilda vid automatisk databehandling av personuppgifter (CETS nr 180) och 2001 års tilläggsprotokoll till denna konvention om tillsynsmyndigheter och gränsöverskridande flöden av personuppgifter (CETS nr. 181).

49 Mauritius, Senegal och Uruguay har ratificerat konventionen. Dessutom har Kap Verde, Marocko och Tunisien uppmanats att ansluta sig till den.

50 Se även ”*OECD Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity*” (OECD:s ministerdeklaration om den digitala ekonomin: innovation, tillväxt och samhälleligt välstånd, även kallad "Cancundeklarationen"), av den 23 juni 2016.

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

Inom ramen för Europeiska kommissionens allmänna ansträngningar för att förbättra medvetenheten om personlig integritet och för att skärpa dataskyddsåtgärderna internationellt godkände kommissionen den 15 november 2016 ett projekt inom ramen för partnerskapsinstrumentet i syfte att stärka samarbetet med partnerländerna på detta område[52]. Detta inbegriper finansiering av verksamheter såsom utbildning och medvetandegörande. I samband med genomförandet av reformen av kan EU i sin tur dra fördel av utbytet av bästa praxis och erfarenheter av andra system där det finns nya utmaningar kopplade till skyddet av privatlivet och nya rättsliga eller tekniska lösningar, bland annat när det gäller verkställighet, verktyg för efterlevnad (t.ex. certifieringsmekanismer, konsekvensanalyser avseende integritetsfrågor) eller skydd av vissa särskilda uppgifter (t.ex. uppgifter om barn).

3.3.2 Samarbete inom området för brottsbekämpning

Ett stärkt samarbete med berörda brottsbekämpande myndigheter och tillsynsmyndigheter i tredjeländer behövs allt oftare med tanke på att multinationella företag som bearbetar stora mängder av personuppgifter i ett stort antal länder har en global räckvidd. Problem med bristande efterlevnad av dataskyddsbestämmelser eller personuppgiftsbrott påverkar ofta många personer samtidigt i mer än en medlemsstats jurisdiktion. I dessa fall kan skyddet för enskilda personer göras effektivare genom gemensamma åtgärder. Samtidigt skulle de ekonomiska aktörerna få en tydligare rättslig miljö där gemensamma tolkningsverktyg och tillämpningsförfaranden utvecklas på global nivå.

I en gränslös och uppkopplad värld av dataflöden är det därför dags att utöka samarbetet mellan verkställande myndigheter[53]. Europeiska unionen är beredd att ta sitt ansvar. Som påpekas ovan innebär den allmänna dataskyddsförordningen att det blir möjligt för kommissionen att utveckla mekanismer för internationellt samarbete i syfte att underlätta en effektiv efterlevnad av dataskyddslagstiftningen, även genom överenskommelser om ömsesidigt bistånd. I detta sammanhang ska möjligheten att ta fram ett ramavtal om samarbete mellan EU:s dataskyddsmyndigheter och tillsynsmyndigheter i vissa tredjeländer också utforskas. Detta arbete ska baseras på de erfarenheter som kommissionen samlat inom andra tillsynsområden, så som områdena för konkurrens och konsumentskydd.

---

[52] Kommissionens genomförandebeslut C(2016) 7198, där den andra fasen av det årliga handlingsprogrammet 2016 (*"Annual Action Programme"*, AAP 2016) för partnerskapsinstrumentet godkänns.

[53] De befintliga nätverken omfattar bl.a. *"Global Privacy Enforcement Network"* (GPEN) som inledde sin verksamhet 2010 under överinseende av OECD. Detta är ett informellt nätverk av myndigheter med ansvar för integritetsskydd. Även EU:s dataskyddsmyndigheter är med i nätverket. Det ansvarar bland annat för samarbete inom området för brottsbekämpning, utbyte av bästa praxis när det gäller hantering av gränsöverskridande utmaningar, samt stöd till gemensamma initiativ för efterlevnad och åtgärder för att öka medvetenheten. Nätverket skapar inte några nya rättsligt bindande skyldigheter för deltagarna och inriktar sig främst på att underlätta samarbete vid tillämpningen av lagar om integritetsskydd för den privata sektorn. Se https://privacyenforcement.net/.

Kommissionen ska göra följande:

- Främja ett snabbt antagande av den reviderade texten i Europarådets konvention 108 så att EU ska kunna bli konventionspart och uppmuntra tredjeländer att ansluta sig.

- Använda multilaterala forum såsom Förenta Nationerna, G20 och APEC för att främja en global kultur med avseende på dataskyddsrättigheter.

- Utveckla mekanismer för internationellt samarbete med viktiga internationella partner för att underlätta en effektiv tillämpning.

4. ETT EFFEKTIVARE BROTTSBEKÄMPANDE SAMARBETE KOMBINERAT MED KRAFTFULLA DATASKYDDSÅTGÄRDER

Utbyte av personuppgifter är en integrerad del av arbetet med förebyggande, utredning och lagföring av brott. I en sammanlänkad värld där brottslighet sällan stannar vid de nationella gränserna är ett snabbt utbyte av personuppgifter avgörande för att det brottsbekämpande samarbetet ska vara framgångsrikt, samtidigt som det är en effektiv reaktion på brott. Sådana utbyten måste understödjas av kraftfulla dataskyddsåtgärder. Detta bidrar också till att bygga upp förtroendet mellan de brottsbekämpande myndigheterna och till att stärka rättssäkerheten när uppgifter samlas in och/eller utbyts.

Bestämmelserna i polisdirektivet om gränsöverskridande dataöverföring reglerar utbytet av uppgifter mellan brottsbekämpande myndigheter inom och utanför EU samt, i vissa situationer, dataöverföringar från brottsbekämpande myndigheter till andra enheter. Detta direktiv inför möjligheten att tillämpa konstateranden om adekvata skyddsnivåer inom den straffrättsliga sektorn. Kommissionen kommer att främja möjligheten att tillämpa sådana konstateranden om adekvata skyddsnivåer tillsammans med godkända tredjeländer, särskilt tillsammans med länder med vilka det krävs ett nära och snabbt samarbete i kampen mot brottslighet och terrorism, och med vilka ett betydande utbyte av personuppgifter redan äger rum. Mot denna bakgrund avser kommissionen att prioritera diskussioner som gäller beslut om adekvat skyddsnivå med tredjeländer som är viktiga partner i denna strävan.

Alternativt är paraplyavtalet om dataskydd[54] som ingicks i december 2016 mellan EU och Förenta staterna ett framgångsrikt exempel på hur brottsbekämpande samarbete med viktiga internationella partner kan förbättras genom att förhandla om en uppsättning kraftfulla dataskyddsåtgärder. Paraplyavtalet kompletterar automatiskt befintliga rättsliga instrument som utbytet av uppgifter bygger på (särskilt bilaterala avtal på både unionsnivå och medlemsstatsnivå), och medför därför direkta och omedelbara fördelar för enskilda personer och stärker det brottsbekämpande samarbetet genom att underlätta utbyte av information.

[54] Ett avtal mellan EU och USA om skyddet av personuppgifter när dessa överförs och behandlas i syfte att förebygga, undersöka, upptäcka eller åtala straffbara gärningar, inklusive terrorism, inom ramen för polissamarbete och rättsligt samarbete i straffrättsliga frågor. Se http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (nedan kallat *paraplyavtalet*)

Genom att fastställa ett standardvärde för överenskommelser om framtida dataöverföringar med Förenta staterna eliminerar paraplyavtalet dessutom behovet av att upprepade gånger omförhandla dessa skyddsåtgärder. Paraplyavtalet är det första bilaterala internationella avtalet med en heltäckande förteckning över rättigheterna och skyldigheterna med koppling till skydd av personuppgifter i enlighet med gemenskapens regelverk. Avtalet kan därför ligga till grund för förhandlingar om liknande avtal med tredjeländer, inte bara inom området för rättsligt och polisiärt samarbete, utan även inom andra områden med offentliga tillsynsåtgärder (t.ex. konkurrenspolitiken, konsumentskydd). Detta skulle inte enbart omfatta utbyte av uppgifter mellan statsförvaltningar, utan även dataöverföring mellan privata företag och brottsbekämpande myndigheter. På detta sätt skulle det också bli lättare för EU att ingå avtal om utbyte av uppgifter mellan de berörda EU-organen (i synnerhet Europol och Eurojust) samt tredjeländer[55]. Därför har kommissionen för avsikt att undersöka möjligheten att ingå liknande ramavtal med viktiga partner inom brottsbekämpning.

Dessutom skapar polisdirektivet en möjlighet för brottsbekämpande myndigheter i EU att enligt strikta skyddsåtgärder och under särskilda omständigheter begära upplysningar direkt från ett privat företag i tredjeland och överföra personuppgifter (vanligtvis ett namn eller en viss IP-adress) i en sådan begäran[56]. Däremot behandlar allmänna dataskyddsförordningen specifikt sådana fall där privata aktörer i EU på begäran överför personuppgifter till brottsbekämpande myndigheter i tredjeland. Sådana överföringar utanför EU är endast tillåtna på vissa villkor, t.ex. på grundval av ett internationellt avtal eller om offentliggörande krävs med stöd av ett viktigt allmänintresse som erkänns på grundval av unionens eller medlemsstaternas lagstiftning[57].

Detta samarbete, som har blivit av avgörande betydelse för att brott och terrorism ska kunna utredas och lagföras framgångsrikt, framhävs i rådets slutsatser om förbättrad straffrätt i cyberrymden. Rådet har uppmanat kommissionen att vidta konkreta åtgärder på grundval av en gemensam EU-strategi, för att förbättra samarbetet med tjänsteleverantörer, göra den ömsesidiga rättsliga hjälpen effektivare och föreslå lösningar på problem med att fastställa behörigheten och se till att rättsbestämmelser verkställs i cyberrymden[58]. Dessa åtgärder omfattar inte enbart utbyten mellan brottsbekämpande myndigheter och tjänsteleverantörer som är baserade i EU, utan även utbyten med myndigheter och företag som inte finns i EU. Kommissionen har för avsikt att beskriva möjligheterna för att få tillgång till elektroniska bevis i juni 2017, med hänsyn till behovet av snabbt och tillförlitligt samarbete. Detta stöds av de strikta standarderna för skydd av personuppgifter i polisdirektivet och i allmänna dataskyddsförordningen, både i situationer inom EU och vid gränsöverskridande dataöverföringar.

---

55 Ingåendet av de operativa avtalen med Europol och Eurojust har också utgjort ett riktmärke i dialogerna om viseringsliberalisering med vissa tredjeländer, t.ex. även inom ramen för den pågående dialogen med Turkiet.

56 Se artikel 39 och skäl 73 i polisdirektivet.

57 Se artikel 48 och skäl 115 i allmänna dataskyddsförordningen.

58 Slutsatserna från Europeiska unionens råd om förbättrad straffrätt i cyberrymden, den 9 juni 2016: www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. Kommissionen har i uppdrag att lägga fram resultat för dessa frågor inför rådet i juni 2017, efter en lägesrapport till rådet i december 2016.

I enlighet med den nya rättsliga grunden för Europol kommer kommissionen slutligen att utvärdera bestämmelserna i dessa operativa samarbetsavtal mellan Europol och berörda tredje parter, som ingåtts i enlighet med rådets beslut 2009/371/RIF, inbegripet deras bestämmelser om dataskydd[59]. Såsom anges i den europeiska säkerhetsagendan för 2015, kommer unionens framtida upplägg för utbyte av passageraruppgifter med länder som inte ingår i EU att inbegripa behovet av att tillämpa enhetliga standarder och särskilda mekanismer för att skydda de grundläggande rättigheterna. Kommissionen kommer att arbeta på lagliga och hållbara lösningar för utbyte av passageraruppgifter (PNR-uppgifter) med tredjeländer, bland annat genom att överväga ett modellavtal om PNR-uppgifter där det fastställs vilka krav tredjeländer måste uppfylla för att motta PNR-uppgifter från EU. Den framtida politiken inom detta område kommer emellertid i första hand att bedömas utifrån ett kommande yttrande från Europeiska unionens domstol om det planerade PNR-avtalet mellan EU och Kanada[60].

ETT EFFEKTIVARE BROTTSBEKÄMPANDE SAMARBETE KOMBINERAT MED KRAFTFULLA DATASKYDDSÅTGÄRDER

Kommissionen ska göra följande:

- Främja möjligheterna att fatta beslut om adekvata skyddsåtgärder enligt polisdirektivet tillsammans med godkända tredjeländer.
- Främja förhandlingarna om avtal på området för brottsbekämpning med viktiga internationella partner enligt den förlaga som ingår i paraplyavtalet med Förenta staterna.
- Följa upp rådets slutsatser om förbättrad straffrätt i cyberrymden i syfte att underlätta gränsöverskridande utbyte av elektroniska bevis i överensstämmelse med dataskyddsbestämmelserna.

5. SLUTSATS

Att skydda och utbyta personuppgifter är åtgärder som inte utesluter varandra. Ett starkt system för skydd av personuppgifter underlättar dataflöden genom att bygga upp konsumenternas förtroende för sådana företag som bryr sig om hur de hanterar sina kunders personuppgifter. Strikta standarder för dataskydd blir därmed en fördel i den globala digitala ekonomin. Detsamma gäller för brottsbekämpande samarbete: skydd av privatlivet är en

[59] Se artikel 25.4 i Europaparlamentets och rådets förordning (EU) 2016/794 av den 11 maj 2016 om Europeiska unionens byrå för samarbete inom brottsbekämpning (Europol) och om ersättande och upphävande av rådets beslut 2009/371/RIF, 2009/934/RIF, 2009/935/RIF, 2009/936/RIF och 2009/968/RIF, EUT L 135, 24.5.2016, s. 53. Kommissionen är skyldig att lägga fram en utvärderingsrapport senast den 14 juni 2021 om Europols samarbetsavtal som ingåtts före den 1 maj 2017.

[60] Domstolens yttrande om utkastet till 2014 års PNR-avtal mellan EU och Kanada som hänvisats till domstolen av Europaparlamentet, dvs. yttrande 1/15. Domstolen ombads bedöma om utkastet till avtal är förenligt med Europeiska unionens stadga om de grundläggande rättigheterna.

integrerad del av ett effektivt och snabbt informationsutbyte i kampen mot brottslighet och baseras på ömsesidigt förtroende och rättssäkerhet.

Efter att ha utfört en reform av sina dataskyddsbestämmelser bör EU aktivt samarbeta med tredjeländer inom detta område. Unionen bör eftersträva ökad internationell samsyn kring dataskyddsprinciper, både på bilateral och på multilateral nivå. Detta ligger i både medborgarnas och företagens intresse och är samtidigt till nytta för dem. De nya lagstiftningsramarna om dataskydd ger EU de nödvändiga och lämpliga verktygen för att uppnå dessa mål. På grundval av den strategi som presenteras i detta meddelande kommer kommissionen att samarbeta aktivt med de viktigaste tredjeländerna för att undersöka möjligheten att godkänna konstateranden om adekvata skyddsnivåer på annat håll, med början i Japan och Korea under 2017, i syfte att främja lagstiftningskonvergens mot EU:s standarder och underlätta handelsförbindelserna. Samtidigt kommer EU att fullt ut utnyttja utbudet av alternativa verktyg för dataöverföring i syfte att skydda dataskyddsrättigheterna och stödja de ekonomiska aktörerna när uppgifter överförs till länder vars nationella lagstiftning inte säkerställer en adekvat skyddsnivå för uppgifterna. Sådana verktyg bör också användas för att ytterligare underlätta samarbetet mellan EU:s tillsynsmyndigheter och brottsbekämpande myndigheter tillsammans med deras internationella partner. Kommissionen kommer att säkerställa samstämmigheten i den interna och externa dimensionen av EU:s dataskyddspolitik och främja ett starkt dataskydd på internationell nivå i syfte att förbättra det brottsbekämpande samarbetet, bidra till att utveckla frihandel och utarbeta höga standarder för skydd av personuppgifter på globalt plan.