



Bryssel den 27.11.2013
COM(2013) 846 final

**MEDDELANDE FRÅN KOMMISSIONEN TILL EUROPAPARLAMENTET OCH
RÅDET**

Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna

1. INLEDNING: DE FÖRÄNDRADE FÖRUTSÄTTNINGARNA FÖR BEHANDLING AV DATA I EU OCH FÖRENTA STATERNA

Europeiska unionen och Förenta staterna är strategiska partner, och detta partnerskap är av största betydelse för att vi ska kunna främja våra gemensamma värderingar, vår säkerhet och vårt gemensamma ledarskap i globala frågor.

Förtroendet för partnerskapet har dock påverkats negativt och behöver återställas. EU, dess medlemsstater och medborgarna har emellertid uttryckt stor oro efter avslöjandena om storskaliga amerikanska program för insamling av underrättelseinformation, särskilt när det gäller skyddet av personuppgifter¹. Massövervakning av privat kommunikation är, oavsett om den drabbar medborgare, företag eller politiska ledare, oacceptabel.

Överföringen av personuppgifter är en viktig och nödvändig del av de transatlantiska förbindelserna. Den utgör en integrerad del av handelsutbytena över Atlanten, också för nya och växande digitala affärsverksamheter, såsom sociala medier eller molntjänster, där stora mängder data överförs från EU till Förenta staterna. De utgör även ett viktigt inslag i samarbetet mellan EU och Förenta staterna i fråga om brottsbekämpning och i samarbetet mellan medlemsstaterna och Förenta staterna på området för nationell säkerhet. För att underlätta dataflödena och samtidigt garantera en sådan hög nivå av uppgiftsskydd som krävs enligt EU-lagstiftningen, har Förenta staterna och EU upprättat en rad avtal och arrangemang. Handelsrelaterade frågor behandlas i beslut 2000/520/EG² (nedan kallat *Safe Harbour-beslutet*). Detta beslut ger en rättslig grund för överföringar av personuppgifter från EU till företag som är etablerade i Förenta staterna och som har anslutit sig till Safe Harbour-principerna om integritetsskydd).

Utbytet av personuppgifter mellan EU och Förenta staterna för brottsbekämpningsändamål, inbegripet förebyggande och bekämpning av terrorism och andra former av allvarlig brottslighet, regleras av ett antal avtal på EU-nivå. Det rör sig om avtalet om ömsesidig rättslig hjälp³, avtalet om användning och överföring av passageraruppgifter (PNR)⁴, avtalet om behandling och överföring av uppgifter om finansiella meddelanden i syfte att bekämpa terrorism (*Terrorism Financing Tracking Programme –TFTP*)⁵, och avtalet mellan Europol och Förenta staterna. Dessa avtal behandlar stora säkerhetsrelaterade utmaningar och främjar EU:s och Förenta staterna gemensamma säkerhetsintressen, samtidigt som de garanterar skyddet av personuppgifter. Dessutom håller EU och Förenta staterna på att förhandla fram ett ramavtal ("paraplyavtal") om dataskydd på området för polissamarbete och straffrättsligt

¹ I detta meddelande inbegriper hänvisningar till EU-medborgare även registrerade personer som inte är medborgare i EU, men som ändå omfattas av Europeiska unionens dataskyddslagstiftning.

² Kommissionens beslut 2000/520/EG av den 26 juli 2000 enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom de principer om integritetsskydd (Safe Harbor Privacy Principles) i kombination med frågor och svar som Förenta staternas handelsministerium utfärdat (EGT L 215, 25.8.2000, s. 7).

³ Rådets beslut 2009/820/Gusp av den 23 oktober 2009 om ingående på Europeiska unionens vägnar av avtalet om utlämning mellan Europeiska unionen och Amerikas förenta stater och av avtalet om ömsesidig rättslig hjälp mellan Europeiska unionen och Amerikas förenta stater (EUT L 291, 7.11.2009, s. 40).

⁴ Rådets beslut 2012/472/EU av den 26 april 2012 om ingående av avtalet mellan Amerikas förenta stater och Europeiska unionen om användning och överföring av passageraruppgifter till Förenta staternas Department of Homeland Security (EUT L 215, 11.8.2012, s. 4)

⁵ Rådets beslut av den 13 juli 2010 om ingående av avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism (TFTP) (EUT L 195, 27.7.2010, s. 3).

samarbete⁶. Syftet är att garantera att personuppgifter som blir föremål för utbyte omfattas av ett gott skydd, och därigenom ytterligare främja samarbetet mellan EU och Förenta staterna i kampen mot brottslighet och terrorism, på grundval av gemensamma värderingar och överenskomna garantier.

Dessa instrument har utformats för en miljö där flödena av personuppgifterna får allt större betydelse.

Å ena sidan har utvecklingen av den digitala ekonomin lett till en exponentiell tillväxt i uppgiftsbehandlingens kvantitet, kvalitet, mångfald och natur. Medborgarnas användning av elektroniska kommunikationstjänster i vardagen har ökat. Personuppgifter har blivit en värdefull tillgång. EU-medborgarnas personuppgifter uppskattades till ett värde av 315 miljarder euro 2011, en siffra som kan komma att öka till nästan en biljon euro till 2020⁷. Marknaden för analys av stora uppgiftsmängder ökar med 40 % om året i världen som helhet⁸. På samma sätt har den tekniska utvecklingen, till exempel i samband med datormoln, satt perspektiv på begreppet internationell överföring av uppgifter, eftersom gränsöverskridande dataflöden håller på att bli en vardagsrealitet.⁹

Den ökade användningen av elektronisk kommunikation och databehandlingstjänster, däribland molntjänster, har också bidragit till att på ett betydande sätt vidga omfattningen och betydelsen av transatlantiska överföringar av personuppgifter. Faktorer som amerikanska företags centrala ställning i den digitala ekonomin¹⁰, det förhållandet att en stor del av den elektroniska kommunikationen dirigeras över Atlanten och volymen av elektroniska dataflöden mellan EU och Förenta staterna, har fått ännu större betydelse.

Å andra sidan ger moderna metoder för överföring av personuppgifter upphov till nya och viktiga frågeställningar. Detta gäller såväl nya metoder för storskalig bearbetning av konsumentdata som utförs av privata företag för kommersiella ändamål och underrättelsemyndigheters ökade förmåga till storskalig övervakning av kommunikationsuppgifter.

Omfattande amerikanska program för insamling av underrättelseinformation, t.ex. Prism, inkräktar på européers grundläggande rättigheter, särskilt rätten till ett privatliv och rätten till skydd av personuppgifter. Dessa program pekar också på ett samband mellan statlig övervakning och uppgiftsbehandling som utförs av privata företag, särskilt amerikanska internetföretag. Som en följd av detta kan de få ekonomiska konsekvenser. Om medborgare är oroade över den omfattande behandling av deras personuppgifter som utförs av privata företag eller av övervakningen av personuppgifter från underrättelsetjänster vid användning av internetjänster, kan detta påverka deras förtroende för den digitala ekonomin, eventuellt med negativa konsekvenser för tillväxten.

Denna utveckling ställer uppgiftsflödena mellan EU och Förenta staterna i ett nytt perspektiv, och det här meddelandet tar upp de utmaningar som vi måste kunna möta. I meddelandet undersöks det fortsatta arbetet på grundval av slutsatserna i rapporten från EU-ledamöterna i EU:s och Förenta staternas gemensamma tillfälliga arbetsgrupp och meddelandet om Safe Harbour.

⁶ Den 3 december antog rådet beslutet om att bemyndiga kommissionen att förhandla om avtalet. Se IP/10/1661 av den 3 december 2010.

⁷ Boston Consulting Group, The Value of our Digital Identity, november 2012.

⁸ McKinsey, Big data: The next frontier for innovation, competition, and productivity, 2011

⁹ Meddelande om frigörande av de molnbaserade tjänsternas potential i Europa, KOM(2012) 529 slutlig.

¹⁰ T.ex. det sammanlagda antalet unika besökare till Microsoft Hotmail, Google Gmail och Yahoo! Antalet e-postmeddelanden från europeiska länder uppgick i juni 2012 till över 227 miljoner, vilket överskuggade alla andra leverantörer. Det samlade antalet unika europeiska besökare på Facebook och Facebook Mobile uppgick i mars 2012 till 196,5 miljoner, vilket gör Facebook till det största sociala nätverket i Europa. Google är den ledande sökmotorn för internet, och används av 90,2 % av världens internetanvändare. Den amerikanska mms-tjänsten What's app användes i juni 2013 av 91 % av alla iPhone-användare i Tyskland.

Det syftar till att tillhandahålla en effektiv strategi för att återskapa förtroendet och förbättra samarbetet mellan EU och Förenta staterna på dessa områden samt stärka de transatlantiska förbindelserna i bredare bemärkelse.

Detta meddelande grundar sig på antagandet att nivån på skyddet av personuppgifter måste behandlas i sitt rätta sammanhang, utan att det påverkar andra aspekter av förbindelserna mellan EU och Förenta staterna, inbegripet de pågående förhandlingarna om ett transatlantiskt partnerskap för handel och investeringar. Därför är det inte aktuellt att diskutera frågan om uppgiftsskyddsnormer inom ramen för det transatlantiska partnerskapet för handel investeringar, som fullt ut kommer att respektera bestämmelserna om skydd av personuppgifter.

Det är viktigt att notera att även om EU kan vidta åtgärder rörande frågor som omfattas av EU:s behörighet, särskilt för att säkerställa en korrekt tillämpning av EU-rätten¹¹, är den nationella säkerheten ett område som helt omfattas av varje medlemsstats eget ansvar¹².

2. INVERKAN PÅ INSTRUMENT FÖR ÖVERFÖRING AV UPPGIFTER

När det gäller uppgifter som överförs för kommersiella ändamål har principen om Safe Harbour visat sig vara ett viktigt verktyg för överföring av uppgifter mellan EU och Förenta staterna. Dess kommersiella betydelse har ökat allteftersom flödena av personuppgifter har fått en större betydelse i de transatlantiska handelsförbindelserna. Över de senaste 13 åren har systemet med Safe Harbour utvecklats så att det nu omfattar över 3 000 företag, av vilka hälften har anmält sig under de senaste fem åren. Trots detta har farhågorna ökat när det gäller nivån på skyddet av EU-medborgares personuppgifter som överförs till Förenta staterna inom ramen för Safe Harbour-systemet. Det faktum att systemet är frivilligt och bygger på förklaringar har lett till ökat fokus på öppenhet och efterlevnad. Även om en majoritet av de berörda amerikanska företagen tillämpar systemets principer, finns det vissa självcertifierade företag som har valt att avstå. Det förhållandet att vissa självcertifierade företag inte följer Safe Harbour-principerna för skydd av privatlivet innebär att dessa företag får en konkurrensfördel jämfört med europeiska företag som är verksamma på samma marknader. Safe Harbour-systemet ger möjlighet att införa inskränkningar i uppgiftsskyddet när det nödvändigt med hänsyn till den nationella säkerheten¹³, men det har ifrågasatts huruvida den storskaliga insamlingen och behandlingen personuppgifter inom ramen för de amerikanska övervakningsprogrammen är nödvändig och proportionerlig för att ta hänsyn till de nationella säkerhetsintressena. Det framgår också av de resultat som EU:s och Förenta staternas tillfälliga arbetsgrupp har kommit fram till att EU-medborgare inte omfattas av samma rättigheter och rättssäkerhetsgarantier som amerikaner inom ramen för dessa program. Räckvidden av dessa övervakningsprogram, i kombination med ojämlik behandling av EU-medborgare, medför att den skyddsnivå som erbjuds genom Safe Harbour-systemet måste ifrågasättas. EU-medborgares personuppgifter som sänds till Förenta staterna inom ramen för Safe Harbour är åtkomliga för och kan behandlas ytterligare av amerikanska myndigheter på ett sätt som är oförenligt med de ändamål för vilka uppgifterna ursprungligen samlades in i EU och sedermera överfördes till Förenta staterna. En majoritet av de amerikanska internetföretag som förefaller vara mer direkt berörda av dessa program är certifierade enligt Safe Harbour-systemet.

¹¹ Se domstolens dom i mål C-300/11, ZZ mot Secretary of State for the Home Department.

¹² Artikel 4.2 i Fördraget om Europeiska unionen.

¹³ Se t.ex. Safe Harbour-beslutet, bilaga I.

När det gäller utbyte av uppgifter för brottsbekämpande ändamål har befintliga avtal (PNR, TFTP) visat sig vara mycket värdefulla verktyg för att möta gemensamma säkerhetshot med koppling till allvarlig gränsöverskridande brottslighet och terrorism, samtidigt som de innehåller skyddsbestämmelser som garanterar en hög nivå på uppgiftsskyddet¹⁴. Dessa garantier omfattar även EU-medborgare, och avtalen föreskriver mekanismer för att se över genomförandet och behandla problem i samband med detta. TFTP-avtalet inför också ett system för tillsyn, där EU:s oberoende övervakare kan kontrollera hur uppgifter som omfattas av avtalet blir föremål för åtgärder från Förenta staternas sida.

Mot bakgrund av de farhågor som framförts i EU med avseende på amerikanska övervakningsprogram, har Europeiska kommissionen använt sig av dessa mekanismer för att kontrollera hur avtalen tillämpas. När det gäller PNR-avtalet gjordes en gemensam översyn med deltagande av experter från både EU och Förenta staterna, där man tittade på hur avtalet har tillämpats¹⁵. Denna översyn gav ingen indikation på att de amerikanska övervakningsprogrammen utsträcker sig till eller påverkar passageraruppgifter som omfattas av PNR-avtalet. När det gäller TFTP-avtalet beslutade kommissionen att inleda formella samråd efter påståenden om att amerikanska underrättelsetjänster fått direkt tillgång till personuppgifter i EU, i strid med avtalet. Vid dessa samråd framkom inget som pekar på en överträdelse av TFTP-avtalet, med fick Förenta staterna att lämna en skriftlig försäkran om att ingen direkt insamling av uppgifter hade ägt rum i strid med bestämmelserna i avtalet.

Den omfattande insamlingen och behandlingen av personuppgifter inom ramen för de amerikanska övervakningsprogrammen föranleder dock en fortsatt mycket ingående övervakning av genomförandet av de PNR och TFTP-avtalen också i framtiden. EU och Förenta staterna därför enats om gå vidare med nästa gemensamma översyn av TFTP-avtalet, som kommer att genomföras under våren 2014. Inom ramen för denna och framtida gemensamma översyner är det viktigt att säkerställa öppenhet om hur tillsynen fungerar och hur den bidrar till att skydda EU-medborgares personuppgifter. Parallellt kommer åtgärder att vidtas för att se till att tillsynssystemet fortsätter att rikta uppmärksamheten på hur uppgifter som överförs till Förenta staterna inom ramen för avtalet behandlas, med fokus på hur uppgifterna delas mellan amerikanska myndigheter.

För det tredje understryker den ökade volymen av behandlade personuppgifter betydelsen av tillämpliga rättsliga och administrativa garantier. Ett av målen med EU:s och Förenta staternas tillfälliga arbetsgrupp var att fastställa vilka skyddsmekanismer som tillämpas för att minimera uppgiftsbehandlings effekter på EU-medborgarnas grundläggande rättigheter. Skyddsåtgärder är också nödvändiga för att skydda företag. Vissa amerikanska lagar, t.ex. Patriot Act, gör det möjligt för amerikanska myndigheter att direkt begära att företag ger tillgång till uppgifter som lagras i EU. Europeiska företag, och amerikanska företag som finns i EU, kan således åläggas att överföra uppgifter till Förenta staterna i strid med EU-rätten och medlemsstaternas lagstiftning. De hamnar således i kläm mellan motstridiga rättsliga skyldigheter. Den rättsosäkerhet som uppstår till följd att sådana direkta uppmaningar att lämna tillgång till uppgifter kan bli till hinder för utvecklingen av nya digitala tjänster, exempelvis datormolntjänster, vilka annars kan ge effektiva och billiga lösningar för enskilda och företag.

¹⁴ Se gemensam rapport från kommissionen och det amerikanska finansdepartementet rörande värdet av uppgifter som tillhandahållits inom ramen för TFTP, i enlighet med artikel 6.6 i avtalet mellan Europeiska unionen och Amerikas förenta stater om behandling och överföring av uppgifter om finansiella betalningsmeddelanden från Europeiska unionen till Förenta staterna i enlighet med programmet för att spåra finansiering av terrorism

¹⁵ Se kommissionens rapport Joint review of the implementation of the Agreement between the European Union and the United States of America on the processing and transfer of passenger name records to the United States Department of Homeland Security.

3. ETT EFFEKTIVT UPPGIFTSSKYDD

Överföringen av personuppgifter mellan EU och Förenta staterna är ett viktigt inslag i de transatlantiska handelsförbindelserna. Informationsutbyte är också en viktig del av säkerhetssamarbetet mellan EU och Förenta staterna, och dessutom avgörande för förutsättningarna att uppnå det gemensamma målet att förebygga och bekämpa allvarlig brottslighet och terrorism. De senaste avslöjandena om de amerikanska programmen för insamling av underrättelseinformation har haft en negativ inverkan på det förtroende som samarbetet bygger på. Det har särskilt påverkat förtroendet för hur personuppgifter behandlas. Följande åtgärder bör vidtas för att återställa förtroendet för överföringar av personuppgifter, till förmån för den digitala ekonomin, säkerheten i såväl EU som Förenta staterna och de transatlantiska förbindelserna i bredare bemärkelse.

3.1 Reformeringen av uppgiftsskyddet i EU

Den uppgiftsskyddsreform som kommissionen föreslog i januari 2012¹⁶ är av stor betydelse för att stärka skyddet av personuppgifter. Fem delar av det föreslagna uppgiftsskyddspaketet är av särskild betydelse.

När det gäller det geografiska tillämpningsområdet klagörs i den föreslagna förordningen att företag som inte är etablerade i EU kommer att vara tvungna att tillämpa EU-lagstiftningen om uppgiftsskydd när de erbjuder varor och tjänster till de europeiska konsumenterna eller övervakar dess beteende. Med andra ord kommer den grundläggande rätten till skydd av personuppgifter att respekteras, oberoende av var ett företag eller dess anläggning för behandling av uppgifter finns¹⁷.

När det gäller internationella överföringar fastställer den föreslagna förordningen villkoren för överföring av uppgifter utanför EU. Överföringar kan endast tillåtas om dessa villkor, som garanterar individens rätt till en hög skyddsnivå, är uppfyllda¹⁸.

De föreslagna bestämmelserna föreskriver proportionerliga och avskräckande sanktioner (upp till 2 % av ett företags årliga omsättning) för att säkerställa att företag följer EU-lagstiftningen¹⁹. Förekomsten av trovärdiga sanktioner kommer att öka företagets incitament att följa EU-lagstiftningen.

Den föreslagna förordningen innehåller klara regler om skyldigheter och ansvar för uppgiftsbehandlare, t.ex. leverantörer av molntjänster, även säkerhetsbestämmelser²⁰. Som avslöjandena rörande de amerikanska programmen för insamling av underrättelseinformation

¹⁶ KOM(2012) 10 slutlig: Förslag till Europaparlamentets och rådets direktiv om skyddet av enskilda vid behöriga myndigheters behandling av personuppgifter i syfte att förebygga, utreda, avslöja eller lagföra brott eller verkställa straffrättsliga påföljder, samt fri rörlighet för sådana uppgifter, Bryssel 25.1.2012, samt KOM(2012) 11 slutlig: Förslag till Europaparlamentets och rådets förordning om skydd för enskilda personer med avseende på behandling av personuppgifter och om det fria flödet av sådana uppgifter (allmän uppgiftsskyddsförordning).

¹⁷ Kommissionen noterar att Europaparlamentet bekräftade och understödde denna viktiga princip, som fastställs i artikel 3 i den föreslagna förordningen, i sin omröstning den 21 oktober 2013 om betänkandena om reformen av uppgiftsskyddet från parlamentsledamöterna Jan-Philipp Albrecht och Dimitrios Droutsas i utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor.

¹⁸ Kommissionen noterar att Europaparlamentets utskott för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor i sin omröstning den 21 oktober 2013 föreslog att man i den framtida förordningen skulle införa en bestämmelse som innebär att framställningar från utländska myndigheter om tillgång till personuppgifter som samlats in i EU endast kan beviljas om det finns förhandsgodkännande från en nationell dataskyddsmyndighet, i sådana fall där framställan görs utanför ramen för ett avtal om ömsesidig rättsligt hjälp eller ett annat internationellt avtal.

¹⁹ Kommissionen noterar att utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor i sin omröstning den 21 oktober 2013 föreslog att kommissionens förslag skulle skärpas ytterligare genom införande av böter på upp till 5 % av ett företags årliga omsättning i världen.

²⁰ Kommissionen noterar att utskottet för medborgerliga fri- och rättigheter samt rättsliga och inrikes frågor i sin omröstning den 21 oktober 2013 stödde att registerförarnas skyldigheter och ansvar skulle skärpas, särskilt med avseende på artikel 26 i den föreslagna förordningen.

har visat är detta av avgörande betydelse, eftersom dessa program påverkar uppgifter som lagras i datormoln. Företag som tillhandahåller lagringsutrymme i molnet, och som uppmanas att lämna ut personuppgifter till utländska myndigheter, kommer inte att kunna kringgå sitt ansvar genom att hänvisa till att de är registerförare och inte registeransvariga. Paketet kommer att leda till att det införs övergripande bestämmelser om skydd av personuppgifter som behandlas i samband med brottsbekämpning. En överenskommelse om paketet kan förväntas under loppet av 2014²¹.

3.2 Ett säkrare Safe Harbour-system

Safe Harbour-systemet är ett viktigt inslag i handelsförbindelserna mellan EU och Förensta staterna, som företag på båda sidor om Atlanten förlitar sig på.

I kommissionens rapport om Safe Harbour-systemets funktion konstaterades brister i systemet. Brist på öppenhet och tillsyn har lett till att vissa självcertifierade Safe Harbour-medlemmar inte följer systemets principer i praktiken. Detta har en negativ inverkan på EU-medborgarnas grundläggande rättigheter. Det medför även att europeiska företag har en nackdel jämfört med de konkurrerande amerikanska företag som verkar inom ramen för systemet utan att tillämpa dess principer i praktiken. Bristen påverkar även den majoritet amerikanska företag som tillämpar systemet korrekt. Safe Harbour fungerar också som en kanal för överföring av personuppgifter om EU-medborgare från EU till Förensta staterna av företag som är skyldiga att överlämna uppgifter till amerikanska underrättelsetjänster inom ramen för amerikanska program för insamling av underrättelseinformation. Om inte dessa brister rättas till kommer konkurrensnackdelarna för EU:s företag och den negativa inverkan på den grundläggande rätten till skydd för personuppgifter i EU att kvarstå.

Bristerna i Safe Harbour-systemet har betonats särskilt i samband med de europeiska dataskyddsmyndigheternas reaktioner på de senaste övervakningsavslöjandena. Enligt artikel 3 i Safe Harbour-beslutet har dessa myndigheter under vissa förutsättningar rätt att stoppa dataflöden till certifierade företag.²² Tyska dataskyddsansvariga har beslutat att inte utfärda några nya tillstånd att överföra uppgifter till länder utanför EU (t.ex. för användning av vissa molntjänster). De kommer också att undersöka om dataöverföringar inom ramen för Safe Harbour-systemet bör stoppas.²³ Risken är dock att sådana åtgärder, om de vidtas på nationell nivå, leder till skillnader i tillämpningen, med följderna att Safe Harbour skulle upphöra att vara ett kärnverktyg för överföring av personuppgifter mellan EU och Förensta staterna.

Enligt direktiv 95/46/EG har kommissionen rätt att upphäva eller återkalla Safe Harbour-beslutet om systemet inte längre ger en tillräcklig skyddsnivå. I artikel 3 i Safe Harbour-beslutet föreskrivs att kommissionen har rätt att upphäva beslutet helt eller tills vidare eller begränsa dess tillämpningsområde. Enligt artikel 4 får kommissionen möjlighet när som helst ändra beslutet mot bakgrund av erfarenheterna från genomförandet.

Mot bakgrund av detta finns det en rad politiska alternativ som kan övervägas, bland annat följande:

²¹ I sina slutsatser från oktober 2013 konstaterade Europeiska rådet följande: ”Det är viktigt att främja medborgarnas och företagens förtroende för den digitala ekonomin. Ett snabbt antagande av en kraftfull allmän uppgiftsskyddsram för EU samt av it-säkerhetsdirektivet är avgörande för att den inre digitala marknaden ska kunna fullbordas 2015”

²² Enligt artikel 3 i Safe Harbour-beslutet kan sådana avbrott särskilt bli aktuella om det finns välgrundad anledning att anta att det föreligger en kränkning av Safe Harbour-principerna och att den berörda genomförandemekanismen inte i tid utmynnar i lämpliga åtgärder för att avgöra ärendet, samt om fortsatt överföring skulle medföra en överhängande risk för att registrerade lider allvarlig skada och de behöriga myndigheterna i EU-medlemsstaten i fråga, med hänsyn till rådande omständigheter, har gjort vad de rimligen har kunnat för att meddela organisationen och ge den tillfälle att vidta åtgärder.

²³ Bundesbeauftragten für den Datenschutz und die Informationsfreiheit, pressmeddelande av den 24 juli 2013.

- Bibehålla status quo.
- Stärka ramen för Safe Harbour-systemet och göra en ingående översyn av dess.
- Upphäva Safe Harbour-beslutet helt eller tills vidare.

Med tanke på de konstaterade bristerna är det inte möjligt att fortsätta med den nuvarande tillämpningen av Safe Harbour-beslutet. Ett återkallande av beslutet skulle emellertid inverka negativt på intressena för de företag i EU och Förenta staterna som deltar i systemet. Kommissionen anser att Safe Harbour-systemet i stället bör stärkas.

Förbättringarna bör utöver de strukturella bristerna rörande öppenhet och tillsyn och de materiella Safe Harbour-principerna omfatta tillämpningen av det undantag som kan åberopas med hänvisning till den nationella säkerheten.

För att Safe Harbour ska fungera på det sätt som var avsett krävs att de amerikanska myndigheterna på ett mer effektivt och systematiskt sätt övervakar hur certifierade företag uppfyller sina åtaganden inom ramen för Safe Harbour-systemet. Insyn i de certifierade företagens strategier för integritetsskydd måste förbättras. EU-medborgarna måste också tillförsäkras tillgång till ekonomiskt överkomliga tvistlösningsmekanismer.

Kommissionen kommer å det snaraste att inleda en dialog med de amerikanska myndigheterna för att diskutera de konstaterade bristerna. Till sommaren 2014 bör det finnas förslag till lösningar. Dessa bör genomföras så snart som möjligt. Med utgångspunkt från detta kommer kommissionen att göra en fullständig genomgång av hur Safe Harbour-systemet fungerar. Denna bredare översyn bör inbegripa öppna samråd och debatter i Europaparlamentet och rådet samt diskussioner med de amerikanska myndigheterna.

Det är också viktigt att möjligheten till undantag med hänvisning till den nationella säkerheten som föreskrivs i Safe Harbour-beslutet endast används i den omfattning som är absolut nödvändig och proportionerlig.

3.3 Stärkt dataskydd i det brottsbekämpande samarbetet

EU och Förenta staterna förhandlar för närvarande om ett ”paraplyavtal” om överföring och behandling av personuppgifter inom ramen för polissamarbete och straffrättsligt samarbete. Ingåendet av ett avtal som ger ett gott skydd för personuppgifter skulle vara ett viktigt bidrag för att stärka förtroendet över Atlanten. Ett bättre skydd för EU-medborgarnas rättigheter skulle bidra till att stärka den del av det transatlantiska samarbetet som syftar till att förebygga och bekämpa brottslighet och terrorism.

Enligt beslutet om att bemyndiga kommissionen att förhandla om paraplyavtalet bör syftet med förhandlingarna vara att garantera en hög skydds nivå i linje med EU:s regelverk på området för skydd av personuppgifter. Detta bör återspeglas i överenskomna regler och garantier när det gäller bland annat ändamålsbegränsning samt villkor och lagringstid vid lagring av personuppgifter. I samband med förhandlingarna bör kommissionen också utverka åtaganden när det gäller lagstadgade rättigheter, däribland införande av möjligheter till rättslig prövning för EU-medborgare som inte är bosatta i Förenta staterna²⁴. Ett nära samarbete mellan EU och Förenta staterna för att åtgärda gemensamma säkerhetsproblem bör

²⁴ Se relevant avsnitt i det gemensamma pressmeddelande som utfärdades efter mötet mellan EU:s och Förenta staternas justitie- och inrikesministrar den 18 november 2013 i Washington: ”Vi är därför, som en fråga av högsta prioritet, fast beslutna att avancera snabbt i förhandlingarna om ett ändamålsenligt och övergripande paraplyavtal om skydd av personuppgifter på brottsbekämpningens område. Avtalet skulle fungera som grund för att underlätta överföring av uppgifter i samband med polissamarbete och straffrättsligt samarbete genom att säkerställa en hög nivå av skydd för amerikanska medborgares och EU-medborgares personuppgifter. Vi är inriktade på att fortsätta arbetet för att lösa återstående frågor som har tagits upp av båda parter, inklusive frågan i möjlighet till rättslig prövning (som är av avgörande betydelse för EU). Vårt mål är att slutföra förhandlingarna om avtalet före sommaren 2014.”

kombineras med insatser för att se till att medborgare omfattas av samma rättigheter när samma personuppgifter behandlas för samma ändamål, oavsett på vilken sida av Atlanten det sker. Det är också viktigt att undantag baserade på nationella säkerhetsöverväganden är snävt definierade. För detta ändamål är det viktigt att säkerställa säkerhetsmekanismer och begränsningar.

Dessa förhandlingar ger tillfälle att klargöra att personuppgifter som innehas av privata företag i EU inte ska vara åtkomliga för eller kunna överföras till amerikanska brottsbekämpande organ utanför de formella samarbetskanalerna, såsom avtal om ömsesidig rättslig hjälp eller sektorsavtal mellan EU och Förenta staterna. All annan åtkomst bör vara utesluten, såvida det inte är fråga om definierade undantagssituationer där det finns möjlighet till rättslig prövning. Förenta staterna bör göra de åtaganden som krävs i detta hänseende²⁵.

Ett ”paraplyavtal” som ingåtts på dessa premisser bör ge den allmänna ram som krävs för att garantera en hög skyddsnivå för personuppgifter som överförs till Förenta staterna i syfte att förebygga eller bekämpa brottslighet och terrorism. Sektorsavtal bör, när det är nödvändigt på grund av dataöverföringens natur, innehålla ytterligare regler och skyddsåtgärder. Utgångspunkten vara PNR- och TFTP-avtalen mellan EU och Förenta staterna, som fastställer stränga villkor för överföring av personuppgifter och särskilda skyddsåtgärder för EU-medborgare.

3.4 Europeiska farhågor när det gäller den pågående reformprocessen i Förenta staterna

Förenta staternas president Barack Obama har aviserat en översyn av den verksamhet som bedrivs av Förenta staternas nationella säkerhetsmyndigheter, också av den tillämpliga rättsliga ramen. Denna pågående process ger ett utmärkt tillfälle att ta upp den oro som de nya avslöjandena om Förenta staternas program för insamling av underrättelseinformation har väckt i EU. De viktigaste förändringarna skulle vara att utsträcka de skyddsåtgärder som finns tillgängliga för amerikanska medborgare och EU-medborgare bosatta i Förenta staterna till EU-medborgare som inte är bosatta i Förenta staterna, skapa ökad insyn i underrättelseverksamhet och ytterligare stärka kontrollen. Sådana förändringar skulle bidra till att återställa förtroendet för datautbyten mellan EU och Förenta staterna och främja européernas användning av internetjänster.

Inför en utvidgning av det skydd som gäller för amerikanska medborgare och EU-medborgare som är bosatta i Förenta staterna till EU-medborgare som inte är bosatta i Förenta staterna, är det viktigt att se över de rättsregler om de amerikanska övervakningsprogrammen som innebär att amerikanska medborgare och EU-medborgare behandlas olika, också ur ett nödvändighets- och proportionalitetsperspektiv, med hänsyn till det nära transatlantiska säkerhetspartnerskapet som grundar sig på gemensamma värderingar, rättigheter och friheter. Detta skulle innebära att européerna inte drabbas på samma sätt av amerikanska program för insamling av underrättelseinformation.

Det behövs bättre insyn beträffande den rättsliga ramen för de amerikanska programmen för insamling av underrättelseinformation och hur denna ram tolkas av de amerikanska

²⁵

Se relevant avsnitt i det gemensamma pressmeddelande som utfärdades efter mötet mellan EU:s och Förenta staternas justitie- och inrikesministrar den 18 november 2013 i Washington: ”Vi vill också understryka betydelse av avtalet om ömsesidig rättslig hjälp mellan EU och Förenta staterna. Vi upprepar vårt åtagande att se till att det används på ett brett och effektivt sätt för bevisupptagningsändamål i straffrättsliga förfaranden. Det har också förekommit diskussioner om behovet av att klargöra att personuppgifter som innehas av privata enheter på en annan parts territorium inte bör vara tillgängliga för brottsbekämpande myndigheter utanför de lagstadgade kanalerna. Vi är också eniga om att se över hur avtalet om ömsesidig rättslig hjälp fungerar, såsom var tänkt i avtalet, och att samråda med varandra vid behov.”

domstolarna, men även beträffande den kvantitativa dimensionen av programmen. Även EU-medborgarna skulle ha nytta av sådana förändringar.

Tillsynen över de amerikanska programmen för insamling av underrättelseinformation skulle förbättras genom en förstärkt roll för domstolen för övervakning av utländsk underrättelseinformation och införande av möjligheter till rättslig prövning för enskilda. Dessa mekanismer skulle minska behandlingen av personuppgifter som saknar betydelse för den nationella säkerheten.

3.5 Främjande av höga standarder när det gäller skydd av personuppgifter

Frågor rörande moderna metoder för uppgiftsskydd är inte begränsade till dataöverföring mellan EU och Förenta staterna. Var och en har rätt till ett bra skydd för sina personuppgifter. EU:s regler om insamling, behandling och överföring av uppgifter bör främjas internationellt. Nyligen har en rad initiativ lagts fram för att främja skyddet av privatlivet, särskilt på internet²⁶. EU bör se till att sådana initiativ, om de genomförs, tar full hänsyn till de principer rörande skydd av de grundläggande rättigheterna, yttrandefriheten, personuppgifter och privatlivet som fastställs i EU-lagstiftningen och i EU:s som anges i EU:s lagstiftning och i EU:s strategi för it-säkerhet, och inte undergräver friheten, öppenheten och säkerheten i cyberrymden. Detta inbegriper en demokratisk och effektiv styrningsmodell med många inblandade parter.

De pågående reformerna av lagstiftningen om uppgiftsskydd på båda sidorna av Atlanten ger också EU och Förenta staterna en unik möjlighet att etablera standarden internationellt. Datautbyten över Atlanten och längre bort skulle gynnas kraftigt om man stärkte Förenta staternas inhemska rättsliga ram och kunde få igenom den konsumentlagstiftning (Consumer Privacy Bill of Rights) som president Barack Obama aviserade i februari 2012, som en del av en större plan för att förbättra skyddet av konsumenters privatliv. En uppsättning starka och verkställbara bestämmelser om dataskydd i både EU och Förenta staterna skulle utgöra en solid grund för dataflöden över gränserna.

För att främja normer om skydd av privatlivet på ett internationellt plan är det viktigt att främja anslutning till Europarådets konvention om skydd av individer med avseende på automatisk behandling av personuppgifter ("konvention 108"), som är öppen för länder som inte är medlemmar i Europarådet²⁷. Skyddsåtgärder och garantier som avtalats i internationella forum bör leda till en högra skyddsnivå i linje med vad EU-lagstiftningen kräver.

4. SLUTSATSER OCH REKOMMENDATIONER

De frågor som behandlas i detta meddelande kräver att åtgärder av såväl Förenta staterna och som av EU och dess medlemsstater.

Oron kring det transatlantiska datautbytet är i första hand en väckarklocka som signalerar att EU och dess medlemsstater måste vidta snabba och ambitiösa åtgärder för att driva igenom uppgiftsskyddsreformen. Den visar att det mer än någonsin behövs en stark rättslig ram med tydliga regler som tillämpas även vid överföring av uppgifter till utlandet. EU-institutionerna bör därför fortsätta arbetet för att anta EU:s uppgiftsskyddsreform till våren 2014, och därigenom se till att personuppgifter omfattas av ett effektivt och övergripande skydd.

Med tanke på att dataflödena över Atlanten är av så stor betydelse är det viktigt att de instrument på vilka detta utbyte vilar är utformade på ett sådant sätt att det blir möjligt att möta utmaningarna och tillvarata möjligheterna i den digitala tidsåldern, inklusive ny teknik

²⁶ Se det utkast till resolution som Tyskland och Brasilien lagt fram för FN:s generalförsamling om skydd av privatlivet såväl på som utanför internet. Förenta staterna är redan medlem i en annan av Europarådets konventioner, nämligen 2001 års konvention om it-relaterad brottslighet (även kallad *Budapestkonventionen*).

som datormoln. Befintliga och framtida bestämmelser och avtal bör garantera en kontinuerligt hög skyddsnivå när det gäller dataflöden över Atlanten.

Medborgare och företag i EU och Förenta staterna har intresse av ett väl fungerande Safe Harbour-system. Systemet bör stärkas genom bättre övervakning och genomförande på kort sikt och, med detta som utgångspunkt, en bredare översyn av dess funktion. Förbättringar är nödvändiga för att säkerställa att de ursprungliga målen med Safe Harbour-beslutet dvs. kontinuerligt uppgiftsskydd, rättssäkerhet och fria dataflöden mellan EU och Förenta staterna, kan uppfyllas även i fortsättningen.

Förbättringarna bör vara inriktade på behovet av att skapa förutsättningar för de amerikanska myndigheterna att bättre kunna övervaka och kontrollera om och hur självcertifierade företag följer Safe Harbour-principerna om integritetsskydd.

Det är också viktigt att möjligheten till undantag med hänvisning till den nationella säkerheten som föreskrivs i Safe Harbour-beslutet endast används i den omfattning som är absolut nödvändig och proportionerlig.

Inom brottsbekämpningens område bör de pågående förhandlingarna om ett paraplyavtal leda till en hög skyddsnivå för medborgare på båda sidor av Atlanten. Ett sådant avtal skulle stärka européernas förtroende för datautbytena mellan EU och Förenta staterna och utgöra en grund för vidareutveckling av samarbete och partnerskap på säkerhetsområdet. I samband med förhandlingarna är det viktigt att utverka åtaganden om att även européer som inte är bosatta i Förenta staterna ska ha tillgång till rättssäkerhetsgarantier, inklusive möjligheter till rättslig prövning.

Den amerikanska förvaltningen bör lämna åtaganden som säkerställer att amerikanska brottsbekämpande myndigheter inte har tillgång till personuppgifter som innehas av privata aktörer i EU utanför de formella samarbetskanalerna, såsom avtal om ömsesidig rättslig hjälp och sektorsavtal mellan EU och Förenta staterna, t.ex. PNR- och TFTP-avtalen, som under väl avgränsade förutsättningar tillåter sådana överföringar, såvida det inte är fråga om klart definierade undantagssituationer där det finns möjlighet till rättslig prövning.

Förenta staterna bör också utsträcka de skyddsåtgärder som finns tillgängliga för amerikanska medborgare och EU-medborgare bosatta i Förenta staterna till EU-medborgare som inte är bosatta i Förenta staterna, se till att programmen motsvarar kraven på nödvändighet och proportionalitet och säkerställa ökad öppenhet och insyn i den rättsliga ram som tillämpas av Förenta staternas säkerhetsmyndigheter.

De frågor som tas upp i detta meddelande kommer att kräva ett konstruktivt engagemang från båda sidor av Atlanten. Som strategiska partner har EU och Förenta staterna tillsammans förmåga att lösa de rådande spänningarna i de transatlantiska förbindelserna och återskapa förtroendet för dataflödena mellan EU och Förenta staterna. Gemensamma politiska och rättsliga åtaganden om närmare samarbete på dessa områden kommer att bidra till att stärka de transatlantiska förbindelserna överlag.