II

(Icke-lagstiftningsakter)

BESLUT

KOMMISSIONENS GENOMFÖRANDEBESLUT (EU) 2016/1250

av den 12 juli 2016

enligt Europaparlamentets och rådets direktiv 95/46/EG om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna

[delgivet med nr C(2016) 4176]

(Text av betydelse för EES)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av 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 ([1]), särskilt artikel 25.6,

efter samråd med Europeiska datatillsynsmannen ([2]), och

av följande skäl:

1. INLEDNING

(1) I direktiv 95/46/EG fastställs regler för överföringar av personuppgifter från medlemsstaterna till tredjeländer i den utsträckning sådana överföringar omfattas av direktivets tillämpningsområde.

(2) Syftet med artikel 1 och skälen 2 och 10 i ingressen i direktiv 95/46/EG är inte endast att säkerställa ett effektivt och fullständigt skydd för fysiska personers grundläggande fri- och rättigheter, särskilt den grundläggande rätten till respekt för privatlivet, i samband med behandling av personuppgifter, utan även att säkerställa en hög skyddsnivå när det gäller dessa grundläggande fri- och rättigheter ([3]).

(3) Betydelsen av både den grundläggande rätten till respekt för privatlivet, som garanteras av artikel 7 i Europeiska unionens stadga om de grundläggande rättigheterna, och den grundläggande rätten till skydd av personuppgifter, som garanteras av artikel 8 i stadgan, betonas i EU-domstolens rättspraxis ([4]).

(4) Enligt direktiv artikel 25.1 i direktiv 95/46/EG ska medlemsstaterna föreskriva att överföring av personuppgifter till tredje land endast får ske om ifrågavarande tredje land säkerställer en adekvat skyddsnivå och om medlemsstatens lagar genom vilka andra bestämmelser i direktivet genomförs, efterlevs före överföringen. Kommissionen kan konstatera att ett tredje land har en adekvat skyddsnivå genom sin interna lagstiftning eller på grund av de internationella förpliktelser som landet har ingått för att skydda enskilda personers rättigheter. I sådana fall, och utan att de påverkar efterlevnaden av de nationella bestämmelser som antagits enligt andra bestämmelser i direktivet, får personuppgifter överföras från medlemsstaterna utan att det behövs några ytterligare garantier.

([1]) EGT L 281, 23.11.1995, s. 31.
([2]) Se yttrande 4/2016 om skölden för skydd av privatlivet i EU och Förenta staterna, utkast till beslut om adekvat skyddsnivå, offentliggjort den 30 maj 2016.
([3]) Mål C-362/14, Maximillian Schrems mot Data Protection Commissioner (nedan kallat *Schrems-målet*) EU:C:2015:650, punkt 39.
([4]) Mål C-553/07, *Rijkeboer*, EU:C:2009:293, punkt 47; förenade målen C-293/12 och C-594/12, *Digital Rights Ireland and Others*, EU:C:2014:238, punkt 53; mål C-131/12, *Google Spain and Google*, EU:C:2014:317, punkterna 53, 66 och 74.

(5) Enligt artikel 25.2 i direktiv 95/46/EG ska bedömningen av skyddsnivån ske på grundval av alla de förhållanden som har samband med en överföring eller en grupp överföringar av uppgifter, inbegripet de allmänna respektive särskilda rättsregler som gäller i ifrågavarande tredje land.

(6) I kommissionens beslut 2000/520/EG ([5]) med avseende på artikel 25.2 i direktiv 95/46/EG, ansågs de principer om integritetsskydd (*Safe Harbor Privacy Principles*) tillämpade i enlighet med den vägledning som ges i de frågor och svar (nedan kallade *FoS*) som utfärdats av Förenta staternas handelsministerium utgöra en adekvat skyddsnivå för personuppgifter som överförs från unionen till organisationer som är etablerade i Förenta staterna.

(7) I sina meddelanden COM(2013) 846 final ([6]) och COM(2013) 847 final av den 27 november 2013 ([7]) ansåg kommissionen att grundprinciperna för safe harbor-systemet måste ses över och stärkas mot bakgrund av en rad faktorer, bland annat den exponentiella ökningen av dataflödena och dataflödenas avgörande betydelse för den transatlantiska ekonomin, den snabba ökningen av antalet företag i Förenta Staterna som är anslutna till safe harbor-systemet och ny information om omfattningen och räckvidden av vissa av Förenta staternas övervakningsprogram, som gav upphov till frågor om den skyddsnivå som det kunde garantera. Dessutom fann kommissionen ett antal brister i safe harbor-systemet.

(8) På grundval av belägg som samlats in av kommissionen, bland annat information från arbetet i EU–Förenta staterna-kontaktgruppen för integritetsskydd ([8]) och den information om Förenta staternas underrättelseprogram som mottagits inom ramen för ad hoc-arbetsgruppen för dataskydd mellan EU och Förenta staterna ([9]), utformade kommissionen 13 rekommendationer för en översyn av safe harbor-systemet. Rekommendationerna inriktades på att stärka de väsentliga sekretessprinciperna, öka insynen i de självcertifierade företagens integritetsskyddsregler i Förenta staterna, förbättra myndigheternas övervakning i Förenta staterna, tillsyn och verkställighet av efterlevnaden av dessa principer, se till att ekonomiskt överkomliga tvistlösningsmekanismer finns tillgängliga och säkerställa att undantaget med hänvisning till den nationella säkerheten och brottsbekämpningen i beslut 2000/520/EG tillämpas enbart då det är absolut nödvändigt och proportionerligt.

(9) I sin dom av den 6 oktober 2015 i mål C-362/14, Maximillian Schrems mot Data Protection Commissioner, ogiltigförklarade EU-domstolens beslut 2000/520/EC ([10]). Utan att undersöka innehållet i principerna om integritetsskydd ansåg domstolen att kommissionen i beslutet inte hade angett att Förenta staterna de facto ”säkerställer” en adekvat skyddsnivå genom sin interna lagstiftning eller på grund av de internationella förpliktelser som åligger landet ([11]).

(10) I detta avseende förklarade domstolen att begreppet ”adekvat skyddsnivå” i artikel 25.6 i direktiv 95/46/EG inte innebär en skyddsnivå som är identisk med den som garanteras i unionens rättsordning, men att begreppet måste förstås som att det krävs att detta tredjeland säkerställer en nivå för skyddet av grundläggande fri- och rättigheter som är väsentligen likvärdig med den skyddsnivå som garanteras inom unionen enligt direktiv 95/46/EG jämfört med stadgan om de grundläggande rättigheterna. Även om de medel som detta tredjeland använder kan skilja sig från dem som används inom unionen, måste dessa medel dock visa sig i praktiken kunna säkerställa ett skydd som är väsentligen likvärdigt ([12]).

(11) EU-domstolen kritiserade att det saknades tillräckliga konstateranden i beslut 2000/520/EG beträffande förekomsten i Förenta staterna av regler som antagits av staten och som syftar till att begränsa eventuella ingrepp i de grundläggande rättigheterna för personer vilkas personuppgifter överförs från unionen till Förenta staterna, ingrepp som statliga organ kan vara tillåtna att göra när de görs i ett legitimt syfte, såsom nationell säkerhet, och att det finns något effektivt rättsligt skydd mot denna typ av ingrepp ([13]).

([5]) 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, 28.8.2000, s. 7).

([6]) Meddelande från kommissionen till Europaparlamentet och rådet – Återskapande av förtroendet för dataflöden mellan EU och Förenta staterna (COM(2013) 846 final, 27.11.2013).

([7]) Meddelande från kommissionen till Europaparlamentet och rådet om hur principerna om integritetsskydd (safe harbour) fungerar när det gäller EU:s medborgare och företag som är etablerade i EU (COM(2013) 847 final, 27.11.2013).

([8]) Se t.ex. Europeiska unionens råd, slutrapporten från EU–Förenta staterna-kontaktgruppen på hög nivå för informationsutbyte, integritetsskydd och skydd av personuppgifter, not 9831/08, 28 maj 2008, tillgänglig på internet på http://www.europarl.europa.eu/document/activities/cont/201010/20101019ATT88359/20101019ATT88359EN.pdf

([9]) Rapport om slutsatserna från EU-ordförandena i ad hoc-arbetsgruppen för dataskydd mellan EU och Förenta staterna, 27.11.2013, tillgänglig på internet på http://ec.europa.eu/justice/data-protection/files/report-findings-of-the-ad-hoc-eu-us-working-group-on-data-protection.pdf

([10]) Se fotnot 3.

([11]) *Schrems*-målet, punkt 97.

([12]) Schrems-målet, punkterna 73–74.

([13]) Schrems-målet, punkterna 88–89.

(12) Under 2014 inledde kommissionen förhandlingar med Förenta staternas myndigheter för att diskutera hur safe harbor-systemet kunde stärkas enligt de 13 rekommendationerna i meddelandet COM(2013) 847 final. Dessa förhandlingar intensifierades efter EU-domstolens dom i Schrems-målet med sikte på ett eventuellt nytt beslut om adekvat skyddsnivå som uppfyller kraven i artikel 25 i direktiv 95/46/EG enligt domstolens tolkning. De dokument som bifogas detta beslut och som även kommer att offentliggöras i Förenta staternas federala register är resultatet av dessa diskussioner. Principerna (bilaga II), tillsammans med de officiella utfästelserna och åtagandena från flera myndigheter Förenta staterna i dokumenten i bilagorna I och III–VII, utgör ”skölden för skydd av privatlivet i EU och Förenta staterna”.

(13) Kommissionen har noggrant analyserat Förenta staternas lagstiftning och praxis, inbegripet dessa officiella utfästelser och åtaganden. På grundval av de konstateranden som görs i skälen 136–140 drar kommissionen slutsatsen att Förenta staterna säkerställer en adekvat skyddsnivå för skydd av personuppgifter som överförs enligt skölden för skydd av privatlivet i EU och Förenta staterna från unionen till självcertifierade organisationer i Förenta staterna.

2. SKÖLDEN FÖR SKYDD AV PRIVATLIVET I EU OCH FÖRENTA STATERNA

(14) Skölden för skydd av privatlivet i EU och Förenta staterna bygger på ett system för självcertifiering genom vilket organisationer i Förenta staterna förbinder sig att följa en uppsättning principer om integritetsskydd – principerna om integritetsskydd för skölden för skydd av privatlivet i EU och UA, inklusive kompletterande principer (nedan tillsammans kallade *principerna*) – som utfärdats av Förenta staternas handelsministerium och ingår i bilaga II till detta beslut. Den gäller för både registeransvariga och registerförare (förmedlare), med det särskilda villkoret att registerförare måste vara bundna av ett avtal att agera endast enligt instruktioner från den EU-registeransvariga och att hjälpa den sistnämnda att tillmötesgå enskilda som utövar sina rättigheter enligt principerna ([14]).

(15) Utan att det påverkar de nationella bestämmelser som antagits i enlighet med direktiv 95/46/EG har detta beslut effekten att överföringar från en registeransvarig eller registerförare i unionen till organisationer i Förenta staterna som har självcertifierat sin anslutning till principerna hos handelsministeriet och har åtagit sig att följa dem tillåts. Principerna gäller endast för behandlingen av personuppgifter som utförs av organisationen i Förenta staterna i den mån som behandling som utförs av sådana organisationer inte omfattas av tillämpningsområdet för unionslagstiftning ([15]). Skölden för skydd av privatlivet påverkar inte tillämpningen av unionslagstiftning som reglerar behandlingen av personuppgifter i medlemsstaterna ([16]).

([14]) Se bilaga II, avsnitt III.10.a. I linje med definitionen i avsnitt I.8.c kommer den EU-registeransvariga att bestämma ändamålet och medlen för behandlingen av personuppgifterna. Dessutom måste avtalet med förmedlaren klargöra huruvida vidare överföringar är tillåtna (se avsnitt III.10.a.ii.2.).

([15]) Detta gäller också när personaluppgifter som överförs från unionen i samband med anställningsförhållandet berörs. Även om principerna betonar det ”primära ansvaret” hos arbetsgivaren i EU (se bilaga II, avsnitt III.9.d.i.), klargör de samtidigt att dennas beteende kommer att omfattas av de regler som är tillämpliga i unionen och/eller respektive medlemsstat, inte principerna. Se bilaga II, avsnitt III.9.a.i., b.ii., c.i., d.i.

([16]) Detta gäller också för behandling som äger rum genom användning av utrustning som befinner sig i unionen men som används av en organisation som är etablerad utanför unionen (se artikel 4.1 c i direktiv 95/46/EG). Från och med den 25 maj 2018 kommer den allmänna dataskyddsförordningen att gälla för behandlingen av personuppgifter i) inom ramen för arbetet på registeransvarigas eller registerförares verksamhetsställen i unionen (även om behandlingen äger rum i Förenta staterna), eller ii) om registrerade personer som befinner sig i unionen vilken utförs av en registeransvarig eller registerförare som inte är etablerad inom unionen om behandlingen avser a) utbjudande av varor eller tjänster, oberoende av om det krävs en betalning av den registrerade eller inte, till sådana registrerade personer i unionen, eller b) övervakning av deras beteende så länge beteendet sker inom unionen. Se artikel 3.2 och 3.2 i 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 (allmän dataskyddsförordning) (EUT L 119, 4.5.2016, s. 1).

(16) Det skydd för personuppgifter som skölden för skydd av privatlivet ger gäller för alla registrerade i EU ([17]) vars personuppgifter har överförts från unionen till organisationer i Förenta staterna som har självcertifierat sin anslutning till principerna hos handelsministeriet.

(17) Principerna blir omedelbart tillämpliga vid certifiering. Ett undantag rör principen om ansvar för vidare överföring i fall där en organisation som självcertifierar sin anslutning till skölden för privatlivet redan har has preexisterande kommersiella förbindelser med tredjeparter. Med tanke på att det kan ta tid att bringa dessa kommersiella förbindelser i överensstämmelse med de regler som är tillämpliga enligt principen om ansvar för vidare överföring, kommer organisationen att bli tvungen att göra detta så snart som möjligt, och i alla händelser senast nio månader efter självcertifiering (förutsatt att detta äger rum under de första två månaderna efter den dag då skölden för privatlivet träder i kraft). Under denna mellanliggande period ska organisationen tillämpa principerna om meddelande och valmöjlighet (och sålunda ge den registrerade i EU möjlighet inte omfattas) och, om personuppgifter överförs till en tredje part som agerar som förmedlare, säkerställa att den sistnämnda tillhandahåller åtminstone samma skyddsnivå som den som krävs enligt principerna ([18]). Denna övergångsperiod ger en rimlig och lämplig balans mellan respekten för den grundläggande rätten till dataskydd och de legitima behoven hos företag att ha tillräckligt med tid till förfogande för att anpassa sig till den nya ramen där detta också är beroende av deras kommersiella förbindelser med tredjeparter.

(18) Systemet kommer att förvaltas och övervakas av handelsministeriet på grundval av dess åtaganden som anges i utfästelserna från Förenta staternas handelsminister (bilaga I till detta beslut). När det gäller verkställandet av principerna har den federala konkurrensmyndigheten (Federal Trade Commission, FTC) och transportministeriet gjort utfästelser som ingår i bilagorna IV och V till detta beslut.

2.1 *Principerna*

(19) Som en del av sin självcertifiering enligt skölden för skydd av privatlivet i EU och Förenta staterna måste organisationer förbinda sig att följa principerna ([19]).

(20) Enligt *principen om meddelande* är organisationerna skyldiga att lämna information till registrerade om en rad viktiga aspekter i behandlingen av deras personuppgifter (t.ex. typ av insamlade uppgifter, ändamålet med behandlingen, rätt till åtkomst och valmöjlighet, villkor för vidare överföring samt ansvarsskyldighet). Ytterligare garantier gäller, särskilt kravet att organisationerna ska offentliggöra sina integritetsskyddspolicyer (som ska avspegla principerna) och ange länkar till handelsministeriets webbplats (med närmare upplysningar om självcertifiering, registrerades rättigheter samt tillgängliga instanser för handläggning av klagomål), den förteckning över organisationer som anslutit sig till skölden (som avses i skäl 30) samt en adress till ett lämpligt alternativt tvistlösningsorgans webbplats.

(21) Enligt *principen om dataintegritet och ändamålsbegränsning* måste personuppgifter begränsas till de uppgifter som är relevanta för ändamålet med behandlingen, vara tillförlitliga för det avsedda ändamålet samt riktiga, fullständiga och aktuella. En organisation får inte behandla personuppgifter på ett sätt som är oförenligt med det ändamål för vilket de ursprungligen samlades in om inte den registrerade i efterhand har gett sitt tillstånd. Organisationer måste säkerställa att personuppgifter är tillförlitliga för det avsedda ändamålet samt riktiga, fullständiga och aktuella.

([17]) Detta beslut är av betydelse för EES. Enligt avtalet om Europeiska ekonomiska samarbetsområdet (EES-avtalet) utvidgas EU:s inre marknad till de tre EES-staterna Island, Liechtenstein och Norge. Unionens dataskyddslagstiftning, inbegripet direktiv 95/46/EG, omfattas av EES-avtalet och har införlivats i bilaga XI till detta. Gemensamma EES-kommittén måste besluta om införlivandet av detta beslut i EES-avtalet. När detta beslut gäller för Island, Liechtenstein och Norge kommer skölden för privatlivet i EU och Förenta staterna också att omfatta dessa tre länder, och hänvisningar i paketet om skölden för privatlivet till EU och dess medlemsstater ska tolkas som att detta inbegriper Island, Liechtenstein och Norge.

([18]) Se bilaga II, avsnitt III.6.e.

([19]) Särskilda regler med ytterligare garantier gäller för personaluppgifter som samlas in inom ramen för anställningsförhållanden enligt den kompletterande principen om ”personaluppgifter”, som ingår i principerna (se bilaga II. avsnitt III.9). Arbetsgivare bör t.ex. göra rimliga ansträngningar för att tillmötesgå den anställdes önskemål om integritetsskydd genom att man begränsar tillgången till personuppgifterna, avidentifierar dem eller inför koder eller pseudonymer. Framför allt måste organisationerna samarbeta och följa rekommendationerna från unionens dataskyddsmyndigheter när det gäller sådana uppgifter.

(22) Om ett nytt (ändrat) ändamål i sak skiljer sig från men fortfarande är förenligt med det ursprungliga ändamålet, ger *principen om valmöjlighet* registrerade rätten att invända (opt-out). *Principen om valmöjlighet* har inte företräde framför det uttryckliga förbudet mot oförenlig behandling ([20]). För direktmarknadsföring gäller särskilda regler som gör det möjligt att ”när som helst” undantas (opt-out) från användning av personuppgifter ([21]). När det gäller känsliga uppgifter måste organisationerna normalt sett inhämta den registrerades uttryckliga samtycke (opt in).

(23) Fortfarande gäller att enligt *principen om dataintegritet och ändamålsbegränsning* får personlig information lagras i en form som identifierar en fysisk person eller gör en fysisk person identifierbar (och således i form av personuppgifter) endast så länge det tjänar de syften för vilka den ursprungligen insamlades eller tillstånd gavs i efterhand. Denna skyldighet hindrar inte organisationer som är anslutna till skölden för skydd av privatlivet från att behandla personuppgifter under längre perioder, men endast för den tid och i den omfattning sådan behandling skäligen tjänar ett av följande särskilda ändamål: arkivering i allmänhetens intresse, journalistik, litteratur och konst, vetenskaplig eller historisk forskning och statistisk analys. Längre lagring av personuppgifter för ett av dessa ändamål kommer att omfattas av garantier som tillhandahålls av principerna.

(24) Enligt *principen om säkerhet* måste organisationer som skapar, lagrar, använder eller sprider personuppgifter vidta ”rimliga och lämpliga” säkerhetsåtgärder, med beaktande av riskerna i samband med behandlingen och personuppgifternas natur. Om uppgiftsbehandlingen läggs ut på entreprenad måste organisationerna ingå ett avtal med underentreprenören som garanterar samma skyddsnivå som principerna, och vidta åtgärder för att säkerställa att avtalet genomförs korrekt.

(25) Enligt *principen om tillgång* ([22]) har registrerade rätt, utan motivering och mot endast en skälig avgift, att få bekräftelse från en organisation om huruvida organisationen behandlar personuppgifter som rör dem samt meddelas dessa personuppgifter inom skälig tid. Denna rätt kan endast begränsas i undantagsfall. Om rätten till tillgång förnekas eller begränsas måste det vara nödvändigt och vederbörligen motiverat. Det är organisationen som ska visa att dessa krav är uppfyllda. Registrerade måste kunna korrigera, ändra eller radera personuppgifter som är felaktiga eller har behandlats i strid mot principerna. Inom områden där företag med största sannolikhet kommer att använda automatiserad behandling av personuppgifter för att fatta beslut som påverkar den enskilde (t.ex. kreditgivning, erbjudanden om hypotekslån, anställning), ger Förenta staternas lagstiftning särskilt skydd mot ogynnsamma beslut ([23]). Typiska inslag i sådana akter är att enskilda har rätt att informeras om de särskilda skäl som ligger till grund för beslutet (t.ex. avslag på ansökan om kredit), att protestera mot ofullständig eller oriktig information (liksom åberopande av illegitima faktorer), och att söka upprättelse. Dessa regler ger skydd i det sannolikt tämligen begränsade antalet fall där automatiserade beslut kommer att fattas av den organisation som är ansluten till skölden ([24]). Med tanke på den ökande användningen av automatiserad behandling (inbegripet profilering) som en grund för beslutsfattande som påverkar enskilda i den moderna digitala ekonomin, är detta ändå ett område som måste övervakas noga. För att underlätta denna övervakning har det överenskommits med Förenta staternas myndigheter att en dialog om automatiserat beslutsfattande, däribland ett utbyte av information om likheterna och skillnaderna mellan EU:s och Förenta staternas tillvägagångssätt i detta avseende, kommer att vara en del av den första årliga översynen samt efterföljande översyner i förekommande fall.

([20]) Detta gäller för alla uppgiftsöverföringar inom ramen för skölden för skydd av privatlivet, däribland om dessa rör uppgifter som insamlats i samband med anställningsförhållandet. En självcertifierad organisation i Förenta staterna får i princip använda personaluppgifter för olika, icke anställningsrelaterade ändamål (t.ex. viss marknadskommunikation), men den måste respektera förbudet mot oförenlig behandling och den får använda uppgifterna endast i enlighet med *principerna om meddelande och valmöjlighet*. Förbudet för organisationen i Förenta staterna att på något sätt bestraffa den anställde på grund av utnyttjandet av en sådan valmöjlighet, däribland genom att på något sätt begränsa den anställdes karriärmöjligheter, kommer att säkerställa att, trots den underordnade ställningen och beroendeförhållandet, den anställde kommer att vara fri från påtryckningar och således kan träffa ett genuint fritt val.

([21]) Se bilaga II, avsnitt III.12.

([22]) Se även den kompletterande principen om ”Tillgång” (Bilaga II, avsnitt III.8).

([23]) Se t.ex. *Equal Credit Opportunity Act* (ECOA, 15 U.S.C. 1691 et seq.), *Fair Credit Reporting Act* (FRCA, 15 USC § 1681 et seq.) eller *Fair Housing Act* (FHA, 42 U.S.C. 3601 et seq.).

([24]) I samband med överföring av personuppgifter som har insamlats i EU kommer avtalsförhållandet med den enskilde (kunden) i de flesta fall att vara med – och därför kommer alla beslut baserade på automatiserad behandling vanligen att fattas av – den EU-registeransvariga, som måste följa EU:s dataskyddsregler. Detta inbegriper scenarier där behandlingen utförs av en organisation som är ansluten till skölden och som agerar som en förmedlare för den EU-registeransvariges räkning.

(26) Enligt *principen om rättsmedel, genomförande och ansvar* ([25]) måste deltagande organisationer tillhandahålla robusta mekanismer för att säkerställa efterlevnad av de andra principerna och tillhandahålla rättsmedel för registrerade i EU vars personuppgifter har behandlats på ett sätt som strider mot bestämmelserna, inklusive effektiva medel för gottgörelse. När en organisation frivilligt har beslutat att självcertifiera ([26]) sig enligt skölden för skydd av privatlivet i EU och Förenta staterna är den skyldig att följa principerna. Organisationerna måste årligen återcertifiera sitt deltagande i skölden för att få fortsätta motta personuppgifter från unionen via skölden. Organisationerna måste också vidta åtgärder för att kontrollera ([27]) att deras offentliggjorda integritetsskyddspolicy överensstämmer med principerna och att de faktiskt följs. Detta kan antingen göras med hjälp av ett självbedömningssystem, som måste omfatta interna förfaranden för att se till att personalen utbildas i genomförandet av organisationens integritetsskyddspolicy och att efterlevnaden regelbundet granskas på ett objektivt sätt, eller genom externa efterlevnadskontroller, som kan omfatta revisioner eller slumpvisa kontroller. Dessutom måste organisationen inrätta en effektiv prövningsmekanism för att hantera eventuella klagomål (se i detta hänseende även skäl 43) samt omfattas av de utrednings- och verkställighetsbefogenheter som tilldelats transportministeriet eller ett annat behörigt lagstadgat organ i Förenta staterna som kommer att säkerställa efterlevnad av principerna.

(27) Särskilda regler gäller för så kallade ”vidare överföringar”, dvs. överföringar av personuppgifter från en organisation till en registeransvarig eller registerförare som är tredjepart, oberoende av om den sistnämnda befinner sig i Förenta staterna eller i ett tredjeland utanför Förenta staterna (och unionen). Syftet med dessa regler är att säkerställa att de skydd som garanteras för personuppgifter om registrerade i EU inte kommer att undermineras, och inte kan kringgås, genom att uppgifterna vidarebefordras till tredjeparter. Detta är särskilt relevant i mer komplexa behandlingskedjor som är typiska för dagens digitala ekonomi.

(28) Inom ramen för *principen om ansvar för vidare överföring* ([28]) kan all vidare överföring ske endast i) för begränsade och specificerade ändamål, ii) på grundval av ett avtal (eller ett jämförbart arrangemang inom en företagskoncern ([29])) och iii) om ett sådant avtal ger samma skyddsnivå som den skyddsnivå som garanteras av principerna, vilket inkluderar kravet på att tillämpningen av principerna får begränsas endast i den mån det är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, rättsefterlevnad och andra ändamål som rör allmänintresset ([30]). Detta bör jämföras med *principen om meddelande* och, när det gäller vidare överföring till en registeransvarig som är tredjepart ([31]), med *principen om valmöjlighet*, enligt vilka registrerade ska informeras (bland annat) om typen av/identiteten hos varje mottagare som är tredjepart, ändamålet med vidareöverföringen samt de valmöjligheter som erbjuds och kan motsätta sig (opt-out), eller, när det gäller känsliga uppgifter, måste ge sitt ”uttryckliga samtycke” (opt in) till vidare överföring. Mot bakgrund av *principen om dataintegritet och ändamålsbegränsning* förutsätter skyldigheten att tillhandahålla samma skyddsnivå som den skyddsnivå som garanteras av principerna att tredjeparten får behandla de personuppgifter som överförs till den endast för ändamål som inte är oförenliga med de ändamål för vilka uppgifterna ursprungligen insamlades eller tillstånd gavs i efterhand av den enskilde.

(29) Skyldigheten att tillhandahålla samma skyddsnivå som den skyddsnivå som krävs enligt principerna gäller för alla tredjeparter som är involverade i behandlingen av de uppgifter som överförs på detta sätt oberoende av var de finns (i Förenta staterna eller i ett annat tredjeland) samt när den ursprungliga tredjepartsmottagaren själv överför dessa uppgifter till en annan tredjepartsmottagare, exempelvis för behandling som utförs av underentreprenörer. I samtliga fall måste avtalet med tredjepartsmottagaren ange att den sistnämnda ska meddela organisationen som är ansluten till skölden om den fastställer att den inte längre kan fullgöra denna skyldighet. När ett sådant

([25]) Se även den kompletterande principen om ”Tvistlösning och efterlevnad” (bilaga II, avsnitt III.11).
([26]) Se även den kompletterande principen om ”Självcertifiering” (Bilaga II, avsnitt III.6).
([27]) Se även den kompletterande principen om ”Kontroll” (Bilaga II, avsnitt III.7).
([28]) Se även den kompletterande principen om ”Obligatoriska avtal om vidare överföring” (bilaga II, avsnitt III.10).
([29]) Se den kompletterande principen om ”Obligatoriska avtal om vidare överföring” (bilaga II, avsnitt III.10.b). Denna princip tillåter överföringar även på grundval av utomobligatoriska instrument (t.ex. koncerninterna efterlevanads- och kontrollprogram), men samtidigt klargör texten att dessa instrument alltid måste ”säkerställa kontinuiteten i skyddet av personuppgifter enligt principerna”. Med tanke på att den självcertifierade organisationen i Förenta staterna även i fortsättningen kommer att vara ansvarig för efterlevnaden av principerna, kommer detta dessutom att vara ett starkt incitament att använda instrument som verkligen är effektiva i praktiken.
([30]) Se bilaga II, avsnitt I.5.
([31]) Enskilda kommer inte att ha rätt att välja att inte delta (opt-out) om personuppgifterna överförs till en tredje part som agerar som en förmedlare för att utföra uppgifter på organisationens (i Förenta staterna) vägnar och enligt dennas instruktioner. Detta kräver dock ett avtal med förmedlaren, och organisationen i Förenta staterna kommer att ha ansvaret för att garantera de skydd som tillhandahålls enligt principerna genom att utöva sina instruktionsbefogenheter.

fastställande har gjorts ska tredjepartens behandling upphöra; i annat fall måste andra rimliga och lämpliga åtgärder vidtas för att rätta till situationen ([32]). Om efterlevnadsproblem uppstår vid behandling som utförs av underentreprenörer måste den organisation som agerar som personuppgiftsansvarig bevisa att den inte är ansvarig för den händelse som gett upphov till skadan. Annars blir den skadeståndsskyldig. Ytterligare skydd gäller för vidare överföring till en tredjepartsförmedlare ([33]).

2.2 *Insyn i och förvaltning av skölden för skydd av privatlivet i EU och Förenta staterna*

(30) Skölden för skydd av privatlivet i EU och Förenta staterna tillhandahåller tillsyns- och verkställighetsmekanismer i syfte att kontrollera och säkerställa att självcertifierade företag i Förenta staterna följer principerna och att varje underlåtenhet att följa principerna tas upp till behandling. Dessa mekanismer fastställs i principerna (bilaga II) och de åtaganden som gjorts av handelsministeriet (bilaga I), FTC (bilaga IV) och transportministeriet (bilaga V).

(31) För att säkerställa korrekt tillämpning av skölden för privatlivet i EU och Förenta staterna måste berörda parter, t. ex. registrerade, exportörer av uppgifter och de nationella dataskyddsmyndigheterna, kunna identifiera de organisationer som har anslutit sig till principerna. I detta syfte har handelsministeriet förbundit sig att föra och göra tillgänglig för allmänheten en förteckning över de organisationer som har självcertifierat sin anslutning till principerna och som lyder under åtminstone en av de brottsbekämpande myndigheter som avses i bilagorna I och II till detta beslut (nedan kallad *förteckningen över organisationer som anslutit sig till skölden*) ([34]). Handelsministeriet kommer uppdatera förteckningen på grundval av de årliga återcertifieringarna och närhelst en organisation drar sig tillbaka eller stryks från skölden. Ministeriet kommer dessutom att upprätthålla och offentliggöra en officiell förteckning över organisationer som har strukits från förteckningen, och ange skälen till att organisationen har strukits. Det kommer också att ange en länk till förteckningen över FTC-ärenden som är relaterade till skölden för skydd av privatlivet som finns på FTC:s webbplats.

(32) Handelsministeriet kommer att göra både förteckningen över organisationer som anslutit sig till skölden och återcertifieringarna allmänt tillgängliga via en särskild webbplats. Självcertifierade organisationer måste i sin tur ange ministeriets webbplats för förteckningen över organisationer som anslutit sig till skölden. Om organisationens integritetsskyddspolicy finns tillgänglig online ska den dessutom innehålla en hyperlänk till webbplatsen för skölden för skydd av privatlivet och en hyperlänk till ett klagomålsformulär som den oberoende instansen för handläggning av klagomål har gjort tillgängligt för att utreda olösta klagomål. För det tredje kommer handelsministeriet, inom ramen för organisationernas certifiering och återcertifiering om anslutning till skölden, att systematiskt kontrollera att deras integritetspolicyer överensstämmer med principerna.

(33) Organisationer som upprepade gånger har överträtt principerna kommer att strykas från förteckningen över organisationer som anslutit sig till skölden, och organisationerna måste återlämna eller radera de personuppgifter som de har mottagit inom ramen för skölden för privatlivet i EU och Förenta staterna. I andra fall av strykningar får organisationen behålla sådana uppgifter om den årligen till handelsministeriet bekräftar sitt åtagande att fortsätta att tillämpa principerna eller tillhandahåller en adekvat skyddsnivå för personuppgifterna genom andra tillåtna medel (t.ex. genom ett avtal som fullständigt avspeglar kraven i de relevanta standardavtalsbestämmelser som antagits av kommissionen). I sådana fall måste organisationen ange en kontaktpunkt inom organisationen för alla frågor som rör skölden.

(34) Handelsministeriet kommer att övervaka organisationer som inte längre deltar i skölden för skydd av privatlivet i EU och Förenta staterna, antingen för att de frivilligt har dragit sig tillbaka eller för att deras certifiering har löpt ut, för att undersöka om organisationerna planerar att återlämna, radera eller behålla ([35]) de personuppgifter som

([32]) Situationerna är olika beroende på om tredjeparten är en registeransvarig eller en registerförare (förmedlare). I det första scenariot måste avtalet med tredjeparten föreskriva att den sistnämnda ska upphöra med behandlingen eller vidta andra rimliga och lämpliga åtgärder för att rätta till situationen. I det andra scenariot är det organisationen som är ansluten till skölden – såsom den som kontrollerar behandlingen och i enlighet med vars instruktioner agenten verkar – att vidta dessa åtgärder.

([33]) I sådana all måste organisationen i Förenta staterna också vidta rimliga och lämpliga åtgärder i) för att säkerställa att förmedlaren på ett effektivt sätt behandlar de personuppgifter som överförs på ett sätt som är förenligt med organisationens skyldigheter enligt principerna för integritetsskydd och ii) för att stoppa och åtgärda otillåten behandling, till följd av ett meddelande.

([34]) Information om förvaltningen av förteckningen över organisationer som anslutit sig till skölden återfinns i bilaga I och bilaga II (avsnitt I.3, avsnitt I.4, III.6.d, och avsnitt III.11.g).

([35]) Se t.ex. bilaga II, avsnitt I.3, avsnitt III.6.f. och avsnitt III.11.g.i.

de tidigare mottagit inom ramen för skölden. Om de behåller dessa uppgifter är organisationerna skyldiga att fortsätta att tillämpa principerna på dem. Om handelsministeriet stryker organisationer från skölden på grund av att de upprepade gånger har överträtt principerna kommer ministeriet att se till att dessa organisationer återlämnar eller raderar de personuppgifter som de har mottagit inom ramen för skölden.

(35) En organisation som av någon anledning lämnar skölden för skydd av privatlivet i EU och Förenta staterna måste avlägsna alla offentliga förklaringar som antyder att organisationen fortsätter att delta i skölden eller omfattas av dess förmåner, särskilt eventuella hänvisningar till skölden i sin offentliggjorda integritetsskyddspolicy. Handelsministeriet kommer att söka efter och ta itu med falska påståenden om deltagande i skölden, inbegripet påståenden från tidigare medlemmar ([36]). All missvisande information från en organisation till allmänheten om organisationens anslutning till principerna i form av vilseledande uttalanden eller metoder är föremål för verkställighetsåtgärder av FTC, transportministeriet eller andra relevanta brottsbekämpande myndigheter i Förenta staterna; oriktiga utfästelser till handelsministeriet kan leda till åtal i enlighet med Förenta staternas lag om osann utsaga (*False Statements Act*, 18 U.S.C. § 1001) ([37]).

(36) Handelsministeriet kommer på eget initiativ att övervaka alla falska påståenden om deltagande i skölden för skydd av privatlivet eller otillbörlig användning av sköldens certifieringsmärkning. Dataskyddsmyndigheter kan uppmana ministeriet att granska organisationer via ministeriets särskilda kontaktpunkt. Om en organisation drar sig tillbaka från deltagande i skölden för skydd av privatlivet i EU och Förenta staterna eller inte återcertifierar sin anslutning till principerna eller stryks från förteckningen över organisationer som har anslutit sig till skölden, kommer handelsministeriet att fortlöpande kontrollera att organisationen har avlägsnat eventuella hänvisningar till skölden i sin integritetsskyddspolicy som antyder ett fortsatt deltagande i skölden. Om organisationen fortsätter att göra falska påståenden kommer ministeriet att hänskjuta ärendet till FTC, transportministeriet eller en annan behörig myndighet för eventuella verkställighetsåtgärder. Ministeriet kommer också att skicka frågeformulär till organisationer vars självcertifiering har löpt ut eller organisationer som frivilligt har dragit sig tillbaka från skölden för skydd av privatlivet, för att ta reda på om organisationen kommer att återlämna, radera eller fortsätta att tillämpa principerna på de personuppgifter som de mottog medan de deltog i skölden och, om personuppgifter kommer att behållas, bekräfta vem inom organisationen som fungerar som fast kontaktpunkt för frågor rörande skölden.

(37) Handelsministeriet kommer fortlöpande att utföra efterlevnadskontroller ([38]) på eget initiativ av självcertifierade organisationer, bland annat genom att skicka ut detaljerade frågeformulär. Det kommer också att systematiskt genomföra granskningar när det mottar ett (seriöst) klagomål och organisationen inte besvarar dess förfrågningar på ett tillfredsställande sätt eller om det finns trovärdiga bevis som tyder på att en organisation kanske inte följer principerna. I förekommande fall kommer handelsministeriet också att samråda med dataskyddsmyndigheter om sådana efterlevnadskontroller.

2.3 *Prövningsmekanismer, klagomålshantering och genomförande*

(38) Skölden för skydd av privatlivet i EU och Förenta staterna, via *principen om rättsmedel, genomförande och ansvar,* kräver att organisationer ska tillhandahålla rättsmedel för enskilda som påverkats av bristande efterlevnad och således ge registrerade i EU möjlighet att inge klagomål mot självcertifierade företag i Förenta staterna rörande bristande efterlevnad samt få dessa klagomål lösta, om nödvändigt via ett beslut om lämplig gottgörelse.

(39) Som en del av sin självcertifiering måste organisationer uppfylla kraven i principen om rättsmedel, genomförande och ansvar genom att tillhandahålla effektiva och lättillgängliga oberoende instanser för handläggning av klagomål genom vilka varje enskilds klagomål och tvister kan handläggas och snabbt lösas utan kostnad för den enskilda personen.

(40) Organisationer får välja oberoende instanser för handläggning av klagomål i antingen unionen eller Förenta staterna. Detta inbegriper möjligheten att frivilligt åta sig att samarbeta med EU:s dataskyddsmyndigheter.

([36]) Se bilaga I, avsnittet om ”Söka efter och hantera falska påståenden om deltagande i skölden”.
([37]) Se bilaga II, avsnitt III.6.h. och avsnitt III.11.f.
([38]) Se bilaga I.

Emellertid finns det ingen sådan valmöjlighet när organisationer behandlar personaluppgifter, eftersom samarbete med dataskyddsmyndigheterna då är obligatoriskt. Alternativt kan man använda sig av oberoende alternativ tvistlösning eller *program för integritetsskydd* som utarbetats inom den privata sektorn och som införlivar principerna i sina regler. De sistnämnda måste inbegripa effektiva mekanismer för kontroll av efterlevnaden i enlighet med kraven i principen om rättsmedel, genomförande och ansvar. Organisationerna är skyldiga att åtgärda eventuella problem som rör bristande efterlevnad. De måste också ange att de omfattas av de utrednings- och verkställighetsbefogenheter som tilldelats FTC, transportministeriet eller något annat behörigt lagstadgat organ i Förenta staterna.

(41) Följaktligen ger ramen för skölden för skydd av privatlivet registrerade personer en rad möjligheter att utöva sina rättigheter, inge klagomål mot självcertifierade företag i Förenta staterna rörande bristande efterlevnad och få sina klagomål lösta, om nödvändigt via ett beslut om lämplig gottgörelse. Enskilda kan inge ett klagomål direkt till en organisation, till ett oberoende tvistlösningsorgan som utsetts av organisationen, till nationella dataskyddsmyndigheter eller till FTC.

(42) I fall där deras klagomål inte har lösts av någon av dessa instanser för handläggning av klagomål eller mekanismer för kontroll av efterlevnaden har enskilda också rätt att begära ett bindande skiljedomsförfarande hos arbetsgruppen för skölden för skydd av privatlivet (bilaga 1 till bilaga II till detta beslut). Med undantag för skiljedomsarbetsgruppen, som kräver att vissa rättsmedel ska vara uttömda innan det alternativet kan väljas, står det enskilda fritt att utnyttja vilken eller vilka som helst av prövningsmekanismerna efter eget val, och de är inte skyldiga att välja en mekanism framför någon annan eller att iaktta någon viss ordningsföljd. Det finns dock en viss logisk ordning som det är tillrådligt att följa och som beskrivs nedan.

(43) För det första kan registrerade i EU driva fall av bristande efterlevnad av principerna genom direkta kontakter med det *självcertifierade företaget i Förenta staterna*. För att underlätta en lösning måste organisationerna införa en effektiv prövningsmekanism för att hantera sådana klagomål. Organisationen måste bland annat i sin integritetsskyddspolicy ge tydlig information om en kontaktpunkt som enskilda personer kan vända sig till, antingen inom eller utanför organisationen, som kommer att handlägga klagomål (inklusive eventuella relevanta organisationer i EU som kan besvara frågor eller handlägga klagomål) och om oberoende mekanismer för handläggning av klagomål.

(44) Efter mottagande av en enskild persons klagomål, direkt från den enskilda eller via handelsministeriet efter ett hänskjutande från en dataskyddsmyndighet, måste organisationen ge den registrerade i EU ett svar inom 45 dagar. Svaret ska innehålla en bedömning av huruvida klagomålet är berättigat och information om hur organisationen kommer att lösa problemet. Organisationer är också skyldiga att utan dröjsmål besvara förfrågningar och andra framställningar om information från handelsministeriet eller från en dataskyddsmyndighet ([39]) (om organisationen har förbundit sig att samarbeta med dataskyddsmyndigheten) som rör deras anslutning till principerna. Organisationer ska behålla sin dokumentation om genomförandet av sina integritetsskyddspolicyer och på begäran göra den tillgänglig för en oberoende instans för handläggning av klagomål eller FTC (eller en annan myndighet i Förenta staterna med behörighet att utreda illojala och bedrägliga metoder) i samband med en undersökning eller ett klagomål om bristande efterlevnad.

(45) För det andra kan enskilda också framföra ett klagomål direkt till det *oberoende tvistlösningsorgan* (antingen i Förenta staterna eller i unionen) som av en organisation utsetts att utreda och lösa individuella klagomål (om de inte är uppenbart ogrundade eller oseriösa) och kostnadsfritt tillhandahålla lämpliga rättsmedel för den enskilda personen. De sanktioner och rättsmedel som beslutas av ett sådant tvistlösningsorgan måste vara tillräckligt stränga för att säkerställa att organisationerna följer principerna och bör föreskriva att organisationen avhjälper eller rättar till följderna av den bristande efterlevnaden och, beroende på omständigheterna, upphör med vidare behandling av de berörda personuppgifterna och/eller raderar dem. Fall av bristande efterlevnad ska offentliggöras. Oberoende tvistlösningsorgan som utsetts av en organisation ska på sina offentliga webbplatser lägga ut relevant information om skölden för skydd av privatlivet i EU och Förenta staterna och om de tjänster de tillhandahåller inom ramen för skölden. De ska offentliggöra en årsrapport varje år med sammanställd statistik om sina tjänster ([40]).

([39]) Detta är den handläggande myndighet som utsetts av den arbetsgrupp bestående av dataskyddsmyndigheter som föreskrivs i den kompletterande principen om "dataskyddsmyndigheternas roll" (bilaga II, avsnitt III.5).

([40]) Årsrapporten ska innehålla 1) totalt antal klagomål rörande skölden som mottagits under rapporteringsåret, 2) typer av mottagna klagomål, 3) åtgärder för att förbättra tvistlösningens kvalitet, t.ex. handläggningstid för klagomål, och 4) resultat av mottagna klagomål, särskilt antal och typer av vidtagna åtgärder och beslutade påföljder.

(46) Som en del av sina förfaranden för efterlevnadskontroller kommer handelsministeriet att kontrollera att självcertifierade företag faktiskt i Förenta staterna har registrerat sig hos den oberoende instans för handläggning av klagomål som de hävdar att de är registrerade hos. Både organisationerna och de ansvariga oberoende instanserna för handläggning av klagomål ska utan dröjsmål besvara förfrågningar och framställningar om information från handelsministeriet som rör skölden för skydd av privatlivet.

(47) Om organisationen inte följer ett beslut från ett tvistlösningsorgan eller ett självreglerande organ måste dessa organ anmäla sådan bristande efterlevnad till handelsministeriet och FTC (eller andra myndigheter i Förenta staterna som är behöriga att utreda illojala och bedrägliga metoder), eller till en behörig domstol ([41]). Om en organisation vägrar att efterleva ett slutligt avgörande från ett organ för självreglering på integritetskyddets område, ett oberoende tvistlösningsorgan eller ett regeringsorgan, eller där ett sådant organ finner att en organisation ofta gör sig skyldig till överträdelser av principerna, kommer detta att betraktas som en upprepad överträdelse, varefter handelsministeriet, efter att först ha gett 30 dagars förvarning och en möjlighet att svara den organisation som gjort sig skyldig överträdelsen, kommer att stryka organisationen från förteckningen ([42]). Om organisationen, efter det att den har strukits från förteckningen, fortsätter att hävda att den är certifierad för deltagande i skölden för skydd av privatlivet, kommer ministeriet att hänskjuta den FTC eller ett annat verkställande organ ([43]).

(48) För det tredje får enskilda också framföra sina klagomål till en nationell *dataskyddsmyndighet*. Organisationer är skyldiga att samarbeta i en dataskyddsmyndighets utredning och lösning av ett klagomål antingen när det gäller behandling av personaluppgifter som samlats in inom ramen för ett anställningsförhållande eller när respektive organisation frivilligt har underställts dataskyddsmyndigheters tillsyn. Organisationerna ska särskilt besvara frågor, följa de rekommendationer som ges av dataskyddsmyndigheten, även om gottgörelse eller kompenserande åtgärder, och ska lämna en skriftlig bekräftelse till dataskyddsmyndigheten om att sådana åtgärder har vidtagits.

(49) Dataskyddsmyndigheternas rekommendationer avges via en informell särskild arbetsgrupp, bestående av dataskyddsmyndigheter och inrättad på unionsnivå, vilken kommer att hjälpa till med att säkerställa att ett enhetligt och konsekvent tillvägagångssätt tillämpas för ett klagomål ([44]). Rekommendationer kommer att avges efter det att båda parter i en tvist har getts en rimlig möjlighet att inkomma med synpunkter och förete eventuella bevis. Arbetsgruppen kommer att avge sina rekommendationer så snabbt som möjligt inom ramen för korrekt handläggning av ärendet, normalt inom 60 dagar efter mottagandet av klagomålet. Om en organisation inte följer dessa rekommendationer inom 25 dagar efter det att rekommendationerna avgetts och inte har någon tillfredsställande förklaring till förseningen, ska arbetsgruppen tillkännage sin avsikt att antingen hänskjuta ärendet till FTC (eller en annan behörig verkställande myndighet i Förenta staterna) eller fastställa att en allvarlig överträdelse av samarbetsåtagandet har skett. Det första alternativet kan föranleda verkställighetsåtgärder på grundval av avsnitt 5 i FTC-lagen (eller en liknande lag). Enligt det andra alternativet kommer arbetsgruppen att informera handelsministeriet, som kommer att betrakta organisationens vägran att följa arbetsgruppens rekommendationer som en upprepad överträdelse, vilket kommer att leda till att organisationen stryks från förteckningen över organisationer som har anslutit sig till skölden.

(50) Om den nationella dataskyddsmyndighet som har mottagit klagomålet inte har vidtagit åtgärder för att behandla klagomålet eller om åtgärderna har varit otillräckliga, har den som framställt klagomålet möjlighet att bestrida sådant handlande eller sådan brist på handlande vid de nationella domstolarna i respektive medlemsstat.

(51) Enskilda får också framställa klagomål till dataskyddsmyndigheter även när arbetsgruppen bestående av dataskyddsmyndigheter inte har utsetts till tvistlösningsorgan för en organisation. I dessa fall får dataskyddsmyndigheten hänskjuta sådana klagomål antingen till handelsdepartementet eller till FTC. För att underlätta och öka samarbetet i frågor som rör enskilda klagomål och fall där organisationer som är anslutna till skölden för skydd av privatlivet gör sig skyldiga till bristande efterlevnad, kommer handelsministeriet att inrätta en särskild kontaktpunkt som ska agera som länk och bistå med dataskyddsmyndigheters undersökningar rörande en organisations efterlevnad av principerna ([45]). Även FTC har förbundit sig att inrätta en särskild kontaktpunkt ([46]) och bistå dataskyddsmyndigheterna med undersökningsassistans i enlighet med *U.S. Safe WEB Act* ([47]).

([41]) Se bilaga II, avsnitt III.11.e.
([42]) Se bilaga II, avsnitt III.11.g, särskilt leden ii och iii.
([43]) Se bilaga I, avsnittet om ”Söka efter och hantera falska påståenden om deltagande i skölden”.
([44]) Arbetsordningen för den informella arbetsgruppen bestående av dataskyddsmyndigheter bör upprättas av dataskyddsmyndigheterna på grundval av deras förmåga att organisera sitt arbete och samarbeta sinsemellan.
([45]) Se bilaga I, avsnitten ”*Ökat samarbete med dataskyddsmyndigheter*” och ”*Åtgärder för att göra det lättare att lösa klagomål om bristande efterlevnad*” och bilaga II, avsnitt II.7.e.
([46]) Se bilaga IV, p. 6.
([47]) *ibid*.

(52) För det fjärde har *handelsministeriet* åtagit sig att ta emot, granska och göra sitt bästa för att lösa klagomål som rör organisationer som inte följer principerna. I detta syfte tillhandahåller handelsministeriet särskilda förfaranden för dataskyddsmyndigheter så att de kan hänskjuta klagomål till en särskild kontaktpunkt samt spåra och följa upp klagomålen med företagen för att underlätta en lösning. För att påskynda handläggningen av enskilda klagomål kommer kontaktpunkten att samarbeta direkt om efterlevnadsfrågor med respektive dataskyddsmyndighet och informera myndigheten om klagomålets status inom en period på högst 90 dagar från hänskjutandet. På så sätt kan registrerade ta upp klagomål om bristande efterlevnad från självcertifierade företags (i Förenta staterna) sida direkt med sina nationella dataskyddsmyndigheter, som vidarebefordrar klagomålen till handelsministeriet i egenskap av den myndighet i Förenta staterna som förvaltar skölden för skydd av privatlivet i EU och Förenta staterna. Handelsministeriet har också åtagit sig att inom ramen för den årliga granskningen av sköldens funktion lämna en rapport med en samlad analys av de klagomål som det mottar varje år ([48]).

(53) Om handelsministeriet på grundval av kontroller på eget initiativ, klagomål eller annan information drar slutsatsen att en organisation upprepade gånger har överträtt principerna kommer den att stryka organisationen från förteckningen över organisationer som anslutit sig till skölden. Vägran att följa ett slutligt avgörande från ett organ för självreglering på integritetskyddets område, ett oberoende tvistlösningsorgan eller ett regeringsorgan, inklusive en dataskyddsmyndighet, kommer att betraktas som en upprepad överträdelse.

(54) För det femte måste en organisation som är ansluten till skölden för skydd av privatlivet omfattas av de utrednings- och verkställighetsbefogenheter som tilldelats myndigheterna i Förenta staterna, särskilt den federala konkurrensmyndigheten (*Federal Trade Commission*) ([49]) som kommer att säkersälla efterlevnad av principerna. FTC kommer att prioritera hänskjutanden av fall av bristande efterlevnad av principerna som mottas från oberoende tvistlösningsorgan eller självreglerande organ, handelsministeriet och dataskyddsmyndigheter (som agerar på eget initiativ eller med anledning av klagomål) för att fastställa om avsnitt 5 i FTC-lagen har överträtts ([50]). FTC har åtagit sig att inrätta ett standardiserat förfarande för hänskjutanden, utse en kontaktpunkt vid myndigheten för hänskjutanden från dataskyddsmyndigheter och utbyta information om hänskjutanden. FTC kommer dessutom att ta emot klagomål direkt från enskilda personer och kommer att genomföra utredningar om frågor som rör skölden för skydd av privatlivet på eget initiativ som ett led av sina allmänna utredningar av integritetsskyddsfrågor.

(55) FTC kan se till att principerna följs genom administrativa beslut (förordnanden) och kommer systematiskt att övervaka efterlevnaden av sådana förordnanden. Om en organisation inte följer principerna kan FTC hänskjuta ärendet till behörig domstol för att utverka civilrättsliga påföljder och annan gottgörelse, även för eventuella skador till följd av det olagliga beteendet. Alternativt kan FTC direkt utverka ett preliminärt eller definitivt föreläggande eller andra rättsåtgärder från en federal domstol. Varje förordnande som utfärdas till en organisation som deltar i skölden för skydd av privatlivet innehåller bestämmelser om egenrapportering ([51]), och organisationerna måste offentliggöra alla eventuella avsnitt i efterlevnads- eller bedömningsrapporter som lämnas in till FTC och som är relevanta för skölden. FTC kommer dessutom att föra en onlineförteckning över företag som omfattas av förordnanden från FTC- eller domstolsbeslut i ärenden som rör skölden.

(56) För det sjätte kan registrerade i EU som en ”sista utväg”, om inget av de andra tillgängliga rättsmedlen har löst deras klagomål på ett tillfredsställande sätt, begära ett bindande skiljedomsförfarande hos ”*arbetsgruppen för skölden för skydd av privatlivet*”. Organisationer måste informera enskilda om deras möjlighet, under vissa omständigheter, att begära ett bindande skiljedomsförfarande och de är skyldiga att svara när en enskild har valt detta alternativ genom att inge ett meddelande till den berörda organisationen ([52]).

([48]) Se bilaga I, avsnittet ”*Åtgärder för att göra det lättare att lösa klagomål om bristande efterlevnad*”.

([49]) En organisation som är ansluten till skölden för skydd av privatlivet ska offentligt förklara att den kommer att följa principerna, offentliggöra sina integritetsskyddspolicyer i linje med dessa principer och till fullo genomföra dem. Underlåtenheten att följa principerna kan leda till åtal i enlighet med avsnitt 5 i FTC-lagen, som förbjuder illojala och bedrägliga handlingar i handeln eller som påverkar handeln.

([50]) Enligt uppgifter från FTC har den inga befogenheter att utföra inspektioner på plats när det gäller integritetsskydd. Den har emellertid befogenhet att tvinga organisationer att lägga fram handlingar och lämna vittnesmål (se avsnitt 20 i FTC-lagen), och får använda domstolsväsendet för att verkställa en sådan order om överträdelse konstateras.

([51]) FTC:s beslut och domstolsbeslut får föreskriva att företagen ska genomföra integritetsskyddsprogram och regelbundet lämna efterlevnadsrapporter eller bedömningar från oberoende tredje parter till FTC.

([52]) Se bilaga II, avsnitt II.1.xi och III.7.c.

(57) Denna skiljedomsarbetsgrupp kommer att bestå av en pool med minst 20 skiljemän som utses av handelsministeriet och kommissionen på grundval av deras oberoende, integritet och erfarenhet av Förenta staternas lagstiftning om integritetsskydd och unionens dataskyddslagstiftning. För varje enskild tvist kommer parterna att välja en arbetsgrupp bestående av en eller tre ([53]) skiljemän från denna pool. Förhandlingarna kommer att ske enligt standardregler för skiljedomsförfaranden som handelsministeriet och kommissionen ska komma överens om. Dessa regler kommer att komplettera den redan inrättade ramen som innehåller flera inslag som gör denna mekanism mer tillgänglig för registrerade i EU: i) Vid förberedande av ett yrkande inför arbetsgruppen får den registrerade bistås av sin dataskyddsmyndighet. ii) Platsen för skiljeförfarandet kommer att vara Förenta staterna, men registrerade i EU kan välja att delta via telefon- eller videoanslutning, som ska tillhandahållas utan kostnad för den enskilde. (ii) Det språk som ska användas i skiljedomsförfarandet ska som regel vara engelska, men tolkning vid skiljedomsförhöret samt översättning kommer normalt sett ([54]) att tillhandahållas på motiverad begäran och utan kostnad för den registrerade. (iv) Slutligen måste varje part stå för sina egna advokatkostnader om de företräds av en advokat inför arbetsgruppen. Emellertid kommer handelsministeriet att inrätta en fond, dit organisationer som är anslutna till skölden för skydd av privatlivet ska betala ett årligt bidrag som ska täcka de berättigade kostnaderna för skiljedomsförfarandet upp till maximala belopp som ska fastställas av Förenta staternas myndigheter i samråd med kommissionen.

(58) Arbetsgruppen för skölden för skydd av privatlivet kommer att ha befogenhet att påföra ”individuella specifika icke-monetära åtgärder” ([55]) för att avhjälpa bristande efterlevnad av principerna. Arbetsgruppen kommer att beakta annan gottgörelse som redan erhållits via andra mekanismer inom ramen för skölden när den fäller sitt avgörande, men enskilda personer kan ändå begära skiljedom om de anser att dessa andra former av gottgörelse är otillräckliga. Detta innebär att registrerade i EU kan åberopa skiljedom i alla ärenden där handlande eller brist på handlande från behöriga myndigheters sida i Förenta staterna (t.ex. FTC) har lett till att deras klagomål inte har fått en tillfredsställande lösning. Skiljedom kan inte åberopas om en dataskyddsmyndighet har rättslig befogenhet att lösa yrkandet i fråga med avseende på det självcertifierade företaget i Förenta staterna, dvs. i de fall där organisationen antingen är skyldig att samarbeta och följa dataskyddsmyndigheternas rekommendationer när det gäller behandling av personaluppgifter som samlats in inom ramen för ett anställningsförhållande, eller frivilligt har förbundit sig att göra detta. Enligt lagen om federal skiljedom (*Federal Arbitration Act*) kan enskilda personer verkställa skiljedomsbeslut i domstolar i Förenta staterna, vilket säkerställer rättsliga åtgärder om företaget inte efterlever bestämmelserna.

(59) Om en organisation inte uppfyller sitt åtagande att respektera principerna och sin offentliggjorda integritetsskyddspolicy kan det finnas andra sätt att söka rättslig prövning enligt Förenta staternas lagstiftning, som föreskriver rättsmedel enligt skadeståndslagstiftningen och i fall av oriktiga utfästelser, illojala eller bedrägliga handlingar eller metoder samt avtalsbrott.

(60) Vidare gäller att om en dataskyddsmyndighet, efter att ha mottagit ett yrkande från en registrerad i EU, anser att överföringen av en personuppgifter om en enskild till en organisation i Förenta staterna genomförs i strid med EU:s dataskyddslagstiftning, inbegripet när EU-exportören av uppgifter har anledning att tro att organisationen inte följer principerna, kan den också utöva sina befogenheter gentemot exportören av uppgifter och, om nödvändigt, beordra att uppgiftsöverföringen ska avbrytas.

(61) Mot bakgrund av informationen i detta avsnitt anser kommissionen att de principer om utfärdats av Förenta staternas handelsministerium som en helhet säkerställer en skyddsnivå för personuppgifter som är väsentligen likvärdig med den skyddsnivå som garanteras genom de väsentliga grundläggande principer som fastställs i direktiv 95/46/EG.

(62) En effektiv tillämpning av principerna garanteras dessutom genom handelsministeriets skyldigheter på insynsområdet och dess förvaltning och efterlevnadskontroll av skölden för skydd av privatlivet.

(63) Kommissionen anser dessutom att, som helhet, de tillsynsmekanismer, de instanser för handläggning av klagomål och de verkställighetsmekanismer som tillhandahålls inom ramen för skölden för skydd av privatlivet dels gör det möjligt att i praktiken upptäcka och bestraffa överträdelser av principerna som begås av organisationer som deltar i skölden, dels ger de registrerade rättsmedel för att få tillgång till personuppgifter som rör dem och, eventuellt, få uppgifterna rättade eller raderade.

([53]) Antalet skiljemän i arbetsgruppen ska överenskommas mellan parterna.

([54]) Arbetsgruppen kan dock finna att täckningen med tanke på de särskilda omständigheterna kring skiljedomsförfarandet skulle leda till omotiverade eller oproportionerliga kostnader.

([55]) Enskilda personer kan inte kräva skadestånd i skiljedomsförfaranden, men åberopande av skiljedom hindrar dock inte den enskilde från att yrka på skadeståndsanspråk i allmänna domstolar i Förenta staterna.

3. TILLGÅNG OCH ANVÄNDNING AV PERSONUPPGIFTER SOM ÖVERFÖRS ENLIGT SKÖLDEN FÖR SKYDD AV PRIVATLIVET I EU OCH FÖRENTA STATERNA AV OFFENTLIGA MYNDIGHETER I FÖRENTA STATERNA

(64) Såsom följer av bilaga II avsnitt I.5 begränsas anslutningen till principerna till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden.

(65) Kommissionen har bedömt begränsningarna och garantierna i Förenta staternas lag när det gäller tillgång till och användning av personuppgifter som överförs inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna av Förenta staternas offentliga myndigheter för ändamål som rör nationell säkerhet, brottsbekämpning och andra ändamål som rör allmänintresset. Dessutom har Förenta staternas regering, via den nationella underrättelsetjänsten ([56]), lämnat detaljerade utfästelser och försäkringar till kommissionen, som ingår i bilaga VI till detta beslut. Genom en skrivelse undertecknad av utrikesministern som bifogas som bilaga III till detta beslut har Förenta staternas regering dessutom förbundit sig att inrätta en ny tillsynsmekanism för ingrepp som hör samman med nationell säkerhet, ombudsmannen för skölden för skydd av privatlivet, som är oberoende gentemot underrättelsegemenskapen. I en framställning från Förenta staternas justitieministerium, som ingår som bilaga VII till detta beslut, beskrivs slutligen de begränsningar och garantier som gäller för offentliga myndigheters tillgång till och användning av uppgifter för brottsbekämpande ändamål och andra ändamål som rör allmänintresset. För att öka insynen och återspegla den rättsliga karaktären hos dessa åtaganden kommer samtliga dokument som förtecknas och bifogas till detta beslut att offentliggöras i Förenta staternas federala register.

(66) Slutsatserna från kommissionen för begränsning av åtkomst till och användning av personuppgifter som överförs från EU till Förenta staterna av Förenta staternas offentliga myndigheter samt förekomsten av effektivt rättsligt skydd diskuteras närmare nedan.

3.1 *Förenta staternas offentliga myndigheters tillgång och användning av personuppgifter av skäl som rör nationell säkerhet*

(67) Kommissionens analys visar att Förenta staternas lagstiftning innehåller dels en rad begränsningar av tillgången till och användningen av personuppgifter som överförs inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna av skäl som rör nationell säkerhet, dels tillsyns- och prövningsmekanismer som ger tillräckliga garantier för ett effektivt skydd av dessa uppgifter mot olagliga ingrepp och risker för missbruk ([57]). Denna rättsliga ram har stärkts avsevärt sedan kommissionen utfärdade sina två meddelanden 2013 (se skäl 7), såsom beskrivs nedan.

3.1.1 Begränsningar

(68) Enligt Förenta staternas konstitution är det presidenten, i egenskap av överbefälhavare och regeringschef, som har ansvaret för att garantera den nationella säkerheten och, när det gäller utländska underrättelser, att föra Förenta staternas utrikespolitik ([58]). Kongressen har befogenheter att införa begränsningar, och har gjort detta i flera avseenden. Presidenten kan leda Förenta staternas underrättelsegemenskaps verksamheter inom dessa gränser, särskilt genom dekret (*Executive Orders*) eller presidentdirektiv (*Presidential Policy Directives*). Detta gäller naturligtvis även inom de områden som kongressen inte har utfärdat vägledning om. För närvarande är de två centrala rättsliga instrumenten i detta avseende *Executive Order* 12333 (nedan kallad *E.O. 12333*) ([59]) och *Presidential Policy Directive 28* (nedan kallat *PPD-28*).

([56]) Den nationella underrättelsetjänsten (*Office of the Director of National Intelligence*, ODNI), fungerar som överordnat organ för underrättelsegemenskapen och är presidentens och det nationella säkerhetsrådets främsta rådgivare. Se *Intelligence Reform and Terrorism Prevention Act* från 2004, Pub. L. 108–458 of 17.12.2004. ODNI ska bland annat fastställa kraven för och förvalta och leda underrättelsegemenskapens fördelning, insamling, analys, produktion och spridning av nationella underrättelseuppgifter, bland annat genom att utforma riktlinjer för hur åtkomst till, användning av och delning av information eller underrättelseuppgifter ska ske. Se avsnitt 1.3 (a), (b) i E.O. 12333.

([57]) Se Schrems-målet, punkt 91.

([58]) Förenta staternas konstitution, artikel II. Se även inledningen till PPD-28.

([59]) E.O. 12333: United States Intelligence Activities, Federal Register vol. 40, nr 235 (8.12.1981). I den mån PPD-28 är allmänt tillgängligt fastställer det mål, inriktning, uppgifter och ansvar för underrättelseinsatserna i Förenta staterna (inklusive rollerna för olika enheter inom underrättelsegemenskapen). I PPD-28 anges även allmänna kriterier för genomförandet av underrättelseverksamhet (särskilt behovet av att utfärda särskilda förfaranderegler). Enligt avsnitt 3.2 i E.O. 12333 ska presidenten, med stöd av det nationella säkerhetsrådet, och DNI utfärda sådana lämpliga riktlinjer, förfaranden och vägledningar som är nödvändiga för att genomföra dekretet.

(69) Genom *Presidential Policy Directive 28* (PPD-28), utfärdat den 17 januari 2014, införs ett antal begränsningar av ”signalspaningsverksamhet” ([60]). Detta presidentdirektiv är bindande för Förenta staternas underrättelsemyndigheter ([61]) och är tillämpligt enligt en ändring i Förensta staternas administration ([62]). PPD-28 är av särskild betydelse för utländska medborgare, inklusive registrerade i EU. Det föreskriver bland annat följande:

a) Insamling av uppgifter via signalspaning måste vara godkänd enligt lag eller ske med presidentens tillstånd, och måste genomföras i enlighet med Förenta staternas konstitution (särskilt fjärde tillägget) och Förenta staternas lagstiftning.

b) Alla människor bör behandlas med värdighet och respekt, oavsett nationalitet och bostadsort.

c) Alla personer har legitima integritetsintressen när det gäller behandlingen av deras personuppgifter.

d) Integritetsskyddet och de medborgerliga fri- och rättigheterna ska vara integrerade överväganden i planeringen av Förenta staternas signalspaningsverksamhet.

e) Förenta staternas signalspaningsverksamhet måste därför omfatta lämpliga garantier för alla enskilda personers personuppgifter, oavsett nationalitet och bostadsort.

(70) Enligt PPD-28 får signalspaningsuppgifter endast samlas in om det finns ett ändamål som rör utländska underrättelser eller kontraspionage för att stödja nationella uppdrag och ministerierelaterade uppdrag, och inte för något annat ändamål (t.ex. för att ge företag i Förenta staterna konkurrensfördelar). I detta avseende klargör ODNI att enheter inom underrättelsegemenskapen ”bör kräva att insamlingen när så är möjligt bör inriktas på specifika utländska underrättelsemål eller frågor genom användning av urvalsfaktorer (t.ex. specifika anläggningar, urvalstermer och identifierare)” ([63]). Utfästelserna ger dessutom garantier för att beslut om underrättelseinsamling inte lämnas åt enskilda underrättelsetjänstemäns godtycke, utan omfattas av de policyer och förfaranden som underrättelsegemenskapens olika enheter i Förenta staterna (myndigheter och byråer) är skyldiga att inrätta för att genomföra PPD-28 ([64]). Forskning om och fastställande av lämpliga urvalstermer sker följaktligen inom den övergripande ”prioriteringsramen för nationell underrättelseverksamhet” (*National Intelligence Priorities Framework. NIPF*), vilket garanterar att underrättelseprioriteringar fastställs av politiskt ansvariga på hög nivå och regelbundet ses över så att de kontinuerligt kan anpassas till aktuella hot mot nationell säkerhet och beaktar möjliga risker, även integritetsrisker ([65]). På denna grundval forskar underrättelsetjänsternas personal om och identifierar specifika urvalstermer som väntas leda till insamling av utländska underrättelser som är anpassade till prioriteringarna ([66]). Urvalstermer måste ses över regelbundet för att kontrollera att de fortfarande ger värdefull underrättelseinformation enligt prioriteringarna ([67]).

([60]) Enligt E.O. 12333 är direktören för Nationella säkerhetsmyndigheten (NSA) funktionell chef för signalspaning och ska driva en enhetlig organisation för signalspaningsverksamhet.
([61]) En definition av begreppet ”underrättelsegemenskap” ges i avsnitt 3.5 (h) i E.O. 12333, tillsammans med nr 1 i PPD-28.
([62]) Se memorandum från *Office of Legal Counsel*, justitieministeriet, till president Clinton, 29.1.2000. Enligt detta rättsliga yttrande har presidentdirektiv ”samma väsentliga rättsverkningar som dekret”.
([63]) ODNI:s utfästelser (bilaga VI), s. 3.
([64]) Se avsnitt 4(b),(c) i PPD-28. Enligt offentliga uppgifter bekräftade översynen 2015 de befintliga sex ändamålen. Se *Signals Intelligence Reform, 2016 Progress Report*.
([65]) ODNI:s utfästelser (bilaga VI), s. 6 (med hänvisning till *Intelligence Community Directive 204*). Se även avsnitt 3 i PPD-28.
([66]) ODNI:s utfästelser (bilaga VI), s. 6. Se t.ex. NSA Civil Liberties and Privacy Office (NSA CLPO), *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333*, 7.10.2014. Se även ODNI:s lägesrapport 2014. För åtkomstförfrågningar enligt avsnitt 702 i FISA-lagen, förfrågningar regleras av FISC:s godkända minimeringsförfaranden. Se NSA CLPO, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, 16.4.2014.
([67]) Se *Signals Intelligence Reform, 2015 Anniversary Report*. Se även ODNI:s utfästelser (bilaga VI), s. 6, 8–9, 11.

(71) Kraven i PPD-28 på att underrättelseinsamling alltid ([68]) ska vara ”så anpassad som möjligt”, och att underrättelsegemenskapen ska prioritera tillgång till annan information samt lämpliga och genomförbara alternativ ([69]), avspeglar dessutom en allmän regel om prioritering av riktad insamling framför bulkinsamling. Enligt den garanti som ges av ODNI säkerställer de i synnerhet att bulkinsamling varken är ”massinsamling” eller ”slumpartad insamling”, och att undantaget inte ”sväljer” regeln ([70]).

(72) I PPD-28 anges att enheter inom underrättelsegemensapen ibland måste samla in signalspaningsuppgifter i bulk under vissa omständigheter, t.ex. för att identifiera och bedöma nya eller framväxande hot, men PPD-28 instruerar samtidigt enheterna att prioritera alternativ som möjliggör riktad signalspaning ([71]). Härav följer att bulkinsamling endast kommer att genomföras när riktad insamling genom användning av urvalsfaktorer – dvs. en identifierare förknippad med ett visst mål (t.ex. målets adress eller telefonnummer) – inte är möjlig ”på grund av tekniska eller operativa överväganden” ([72]). Detta gäller både det sätt som signalspaningsuppgifter samlas in på och vilka uppgifter som faktiskt samlas in ([72]).

(73) Enligt utfästelserna från ODNI kommer den att sträva efter att avgränsa insamlingen ”så mycket som möjligt”, även när underrättelsegemenskapen inte kan använda specifika identifierare för riktad insamling. För att säkerställa detta använder den ”filter och andra tekniska verktyg för att inrikta insamlingen på de anläggningar som sannolikt innehåller meddelanden av värde när det gäller utländska underrättelser” (och därmed kommer den att kunna anpassas till de krav som uttalas av politiskt ansvariga i Förenta staterna i enlighet med den process som beskrivs ovan i skäl 70). Som en konsekvens av detta kommer bulkinsamling att målinriktas på minst två sätt: För det första kommer den alltid att avse särskilda utländska underrättelsemål (t.ex. signalspaning för att inhämta information om en terroristgrupps verksamhet i en viss region) och inrikta insamlingen på kommunikation som har en sådan koppling. Enligt den garanti som ges av ODNI avspeglas detta i det faktum att ”Förenta staternas signalspaningsverksamhet berör endast en bråkdel av den kommunikation som sker via internet” ([73]). För det andra klargörs i ODNI:s utfästelser att filtren och andra tekniska verktyg som används kommer att utformas för att inrikta insamlingen ”så precist som möjligt” för att säkerställa att man minierar mängden ”irrelevant information” som samlas in.

(74) Även om Förenta staterna anser det nödvändigt att samla in signalspaningsuppgifter i bulk, enligt de villkor som anges i skälen 70–73, begränsar PPD-80 användningen av sådan information till en särskild förteckning över sex ändamål som rör nationell säkerhet i syfte att skydda alla människors integritet och medborgerliga friheter, oavsett nationalitet och bostadsort ([74]). Dessa tillåtna ändamål omfattar åtgärder för att upptäcka och motverka

([68]) Se fotnot 63.

([69]) Det bör också noteras att enligt avsnitt 2.4 i E.O. 12333 ska enheterna inom underrättelsegemenskapen ”använda insamlingsmetoder som inkräktar så lite som möjligt inom Förenta staterna”. När det gäller begränsningarna avseende ersättning av bulkinsamling med riktade insamlingar, se resultaten av en bedömning som genomförts av *National Research Council* enligt en rapport från Europeiska unionens byrå för grundläggande rättigheter: *Surveillance by intelligence services: fundamental rights, safeguards and remedies in the EU* (2015), s. 18.

([70]) ODNI:s utfästelser (bilaga VI), s. 4.

([71]) Se även avsnitt 5(d) i PPD-28, enligt vilket den chefen för den nationella underrättelsetjänsten, i samordning med cheferna för berörda enheter inom underrättelsegemenskapen och *Office of Science and Technology Policy*, ska lämna en rapport till presidenten ”med en bedömning av möjligheterna att skapa programvara som skulle göra det lättare för underrättelsegemenskapen att genomföra riktad informationsinsamling i stället för bulkinsamling”. Enligt offentlig information blev resultatet av denna rapport att man konstaterade att ”det inte finns något programvarubaserat alternativ som helt kan ersätta bulkinsamling när det gäller att upptäcka vissa hot mot den nationella säkerheten”. Se *Signals Intelligence Reform, 2015 Anniversary Report*.

([72]) Se fotnot 63.

([73]) ODNI:s utfästelser (bilaga VI). Detta avser särskilt den oro som de nationella dataskyddsmyndigheterna uttryckt i sitt yttrande om utkastet till beslut om adekvat skyddsnivå. Se artikel 29-gruppens (arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter) yttrande 01/2016 om skölden för skydd av privatlivet i EU och Förenta staterna, utkastet till beslut om adekvat skyddsnivå (antaget den 13 april 2016), s. 38, nr 47.

([74]) Se avsnitt 2 i PPD-28.

hot från spionage, terrorism, massförstörelsevapen, hot mot cybersäkerhet, mot försvarsmakten eller militär personal samt transnationella kriminella hot som är relaterade till de övriga fem ändamålen, och förteckningen kommer att ses över minst årligen. Enligt utfästelserna från Förenta staternas regering har enheter inom underrättelsegemenskapen förstärkt sina analysmetoder och analysstandarder för sökning i signalunderrättelser som inte tidigare utvärderats så att de överensstämmer med dessa krav. Användningen av riktade sökningar ”säkerställer att endast de uppgifter som anses ha ett eventuellt värde som underrättelseuppgifter lämnas till analytiker för undersökning” ([75]).

(75) Dessa begränsningar är särskilt relevanta för personuppgifter som överförts inom ramen för skölden för skydd av personuppgifter i EU och Förenta staterna, särskilt om insamling av personuppgifter skulle äga rum utanför Förenta staterna, inbegripet under överföringen av uppgifterna via de transatlantiska kablarna från unionen till Förenta staterna. Såsom bekräftats av Förenta staternas myndigheter i ODNI:s utfästelser gäller de begränsningar och garantier som anges där – inklusive de som omfattas av PPD-28 – för sådan insamling ([76]).

(76) Även om de inte är formulerade i juridiska termer återspeglar dessa principer det väsentliga i principerna om nödvändighet och proportionalitet. Riktad insamling prioriteras tydligt, medan bulkinsamling begränsas till (exceptionella) situationer där riktad insamling inte är möjlig av tekniska eller operativa skäl. Även där *bulkinsamling* inte kan undvikas är vidare ”användning” av sådana uppgifter genom åtkomst *strikt begränsad* till särskilda och legitima nationella säkerhetsändamål ([77]).

(77) Eftersom dessa krav ingår i ett direktiv som har utfärdats av presidenten i egenskap av regeringschef är de bindande för hela underrättelsegemenskapen och har genomförts ytterligare i form av regler och förfaranden för underrättelsetjänsterna som införlivar de allmänna principerna i uttryckliga riktlinjer för den dagliga verksamheten. Kongressen i sig är inte bunden av PPD-28, men har också vidtagit åtgärder för att se till att insamlingen av och åtkomsten till personuppgifter i Förenta staterna är riktad i stället för att utföras ”på ett generaliserat sätt”.

(78) Av tillgängliga uppgifter, bland annat de utfästelser som mottagits från Förenta staternas regering, framgår att när uppgifterna väl har överförts till organisationer i Förenta staterna som är självcertifierade enligt skölden för skydd av privatlivet i EU och Förenta staterna kan underrättelsetjänsterna endast ([78]) ansöka om att få åtkomst till personuppgifter när en sådan förfrågan är förenlig med lagen om underrättelseverksamhet och övervakning utomlands (*Foreign Intelligence Surveillance Act*, FISA) eller görs av FBI, baserat på en s.k. nationell säkerhetsskrivelse (*National Security Letter*, NSL) ([79]). FISA innehåller flera rättsliga grunder som kan användas för att samla in (och därefter behandla) personuppgifter om registrerade i EU som överförs inom ramen för skölden för skydd av

([75]) ODNI:s utfästelser (bilaga VI), s. 4. Se även *Intelligence Community Directive* 203.
([76]) ODNI:s utfästelser (bilaga VI), s. 2. De begränsningar som anges i E.O. 12333 (t.ex. att insamlad information ska motsvara de underrättelseprioriteringar som fastställts av presidenten) gäller också.
([77]) Se Schrems-målet, punkt 93.
([78]) FBI:s uppgiftsinsamling kan dessutom grundas på verkställighetsbeslut (se avsnitt 3.2 i detta beslut).
([79]) Närmare förklaringar om användningen av NSL ges i ODNI:s utfästelser (bilaga VI), s. 13–14, nr 38. Såsom anges där får FBI endast använda nationella säkerhetsskrivelser för att begära innehållslös information som är relevant för en undersökning avseende nationell säkerhet när syftet är att skydda nationen mot internationell terrorism eller hemlig underrättelseverksamhet. När det gäller överföringar av uppgifter inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna förefaller den mest relevanta rättsliga befogenheten vara lagen om elektronisk brevhemlighet (*Electronic Communications Privacy Act*) (18 U.S.C. § 2709), enligt vilken förfrågningar om abonnentuppgifter eller transnationella register ska innehålla en ”term som uttryckligen identifierar en person, en enhet, ett telefonnummer eller ett konto”.

privatlivet. Förutom avsnitt 104 i FISA ([80]) som omfattar traditionell individualiserad elektronisk övervakning och avsnitt 402 i FISA ([81]) om installation av ”pen registers” eller ”trap and trace”-anordningar, är de två centrala instrumenten avsnitt 501 i FISA (f.d. avsnitt 215 i *U.S. PATRIOT ACT*) och avsnitt 702 i FISA ([82]).

(79) I detta avseende innehåller *Förenta staterna FREEDOM Act*, som antogs den 2 juni 2015, ett förbud mot bulkinsamling av register baserat på avsnitt 402 i FISA (godkännande av användning av ”pen registers” och ”trap and trace”-anordningar), avsnitt 501 i FISA (f.d. avsnitt 215 i *U.S. PATRIOT ACT*) ([83]) och genom användning av NSL, och kräver i stället användning av särskilda ”urvalstermer” ([84]).

(80) FISA innehåller ytterligare rättsliga befogenheter för genomförandet av nationell underrättelseverksamhet, inklusive signalspaning, men kommissionens bedömning visar att dessa befogenheter, när det gäller överföring av personuppgifter inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna, också begränsar offentliga myndigheters ingrepp till riktad insamling och åtkomst.

(81) Detta gäller helt klart för individualiserad elektronisk övervakning enligt avsnitt 104 i FISA ([85]). När det gäller avsnitt 702 i FISA, som utgör grunden för två viktiga underrättelseprogram som drivs av Förenta staternas underrättelsetjänster (Prism, Upstream), utförs sökningarna på ett riktat sätt med användning av individuella urvalstermer som identifierar särskilda kommunikationsmedel, t.ex. målets e-postadress eller telefonnummer, men inte nyckelord eller ens de berörda personernas namn ([86]). Såsom styrelsen för tillsyn av personlig integritet och

([80]) 50 U.S.C. § 1804. Enligt denna rättsliga befogenhet krävs ”en redogörelse för de fakta och omständigheter som sökanden åberopar för att motivera sin åsikt att A) målet för den elektroniska övervakningen är en utländsk makt eller ett ombud för en utländsk makt”. De sistnämnda kan vara utländska medborgare som är involverade i internationell terrorism eller internationell spridning av massförstörelsevapen (inklusive förberedande handlingar) (50 U.S.C. § 1801 (b)(1)). Kopplingen till personuppgifter som överförs inom ramen för skölden för skydd av privatlivet är dock endast teoretisk, eftersom faktaredogörelsen också måste innehålla en motivering av åsikten att ”varje anläggning eller plats som den elektroniska övervakningen riktas mot används, eller står i begrepp att användas, av en utländsk makt eller ett ombud för en utländsk makt”. För att tillämpa denna befogenhet krävs i alla händelser en ansökan till domstolen för övervakning av utländsk underrättelseinformation (FISC). Domstolen kommer bland annat att bedöma om det på grundval av de åberopade omständigheterna finns en trolig orsak till att så är fallet.

([81]) 50 U.S.C. § 1842 samt § 1841(2) och avsnitt 3127 i avdelning 18. Befogenheten omfattar inte kommunikationens innehåll, utan inriktas snarare på information om en kund eller abonnent som använder en viss tjänst (t.ex. namn, adress, abonnentnummer, varaktighet/typ av mottagen tjänst, betalningskälla/betalningsmetod). Det krävs en ansökan om ett beslut från FISC (eller en fredsdomare i Förenta staterna) och en särskild urvalsterm måste användas i den mening som avses i § 1841(4), dvs. en term som specifikt identifierar en person, ett konto osv., och som används för att i största möjliga utsträckning begränsa omfattningen av den information som söks.

([82]) Avsnitt 501 i FISA (f.d. avsnitt 215 *U.S. PATRIOT ACT*) bemyndigar FBI att begära ett domstolsbeslut för att få fram ”konkreta ting” (särskilt telefonmetadata, men även företagsregister) för ändamål avseende utländska underrättelser, och enligt avsnitt 702 i FISA kan enheter inom underrättelsegemenskapen i Förenta staterna ansöka om tillgång till information, inklusive innehåll i internetkommunikation, som kommer från Förenta staterna, men som inriktas på vissa utländska medborgare utanför Förenta staterna.

([83]) På grundval av denna bestämmelse kan FBI begära ”konkreta ting” (t.ex. register, skrivelser, dokument), men måste visa domstolen för övervakning av utländsk underrättelseinformation (*Foreign Intelligence Surveillance Court*, FISC) att det finns rimliga skäl att anse att sådana ting är relevanta för en viss FBI-utredning. FBI måste använda urvalstermer som godkänts av FISC i sina sökningar, och det måste finnas en ”skälig uttalad misstanke” om att termen är förknippad med en eller flera utländska makter eller deras ombud som är involverade i internationell terrorism eller förberedelser för sådana handlingar. Se PCLOB, avsnitt 215 *Report*, s. 59. Se NSA CLOP, *Transparency Report: The Förenta staterna Freedom Act Business Records FISA Implementation*, 15.1.2016, s. 4–6.

([84]) ODNI:s utfästelser (bilaga VI), s. 13 (nr 38).

([85]) Se fotnot 81.

([86]) PCLOB avsnitt 702 Report, s. 32–33 med ytterligare hänvisningar. Enligt NSA:s dataskyddsenhet måste NSA kontrollera att det finns en koppling mellan målet och urvalstermen och dokumentera den utländska underrättelseinformation som man räknar med att inhämta. Informationen måste granskas och godkännas av två överordnade NSA-analytiker, och hela processen kommer att spåras för senare efterlevnadsgranskningar av ODNI och justitieministeriet. Se NSA CLPO, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, 16.4.2014.

medborgerliga friheter (*Privacy and Civil Liberties Oversight Board*, PCLOB) har konstaterat består övervakning enligt avsnitt 702 ”endast av att inrikta sökningarna på vissa [utländska] personer för vilka ett individualiserat beslut har fattats” ([87]). Till följd av en ”tidsfristklausul” ska avsnitt 702 i FISA ses över 2017. Kommissionen kommer då att behöva göra en ny bedömning av de garantier som är tillgängliga för registrerade i EU.

(82) I sina utfästelser har Förenta staternas regering dessutom gett Europeiska kommissionen uttryckliga garantier för att Förenta staternas underrättelsegemenskap ”inte bedriver någon godtycklig övervakning av någon, inte heller av vanliga EU-medborgare” ([88]). När det gäller personuppgifter som samlas in inom Förenta staterna stöds detta uttalande av empiriska bevis, som visar att *åtkomstförfrågningar* via nationella säkerhetsskrivelser och enligt FISA, både individuellt och tillsammans, endast rör ett relativt litet antal mål jämfört med det totala uppgiftsflödet på internet ([89]).

(83) När det gäller *åtkomst* till insamlade uppgifter och *datasäkerhet* föreskriver PPD-28 att åtkomst ”ska begränsas till behörig personal som behöver känna till informationen för att kunna utföra sitt uppdrag”, och att personuppgifter ”ska behandlas och lagras under förhållanden som ger en adekvat skyddsnivå och förhindrar åtkomst av obehöriga, enligt tillämpliga garantier för känslig information”. Underrättelsepersonal ges lämplig och adekvat utbildning i de principer som anges i PPD-28 ([90]).

(84) I fråga om *lagring* och vidare *spridning* av personuppgifter om registrerade i EU som samlas in av Förenta staternas underrättelsemyndigheter föreskriver PPD-28 att alla personer (inklusive utländska medborgare) ska behandlas med värdighet och respekt, att alla personer har legitima integritetsintressen när det gäller behandlingen av deras personuppgifter och att enheter inom underrättelsegemenskapen därför måste inrätta policyer som ger lämpliga garantier för sådana uppgifter och som är ”skäligt utformade för att minimera spridning och lagring av uppgifterna” ([91]).

([87]) PCLOB avsnitt 702 *Report*, s. 111. Se även ODNI:s utfästelser (bilaga VI), s. 9 (”Insamling enligt avsnitt 702 i [FISA] är inte ‘slumpartad massinsamling’, utan är snävt inriktad på insamling av utländska underrättelseuppgifter om individuellt identifierade legitima mål.”) och s. 13, nr 36 (med hänvisning till ett FISC-yttrande från 2014). Se NSA CLPO, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, 16.4.2014. Även när det gäller Upstream kan NSA endast begära avlyssning av elektronisk kommunikation till, från eller om avdelade urvalstermer.

([88]) ODNI:s utfästelser (bilaga VI), s. 18. Se även s. 6, där det anges att de tillämpliga förfarandena ”visar ett tydligt åtagande att förhindra godtycklig och slumpartad insamling av signalspaningsuppgifter och att genomföra principen om skälighet – från högsta regeringsnivå”.

([89]) Se rapporten *Statistical Transparency Report Regarding Use of National Security Authorities*, 22.4.2015. När det gäller det övergripande uppgiftsflödet på internet, se t.ex. Europeiska unionens byrå för grundläggande rättigheter, Underrättelsetjänsters övervakning: garantier för grundläggande rättigheter och rättsmedel i Europeiska unionen (2015), s. 15–16. I fråga om Upstream-programmet visar ett FISC-yttrande från 2011 för vilket sekretessen har hävts att över 90 procent av de elektroniska meddelanden som inhämtats enligt avsnitt 702 i FISA kom från Prism-programmet, medan mindre än 10 procent kom från Upstream. Se FISC, *Memorandum Opinion*, 2011 WL 10945618 (FISA Ct., 3.10.2011), nr 21 (http://www.dni.gov/files/documents/0716/October-2011-Bates-Opinion-and%20Order-20140716.pdf).

([90]) Se avsnitt 4(a)(ii) i PPD-28. Se även ODNI, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, juli 2014, s. 5, där följande anges: ”Policyer hos enheter inom underrättelsegemenskapen bör bidra till att förstärka befintliga analysmetoder och normer, vilket innebär att analytikerna måste sträva efter att strukturera frågor och andra söktermer och tekniker för att identifiera underrättelseuppgifter som är relevanta för ett godkänt underrättelseuppdrag eller brottsbekämpande verksamhet. Frågor om personer ska inriktas på de kategorier av underrättelseuppgifter som motsvarar ett visst behov i fråga om underrättelseverksamhet eller brottsbekämpande verksamhet, och granskning av personuppgifter som inte är relevanta för sådana behov ska minimeras.” Se t.ex. *CIA, Signals Intelligence Activities*, s. 5; *FBI, Presidential Policy Directive 28 Policies and Procedures*, s. 3. Enligt rapporten *2016 Progress Report on the Signals Intelligence Reform*, har enheter inom underrättelsegemenskapen (inklusive FBI, CIA och NSA) vidtagit åtgärder för att utbilda sin personal i kraven i PPD-28 genom att inrätta nya eller ändra befintliga utbildningspolicyer.

([91]) Enligt ODNI:s utfästelser gäller dessa restriktioner oberoende av om uppgifterna har insamlats i bulk eller genom riktad insamling, och oberoende av den enskildes nationalitet.

(85) Förenta staternas regering har förklarat att detta skälighetskrav innebär att enheter inom underrättelsegemenskapen inte ska vidta ”teoretiskt möjliga åtgärder”, utan ska ”balansera insatserna när det gäller att skydda legitima intressen rörande integritetsskydd och medborgerliga friheter med signalspaningsverksamhetens praktiska behov” ([92]). I detta avseende kommer utländska medborgare att behandlas på samma sätt som Förenta staternas medborgare, enligt de förfaranden som har godkänts av justitieministern ([93]).

(86) Enligt dessa regler begränsas lagringen vanligen till högst fem år, om det inte finns särskilda lagbestämmelser eller ett uttryckligt avgörande från den nationella underrättelsetjänsten, efter en noggrann utvärdering av integritetsskyddet – med beaktande av åsikterna från ODNI:s tjänsteman med ansvar för skyddet av medborgerliga friheter samt underrättelsetjänstens tjänstemän med ansvar för integritetsskydd och medborgerliga friheter – om att fortsatt lagring ligger i den nationella säkerhetens intresse ([94]). Spridning begränsas till fall där informationen är relevant för det underliggande syftet med insamlingen och således motsvarar ett godkänt behov i fråga om utländsk underrättelseverksamhet eller brottsbekämpande verksamhet ([95]).

(87) Enligt de garantier som getts av Förenta staternas regering får personuppgifter inte spridas enbart på grund av att den berörda personen inte är medborgare i Förenta staterna, och ”signalspaning som riktas mot en utländsk persons rutinmässiga aktiviteter anses inte utgöra utländska underrättelseuppgifter som kan spridas eller lagras permanent endast på grundval av detta faktum, om spaningen inte på annat sätt motsvarar ett godkänt krav rörande utländska underrättelseuppgifter” ([96]).

(88) På grundval av allt som anförts ovan drar kommissionen slutsatsen att Förenta staterna har regler som är utformade för att se till att eventuella ingrepp av skäl som rör nationell säkerhet i de grundläggande rättigheterna för de personer vars personuppgifter överförs från EU till Förenta staterna inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna begränsas till vad som är absolut nödvändigt för att uppnå det legitima målet i fråga.

(89) Som analysen ovan har visat säkerställer Förenta staternas lagstiftning att övervakningsåtgärder kommer att användas endast för att inhämta utländska underrättelseuppgifter – vilket är ett legitimt policymål ([97]) – och att

([92]) Se ODNI:s utfästelser (bilaga VI).

([93]) Se avsnitt 4(a)(i) i PPD-28 samt avsnitt 2.3 i E.O. 12333.

([94]) Avsnitt 4(a)(ii) i PPD-28. ODNI:s utfästelser (bilaga VI), s. 7. Till exempel personuppgifter som samlats in enligt avsnitt 702 i FISA. NSA:s FISC-godkända minimeringsförfaranden föreskriver att metadata och ej utvärderat innehåll för Prism i regel lagras i högst fem år, medan Upstream-uppgifter lagras i högst två år. NSA uppfyller dessa lagringskrav genom en automatisk process som raderar insamlade uppgifter i slutet av respektive lagringsperiod. Se NSA avsnitt 702, *FISA Minimization Procedures,* avsnitt 7 samt avsnitt 6(a)(1); Se NSA CLPO, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702,* 16.4.2014. Likaså begränsas lagring enligt avsnitt 501 i FISA (f.d. avsnitt 215 *U.S. PATRIOT ACT*) till fem år, om inte personuppgifterna i fråga ingår i vederbörligen godkänd spridning av utländska underrättelseuppgifter, eller om justitieministeriet skriftligen informerar NSA om att registren omfattas av lagringskrav med anledning av en pågående eller väntad rättstvist. Se NSA, CLOP, *Transparency Report: The Förenta staterna Freedom Act Business Records FISA Implementation,* 15.1.2016.

([95]) Särskilt när det gäller avsnitt 501 i FISA (f.d. avsnitt 215 *U.S. PATRIOT ACT*) får personuppgifter endast spridas för att bekämpa terrorism eller om de är bevis för brott. När det gäller avsnitt 702 i FISA får spridning endast ske inom ramen för ett giltigt ändamål som rör utländsk underrättelseverksamhet eller brottsbekämpning. Se NSA CLPO, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702,* 16.4.2014. *Transparency Report*: *The Förenta staterna Freedom Act Business Records FISA Implementation,* 15.1.2016. Se även *NSA's Civil Liberties and Privacy Protections for Targeted SIGINT Activities under Executive Order 12333,* 7.10.2014.

([96]) ODNI:s utfästelser (bilaga VI), s. 7 (med hänvisning till *Intelligence Community Directive* (ICD) 203).

([97]) Domstolen har klargjort att nationell säkerhet utgör ett legitimt policymål. Se Schrems-målet, punkt 88. Se även *Digital Rights Ireland and Others*, punkterna 42–44 och 51, där domstolen fann att kampen mot grov brottslighet, i synnerhet organiserad brottslighet och terrorism, i stor utsträckning kan vara beroende av användningen av moderna utredningstekniker. Till skillnad från vad som gäller för brottsutredningar, som vanligen handlar om att retroaktivt fastställa ansvar och skuld för tidigare beteende, är underrättelseverksamhet dessutom ofta inriktad på att förebygga hot mot den nationella säkerheten innan någon skada har skett. Sådana utredningar kan därför ofta behöva omfatta ett bredare spektrum av aktörer (”mål”) och ett större geografiskt område. Se ECtHR, *Weber and Saravia v. Germany,* beslut av den 29.06.2006, ansökan nr 54934/00, punkterna 105–118 (om så kallad ”strategisk övervakning”).

de kommer att vara anpassade så långt det är möjligt. I synnerhet kommer bulkinsamling att godkännas endast i undantagsfall där riktad insamling inte är möjlig, och den kommer att åtföljas av ytterligare garantier för att minimera mängden insamlade uppgifter och efterföljande åtkomst (som måste vara riktad och endast medges för särskilda ändamål).

(90) I kommissionens bedömning överensstämmer detta med den standard som domstolen fastställde i *Schrems*-målet, enligt vilken lagstiftning som innebär ett ingrepp i de grundläggande rättigheter som garanteras av artiklarna 7 och 8 i stadgan måste slå fast ”minimikrav” ([98]) och att den ”inte är begränsad till vad som är strängt nödvändigt när den generellt tillåter lagring av samtliga personuppgifter om alla personer vilkas uppgifter har överförts från unionen till Förenta staterna, utan att det görs några åtskillnader, begränsningar eller undantag med beaktande av det eftersträvade syftet och utan att det föreskrivs något objektivt kriterium som gör det möjligt att avgränsa myndigheternas åtkomst till uppgifterna och att avgränsa deras senare användning till bestämda, strängt begränsade syften som kan motivera det ingrepp som såväl åtkomst som användning av uppgifterna innebär” ([99]). Inte heller kommer det att förekomma obegränsad insamling och lagring av uppgifter om alla personer utan några begränsningar, och inte heller obegränsad åtkomst. De utfästelser som kommissionen mottagit, däribland en försäkran om att Förenta staternas signalspaningsverksamhet berör endast en bråkdel av den kommunikation som sker via internet, utesluter dessutom att det skulle förekomma ”generell” ([100]) åtkomst till innehållet i elektronisk kommunikation.

3.1.2 Effektivt rättsligt skydd

(91) Kommissionen har bedömt både de tillsynsmekanismer som finns i Förenta staterna när det gäller eventuella ingrepp från Förenta staternas underrättelsemyndigheters sida i personuppgifter som överförs till Förenta staterna och de möjligheter som finns för registrerade i EU att ansöka om individuell gottgörelse.

Tillsyn

(92) Förenta staternas underrättelsegemenskap är föremål för olika granskning- och tillsynsmekanismer som ombesörjs av statens tre grenar. Dessa omfattar interna och externa organ inom den verkställande grenen, ett antal kongressutskott samt rättslig tillsyn, särskilt med avseende på verksamhet som lyder under *Foreign Intelligence Surveillance Act*.

(93) För det första är underrättelseverksamhet som bedrivs av Förenta staternas myndigheter föremål för omfattande tillsyn som utförs inom den verkställande grenen.

(94) Enligt avsnitt 4(a)(iv) i PPD-28 ska policyer och förfaranden hos enheter inom underrättelsegemenskapen ”innehålla lämpliga åtgärder för att underlätta tillsyn över genomförandet av garantier för personuppgiftsskydd”. Dessa åtgärder bör omfatta regelbundna granskningar ([101]).

([98]) Schrems-målet, punkt 91, med ytterligare hänvisningar.
([99]) *Schrems*-målet, punkt 93.
([100]) Schrems-målet, punkt 94.
([101]) ODNI, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, s. 7. Se t.ex. *CIA, Signals Intelligence Activities*, s. 6 (*Compliance*); *FBI, Presidential Policy Directive 28 Policies and Procedures*, avsnitt III (A)(4), (B)(4); *NSA, PPD-28 Section 4 Procedures, 12.1.2015*, avsnitt 8.1, 8.6(c).

(95) Flera tillsynsnivåer har införts i detta avseende, bland annat tjänstemän med ansvar för medborgerliga friheter eller för integritetsskydd, generalinspektörer, *ODNI Civil Liberties and Privacy Office*, styrelsen för tillsyn av personlig integritet och medborgerliga fri- och rättigheter (PCLOB) och presidentens styrelse för tillsyn av underrättelseverksamheten (*President's Intelligence Oversight Board*). Dessa tillsynsfunktioner stöds av personal med ansvar för efterlevnadsfrågor vid alla underrättelsetjänster ([102]).

(96) Som Förenta staternas regering har förklarat ([103]) finns det *tjänstemän med ansvar för medborgerliga friheter eller integritetsskydd*, som också har tillsynsansvar, vid flera myndigheter med underrättelseansvar och underrättelsetjänster ([104]). De specifika befogenheterna för dessa tjänstemän kan variera något beroende på bemyndigande lagstiftning, men de omfattar vanligen övervakning av förfaranden för att säkerställa att respektive myndighet/tjänst beaktar integritetsskydd och medborgerliga friheter på lämpligt sätt. Lämpliga förfaranden har också införts för att behandla klagomål från enskilda personer som anser att deras integritetsskydd eller medborgerliga friheter har kränkts (och i vissa fall, t.ex. ODNI, kan de själva ha behörighet att utreda klagomål ([105])). Chefen för myndigheten/tjänsten ska i sin tur säkerställa att tjänstemännen får all information och ges åtkomst till allt material som de behöver för att kunna fullgöra sina uppgifter. Tjänstemännen med ansvar för medborgerliga friheter och integritetsskydd rapporterar regelbundet till kongressen och PCLOB, bland annat om antal och typer av klagomål som mottas av myndigheten/tjänsten, en sammanfattning av klagomålens disposition, utförda granskningar och utredningar samt effekterna av den verksamhet som bedrivs av tjänstemannen ([106]). Enligt den bedömning som genomförts av de nationella dataskyddsmyndigheterna kan den interna tillsyn som utövas av tjänstemännen med ansvar för medborgerliga friheter och integritetsskydd betraktas som "tämligen robust", även om tjänstemännen, enligt dataskyddsmyndigheternas åsikt, inte i tillräcklig grad uppfyller kravet på oberoende ([107]).

(97) Dessutom har varje enhet underrättelsegemenskapen sin egen *generalinspektör*, som bland annat ansvarar för tillsynen över utländsk underrättelseverksamhet ([108]). Detta inbegriper, inom ODNI, ett generalinspektörskontor med omfattande behörighet för hela underrättelsegemenskapen och befogenhet att utreda klagomål eller information om påstått olagligt handlande eller maktmissbruk i samband med ODNI:s och/eller underrättelsegemenskapens program och verksamheter ([109]). Generalinspektörerna är lagstadgat oberoende ([110]) enheter med ansvar för att utföra granskningar och utredningar som rör de program och verksamheter som genomförs av respektive underrättelsetjänst för nationella underrättelseändamål, även när det gäller missbruk eller överträdelse av lagstiftningen ([111]). De har rätt att få åtkomst till alla register, rapporter, revisioner, granskningar, dokument, skrivelser, rekommendationer och annat relevant material, vid behov genom föreläggande, och får ta upp

([102]) NSA sysselsätter t.ex. över 300 personer som arbetar med efterlevnadsfrågor vid sitt direktorat för efterlevnad. Se ODNI:s utfästelser (bilaga VI), s. 7.

([103]) Se ombudsmannamekanismen (bilaga III), avsnitt 6(b) (i) till (iii).

([104]) Se 42 U.S.C. § 2000ee-1. Detta omfattar t.ex. *Department of State, Department of Justice* (inklusive FBI), *Department of Homeland Security, Department of Defense*, NSA, CIA och ODNI.

([105]) Förenta staternas regering förklarar att om ODNI:s *Civil Liberties and Privacy Office* (CLPO) mottar ett klagomål kommer det också att samordna arbetet med andra enheter inom underrättelsegemenskapen om hur klagomålet bör behandlas vidare inom underrättelsegemenskapen. Se ombudsmannamekanismen (bilaga III), avsnitt 6(b) (ii).

([106]) Se 42 U.S.C. § 2000ee-1 (f)(1),(2).

([107]) Artikel 29-gruppen (arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter), yttrande 01/2016 om skölden för skydd av privatlivet i EU och Förenta staterna, utkastet till beslut om adekvat skyddsnivå (antaget den 13 april 2016), s. 41.

([108]) ODNI:s utfästelser (bilaga VI), s. 7. Se t.ex. NSA, PPD-28 *Section 4 Procedures*, 12.1.2015, avsnitt 8.1; *CIA, Signals Intelligence Activities*, s. 7 (*Responsibilities*).

([109]) Denna generalinspektör (befattningen inrättades i oktober 2010) utses av presidenten med senatens bekräftelse, och kan endast avsättas av presidenten, inte av DNI.

([110]) Generalinspektörerna har fast anställning och kan endast avsättas av presidenten, som måste informera kongressen skriftligen om skälen till ett sådant avsättande. Detta betyder inte nödvändigtvis att de arbetar helt utan instruktioner. I vissa fall får myndighetschefen förbjuda generalinspektören att inleda, genomföra eller slutföra en granskning eller utredning om så anses nödvändigt för att tillvarata viktiga nationella (säkerhets)intressen. Kongressen måste dock informeras om utövandet av denna befogenhet och kan på denna grundval ställa respektive generalinspektör till svars. Se t.ex. *Inspector General Act of 1978*, § 8 (*IG of the Department of Defense*); § 8E (*IG of the DOJ*), § 8G (d)(2)(A),(B) (*IG of the NSA*); 50. U.S.C. § 403q (b) (*IG for the CIA*); *Intelligence Authorization Act For Fiscal Year 2010*, Sec 405(f) (*IG for the Intelligence Community*). Enligt den bedömning som genomförts av de nationella dataskyddsmyndigheterna "*uppfyller generalinspektörerna sannolikt kriteriet avseende organisatoriskt oberoende såsom detta definierats av Europeiska unionens domstol och Europeiska domstolen för de mänskliga rättigheterna (ECtHR), åtminstone från och med den tidpunkt då den nya utnämningsprocessen gäller för alla*." Se artikel 29-gruppen (arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter), yttrande 01/2016 om skölden för skydd av privatlivet i EU och Förenta staterna, utkastet till beslut om adekvat skyddsnivå (antaget den 13 april 2016), s. 40.

([111]) Se ODNI:s utfästelser (bilaga VI), s. 7. Se även *Inspector General Act* från 1978, i dess ändrade lydelse, Pub. L. 113–126 of 7.07.2014.

vittnesmål ([112]). Generalinspektörerna kan endast utfärda icke-bindande rekommendationer om korrigerande åtgärder, men deras rapporter, även om uppföljningsåtgärder (eller avsaknad av sådana), offentliggörs och överlämnas dessutom till kongressen, som kan utöva sin tillsynsbefogenhet på denna grundval ([113]).

(98) Dessutom har *styrelsen för tillsyn av personlig integritet och medborgerliga friheter (Privacy and Civil Liberties Oversight Board)*, en oberoende myndighet ([114]) inom den verkställande grenen som består av en styrelse ([115]), stödd av två partier, med fem ledamöter som utses av presidenten för en fast mandatperiod på sex år med senatens godkännande, anförtrotts ansvar när det gäller förfaranden för terrorismbekämpning och genomförandet av dessa, med målet att skydda integriteten och de medborgerliga fri- och rättigheterna. I sin granskning av underrättelsegemenskapens verksamhet har den rätt att få åtkomst till underrättelsetjänsternas relevanta register, rapporter, revisioner, granskningar, dokument, skrivelser och rekommendationer, inklusive sekretessbelagd information, och får genomföra intervjuer och ta upp vittnesmål. Styrelsen får rapporter från tjänstemän med ansvar för medborgerliga friheter eller integritetsskydd vid flera federala myndigheter/underrättelsetjänster ([116]), kan utfärda rekommendationer till dem och rapporterar regelbundet till kongressutskott och till presidenten ([117]). Styrelsen ska också, inom ramen för sitt mandat, utarbeta en rapport med en bedömning av genomförandet av PPD-28.

(99) Dessutom kompletteras de tidigare nämnda tillsynsmekanismerna med *styrelsen för tillsyn av underrättelseverksamhet* (*Intelligence Oversight Board*), som inrättats inom ramen för presidentens rådgivande styrelse för underrättelseverksamhet (*Intelligence Advisory Board*). Denna styrelse har i uppdrag att övervaka Förenta staternas underrättelsemyndigheternas efterlevnad av konstitutionen och alla tillämpliga regler.

(100) För att underlätta tillsynen uppmuntras enheterna inom underrättelsegemenskapen att utforma informationssystem för att möjliggöra övervakning, registrering och granskning av förfrågningar eller andra sökningar avseende personuppgifter ([118]). Tillsyns- och efterlevnadsorganen kontrollerar regelbundet de metoder som tillämpas av enheter inom underrättelsegemenskapen för att skydda personuppgifter i signalspaning och hur de efterlever sådana förfaranden ([119]).

(101) Dessa tillsynsfunktioner stöds dessutom av omfattande rapporteringskrav i fråga om bristande efterlevnad. Underrättelsetjänsternas måste i sina förfaranden särskilt säkerställa att allvarliga fall av bristande efterlevnad som omfattar personuppgifter för alla personer, oavsett nationalitet, som samlats in genom signalspaning, omedelbart ska rapporteras till chefen för den berörda enheten inom underrättelsegemenskapen, som i sin tur kommer att informera chefen för den nationella underrättelsetjänsten. Denne ska enligt PPD-28 fastställa om korrigerande åtgärder är nödvändiga ([120]). Enligt E.O. 12333 är dessutom alla enheter inom underrättelsegemenskapen skyldiga att rapportera fall av bristande efterlevnad till styrelsen för tillsyn av underrättelseverksamheten ([121]). Dessa mekanismer säkerställer att sådana frågor behandlas på högsta nivå inom underrättelsegemenskapen. Om det rör

([112]) Se lagen om generalinspektörer från 1978, § 6.
([113]) Se ODNI:s utfästelser (bilaga VI), s. 7. Se även lagen om generalinspektörer från 1978, §§ 4(5), 5. Enligt avsnitt 405(b)(3),(4) i Intelligence Authorization Act For Fiscal Year 2010, Pub. L. 111–259, 7.10.2010, ska generalinspektören för underrättelsegemenskapen hålla såväl DNI som kongressen informerade om behovet av, och framstegen med, korrigerande åtgärder.
([114]) Enligt de nationella dataskyddsmyndigheternas bedömning har PCLOB tidigare ”demonstrerat sitt oberoende utövande av sina befogenheter”. Se artikel 29-gruppen (arbetsgruppen för skydd av enskilda med avseende på behandlingen av personuppgifter), yttrande 01/2016 om skölden för skydd av privatlivet i EU och Förenta staterna, utkastet till beslut om adekvat skyddsnivå (antaget den 13 april 2016), s. 42.
([115]) Styrelsen har dessutom cirka 20 fast anställda. Se https://www.pclob.gov/about-us/staff.html
([116]) Dessa inkluderar minst *Department of Justice, Department of Defense, Department of Homeland Security, Director of National Intelligence* och *Central Intelligence Agency*, plus eventuella andra ministerier, myndigheter eller enheter i den verkställande grenen som PCLOB anser bör omfattas.
([117]) Se 42 U.S.C. § 2000ee. Se även ombudsmannamekanismen (bilaga III), avsnitt 6(b) (iv). PCLOB har bland annat skyldighet att rapportera när ett organ under den verkställande grenen underlåter att följa dess rekommendationer.
([118]) ODNI, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, s. 7–8.
([119]) Idem, s. 8. Se även ODNI:s utfästelser (bilaga VI), s. 9.
([120]) ODNI, *Safeguarding the Personal Information of all People: A Status Report on the Development and Implementation of Procedures under Presidential Policy Directive 28*, s. 7. Se t.ex. NSA, PPD-28 Section 4 Procedures, 12.1.2015, avsnitt 7.3, 8.7(c). *FBI, Presidential Policy Directive 28 Policies and Procedures*, avsnitt III (A)(4), (B)(4); *CIA, Signals Intelligence Activities*, s. 6 (*Compliance*) och s. 8 (*Responsibilities*).
([121]) Se E.O. 12333, avsnitt 1.6(c).

sig om personer som inte är medborgare i Förenta staterna ska chefen för den nationella underrättelsetjänsten, i samråd med utrikesministern och chefen för det anmälande ministeriet eller den anmälande myndigheten, avgöra om åtgärder bör vidtas för att meddela den berörda utländska regeringen, med beaktande av källskyddet samt skyddet av metoder och Förenta staternas personal ([122]).

(102) För det andra, förutom dessa tillsynsmekanismer inom den verkställande grenen, har Förenta staternas kongress, särskilt *House and Senate Intelligence and Judiciary Committees*, tillsynsansvar när det gäller all utländsk underrättelseverksamhet som bedrivs av Förenta staterna, inbegripet Förenta staternas signalspaning. Enligt *National Security Act*"ska presidenten säkerställa att kongressens utskott för underrättelseverksamhet hålls fullständigt och fortlöpande informerade om Förenta staternas underrättelseverksamhet, bland annat eventuell viktig planerad underrättelseverksamhet enligt vad som krävs i detta underkapitel" ([123]). Det anges även att "presidenten ska säkerställa att eventuell olaglig underrättelseverksamhet samt eventuella korrigerande åtgärder som har vidtagits eller planeras i samband med sådan olaglig verksamhet omedelbart rapporteras till kongressens underrättelseutskott" ([124]). Ledamöterna av dessa utskott har tillgång till sekretessbelagd information samt information om underrättelsemetoder och underrättelseprogram ([125]).

(103) Rapporteringskraven har utökats och förbättrats genom senare lagstiftning, både när det gäller enheter inom underrättelsegemenskapen, berörda generalinspektörer och justitieministern. Enligt FISA ska justitieministern t.ex. "fullständigt informera" senatens och representanthusets utskott för underrättelseverksamhet respektive rättsväsendet om regeringens verksamheter enligt vissa avsnitt i FISA ([126]). Lagstiftningen föreskriver också att regeringen ska förse kongresskommittéerna med "kopior av alla beslut, föreskrifter eller yttranden som utfärdas av *Foreign Intelligence Surveillance Court* eller *Foreign Intelligence Surveillance Court of Review* och som innehåller viktiga diskussioner om eller tolkningar" av FISA-bestämmelser. När det gäller övervakning enligt avsnitt 702 i FISA utövas tillsynen genom obligatoriska rapporter till kommittéerna för underrättelseverksamhet respektive rättsväsendet samt täta genomgångar och utfrågningar. Dessa inbegriper en halvårsrapport från justitieministern om tillämpningen av avsnitt 702 i FISA med styrkande dokument, särskilt justitieministeriets och ODNI:s efterlevnadsrapporter och en redogörelse för eventuella fall av bristande efterlevnad ([127]) och en separat halvårsbedömning av justitieministern och DNI om efterlevnaden av förfarandena för målinriktning och minimering samt efterlevnaden av de förfaranden som har tagits fram för att se till att insamlingen sker för ett godkänt ändamål i fråga om utländska underrättelseuppgifter ([128]). Kongressen får också rapporter från generalinspektörer som är behöriga att utvärdera underrättelsetjänsternas efterlevnad av förfarandena för målinriktning och minimering samt justitieministerns riktlinjer.

(104) Enligt *Förenta staterna FREEDOM Act* från 2015 måste Förenta staternas regering varje år till kongressen (och allmänheten) lämna ut information om antalet FISA-förelägganden och direktiv som har sökts och beviljats samt bland annat uppskattningar av antalet utländska medborgare och medborgare i Förenta staterna som är föremål för övervakning ([129]). Lagen kräver dessutom ytterligare offentlig rapportering om antalet utfärdade nationella

([122]) PPD-28, avsnitt 4(a)(iv).
([123]) Se avsnitt 501(a)(1) (50 U.S.C. § 413(a)(1)). Denna bestämmelse innehåller de allmänna kraven när det gäller kongressens tillsyn inom området nationell säkerhet.
([124]) Se avsnitt 501(b) (50 U.S.C. § 413(b)).
([125]) Se avsnitt 501(d) (50 U.S.C. § 413(d)).
([126]) Se 50 U.S.C. §§ 1808, 1846, 1862, 1871, 1881f.
([127]) Se 50 U.S.C. § 1881f.
([128]) Se 50 U.S.C. § 1881a(l)(1).
([129]) Se *Förenta staterna FREEDOM Act* från 2015, Pub. L. nr 114–23, avsnitt 602(a). Enligt avsnitt 402 ska "chefen för den nationella säkerhetstjänsten, i samråd med justitieministern, göra en granskning om hävande av sekretess för varje beslut, föreskrift eller yttrande som utfärdas av *Foreign Intelligence Surveillance Court* eller the *Foreign Intelligence Surveillance Court of Review* (enligt definitionen i avsnitt 601(e)), och som innehåller viktiga diskussioner om eller tolkningar av lagbestämmelser, även eventuella nya eller viktiga diskussioner om och tolkningar av begreppet "specifik urvalsterm" och, i enlighet med denna granskning, i största möjliga utsträckning göra sådana beslut, föreskrifter eller yttranden allmänt tillgängliga".

säkerhetsskrivelser, även här både rörande Förenta staternas medborgare och utländska medborgare (samtidigt får mottagare av FISA-beslut och certifieringar samt NSL-förfrågningar utfärda insynsrapporter på vissa villkor) ([130]).

(105) För det tredje ska underrättelseverksamhet som bedrivs av Förenta staternas offentliga myndigheter på grundval av FISA medge granskning, och i vissa fall förhandsgodkännande av åtgärderna, av *domstolen för övervakning av utländsk underrättelseinformation* (FISC) ([131]), en oberoende domstol ([132]) vars beslut kan bestridas inför *Foreign Intelligence Court of Review* (FISCR) ([133]) och, i sista hand, Förenta staternas högsta domstol ([134]). När det gäller förhandsgodkännande måste de begärande myndigheterna (FBI, NSA, CIA osv.) lämna ett utkast till ansökan till juristerna vid justitieministeriets avdelning för nationell säkerhet, som kommer att kontrollera den och vid behov kräva ytterligare information ([135]). När ansökan har färdigbehandlats måste den godkännas av justitieministern, vice justitieministern eller den biträdande ministern för nationell säkerhet ([136]). Justitieministeriet lämnar sedan ansökan till FISC, som bedömer den och fattar ett preliminärt beslut om hur man bör gå till väga ([137]). Om en utfrågning genomförs är FISC behörig att ta upp vittnesmål, vilket kan omfatta råd från sakkunniga ([138]).

(106) FISC (och FISCR) stöds av en permanent arbetsgrupp som består av fem personer med sakkunskap i nationella säkerhetsfrågor och medborgerliga friheter ([139]). Från denna grupp ska domstolen utse en person som ska agera som sakkunnig för att bistå i övervägandet av ansökningar om beslut eller granskning som, enligt domstolens åsikt, utgör en ny eller väsentlig lagtolkning, om inte domstolen finner att det är olämpligt att utse en sakkunnig ([140]). Syftet med detta är särskilt att se till att integritetsöverväganden avspeglas på lämpligt sätt i domstolens bedömningar. Domstolen kan utse en person eller en organisation som sakkunnig, även för tekniska frågor, om den anser att så är lämpligt, eller, på förslag tillåta att en person eller en organisation inger en sakkunnigrapport ([141]).

([130]) *Förenta staterna FREEDOM Act*, avsnitt 602(a), 603(a).

([131]) För vissa typer av övervakning kan alternativt en fredsdomare i Förenta staterna som officiellt utsetts av chefsdomaren i Förenta staternas högsta domstol vara behörig att behandla ansökningar och bevilja beslut.

([132]) FISC består av elva domare som utses av chefsdomaren i Förenta staternas högsta domstol bland tjänstgörande domare vid Förenta staternas distriktsdomstolar, som tidigare har utsetts av presidenten och bekräftats av senaten. Domarna sitter på livstid, kan endast avsättas på goda grunder och tjänstgör vid FISC i perioder med en förskjutning på sju år. Enligt FISA ska domarna väljas ut från minst sju olika domsagor i Förenta staterna. Se avsnitt 103 i FISA (50 U.S.C. 1803 (a)), PCLOB, avsnitt PCLOB avsnitt 215 *Report*, s. 174–187. Domarna stöds av erfarna rättssekreterare som utgör domstolens juridiska personal och utarbetar rättsliga analyser av ansökningar om insamling. Se PCLOB, avsnitt 215 *Report*, s. 178. Skrivelse från Reggie B. Walton, ordförande, Förenta staternas domstol för övervakning av utländsk underrättelseinformation, till Patrick J. Leahy, ordförande, kommittén för rättsväsendet, Förenta staternas senat (29 juli 2013) ("Walton-skrivelsen"), s. 2–3.

([133]) FISCR består av tre domare som utses av chefsdomaren i Förenta staternas högsta domstol och väljs från distriktsdomstolar i Förenta staterna eller appellationsdomstolar. De tjänstgör i perioder med en förskjutning på sju år. Se avsnitt 103 i FISA (50 U.S.C. § 1803 (b)).

([134]) Se 50 U.S.C. §§ 1803 (b), 1861 a (f), 1881 a (h), 1881 a (i)(4).

([135]) Exempelvis ytterligare uppgifter om övervakningsmålet, teknisk information om övervakningsmetoden eller garantier för hur den inhämtade informationen kommer att användas eller spridas. Se PCLOB, avsnitt 215 *Report*, s. 177.

([136]) 50 U.S.C. §§ 1804 (a), 1801 (g).

([137]) FISC kan godkänna ansökan, begära ytterligare information, besluta att det krävs en utfrågning eller förklara att ansökan bör avslås. Regeringen utformar sin slutliga ansökan på grundval av detta preliminära avgörande. Ansökan kan innehålla väsentliga ändringar av den ursprungliga ansökan på grundval av domarens preliminära synpunkter. Även om en stor andel av de slutliga ansökningarna godkänns av FISC innehåller många av dem väsentliga ändringar av den ursprungliga ansökan. Av de ansökningar som godkändes under perioden juli–september 2013 hade t.ex. väsentliga ändringar gjorts av 24 procent av ansökningarna. Se PCLOB, avsnitt 215 *Report*, s. 179; Se Walton-skrivelsen, s. 3.

([138]) PCLOB avsnitt 215 Report, s.179, nr 619.

([139]) 50 U.S.C. § 1803 (i)(1),(3)(A). Denna nya lagstiftning genomför rekommendationer från PCLOB för att inrätta en pool av experter på integritetsskydd och medborgerliga friheter som kan agera som sakkunniga i syfte att bistå domstolen med juridiska argument för främjande av integritetsskydd och medborgerliga friheter. Se PCLOB, avsnitt 215 Report, s. 183–187.

([140]) 50 U.S.C. § 1803 (i)(2)(A). Enligt uppgifter från ODNI har sådana utnämningar redan gjorts. Se *Signals Intelligence Reform, 2016 Progress Report*.

([141]) 50 U.S.C. § 1803 (i)(2)(B).

(107) FISC:s tillsyn skiljer sig när det gäller de två rättsliga befogenheter för övervakning enligt FISA som är viktigast för överföringar av uppgifter enligt skölden för skydd av privatlivet i EU och Förenta staterna.

(108) Enligt avsnitt 501 i FISA ([142]), enligt vilket insamling av ”alla konkreta föremål (inklusive böcker, register, skrivelser, dokument och andra föremål)” är tillåten, måste ansökan till FISC innehålla en faktaredogörelse som visar att det finns skäliga grunder för att anse att de konkreta föremål som eftersöks är relevanta för en godkänd utredning (förutom hotbedömningar) som genomförs för att inhämta utländska underrättelseuppgifter som inte rör Förenta staternas medborgare eller skydda nationen mot internationell terrorism eller hemlig underrättelseverksamhet. Ansökan ska även innehålla en redogörelse för de minimeringsförfaranden som har införts av justitieministern för lagring och spridning av de insamlade underrättelseuppgifterna ([143]).

(109) Enligt avsnitt 702 i FISA ([144]) godkänner FISC dock inte individuella övervakningsåtgärder, utan snarare övervakningsprogram (såsom Prism och Upstream) på grundval av årliga certifieringar som utarbetas av justitieministern och chefen för den nationella underrättelsetjänsten. Enligt avsnitt 702 i FISA är målinriktning mot personer som skäligen kan antas befinna sig utanför Förenta staterna tillåten för att inhämta utländska underrättelseuppgifter ([145]). Målinriktningen utförs av NSA i två steg: Först identifierar NSA:s analytiker de personer som inte är medborgare i Förenta staterna som befinner sig utomlands och av vilka övervakningen, enligt analytikerns bedömning, kommer att ge de relevanta utländska underrättelseuppgifter som anges i certifieringen. Därefter, när dessa enskilda personer har identifierats och målinriktningen har godkänts genom en grundlig granskningsmekanism inom NSA ([146]) avdelas urvalstermer för att identifiera kommunikationsmedel (t.ex. e-postadresser) som används av målen ([147]). Som påpekats innehåller de certifieringar som ska godkännas av FISC inte någon information om de enskilda personer som målinriktningen gäller, utan anger snarare kategorier av utländska underrättelseuppgifter ([148]). FISC bedömer inte – enligt trolig orsak eller någon annan norm – huruvida målinriktningen för de utvalda personerna är lämplig för att inhämta utländska underrättelseuppgifter ([149]), utan kontrollen rör villkoret att ”ett viktigt syfte med insamlingen är att erhålla utländska underrättelseuppgifter” ([150]). Enligt avsnitt 702 i FISA får NSA endast samla in meddelanden från utländska medborgare utanför Förenta staterna om det skäligen kan antas att ett visst kommunikationsmedel används för att kommunicera utländsk underrättelseinformation (som t.ex. är relaterad till internationell terrorism, kärnvapenspridning eller fientlig internetverksamhet. Sådana avgöranden är föremål för rättslig granskning ([151]). Certifieringarna måste även omfatta förfaranden för målinriktning och minimering ([152]). Justitieministern och chefen för den nationella underrättelsetjänsten kontrollerar efterlevnaden, och underrättelsetjänsterna är skyldiga att rapportera eventuella

([142]) 50 U.S.C. § 1861.
([143]) 50 U.S.C. § 1861 (b).
([144]) 50 U.S.C. § 1881.
([145]) 50 U.S.C. § 1881a (a).
([146]) PCLOB avsnitt 702 *Report*, s. 46.
([147]) 50 U.S.C. § 1881a (h).
([148]) 50 U.S.C. § 1881a (g). Enligt PCLOB har dessa kategorier hittills främst rört internationell terrorism och frågor som förvärv av massförstörelsevapen. Se PCLOB, avsnitt 702 *Report*, s. 25.
([149]) PCLOB avsnitt 702 *Report*, s. 27.
([150]) 50 U.S.C. § 1881a.
([151]) *Liberty and Security in a Changing World*, rapport och rekommendationer från presidentens granskningsgrupp för underrättelseverksamhet och kommunikationstekniker, 12.12.2013, s. 152.
([152]) 50 U.S.C.1881a (i).

fall av bristande efterlevnad till FISC ([153]) (och till kongressen och presidentens styrelse för tillsyn av underrättelseverksamheten) ([154]).

(110) För att öka effektiviteten i FISC:s tillsyn har Förenta staternas administration dessutom samtyckt till att genomföra en rekommendation från PCLOB om att lämna dokumentation till FISC rörande beslut om målinriktning enligt avsnitt 702, inklusive ett slumpmässigt urval av checklistor, så att FISC kan bedöma hur kravet på underrättelsesyfte tillgodoses i praktiken ([155]). Samtidigt gick Förenta staternas administration med på och har vidtagit åtgärder för att granska den nationella säkerhetstjänstens förfaranden för målinriktning för att bättre dokumentera de skäl för att samla in utländska underrättelseuppgifter som ligger till grund för beslut om målinriktning ([156]).

Rättslig prövning för enskilda

(111) Förenta staternas lagstiftning föreskriver ett antal möjligheter för registrerade i EU som undrar om deras personuppgifter har behandlats (insamling, åtkomst osv) av enheter inom Förenta staternas underrättelsegemenskap, och om så är fallet, huruvida de begränsningar som är tillämpliga enligt Förenta staternas lagstiftning har följts. Dessa avser framför allt tre områden: ingrepp enligt FISA, olaglig och avsiktlig tillgång till personuppgifter av regeringstjänstemän, och tillgång till information enligt *Freedom of Information Act* (FOIA) ([157]).

(112) För det första föreskriver *Foreign Intelligence Surveillance Act* ett antal rättsmedel, som även finns tillgängliga för utländska medborgare, för att bestrida olaglig elektronisk övervakning ([158]). Till detta hör möjligheten för enskilda att åberopa civilrättsliga grunder för skadestånd mot Förenta staterna när information om dem har använts eller lämnats ut på ett olagligt och medvetet sätt ([159]), stämma enskilda tjänstemän vid Förenta staternas regering (under falska lagliga förespeglingar) och begära skadestånd ([160]), och att bestrida lagenligheten i övervakningen (och begära att informationen hemlighålls) i den händelse Förenta staternas regering har för avsikt att använda eller lämna ut information som har erhållits eller härrör från elektronisk övervakning mot den enskilde i rättsliga eller administrativa förfaranden i Förenta staterna ([161]).

(113) För det andra har den amerikanska regeringen informerat kommissionen om ett antal ytterligare möjligheter som registrerade i EU kan använda för att väcka talan mot regeringstjänstemän för olaglig åtkomst eller användning av

([153]) Enligt regel 13(b) i FISC:s arbetsordning ska regeringen omedelbart inge ett skriftligt meddelande till domstolen om den upptäcker att en befogenhet eller ett godkännande som beviljats av domstolen har genomförts på ett sätt som inte överensstämmer med domstolens beviljande eller godkännande, eller med tillämplig lag. Regeln föreskriver även att regeringen skriftligen ska underrätta domstolen om relevanta fakta och omständigheter för sådan bristande överensstämmelse. Regeringen inger vanligen ett slutligt meddelande enligt regel 13(a) först när relevanta fakta är kända och eventuell otillåten insamling har förstörts. Se Walton-skrivelsen, s. 10.

([154]) 50 U.S.C. § 1881 (l). Se även PCLOB, avsnitt 702 Report, s. 66–76; NSA CLPO, *NSA's Implementation of Foreign Intelligence Surveillance Act Section 702*, 16 april 2014. Insamling av personuppgifter för underrättelsesyften enligt avsnitt 702 i FISA är föremål för både intern och extern tillsyn inom den verkställande makten. Den interna tillsynen omfattar bland annat interna efterlevnadsprogram för att utvärdera och övervaka efterlevnaden av förfarandena för målinriktning och minimering, rapportering om fall av bristande efterlevnad, både internt och externt, till ODNI, justitieministeriet, kongressen och FISC, samt årliga granskningar som överlämnas till dessa organ. Den externa tillsynen består främst av granskningar av målinriktning och minimering som utförs av ODNI, justitieministeriet och generalinspektörerna, som i sin tur rapporterar till kongressen och FISC, även om fall av bristande efterlevnad. Allvarliga fall av bristande efterlevnad måste omedelbart rapporteras till FISC, övriga fall redovisas i en kvartalsrapport. Se PCLOB, avsnitt 702 Report, s. 66–77.

([155]) PCLOB, *Recommendations Assessment Report*, 29.1.2015, s. 20.

([156]) PCLOB, *Recommendations Assessment Report*, 29.1.2015, s. 16.

([157]) Dessutom föreskrivs i avsnitt 10 i lagen om förfaranden för sekretessbelagd information (*Classified Information Procedures Act*) att Förenta staterna, i alla åtal där det måste fastställas att materialet i fråga utgör sekretessbelagd information (t.ex. för att det måste skyddas mot obehörigt utlämnande av nationella säkerhetsskäl), måste informera den svarande om de delar av materialet som rimligen förväntas användas för att fastställa den sekretessbelagda delen av brottet.

([158]) Se ODNI:s utfästelser (bilaga VI), s. 16.

([159]) 18 U.S.C. § 2712.

([160]) 50 U.S.C. § 1810.

([161]) 50 U.S.C. § 1806.

personuppgifter från regeringens sida, inklusive i påstått nationella säkerhetssyften (*Computer Fraud and Abuse Act* ([162]), *Electronic Communications Privacy Act* ([163]) och *Right to Financial Privacy Act* ([164])). Alla dessa grunder för talan rör specifika uppgifter, mål och/eller typer av åtkomst (t.ex. fjärråtkomst till en dator via internet) och får åberopas på vissa villkor (t.ex. avsiktligt/uppsåtligt agerande, agerande utanför officiell behörighet, liden skada) ([165]). En mer allmän möjlighet till rättslig prövning finns i *Administrative Procedure Act* (5 U.S.C. § 702), enligt vilken en person som felaktigt drabbats av rättsliga åtgärder till följd av ett organs agerande eller som skadats eller förfördelats till följd av ett organs agerande, har rätt att söka rättslig prövning. Detta inbegriper möjligheten att be domstolen att hejda olagliga åtgärder och upphäva ett organs åtgärder samt avgöranden och slutsatser som anses vara godtyckliga och nyckfulla, innebära maktmissbruk eller på annat sätt oförenliga med lagstiftningen ([166]).

(114) Förenta staternas regering har slutligen hänvisat till FOIA som ett medel för utländska medborgare att ansöka om åtkomst till federala myndighetsregister, även när registren innehåller den enskildes personuppgifter ([167]). Med tanke på sin inriktning kan FOIA inte åberopas som ett rättsmedel för enskilda mot ingrepp i personuppgifter i sig, även om den i princip kan ge enskilda personer möjlighet att få åtkomst till relevant information som innehas av nationella underrättelsetjänster. Även i detta avseende förefaller möjligheterna vara begränsade, eftersom underrättelsetjänsterna kan undanhålla information som omfattas av vissa angivna undantag, inklusive åtkomst till sekretessbelagd nationell säkerhetsinformation och information som avser brottsutredningar ([168]). De nationella underrättelsetjänsternas utnyttjande av sådana undantag kan dock bestridas av enskilda personer, som kan begära både administrativ och rättslig granskning.

(115) Enskilda personer, inklusive registrerade i EU, har därför ett antal möjligheter till rättslig prövning när de har varit föremål för olaglig (elektronisk) övervakning av nationella säkerhetsskäl, och det står också klart att åtminstone några av de rättsliga grunder som Förenta staternas underrättelsemyndigheter kan tillämpa (t.ex. E.O. 12333) inte omfattas. Även om det i princip finns möjligheter för utländska medborgare att söka rättslig prövning, t.ex. rörande övervakning enligt FISA, är tillgängliga grunder för talan dock begränsade ([169]), och talan som väcks av enskilda personer (inklusive medborgare i Förenta staterna) kommer att förklaras oacceptabel när den saknar grund ([170]), vilket begränsar möjligheterna att väcka talan vid allmänna domstolar ([171]).

(116) För att ge alla registrerade i EU en ytterligare möjlighet att söka rättslig prövning har Förenta staternas regering beslutat att inrätta en ny ombudsmannamekanism, vilket beskrivs i den skrivelse från Förenta staternas utrikesminister till kommissionen som finns i bilaga III till detta beslut. Denna mekanism bygger på utnämningen av en chefssamordnare enligt PPD-28 (på statssekreterarnivå) vid utrikesdepartementet som kontaktpunkt för utländska regeringar som vill ta upp frågor angående Förenta staternas signalspaningsverksamhet, men går betydligt längre.

([162]) 18 U.S.C. § 1030.
([163]) 18 U.S.C. §§ 2701–2712.
([164]) 12 U.S.C. § 3417.
([165]) ODNI:s utfästelser (bilaga VI), s. 17.
([166]) 5 U.S.C. § 706(2)(A).
([167]) 5 U.S.C. § 552. Liknande lagar finns på statlig nivå.
([168]) Om så är fallet får den berörda personen vanligen endast ett standardsvar, där underrättelsetjänsten varken bekräftar eller förnekar förekomsten av sådana register. Se *ACLU v. CIA*, 710 F.3d 422 (D.C. Cir. 2014).
([169]) Se ODNI:s utfästelser (bilaga VI), s. 16. Enligt de förklaringar som lämnats kräver grunder för talan antingen att det föreligger *skada* (18 U.S.C. § 2712; 50 U.S.C. § 1810) eller att det måste bevisas att *regeringen har för avsikt att använda eller lämna ut information* som erhållits eller härrör från elektronisk övervakning av den berörda personen mot den personen *i rättsliga eller administrativa förfaranden* i Förenta staterna (50 U.S.C. § 1806). För att fastställa om det föreligger ett ingrepp i den grundläggande rätten till privatliv har det emellertid föga betydelse huruvida den berörda personen har fått utstå eventuella olägenheter på grund av ingreppet, vilket EU-domstolen vid upprepade tillfällen har betonat. Se Schrems-målet, punkt 87, med ytterligare hänvisningar.
([170]) Detta tillåtlighetskriterium härrör från kravet om ”mål eller tvist” (*case or controversy*) i artikel III i Förenta staternas konstitution.
([171]) Se *Clapper v. Amnesty Int'l Förenta staterna*, 133 S.Ct. 1138, 1144 (2013). När det gäller användningen av nationella säkerhetsskrivelser föreskriver *Förenta staterna Freedom Act* (avsnitt 502(f)-503) att sekretesskraven måste ses över regelbundet, och att *mottagarna* av nationella säkerhetsskrivelser ska meddelas när fakta inte längre stöder ett sekretesskrav (se ODNI:s utfästelser (bilaga VI), s. 13). Detta garanterar dock inte att registrerade i EU skulle bli informerade om de har varit föremål för en utredning.

(117) Enligt åtagandena från Förenta staternas regering kommer ombudsmannamekanismen att säkerställa att individuella klagomål utreds ordentligt och att enskilda personer får en oberoende bekräftelse av att Förenta staternas lagstiftning har följts eller, i händelse av överträdelse, att den bristande efterlevnaden har åtgärdats ([172]). Mekanismen omfattar ”ombudsmannen för skölden”, dvs. statssekreteraren och ytterligare personal samt andra tillsynsorgan som är behöriga att kontrollera de olika enheterna inom underrättelsegemenskapen på vars samarbete ombudsmannen för skölden kommer att förlita sig vid behandlingen av klagomål. När en enskild persons begäran avser övervakningens förenliget med Förenta staternas lagstiftning kommer ombudsmannen för skölden att kunna förlita sig på oberoende tillsynsorgan med utredningsbefogenheter (t.ex. generalinspektörerna eller PCLOB). I varje fall säkerställer utrikesministern att ombudsmannen har resurser för att säkerställa att svaret på en enskild begäran bygger på all nödvändig information.

(118) Genom denna ”sammansatta struktur” garanterar ombudsmansmekanismen oberoende tillsyn och enskild prövning. Samarbetet med andra tillsynsorgan säkerställer dessutom tillgång till nödvändig expertis. Genom att ålägga ombudsmannen för skölden att bekräfta efterlevnad eller avhjälpa bristande efterlevnad återspeglar mekanismen ett åtagande av Förenta staternas regering i sin helhet att ta itu med och åtgärda klagomål från enskilda i EU.

(119) För det första kommer ombudsmannen för skölden, till skillnad från en ren mellanstatlig mekanism, att motta och besvara individuella klagomål. Sådana klagomål kan göras hos medlemsstaternas tillsynsmyndigheter med behörighet för tillsyn över nationella säkerhetstjänster och/eller offentliga myndigheters behandling av personuppgifter, vilka översänder dem till ett centraliserat EU-organ varifrån de vidarebefordras till ombudsmannen för skölden ([173]). Detta gynnar i själva verket enskilda i EU, eftersom de kan vända sig till ett nationellt organ som ”finns nära” och på sitt eget språk. Detta organ kommer att ha uppgiften att hjälpa personer med att göra en begäran till ombudsmannen för skölden, så att den innehåller grundläggande information och därför kan anses vara ”fullständig”. Den enskilde behöver inte visa att Förenta staternas regering faktiskt har haft åtkomst till personuppgifterna genom signalspaning.

(120) För det andra åtar sig Förenta staternas regering att, då den utför sina uppgifter, säkerställa att ombudsmannen för skölden kan förlita sig på samarbetet med andra befintliga mekanismer för tillsyn och efterlevnadskontroll som finns i Förenta staternas lagstiftning. Detta kommer ibland att involvera nationella underrättelsemyndigheter, särskilt om begäran ska tolkas som att avse tillgång till handlingar i enlighet med *Freedom of Information Act*. I andra fall, särskilt när en begäran avser övervakningens förenlighet med Förenta staternas lagstiftning, kommer samarbetet bl.a. att omfatta oberoende tillsynsorgan (t.ex. generalinspektörer) med ansvar och behörighet att genomföra en grundlig utredning (särskilt genom tillgång till alla relevanta handlingar och befogenheten att begära information och rapporter) och att ta itu med bristande efterlevnad ([174]). Ombudsmannen för skölden kommer även att kunna hänskjuta ärenden till PCLOB för övervägande ([175]). Om bristande efterlevnad har konstaterats av en av dessa tillsynsorgan måste berörd enhet inom underrättelsegemenskapen (t.ex. en underrättelsetjänst) avhjälpa denna bristande efterlevnad, då endast detta gör det möjligt för ombudsmannen att ge ett ”positivt” svar till den enskilde (dvs. att eventuell bristande efterlevnad har avhjälpts), som Förenta staternas

([172]) Om den klagande begär tillgång till handlingar som innehas av Förenta staternas myndigheter tillämpas reglerna och förfarandena i *Freedom of Information Act*. Detta inbegriper möjligheten att söka rättslig prövning (i stället för oberoende tillsyn) om begäran avslås, i enlighet med villkoren i FOIA.

([173]) Enligt ombudsmannamekanismen (bilaga III), avsnitt 4(f), kommer ombudsmannen för skölden att kommunicera direkt med EU-organet för handläggning av klagomål, som i sin tur är ansvarig för kommunikationen med den enskilda person som lämnar in begäran. Om direkt kommunikation ingår i de ”underliggande processer” som kan ge den begärda upprättelsen (t.ex. en åtkomstförfrågan enligt FOIA, se avsnitt 5) kommer kommunikationen att ske enligt tillämpliga förfaranden.

([174]) Se ombudsmannamekanismen (bilaga III), avsnitt 2(a). Se även skälen 0–0.

([175]) Se ombudsmannamekanismen (bilaga III), avsnitt 2(c). Enligt de förklaringar som lämnats av Förenta staternas regering ska PCLOB fortlöpande granska policyer och förfaranden, och genomförandet av dem, inom Förenta staternas myndigheter med ansvar för terrorismbekämpning för att avgöra huruvida deras åtgärder skyddar integriteten och de medborgerliga fri- och rättigheterna på lämpligt sätt och är förenliga med gällande lagar, föreskrifter och policyer för integritetsskydd och medborgerliga friheter. Den ska även motta rapporter och annan information från tjänstemän med ansvar för integritetsskydd och medborgerliga rättigheter och ska vid behov lämna rekommendationer när det gäller deras verksamhet.

regering har gjort åtagande om. Som en del av samarbetet kommer ombudsmannen för skölden att informeras om resultatet av utredningen, och ombudsmannen kommer att ha möjlighet att säkerställa att den får all nödvändig information för att förbereda sitt svar.

(121) Slutligen ska ombudsmannen för skölden vara oberoende av, och således inte ta emot instruktioner från, Förenta staternas underrättelsegemenskap ([176]). Detta är av avgörande betydelse, eftersom ombudsmannen kommer att behöva ”bekräfta” att i) klagomålet har blivit ordentligt utrett och att ii) Förenta staternas relevanta lagstiftning – inklusive i synnerhet de begränsningar och garantier som anges i bilaga VI – har följts eller, vid bristande efterlevnad, sådana brister har åtgärdats. För att kunna lämna denna oberoende bekräftelse måste ombudsmannen för skölden få nödvändig information om utredningen för att kunna ge ett exakt svar på klagomålet. Dessutom har utrikesministern åtagit sig att se till att statssekreteraren kommer att fungera som ombudsman för skölden på ett objektivt sätt och fri från otillbörlig påverkan som kan påverka det svar som ska ges.

(122) På det hela taget säkerställer denna mekanism att enskilda klagomål kommer att utredas grundligt samt lösas, och att detta åtminstone när det gäller övervakning kommer att inbegripa oberoende tillsynsorgan med erforderlig expertis och utredningsbefogenheter och en ombudsman som kommer att kunna fullgöra sina uppgifter utan att utsättas för otillbörlig, särskilt politisk, påverkan. Dessutom kommer enskilda att kunna framföra klagomål utan att behöva visa, eller ens indikera, att de har varit föremål för övervakning ([177]). Mot bakgrund av dessa förhållanden är kommissionen övertygad om att det finns adekvata och effektiva garantier mot missbruk.

(123) På grundval av allt som anförts ovan drar kommissionen slutsatsen att Förenta staterna garanterar ett effektivt rättsligt skydd mot ingrepp från dess underrättelsemyndigheter i de grundläggande rättigheterna för personer vars uppgifter överförs från unionen till Förenta staterna inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna.

(124) I detta hänseende noterar kommissionen domstolens dom i *Schrems*-målet, enligt vilken en ”lagstiftning i vilken det inte föreskrivs någon möjlighet för enskilda att använda rättsmedel för att erhålla tillgång till, rätta eller radera uppgifter som rör dem, respekterar inte det väsentliga innehållet i den grundläggande rätten till effektivt domstolsskydd, vilken är stadfäst i artikel 47 i stadgan” ([178]). Kommissionens bedömning har bekräftat att sådana rättsmedel tillhandahålls i Förenta staterna, däribland genom införandet av ombudsmannamekanismen. Ombudsmansmekanismen omfattar oberoende tillsyn med utredningsbefogenheter. Inom ramen för kommissionens fortlöpande övervakning av skölden för skydd av privatlivet, inbegripet genom den årliga gemensamma översynen som också ska involvera ombudsmannen, kommer effektiviteten i denna mekanism att omprövas.

3.2 *Tillgång till och användning av personuppgifter, av Förenta staternas offentliga myndigheter, för brottsbekämpande ändamål och andra ändamål som rör allmänintresset*

(125) När det gäller ingrepp i personuppgifter som överförs enligt skölden för skydd av privatlivet i EU och Förenta staterna har Förenta staternas regering (via justitieministeriet) visat på tillämpliga begränsningar och garantier som enligt kommissionens bedömning ger en adekvat skyddsnivå.

([176]) Se *Roman Zakharov v. Russia*, dom av den 4 december 2015 (stora avdelningen), ansökan nr 47143/06, punkt 275 (även om det i princip är önskvärt att överlåta kontrollen av tillsynen till en domare kan icke-rättsliga organs tillsyn anses vara förenlig med konventionen, förutsatt att tillsynsorganet är oberoende i förhållande till de myndigheter som utför övervakningen och ges tillräckliga och effektiva kontrollbefogenheter).

([177]) Se *Kennedy v. the United Kingdom*, dom av den 18.5.2010, ansökan nr 26839/05, punkt 167.

([178]) *Schrems*-målet, punkt 95. Såsom framgår av punkterna 91 och 96 i domen berör punkt 95 den skyddsnivå som garanteras i unionens rättsordning, i förhållande till vilken skyddsnivån i tredjelandet måste vara ”väsentligen likvärdig”. Enligt punkterna 73 och 74 i domen kräver detta inte att skyddsnivån eller de medel som detta tredjeland använder måste vara identisk, även om de medel som ska användas måste visa sig vara, i praktiken, effektiva.

(126) Enligt denna information krävs enligt fjärde tillägget till den amerikanska konstitutionen ([179]) i princip ([180]) en husrannsakningsorder från domstol, grundad på ”sannolika skäl”, för att brottsbekämpande myndigheter ska få utföra husrannsakningar och göra beslagtaganden. I de få fastställda undantagsfall där kravet på husrannsakningsorder inte gäller ([181]) är den brottsbekämpande åtgärden föremål för ett ”skälighetstest” ([182]). Huruvida husrannsakningar eller beslagtaganden är skäliga avgörs genom en bedömning av å ena sidan graden av ingrepp i en persons privatliv, och å andra sidan hur pass nödvändiga sådana åtgärder för att främja legitima statliga intressen ([183]). Mer generellt garanterar fjärde tillägget integritet och värdighet, och utgör ett skydd mot godtyckliga och inkräktande handlingar som begås av statstjänstemän ([184]). Dessa begrepp motsvarar begreppen nödvändighet och proportionalitet i unionslagstiftningen. När beslagtagna föremål inte längre behövs för brottsbekämpande ändamål ska de återlämnas ([185]).

(127) Rättigheterna enligt den fjärde ändringen omfattar visserligen inte personer från tredjeländer som inte är bosatta i Förenta staterna, men dessa åtnjuter ändå indirekt detta skydd, eftersom personuppgifterna innehas av amerikanska företag, vilket innebär att de brottsbekämpande myndigheterna i alla händelser måste söka tillstånd hos en domstol (eller åtminstone respektera kravet på skälighet) ([186]). Ytterligare skydd ges genom särskilda lagstadgade befogenheter samt av justitieministeriets riktlinjer, som begränsar brottsbekämpande myndigheters åtkomst till uppgifter på grunder som motsvarar principerna om nödvändighet och proportionalitet (t.ex. genom att kräva att FBI ska använda utredningsmetoder som inkräktar så lite som möjligt med tanke på följderna för integritetsskyddet och de medborgerliga fri- och rättigheterna) ([187]). Enligt de utfästelser som gjorts av Förenta staternas regering gäller samma eller högre skydd för brottsbekämpande myndigheters utredningar på delstatsnivå (när det gäller undersökningar som omfattas av delstatens lagar) ([188]).

(128) Även om det inte alltid krävs ett rättsligt förhandsbeslut från en domstol eller åtalsjury (domstolens utredande gren som utses av en domare eller en fredsdomare) ([189]), begränsas administrativa förelägganden till särskilda fall och är föremål för oberoende rättslig granskning, åtminstone när staten söker verkställande i domstol ([190]).

([179]) Enligt fjärde tillägget ska folkets rätt till säkerhet, till sin person, i sina hem, beträffande dokument och ägodelar, mot oskälig husrannsakan och gripande inte överträdas och inga rannsaknings- eller arresteringsorder ska utgå, utom med sannolika skäl, grundat på ed eller försäkran, och med en noggrann beskrivning av den plats som ska rannsakas och de personer som ska gripas eller föremål som ska beslagtas. (”[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”) Endast domare för utfärda rannsakningsorder. Federala rannsakningsorder för kopiering av elektroniskt lagrade uppgifter omfattas dessutom av bestämmelse 41 i Federal Rules of Criminal Procedure.

([180]) Högsta domstolen (Supreme Court) har upprepade gånger hänvisat till sökningar utan arresteringsorder som ”exceptionella”. Se bl.a. *Johnson mot Förenta staterna*, 333 U.S. 10, 14 (1948), *McDonald mot Förenta staterna*, 335 U.S. 451, 453 (1948), *Camara mot Municipal Court*, 387 U.S. 523, 528–29 (1967), *G.M. Leasing Corp. mot Förenta staterna*, 429 U.S. 338, 352–53, 355 (1977). Likaså betonar Högsta domstolen regelbundet att den mest grundläggande konstitutionella principen i detta sammanhang är att rannsakningar som genomförs utanför rättsprocessen och utan en domares förhandsgodkännande *i sig* är oskäliga enligt fjärde tillägget–, och endast omfattas av ett fåtal särskilt fastställda och väldefinierade undantag. Se bl.a. *Coolidge mot New Hampshire*, 403 U.S. 443, 454–55 (1971). *G.M. Leasing Corp. mot Förenta staterna*, 429 U.S. 338, 352–53, 358 (1977).

([181]) *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010).

([182]) PCLOB avsnitt 215 Report, s. 107, som hänvisar till *Maryland v. King*, 133 S. Ct. 1958, 1970 (2013).

([183]) PCLOB avsnitt 215 Report, s. 107, som hänvisar till *Samson v. California*, 547 U.S. 843, 848 (2006).

([184]) *City of Ontario, Cal. v. Quon*, 130 S. Ct. 2619, 2630 (2010), 2627.

([185]) Se t.ex. *Förenta staterna mot Wilson*, 540 F.2d 1100 (D.C. CIR. 1976).

([186]) Se *Roman Zakharov mot Ryssland*, dom av den 4.12.2015 (stora avdelningen), ansökan nr 47143/06, punkt 269, enligt vilken kravet att visa ett avlyssningstillstånd för tillhandahållaren av kommunikationstjänsten innan tillgång ges till en persons kommunikation är ett av de viktigaste skydden mot missbruk från de brottsbekämpande myndigheternas sida, och garanterar att vederbörligt tillstånd sökas för alla fall av avlyssning.

([187]) Justitieministeriets utfästelser (bilaga VII), s. 4 med ytterligare hänvisningar.

([188]) Justitieministeriets utfästelser (bilaga VII), nr 2.

([189]) Enligt den information kommissionen har mottagit, och förutom specifika områden som sannolikt inte är relevanta för uppgiftsöverföringar enligt skölden för skydd av privatlivet i EU och Förenta staterna (t.ex. utredningar av bedrägerier inom hälsovården, övergrepp mot barn och ärenden rörande kontrollerade ämnen), omfattar detta främst vissa befogenheter enligt lagen om elektronisk brevhemlighet, nämligen begäranden om abonnentuppgifter (18 U.S.C. § 2703(c)(1)) och om innehållet i e-postmeddelanden som är äldre än 180 dagar (18 U.S.C. § 2703(b)). I det senare fallet måste den berörda personen dock informeras och har således möjlighet att bestrida begäran i domstol. Se även översikten i Justitiedepartementets skrift *Searching and Seizing Computers and Obtaining Electronic Evidence in Criminal Investigations* (sökning och beslagtagande av datorer och elektronisk bevisning i brottsutredningar), Kap- 3: The Stored Communications Act, s. 115–138.

([190]) Enligt Förenta staternas regerings utfästelser kan personer som är föremål för administrativa förelägganden bestrida dem i domstol med motivering att de är oskäliga, till exempel för allmänt utformade eller betungande. Se justitieministeriets utfästelser (bilaga VII), s. 2.

(129) Detsamma gäller för användning av administrativa föreläggande för ändamål som rör allmänintresset. Enligt den amerikanska regeringens utfästelser gäller liknande väsentliga begränsningar eftersom myndigheterna endast får ansöka om åtkomst till uppgifter som är relevanta för de områden som omfattas av deras behörighet, och måste respektera skälighetskriteriet.

(130) Dessutom har enskilda enligt Förenta staternas lagstiftning ett antal möjligheter till domstolsprövning mot en offentlig myndighet eller dess tjänstemän, när dessa myndigheter hanterar personuppgifter. Dessa möjligheter, i synnerhet förvaltningslagen (*Administrative Procedure Act*, APA), lagen om informationsfrihet (*Freedom of Information Act*, FOIA) och lagen om integritet för elektroniska kommunikationer (*Electronic Communications Privacy Act*. ECPA), kan utnyttjas av alla enskilda, oberoende av deras nationalitet och med förbehåll för eventuella gällande villkor.

(131) Allmänt gäller att enligt bestämmelserna om rättslig prövning i förvaltningslagen (*Administrative Procedure Act*) ([191]) har den som felaktigt drabbats av rättsliga åtgärder till följd av ett organs agerande eller som skadats eller förfördelats till följd av ett organs agerande, rätt att söka rättslig prövning ([192]). Detta inbegriper möjligheten att be domstolen att hejda olagliga åtgärder och upphäva ett organs åtgärder samt avgöranden och slutsatser som anses vara godtyckliga och nyckfulla, innebära maktmissbruk eller på annat sätt vara oförenliga med lagstiftningen ([193]).

(132) Mer specifikt fastställs i avdelning II i lagen om elektronisk brevhemlighet (*Electronic Communications Privacy Act*) ([194]) ett system med lagstadgad rätt till integritet; den lagen styr brottsbekämpande myndigheters tillgång till innehållet kommunikationer via ledning, muntligen eller i elektronisk form som lagras av tredjeparts-tjänsteleverantörer ([195]). Där kriminaliseras rättsstridig tillgång (dvs. tillgång som inte godkänts av domstol eller på annat sätt är tillåten) till sådana uppgifter och ger tillgång till berörda personer möjlighet att väcka civilrättslig talan vid federal domstol i Förenta staterna för faktiska skadestånd och straffskadestånd samt skäliga lättnader eller fastställelsetalan mot en statstjänsteman som uppsåtligen har begått sådana brott, eller mot Förenta staterna.

(133) Enligt lagen om informationsfrihet (*Freedom of Information Act*, FOIA, 5 U.S.C. § 552) ska varje person ha rätt att få ut uppgifter ur federala myndighetsregister, och, om de administrativa rättsmedlen uttömts, att genomdriva denna rätt i domstol, utom i den mån som sådana register skyddas från offentliggörande av undantag eller särskilda brottsbekämpande uteslutanden ([196]).

([191]) 5 U.S.C. § 702.

([192]) Generellt omfattas endast ”slutliga” beslut – och inte ”preliminära, förfarandemässiga eller mellanliggande” beslut – av rättslig prövning. Se 5 U.S.C. § 704.

([193]) 5 U.S.C. § 706(2)(A).

([194]) 18 U.S.C. §§ 2701–2712.

([195]) ECPA skyddar kommunikation som innehas av två fastställda klasser av nättjänsteleverantörer, nämligen i) leverantörer av elektroniska kommunikationstjänster, som telefoni eller e-post, ii) och leverantörer av datatjänster som datalagring eller datahantering.

([196]) Sådana undantag är emellertid strängt begränsade. Exempelvis undantas sådana rättigheter enligt 5 U.S.C. § 552 (b)(7), FOIA för register eller uppgifter som samlats in för brottsbekämpande ändamål, men endast i sådan utsträckning att tillhandahållandet av sådana brottsbekämpningsregister eller -uppgifter A) rimligen kan väntas påverka verkställigheten, B) skulle beröva en enskild dennas rätt till rättvis rättegång eller opartisk behandling, C) rimligen kan väntas utgöra omotiverad integritetskränkning, D) rimligen kan väntas avslöja en konfidentiell källas identitet, som till exempel en statlig, lokal eller utländsk myndighet eller en privat institution som lämnat uppgifter på konfidentiella grunder, och, när det rör sig om register eller uppgifter som samlats in av en brottsbekämpande myndighet i samband med en brottsutredning eller av ett organ som utför en lagenlig underrättelseutredning för den nationella säkerheten, uppgifter som lämnats av en hemlig källa, E) skulle avslöja teknik eller förfaranden för brottsbekämpningsutredningar eller lagförings-förfaranden, eller skulle avslöja riktlinjer för brottsbekämpningsutredningar eller lagföringsförfaranden där ett sådant avslöjande rimligen kan väntas medföra kringgående av lagstiftningen, eller F) rimligen kan väntas medföra risk för enskildas liv eller fysiska säkerhet. Likaså, om en begäran görs som omfattar tillgång till registeruppgifter vars tillhandahållande rimligen kan väntas påverka verkställighetsförfarandet och – A) om utredningen eller förfarandet omfattar ett potentiellt brott mot straffrättslagstiftningen och B) det finns skäl att tro att i) den som omfattas av utredningen eller förfarandet inte känner till att utredningen eller förfarandet pågår och ii) avslöjande av registeruppgifternas existens rimligen kan förväntas påverka verkställighetsförfaranden får byrån endast under den tid som denna situation består behandla registeruppgifterna som om de inte omfattas av kraven i detta avsnitt. (5 U.S.C. § 552 (c)(1)).

(134) Dessutom ger en rad andra lagar enskilda rätt att väcka talan mot en offentlig myndighet i Förenta staterna eller mot en sådan myndighets tjänstemän, avseende hanteringen av deras personuppgifter, exempelvis avlyssningslagen (*Wiretap Act*) ([197]), lagen om datorbedrägeri (*Computer Fraud and Abuse Act*) ([198]), federala skadeståndslagen (*Federal Torts Claim Act*) ([199]), lagen om integritetsskydd för finansiella uppgifter (*Right to Financial Privacy Act*) ([200]) och lagen om rättvis kreditrapportering (*Fair Credit Reporting Act*) ([201]).

(135) Kommissionen drar därför slutsatsen att Förenta staterna har regler som är utformade för att se till att eventuella ingrepp för brottsbekämpande ändamål ([202]) eller andra ändamål som rör allmänintresset i de grundläggande rättigheterna för de personer vars personuppgifter överförs från EU till Förenta staterna inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna begränsas till vad som är absolut nödvändigt för att uppnå det legitima målet i fråga, och garanterar ett effektivt rättsligt skydd mot sådana ingrepp.

4. ADEKVAT SKYDDSNIVÅ ENLIGT SKÖLDEN FÖR SKYDD AV PRIVATLIVET I EU OCH FÖRENTA STATERNA

(136) Mot bakgrund av dessa slutsatser anser kommissionen att Förenta staterna säkerställer en adekvat skyddsnivå för skydd av personuppgifter som överförs från unionen till självcertifierade organisationer i Förenta staterna inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna.

(137) Kommissionen anser i synnerhet att de principer som utfärdats av Förenta staternas handelsministerium på det hela taget säkerställer en skyddsnivå för personuppgifter som i allt väsentligt är likvärdig med den som garanteras av de grundläggande principerna i direktiv 95/46/EG.

(138) En effektiv tillämpning av principerna garanteras dessutom genom handelsministeriets skyldigheter på insynsområdet och förvaltning av skölden för skydd av privatlivet.

(139) Kommissionen anser dessutom att de tillsynsmekanismer och de mekanismer för handläggning av klagomål som tillhandahålls genom skölden för skydd av privatlivet gör det möjligt att i praktiken upptäcka och bestraffa överträdelser av principerna som begås av organisationer som är anslutna till skölden, och att de erbjuder de registrerade rättsmedel för att få tillgång till personuppgifter som rör dem och få uppgifterna rättade eller raderade.

(140) Slutligen, och på grundval av tillgänglig information om Förenta staterna:s rättsordning, inklusive utfästelser och garantier från Förenta staternas regering, anser kommissionen att eventuella ingrepp från Förenta staternas myndigheter i de grundläggande rättigheterna för personer vars uppgifter överförs från unionen till Förenta staterna inom ramen för skölden för ändamål som rör brottsbekämpning, nationell säkerhet eller andra ändamål som rör allmänintresset, samt de påföljande begränsningar som införs för självcertifierade organisationer med avseende på deras anslutning till principerna, begränsas till vad som är absolut nödvändigt för att uppnå det legitima målet i fråga, och att det finns ett effektivt rättsligt skydd mot sådana ingrepp.

([197]) 18 U.S.C. §§ 2510 ff. Enligt *Wiretap Act* (18 U.S.C. § 2520) kan personer vars kommunikation via ledning, muntligen eller elektroniskt avlyssnas, avslöjas eller uppsåtligen används väcka civilrättslig talan för brott mot *Wiretap Act*, bland annat under vissa omständigheter mot enskilda statstjänstemän eller mot Förenta staterna. För insamling av adressuppgifter och andra uppgifter utan innehåll (t.ex. IP-adress, e-postadress till/från), se även avsnittet om "pen registers" och "trap and trace devices" i avdelning 18 (18 U.S.C. §§ 3121–3127 och, för civilmål, § 2707).

([198]) 18 U.S.C. § 1030. Enligt lagen om datorbedrägeri (*Computer Fraud and Abuse Act*) har en person rätt att väcka talan mot en person när det gäller avsiktliga intrång (eller överskridande av tillåten tillgång) i syfte att erhålla information från ett finansinstitut, ett statligt datasystem eller andra specificerade datorer, bland annat under vissa omständigheter mot enskilda statstjänstemän.

([199]) 28 U.S.C. §§ 2671 ff. Enligt skadeståndslagen (*Federal Tort Claims Act*) kan en enskild person under vissa omständigheter väcka talan mot Förenta staterna avseende statstjänstemäns försumlighet eller tjänstefel som begåtts i tjänsten.

([200]) 12 U.S.C. §§ 3401 ff. Enligt lagen om integritetsskydd för finansiella uppgifter (*Right to Financial Privacy Act*) kan en enskild person under vissa omständigheter väcka talan mot Förenta staterna avseende tillgång till eller avslöjande av finansiella uppgifter i strid med lagen. Myndigheternas tillgång till skyddade bokföring är generellt förbjuden om inte staten gör begäran på grundval av en lagligt stämning eller husrannsakningsorder eller, med vissa begränsningar, genom en formell skriftlig begäran och om den person vars uppgifter har begärts informeras om denna begäran.

([201]) 15 U.S.C. §§ 1681–1681x. Enligt lagen om rättvis kreditrapportering (*Fair Credit Reporting Act*) har en person rätt att väcka talan mot varje person som inte uppfyller kraven (i synnerhet kravet på vederbörligt tillstånd) för insamling, spridning och användning av registerutdrag om konsumentkrediter, eller, under vissa omständigheter, mot en statlig myndighet.

([202]) Domstolen har erkänt att brottsbekämpning utgör ett legitimt policymål. Se de förenade målen C-293/12 och C-594/12, *Digital Rights Ireland and Others*, EU:C:2014:238, punkt 42. Se även artikel 8.2 i Europakonventionen om de mänskliga rättigheterna och Europadomstolens dom i målet *Weber and Saravia v. Germany*, ansökan nr 54934/00, punkt 104.

(141) Kommissionen drar slutsatsen att detta uppfyller normerna i artikel 25 i direktiv 95/46/EG, tolkad mot bakgrund av Europeiska unionens stadga om de grundläggande rättigheterna, såsom EU-domstolen har förklarat, särskilt i sin dom i *Schrems*-målet.

5. DATASKYDDSMYNDIGHETERS ÅTGÄRDER SAMT INFORMATION TILL KOMMISSIONEN

(142) I sin dom i *Schrems*-målet klargjorde EU-domstolen att kommissionen inte är behörig att begränsa de befogenheter som dataskyddsmyndigheter har enligt artikel 28 i direktiv 95/46/EG (inklusive befogenheten att tillfälligt förbjuda överföringen av uppgifter), när en person i samband med en begäran i enlighet med denna bestämmelse ifrågasätter huruvida ett beslut om adekvat skyddsnivå från kommissionen är förenligt med de grundläggande rättigheterna till privatliv och dataskydd ([203]).

(143) För effektiv övervakning av hur skölden fungerar bör medlemsstaterna underrätta kommissionen om relevanta åtgärder som vidtas av dataskyddsmyndigheter.

(144) Domstolen ansåg dessutom att medlemsstaterna och deras organ, i enlighet med artikel 25.6 andra stycket i direktiv 95/46/EG, måste vidta de åtgärder som är nödvändiga för att följa rättsakter från unionens institutioner, eftersom dessa i princip antas vara lagenliga och ha rättsverkan så länge de inte har återkallats, eller förklarats vara ogiltiga efter en talan om ogiltigförklaring eller till följd av en begäran om förhandsavgörande eller invändning om rättsstridighet. Ett beslut om adekvat skyddsnivå från kommissionen som antas i enlighet med artikel 25.6 i direktiv 95/46 är följaktligen bindande för alla organ i medlemsstaterna som det riktar sig till, inklusive deras oberoende tillsynsmyndigheter ([204]). Om en sådan myndighet har mottagit ett klagomål som ifrågasätter förenligheten hos ett kommissionsbeslut om adekvat skyddsnivå med den grundläggande rätten till privatliv och dataskydd, och anser att det finns fog för de invändningar som framförts, måste den nationella lagstiftaren föreskriva rättsmedel som gör det möjligt att vid nationella domstolar göra gällande dessa invändningar; dessa domstolar är då skyldiga att vilandeförklara målet och hänskjuta en giltighetsfråga till EU-domstolen för förhandsavgörande ([205]).

6. REGELBUNDEN ÖVERSYN AV KONSTATERANDET OM ADEKVAT SKYDDSNIVÅ

(145) Mot bakgrund av omständigheten att den skyddsnivå som säkerställs genom Förenta staternas rättsordning kan komma att förändras kommer kommissionen, efter antagandet av detta beslut, att regelbundet kontrollera att konstaterandet att Förenta staterna säkerställer en adekvat skyddsnivå inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna fortfarande är sakligt och rättsligt motiverat. En sådan kontroll krävs under alla förhållanden när kommissionen får uppgifter som ger upphov till ett motiverat tvivel i detta hänseende ([206]).

(146) Kommissionen kommer därför att fortlöpande övervaka den övergripande ram för överföring av personuppgifter som skapas genom skölden för skydd av privatlivet i EU och Förenta staterna, samt hur myndigheterna i Förenta staterna efterlever de utfästelser och åtaganden som ingår i de dokument som bifogas detta beslut. För att underlätta denna process har Förenta staterna åtagit sig att informera kommissionen om väsentliga förändringar i Förenta staternas lagstiftning när detta är av relevans för skölden för skydd av privatlivet i fråga om dataskydd och de begränsningar och garantier som gäller för offentliga myndigheters tillgång till personuppgifter. Detta beslut kommer dessutom att vara föremål för en årlig gemensam översyn, som kommer att omfatta alla aspekter av hur skölden för skydd av privatlivet i EU och Förenta staterna fungerar, inbegripet tillämpningen av undantagen för nationell säkerhet och brottsbekämpning från principerna. Eftersom konstaterandet om adekvat skyddsnivå också kan påverkas av förändringar i unionens lagstiftning kommer kommissionen att bedöma skyddsnivån enligt skölden för skydd av privatlivet efter ikraftträdandet av den allmänna dataskyddsförordningen.

(147) För att genomföra den årliga gemensamma översyn som avses i bilagorna I, II och VI kommer kommissionen att hålla ett möte med handelsministeriet och FTC, vid behov åtföljda av andra ministerier och myndigheter som deltar i genomförandet av arrangemangen kring skölden för skydd av privatlivet, samt för frågor som rör nationell säkerhet, företrädare för den nationella underrättelsetjänsten, andra enheter inom underrättelsegemenskapen och ombudsmannen. Dataskyddsmyndigheter i EU och företrädare för artikel 29-arbetsgruppen kommer att kunna delta i mötet.

([203]) *Schrems*-målet, punkterna 40 ff samt punkterna 101–103.
([204]) *Schrems*-målet, punkterna 51, 52 och 62.
([205]) *Schrems*-målet, punkt 65.
([206]) *Schrems*-målet, punkt 76.

(148) Inom ramen för den årliga gemensamma översynen kommer kommissionen att begära att handelsministeriet lämnar omfattande information om alla relevanta aspekter av hur skölden för skydd av privatlivet i EU och Förenta staterna fungerar, inbegripet hänskjutanden som handelsministeriet mottagit från dataskyddsmyndigheter samt resultaten av efterlevnadskontroller som genomförts på eget initiativ. Kommissionen kommer också att söka förklaringar på eventuella frågor rörande skölden för skydd av privatlivet i EU och Förenta staterna och dess funktion utifrån alla annan tillgänglig information, inbegripet insynsrapporter enligt *Förenta staterna Freedom Act*, offentliga rapporter från Förenta staternas underrättelsemyndigheter, dataskyddsmyndigheterna, intresseorganisationer på integritetsskyddets område, rapporter från media eller andra möjliga källor. För att underlätta kommissionens arbete i detta avseende bör medlemsstaterna dessutom informera kommissionen om fall där de åtgärder som vidtagits av organ som ansvarar för att säkerställa efterlevnaden av principerna i Förenta staterna inte leder till sådan efterlevnad, och om eventuella indikationer på att åtgärder som vidtas av Förenta staternas offentliga myndigheter med ansvar för nationell säkerhet eller för förebyggande, utredning, upptäckt eller åtal av brott inte säkerställer den nödvändiga skyddsnivån.

(149) På grundval av den årliga gemensamma översynen kommer kommissionen att utarbeta en rapport till Europaparlamentet och rådet.

7. UPPHÄVANDE AV BESLUTET OM ADEKVAT SKYDDSNIVÅ

(150) Om kommissionen på grundval av kontroller eller annan tillgänglig information drar slutsatsen att skyddsnivån enligt skölden för skydd av privatlivet inte längre kan betraktas som väsentligen likvärdig med unionens, eller det finns tydliga indikationer på att en effektiv efterlevnad av principerna om integritetsskydd i Förenta staterna inte längre kan säkerställas, eller på att åtgärder som vidtas av Förenta staternas offentliga myndigheter som ansvarar för nationell säkerhet eller förebyggande, utredning, upptäckt eller åtal av brott inte säkerställer den nödvändiga skyddsnivån, kommer den att informera handelsministeriet om detta och begära att lämpliga åtgärder vidtas för att utan dröjsmål hantera eventuell bristande efterlevnad av principerna inom en fastställd rimlig tidsram. Om Förenta staternas myndigheter, efter det att den fastställda tidsramen har löpt ut, inte på ett tillfredsställande sätt kan visa att skölden för skydd av privatlivet i EU och Förenta staterna fortsätter att garantera effektiv efterlevnad och en adekvat skyddsnivå kommer kommissionen att inleda förfarandet för att delvis eller fullständigt upphäva eller återkalla detta beslut ([207]). Alternativt kan kommissionen föreslå att detta beslut ska ändras, t.ex. genom att begränsa omfattningen av konstaterandet om adekvat skyddsnivå till att endast gälla uppgiftsöverföringar som är föremål för ytterligare villkor.

(151) Kommissionen kommer i synnerhet att inleda förfarandet för upphävande eller återkallande vid

a) indikationer på att Förenta staternas myndigheter inte uppfyller de utfästelser och åtaganden som ingår i de dokument som bifogas detta beslut, även när det gäller villkoren för och begränsningarna av dessa myndigheters åtkomst till personuppgifter som överförs enligt skölden för ändamål som rör brottsbekämpning, nationell säkerhet eller andra ändamål som rör allmänintresset,

b) underlåtande att effektivt behandla klagomål från registrerade i EU; i detta avseende kommer kommissionen att beakta alla omständigheter som inverkar på de registrerades möjlighet att utöva sina rättigheter, inbegripet, i synnerhet, frivilliga åtaganden av självcertifierade företag i Förenta staterna att samarbeta med dataskyddsmyndigheterna och följa deras rekommendationer; eller

c) underlåtande av ombudsmannen för skölden att utan dröjsmål och på lämpligt sätt svara på förfrågningar från registrerade i EU.

(152) Kommissionen kommer också att överväga att inleda förfarandet för ändring, upphävande eller återkallande av detta beslut om, inom ramen för den årliga gemensamma översynen av hur skölden för skydd av privatlivet i EU och Förenta staterna fungerar eller på annat sätt, handelsministeriet eller andra ministerier eller myndigheter som deltar i genomförandet av skölden för skydd av privatlivet, eller, när det gäller frågor som rör nationell säkerhet, företrädare för Förenta staternas underrättelsegemenskap eller ombudsmannen, underlåter att lämna uppgifter eller klargöranden som är nödvändiga för bedömningen av efterlevnaden av principerna, effektiviteten i förfaranden för handläggning av klagomål, eller sänkningar av den nödvändiga skyddsnivån till följd av åtgärder

([207]) Från och med den dag då den allmänna dataskyddsförordningen träder i kraft kommer kommissionen att använda sin befogenhet att, när det föreligger vederbörligen motiverade och tvingande skäl till skyndsamhet, anta en genomförandeakt för att upphäva detta beslut, som ska träda i kraft omedelbart utan att först läggas fram för den berörda kommittén inom kommittéförfarandet och gälla under en period av högst sex månader.

av Förenta staternas underrättelsemyndigheter, särskilt till följd av insamling och/eller åtkomst till personuppgifter som inte begränsas till vad som är absolut nödvändigt och proportionerligt. I detta avseende kommer kommissionen att beakta i vilken utsträckning det är möjligt att få relevant information från andra källor, inbegripet rapporter från Förenta staternas självcertifierade företag enligt *Förenta staterna Freedom Act*.

(153) Arbetsgruppen för skydd av enskilda med avseende på behandling av personuppgifter som inrättats genom artikel 29 i direktiv 95/46/EG har avgivit sitt yttrande om den skyddsnivå som erbjuds av skölden för skydd av privatlivet i EU och Förenta staterna ([208]), och vid utarbetandet av föreliggande beslut har hänsyn tagits till detta yttrande.

(154) antog Europaparlamentet en resolution om transatlantiska dataflöden ([209]).

(155) De åtgärder som föreskrivs i detta beslut är förenliga med yttrandet från den kommitté som inrättats genom artikel 31.1 i direktiv 95/46/EG.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

1. Vid tillämpningen av artikel 25.2 i direktiv 95/46/EG säkerställer Förenta staterna en adekvat skyddsnivå för personuppgifter som överförs från unionen till organisationer i Förenta staterna inom ramen för skölden för skydd av privatlivet i EU och Förenta staterna.

2. Skölden för skydd av privatlivet i EU och Förenta staterna utgörs av de principer som utfärdades av Förenta staterna:s handelsministerium den 7 juli 2016 enligt vad som anges i bilaga II samt de officiella utfästelser och åtaganden som ingår i de dokument som anges i bilagorna I samt III–VII.

3. Vid tillämpningen av punkt 1 överförs personuppgifter enligt skölden för skydd av privatlivet i EU och Förenta staterna när de överförs från unionen till organisationer i Förenta staterna som ingår i den ”förteckning över organisationer som anslutit sig till skölden” som förvaltas och offentliggörs av Förenta staternas handelsministerium i enlighet med avsnitten I och III i de principer som anges i bilaga II.

Artikel 2

Detta beslut påverkar inte tillämpningen av bestämmelserna i direktiv 95/46/EG, förutom artikel 25.1 som gäller behandling av personuppgifter inom medlemsstaterna, särskilt artikel 4.

Artikel 3

När de behöriga myndigheterna i medlemsstaterna utövar sina befogenheter enligt artikel 28.3 i direktiv 95/46/EG och detta leder till ett tillfälligt eller slutligt förbud mot dataflöden till en organisation i Förenta staterna som är upptagen i förteckningen över organisationer som anslutit sig till skölden i enlighet med avsnitten I och III i de principer som anges i bilaga II för att skydda enskilda personer med avseende på behandlingen av deras personuppgifter ska den berörda medlemsstaten underrätta kommissionen utan dröjsmål.

Artikel 4

1. Kommissionen ska fortlöpande övervaka hur skölden för skydd av privatlivet i EU och Förenta staterna fungerar för att bedöma huruvida Förenta staterna fortsätter att säkerställa en adekvat skyddsnivå för personuppgifter som överförs från unionen till organisationer i Förenta staterna.

([208]) Yttrande 01/2016 om skölden för skydd av privatlivet i EU och Förenta staterna, utkast till beslut om adekvat skyddsnivå, antaget den 13 april 2016.

([209]) Europaparlamentets resolution av den 26 maj 2016 om transatlantiska dataflöden ((2016/2727 (RSP)).

2. Medlemsstaterna och kommissionen ska underrätta varandra om de fall där regeringsorgan i Förenta staterna med lagstadgade befogenheter att se till att de principer följs som anges i bilaga II inte förefaller tillhandahålla effektiva mekanismer för upptäckt och övervakning som gör det möjligt att i praktiken identifiera och bestraffa överträdelser av principerna.

3. Medlemsstaterna och kommissionen ska underrätta varandra om indikationer på att ingreppen av offentliga myndigheter i Förenta staterna med ansvar för nationell säkerhet, brottsbekämpning eller andra allmänintressen i enskilda personers rätt till skydd av sina personuppgifter går utöver vad som är absolut nödvändigt, och/eller på att det inte finns något effektivt rättsligt skydd mot sådana ingrepp.

4. Kommissionen ska, inom ett år från den dag då detta beslut delges medlemsstaterna och därefter varje år, utvärdera tillämpningen av artikel 1.1 på grundval av all tillgänglig information, inbegripet information som mottas som en del av den årliga gemensamma översyn som avses i bilagorna I, II och VI.

5. Kommissionen ska rapportera eventuella relevanta konstateranden till den kommitté som inrättats i enlighet med artikel 31 i direktiv 95/46/EG.

6. Kommissionen ska lägga fram förslag till åtgärder enligt det förfarande som avses i artikel 31.2 i direktiv 95/46/EG i syfte att upphäva, ändra eller återkalla detta beslut eller begränsa dess tillämpningsområde, bland annat när det finns indikationer på

— att de offentliga myndigheterna i Förenta staterna inte uppfyller de utfästelser och åtaganden som ingår i de dokument som bifogas detta beslut, även när det gäller villkoren för och begränsningarna av dessa myndigheters åtkomst till personuppgifter som överförs enligt skölden för skydd av privatlivet i EU och Förenta staterna för ändamål som rör brottsbekämpning, nationell säkerhet eller andra ändamål som rör allmänintresset,

— systematiskt underlåtande att effektivt behandla klagomål från registrerade i EU, eller

— systematiskt underlåtande av ombudsmannen för skölden att utan dröjsmål och på lämpligt sätt svara på förfrågningar från registrerade i EU i enlighet med avsnitt 4.e i bilaga III.

Kommissionen ska också lägga fram sådana förslag till åtgärder om bristande samarbete från de organ som ska säkerställa att skölden för skydd av privatlivet i EU och Förenta staterna fungerar förhindrar kommissionen att avgöra huruvida tillämpningen av artikel 1.1 påverkas.

Artikel 5

Medlemsstaterna ska vidta alla åtgärder som är nödvändiga för att följa detta beslut.

Artikel 6

Detta beslut riktar sig till medlemsstaterna.

Utfärdat i Bryssel den 12 juli 2016.

På kommissionens vägnar

Věra JOUROVÁ

Ledamot av kommissionen

BILAGA I

Skrivelse från Förenta staternas handelsminister Penny Pritzker

7 juli 2016

Věra Jourová
Kommissionsledamot med ansvar för rättsliga frågor, konsumentfrågor och jämställdhet
Europeiska kommissionen
Rue de la Loi/Wetstraat 200
1049 Bryssel
BELGIEN

Bästa kommissionär Jourová,

På Förenta staternas vägnar har jag nöjet att härmed översända ett paket med material om skölden för skydd av privatlivet i EU och Förenta staterna, som är resultatet av två års givande diskussioner mellan våra lag. Detta paket, tillsammans med annat material som kommissionen har tillgång till via offentliga källor, ger en mycket stark grund för ett nytt konstaterande om adekvat skyddsnivå från kommissionen ([1]).

Båda parter bör vara stolta över förbättringarna av ramen. Skölden för skydd av privatlivet bygger på principer som har starkt stöd från båda sidor av Atlanten, och vi har stärkt principernas funktion. Tack vare vårt gemensamma arbete har vi en verklig möjlighet att förbättra skyddet av privatlivet runtom i världen.

Skölden för skydd av privatlivet omfattar principerna om skölden om skydd för privatlivet samt en skrivelse, bifogad som bilaga 1, från *International Trade Administration* (ITA) (Internationella handelsförvaltningen), som förvaltar programmet, med en beskrivning av de åtaganden som vårt ministerium har gjort för att säkerställa att skölden för skydd av privatlivet fungerar effektivt. I paketet ingår även bilaga 2, som innehåller andra åtaganden från handelsministeriet om den nya skiljedomsmodell som finns tillgänglig inom ramen för skölden för skydd av privatlivet.

Jag har gett anvisningar åt min personal om att ägna alla nödvändiga resurser för att genomföra skölden för skydd av privatlivet ändamålsenligt och fullständigt och säkerställa att åtagandena i bilagorna 1 och 2 uppfylls i tid.

Skölden för skydd av privatlivet innehåller också andra dokument från andra myndigheter i Förenta staterna, nämligen

— en skrivelse från *Federal Trade Commission* (den federala konkurrensmyndigheten, FTC), med en beskrivning av dess genomförande av skölden för skydd av privatlivet,

— en skrivelse från *Department of Transportation*, med en beskrivning av dess genomförande av skölden för skydd av privatlivet,

— två skrivelser från den nationella underrättelsetjänsten (*Office of the Director of National Intelligence*, ODNI) om de garantier och begränsningar som är tillämpliga på Förenta staternas myndigheter för nationell säkerhet,

— en skrivelse från Förenta staternas utrikesdepartement och ett kompletterande memorandum med en beskrivning av utrikesdepartementets åtagande att tillsätta en ny ombudsman för skölden för skydd av privatlivet som kommer att besvara frågor om Förenta staternas signalspaningsmetoder,

— en skrivelse från justitieministeriet om garantier och begränsningar för den amerikanska regeringens tillgång för ändamål som rör brottsbekämpning och allmänintresset.

Ni kan vara säker på att Förenta staterna tar dessa åtaganden på allvar.

([1]) Under förutsättning att kommissionens beslut om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna gäller för Island, Liechtenstein och Norge kommer skölden för skydd av privatlivet att omfatta både EU och dessa tre länder.

Inom 30 dagar från det slutliga godkännandet av fastställandet av adekvat skyddsnivå kommer den fullständiga skölden för skydd av privatlivet att översändas till det *federala registret* för offentliggörande.

Vi ser fram emot att samarbeta med er om genomförandet av skölden för skydd av privatlivet när vi nu inleder nästa fas i denna process tillsammans.

Högaktningsfullt,

Penny Pritzker

Bilaga 1

Skrivelse från Ken Hyatt, tillförordnad statssekreterare för internationell handel

Věra Jourová
Kommissionsledamot med ansvar för rättsliga frågor, konsumentfrågor och jämställdhet
Europeiska kommissionen
Rue de la Loi/Wetstraat 200
1049 Bryssel
BELGIEN

Bästa kommissionär Jourová,

På Internationella handelsförvaltningens vägnar har jag nöjet att beskriva det förstärkta skydd av personuppgifter som ges genom skölden för skydd av privatlivet i EU och Förenta staterna (nedan kallad *skölden för skydd av privatlivet* eller *skölden*) och de åtaganden som *Department of Commerce* (handelsministeriet) har gjort för att säkerställa att skölden för skydd av privatlivet fungerar effektivt. Att slutföra detta historiska arrangemang är ett stort framsteg för personuppgiftsskyddet och för företag på båda sidor av Atlanten. Privatpersoner i EU kan nu ha förtroende för att deras uppgifter kommer att skyddas och att de har tillgång till rättsmedel för att utreda eventuella farhågor. Skölden för skydd av privatlivet ger säkerhet, vilket kommer att bidra till den transatlantiska ekonomins tillväxt genom att det säkerställs att tusentals europeiska och amerikanska företag kan fortsätta att investera och bedriva verksamhet över våra gränser. Skölden för skydd av privatlivet är resultatet av över två års hårt arbete och samarbete med er, våra kolleger vid Europeiska kommissionen. Vi ser fram emot att fortsätta att samarbeta med kommissionen för att se till att skölden för skydd av privatlivet fungerar som avsett.

Vi har arbetat med kommissionen för att utforma skölden på ett sådant sätt att organisationer som är etablerade i Förenta staterna uppfyller kraven avseende adekvat skyddsnivå för uppgiftsskydd enligt EU-lagstiftningen. Den nya ramen kommer att ge flera viktiga fördelar för både privatpersoner och företag. För det första innehåller den en uppsättning viktiga åtgärder för skydd av personuppgifter för personer i EU. Deltagande amerikanska organisationer är skyldiga att utforma ett överensstämmande integritetsskydd, göra ett offentligt åtagande om att de kommer att följa principerna för skölden för skydd av privatlivet så att åtagandet blir verkställbart enligt amerikansk lag, årligen återbekräfta sitt åtagande till ministeriet, tillhandahålla kostnadsfri oberoende tvistlösning för personer i EU och vara underställda *Federal Trade Commission* (FTC), *Department of Transportation* (DOT) eller andra verkställande organ. För det andra kommer skölden för skydd av privatlivet att ge tusentals företag i Förenta staterna och dotterföretag till europeiska företag i Förenta staterna möjlighet att motta personuppgifter från Europeiska unionen för att underlätta dataflöden som stöder den transatlantiska handeln. De transatlantiska ekonomiska förbindelserna är redan världens största, står för hälften av globala ekonomiska produktionen och genererar nästan en biljon US-dollar i handel med varor och tjänster, samtidigt som de stöder miljontals arbetstillfällen på båda sidor av Atlanten. Företag som är beroende av transatlantiska dataflöden återfinns i alla industribranscher och inkluderar företag från Fortune 500-listan samt många små och medelstora företag. Tack vare de transatlantiska dataflödena kan amerikanska organisationer behandla de uppgifter som krävs för att erbjuda varor, tjänster och sysselsättningsmöjligheter till privatpersoner i EU. Skölden för skydd av personuppgifter stöder gemensamma principer om integritetsskydd och bidrar till att överbrygga skillnaderna i våra rättssystem, samtidigt som vi gör framsteg med både EU:s och Förenta staternas handelsmässiga och ekonomiska mål.

Företagens beslut att genom självcertifiering förbinda sig att följa denna nya ram kommer att vara frivilliga. När företagen väl gör ett offentligt åtagande gentemot skölden för skydd av privatlivet blir åtagandet dock verkställbart enligt amerikansk lag, antingen av *Federal Trade Commission* eller *Department of Transportation*, beroende på vilken myndighet som är behörig för organisationen i fråga.

Förbättringar enligt principerna för skölden för skydd av privatlivet

Skölden för skydd av privatlivet stärker integritetsskyddet på följande sätt:

— Ett krav på att ytterligare information ska lämnas till privatpersoner enligt principen om meddelande, inklusive en redogörelse för organisationens deltagande i skölden för skydd av privatlivet, en förklaring om privatpersoners rätt att få tillgång till sina personuppgifter samt en angivelse av relevant oberoende tvistlösningsorgan.

— Stärkt skydd av personuppgifter som överförs från en organisation som har åtagit sig att följa bestämmelserna om skölden för skydd av privatlivet till en tredje part som agerar som personuppgiftsansvarig genom att kräva att parterna ska ingå ett avtal om att sådana uppgifter endast får behandlas för begränsade och uttryckligt angivna ändamål som är förenliga med den enskilda personens samtycke och att mottagaren kommer att tillhandahålla samma skyddsnivå som enligt principerna.

— Stärkt skydd av personuppgifter som överförs från en organisation som har åtagit sig att följa bestämmelserna om skölden för skydd av privatlivet till en tredje part som agerar som förmedlare, även genom att kräva att organisationen i fråga vidtar rimliga och lämpliga åtgärder för att se till att förmedlaren faktiskt behandlar de överförda personuppgifterna på ett sätt som är förenligt med organisationens skyldigheter enligt principerna, att förmedlaren på begäran vidtar skäliga och lämpliga åtgärder för att stoppa och korrigera otillåten behandling och på begäran lämnar en sammanfattning eller en representativ kopia av de relevanta integritetsskyddsbestämmelserna i sitt avtal med förmedlaren till myndigheten.

— Ett krav på att organisationer som har åtagit sig att följa bestämmelserna om skölden för skydd av privatlivet är ansvariga för behandlingen av de personuppgifter som de mottar inom ramen för skölden och för efterföljande överföringar till en tredje part som agerar som förmedlare för organisationens räkning, och att organisationen i fråga förblir ansvarig enligt principerna om dess förmedlare behandlar sådana personuppgifter på ett sätt som är oförenligt med principerna, om inte organisationen kan visa att den inte bär ansvaret för den händelse som ger upphov till skada.

— Ett klargörande om att organisationer som har åtagit sig att följa bestämmelserna om skölden för skydd av privatlivet måste begränsa personuppgifter till sådana uppgifter som är relevanta för behandlingens ändamål.

— Ett krav på att organisationerna årligen inför ministeriet ska intyga sitt åtagande att tillämpa principerna på de uppgifter som de mottagit medan de deltog i skölden för skydd av personuppgifter om de lämnar skölden och väljer att behålla sådana uppgifter.

— Ett krav på att oberoende instanser för handläggning av klagomål ska tillhandahållas, utan kostnad för den enskilda personen.

— Ett krav på organisationer och deras valda oberoende instanser för handläggning av klagomål utan dröjsmål ska besvara förfrågningar och ansökningar avseende skölden för skydd av privatlivet från ministeriets informationsavdelning.

— Ett krav på att organisationerna på lämpligt sätt via informationsavdelningen ska besvara klagomål rörande överensstämmelse med principerna som hänskjuts från myndigheter i EU-medlemsstaterna.

— Ett krav på att organisationer som har åtagit sig att följa bestämmelserna om skölden för skydd av privatlivet ska offentliggöra eventuella avsnitt i efterlevnads- eller bedömningsrapporter som lämnas in till FTC och som är relevanta för skölden om organisationerna blir föremål för ett rättsligt avgörande från FTC eller en domstol baserat på bristande efterlevnad.

Handelsministeriets förvaltning och tillsyn av programmet för skölden för skydd av privatlivet

Ministeriet upprepar sitt åtagande att upprätthålla och offentliggöra en officiell förteckning över amerikanska organisationer som genom självcertifiering till handelsministeriet har anslutit sig till principerna (nedan kallad *förteckningen över organisationer som anslutit sig till skölden*. Ministeriet kommer att hålla förteckningen över organisationer som anslutit sig till skölden aktuell genom att stryka organisationer som frivilligt drar sig tillbaka, inte självcertifierar sig varje år enligt ministeriets förfaranden eller begår upprepade överträdelser av principerna. Ministeriet kommer också att föra och offentliggöra ett officiellt register över amerikanska organisationer som tidigare har lämnat in en självcertifiering till ministeriet, men som har strukits från förteckningen över organisationer som anslutit sig till skölden, inbegripet organisationer som har strukits på grund av upprepade överträdelser av principerna. Ministeriet kommer att ange skälet till att en organisation stryks från förteckningen.

Dessutom åtar sig ministeriet att stärka förvaltningen och tillsynen av skölden för skydd av privatlivet. Ministeriet kommer närmare bestämt att göra följande:

Tillhandahålla ytterligare information på webbplatsen för skölden för skydd av privatlivet.

— Underhålla förteckningen över organisationer som har anslutit sig till skölden samt ett register över organisationer som tidigare har anslutit sig till principerna genom självcertifiering, men som inte längre omfattas av de fördelar som skölden medför.

— Inbegripa en redogörelse på en framträdande plats, med ett klargörande av att alla organisationer som stryks från förteckningen över organisationer som har anslutit sig till skölden inte längre omfattas av de fördelar som skölden medför, men att de trots detta måste fortsätta att tillämpa principerna på personuppgifter som de mottagit medan de deltog i skölden så länge de behåller sådana uppgifter.

— Ange en länk till förteckningen över FTC-ärenden som är relaterade till skölden för skydd av privatlivet som finns på FTC:s webbplats.

Kontrollera självcertifieringskraven.

— Innan en organisation slutför sin självcertifiering (eller årliga återcertifiering) och tas upp på förteckningen över organisationer som anslutit sig till skölden för skydd av privatlivet kommer ministeriet att kontrollera att organisationerna gör följande:

  — Anger erforderlig kontaktinformation för organisationen.

  — Beskriver den del av organisationens verksamhet som rör personuppgifter som tas emot från EU.

  — Anger vilka personuppgifter som omfattas av självcertifieringen.

  — Om organisationen har en offentlig webbplats, att den anger den webbadress där dess policy för integritetsskydd finns tillgänglig, eller om organisationen inte har en offentlig webbplats, att organisationen har angett var dess policy för integritetsskydd finns tillgänglig för allmänheten.

  — I sin relevanta integritetsskyddspolicy inbegriper en redogörelse för att organisationen följer principerna, och om policyn för integritetsskydd finns tillgänglig online, en hyperlänk till ministeriets webbplats för skölden för skydd av privatlivet.

  — Anger det särskilda lagstadgade organ som är behörigt för att behandla eventuella yrkanden som riktas mot organisationen avseende illojala eller bedrägliga metoder och överträdelser av lagstiftning eller andra föreskrifter som reglerar integritetsfrågor (och anges i principerna eller i framtida bilagor till dessa).

  — Om organisationen väljer att uppfylla kraven i punkterna a.i och a.iii i principen om rättsmedel, verkställande och ansvar genom att förbinda sig att samarbeta med berörda dataskyddsmyndigheter i EU, att den har förklarat sin avsikt att samarbeta med dessa myndigheter för att utreda och lösa klagomål som tas upp inom ramen för skölden för skydd av privatlivet, särskilt genom att besvara deras förfrågningar när registrerade i EU har ingett klagomål direkt till sina nationella dataskyddsmyndigheter.

  — Anger eventuella integritetsprogram som organisationen är medlem i.

  — Anger kontrollmetod för att säkerställa efterlevnad av principerna (*t.ex.* internt, en tredje part).

  — Både i självcertifieringen och policyn för integritetsskydd, ange den oberoende instans för handläggning av klagomål som finns tillgänglig för att utreda och lösa klagomål.

  — I sin relevanta policy för integritetsskydd, om policyn finns tillgänglig online, ange en hyperlänk till webbplatsen eller till ett klagomålsformulär som den oberoende instansen för handläggning av klagomål har gjort tillgängligt för att utreda olösta klagomål.

  — Om organisationen har angett att den har för avsikt att motta information om personal som överförs från EU inom ramen för anställningsförhållanden, att den förklarar att den förbinder sig att samarbeta med och följa dataskyddsmyndigheternas bestämmelser för att lösa klagomål på organisationens verksamheter med avseende på sådana uppgifter, lämnar en kopia av sin personalpolicy till ministeriet och anger var policyn för integritetsskydd finns tillgänglig för berörda anställda.

— Samarbeta med den oberoende instansen för handläggning av klagomål för att kontrollera att organisationen verkligen har registrerat sig hos den instans som anges i självcertifieringen, om sådan registrering krävs.

Ökade ansträngningar för att följa upp organisationer som har strukits från förteckningen över organisationer som har anslutit sig till skölden

— Meddela organisationer som stryks från förteckningen över organisationer som har anslutit sig till skölden på grund av ”upprepade överträdelser av principerna” att de inte har rätt att behålla information som samlats in inom ramen för skölden för skydd av privatlivet, och om de

— Skicka frågeformulär till organisationer vars självcertifiering har löpt ut eller organisationer som frivilligt har dragit sig tillbaka från skölden för skydd av privatlivet, för att ta reda på om organisationen kommer att återvända, stryka sig eller fortsätta att tillämpa principerna på de personuppgifter som de mottog medan de deltog i skölden, och om personuppgifter kommer att behållas, bekräfta vem inom organisationen som fungerar som fast kontaktpunkt för frågor rörande skölden.

Söka efter och hantera falska påståenden om deltagande i skölden

— Granska policyn för integritetsskydd för organisationer som tidigare har deltagit i programmet för skölden för skydd av privatlivet men som har strukits från förteckningen över organisationer som anslutit sig till skölden, i syfte att upptäcka eventuella falska påståenden om att organisationer deltar i skölden.

— Fortlöpande, när en organisation a) drar sig tillbaka från deltagande i skölden för skydd av privatlivet, b) inte återcertifierar sin anslutning till principerna, eller c) stryks som deltagare i skölden på grund av ”upprepade överträdelser av principerna”, på eget initiativ kontrollera att organisationen har avlägsnat eventuella hänvisningar till skölden i relevanta offentliggjorda integritetsskyddspolicyer som antyder att organisationen fortsätter att aktivt delta i skölden och har rätt att utnyttja fördelarna i samband med detta. Om ministeriet konstaterar att sådana hänvisningar inte har avlägsnats kommer ministeriet att varna organisationen om att det, i förekommande fall, kommer att hänskjuta saken till relevant organ för eventuella verkställighetsåtgärder om organisationen fortsätter att hävda att den är certifierad för deltagande i skölden för skydd av privatlivet. Om organisationen varken avlägsnar hänvisningar eller har anslutit sig till skölden genom självcertifiering kommer ministeriet på eget initiativ att hänskjuta saken till FTC, DOT eller ett annat verkställande organ eller, i förekommande fall, vidta åtgärder för att verkställa sköldens certifieringsmärkning.

— Ministeriet kommer att vidta andra åtgärder för att upptäcka falska påståenden om deltagande i skölden för skydd av privatlivet och oegentlig användning av sköldens certifieringsmärkning, bland annat genom internetsökningar för att upptäcka om sköldens certifieringsmärkning visas och hänvisningar görs till skölden i organisationernas policyer för integritetsskydd.

— Ministeriet kommer att utan dröjsmål behandla problem som vi upptäcker inom ramen för vår övervakning på eget initiativ av falska påståenden om deltagande och missbruk av certifieringsmärkningen, även genom att varna organisationer som inte sköter sitt deltagande i programmet för skölden för skydd av privatlivet enligt beskrivningen ovan.

— Ministeriet kommer att vidta andra korrigerande åtgärder, bland annat genom att väcka talan i ärenden som det är behörigt att agera i och hänskjuta ärenden till FTC, DOT eller ett annat verkställande organ.

— Ministeriet kommer utan dröjsmål att granska och behandla klagomål om falska påståenden om deltagande som vi mottar.

Ministeriet kommer att granska organisationers policyer för integritetsskydd för att mer effektivt kunna upptäcka och hantera falska påståenden om deltagande i skölden. Ministeriet kommer i synnerhet att granska policyer för integritetsskydd för organisationer vars självcertifiering har löpt ut på grund av att de inte har återcertifierat sin anslutning till principerna. Ministeriet kommer att göra denna typ av granskningar för att kontrollera att organisationerna har avlägsnat eventuella hänvisningar från relevanta offentliggjorda integritetsskyddspolicyer som antyder att organisationerna fortsätter att aktivt delta i skölden för skydd av privatlivet. På grundval av dessa typer av granskningar kommer vi att identifiera organisationer som inte har avlägsnat sådana hänvisningar och skicka en skrivelse från ministeriets chefsjuridiska avdelning, med en varning om eventuella verkställighetsåtgärder om hänvisningarna inte avlägsnas. Ministeriet kommer att vidta uppföljningsåtgärder för att se till att organisationerna antingen avlägsnar de olämpliga hänvisningarna eller återcertifierar sin anslutning till principerna. Dessutom kommer ministeriet att vidta åtgärder för att upptäcka falska påståenden om deltagande i skölden om skydd för privatlivet från organisationer som aldrig har deltagit i programmet, och kommer att vidta liknande korrigerande åtgärder med avseende på sådana organisationer.

Ministeriet kommer att genomföra regelbundna granskningar och bedömningar av efterlevnad på eget initiativ

— genom att löpande övervaka att kraven verkligen efterlevs, bland annat genom att skicka detaljerade frågeformulär till deltagande organisationer för att identifiera problem som kan kräva ytterligare uppföljningsåtgärder. Sådan efterlevnadsövervakning ska särskilt ske när a) ministeriet har mottagit särskilt välgrundade klagomål beträffande en organisations efterlevnad av principerna, b) om en organisation inte besvarar informationsförfrågningar från ministeriet om skölden för skydd av privatlivet på lämpligt sätt, eller c) det finns trovärdiga bevis för att en organisation inte uppfyller sina åtaganden enligt skölden. Ministeriet ska i tillämpliga fall rådfråga behöriga dataskyddsmyndigheter om sådana efterlevnadsgranskningar, och

— regelbundet utvärdera förvaltningen och tillsynen av programmet för skölden för skydd av privatlivet för att se till att övervakningsåtgärderna är lämpliga för att hantera eventuella nya frågor som kan uppstå.

Ministeriet har ökat resurserna för förvaltningen och tillsynen av programmet för skölden för skydd av privatlivet, bland annat genom att fördubbla antalet anställda som ansvarar för förvaltningen och tillsynen av programmet. Vi kommer även fortsättningsvis att anslå lämpliga resurser för sådana insatser för att säkerställa en effektiv övervakning och förvaltning av programmet.

Skräddarsy webbplatsen för skölden för skydd av privatlivet till särskilda målgrupper

Ministeriet kommer att skräddarsy webbplatsen för skölden för skydd av privatlivet så att den inriktas på följande tre målgrupper: Enskilda personer och företag i EU samt amerikanska företag. Material på webbplatsen som riktas direkt till enskilda personer och företag i EU kommer att öka öppenheten på flera sätt. När det gäller enskilda personer i EU kommer webbplatsen att innehålla tydlig information om 1) de rättigheter som enskilda personer i EU har enligt skölden för skydd av privatlivet, 2) de instanser för handläggning av klagomål som finns tillgängliga för enskilda personer i EU när de anser att en organisation har brutit mot sitt åtagande att följa principerna, och 3) hur de kan finna information om självcertifieringar för organisationer som är anslutna till skölden. När det gäller företag i EU kommer webbplatsen att göra det lättare för dem att kontrollera 1) om en viss organisation omfattas av fördelarna i samband med skölden för skydd av privatlivet, 2) vilken typ av information som ingår i en organisations självcertifiering enligt skölden, 3) vilken policy för integritetsskydd som gäller för den information som omfattas, och 4) den metod organisationen använder för att visa att den följer principerna.

Ökat samarbete med dataskyddsmyndigheter

För att öka möjligheterna till samarbete med dataskyddsmyndigheterna kommer ministeriet att utse en särskild person vid ministeriet som kommer att fungera som kontaktperson för dataskyddsmyndigheterna. Om en dataskyddsmyndighet anser att en viss organisation inte följer principerna, även till följd av ett klagomål från en enskild person i EU, kan dataskyddsmyndigheten kontakta den utsedda kontaktpersonen vid ministeriet för att be det att ytterligare granska organisationen. Kontaktpersonen kommer också att motta hänskjutanden rörande organisationer som felaktigt påstår att den deltar i skölden för skydd av privatlivet, trots att de aldrig har självcertifierat sin anslutning till skölden. Kontaktpersonen kommer att bistå dataskyddsmyndigheter som söker information om en viss organisations självcertifiering eller tidigare deltagande i programmet, och kommer att besvara förfrågningar från dataskyddsmyndigheterna om genomförandet av de krav som gäller för skölden. Ministeriet kommer dessutom att förse dataskyddsmyndigheterna med material om skölden för skydd av privatlivet som de kan lägga upp på sina webbplatser för att öka insynen för enskilda personer och företag i EU. Ökad kunskap om skölden för skydd av privatlivet och de rättigheter och ansvarsuppgifter som den medför bör göra det lättare att upptäcka eventuella problem, så att de kan lösas på lämpligt sätt.

Åtgärder för att göra det lättare att lösa klagomål om bristande efterlevnad

Via den särskilda kontaktpersonen kommer ministeriet att ta emot eventuella klagomål till ministeriet från dataskyddsmyndigheter om organisationer som är anslutna till skölden för skydd av privatlivet som inte följer principerna. Ministeriet kommer att göra sitt bästa för att lösa klagomålet med den berörda organisationen. Inom 90 dagar efter mottagandet av ett klagomål kommer ministeriet att informera dataskyddsmyndigheten om hur ärendet utvecklas. För att det ska bli lättare att lämna in klagomål kommer ministeriet att ta fram ett standardformulär som dataskyddsmyndigheterna kan använda för att inge klagomål till den särskilda kontaktpersonen. Kontaktpersonen kommer att spåra alla hänskjutanden från dataskyddsmyndigheter som mottagits av ministeriet, och ministeriet kommer i den årliga granskning som beskrivs redan att lämna en rapport med en samlad analys av de klagomål som det mottar varje år.

Införa skiljedomsförfaranden och välja skiljemän i samråd med kommissionen

Ministeriet kommer att fullgöra sina åtaganden enligt bilaga I och offentliggöra förfarandena efter det att en överenskommelse har nåtts.

System för gemensam översyn av hur skölden för skydd av privatlivet fungerar

Handelsministeriet, FTC och andra myndigheter, i förekommande fall, kommer att hålla årliga möten med kommissionen, berörda dataskyddsmyndigheter och lämpliga företrädare från artikel 29-arbetsgruppen, där ministeriet kommer att lämna uppdateringar om programmet för skölden för skydd av privatlivet. Under de årliga mötena kommer man även att diskutera aktuella frågor rörande funktion, genomförande, tillsyn och verkställande av skölden för skydd av privatlivet, inklusive hänskjutanden som ministeriet mottagit från dataskyddsmyndigheter och efterlevnadsgranskningar på eget initiativ. Diskussionerna kan även omfatta relevanta lagändringar. Den första årliga översynen och efterföljande översyner i förekommande fall kommer att inbegripa en dialog om andra frågor, t.ex. på området automatiska beslut, inklusive aspekter rörande likheter och skillnader i tillvägagångssätt i EU och Förenta staterna.

Uppdatering av bestämmelser

Ministeriet kommer att göra rimliga ansträngningar för att underrätta kommissionen om väsentliga förändringar i Förenta staterna:s lagstiftning, i den mån de är relevanta för skölden för skydd av privatlivet när det gäller skydd av personuppgifter och de begränsningar och garantier för tillgång till personuppgifter av Förenta staterna:s myndigheter och senare användning av dem.

Begränsning på grund av nationell säkerhet

När det gäller begränsningar av anslutning till skölden för skydd av privatlivet av nationella säkerhetsskäl har Robert Litt, chefsjurist vid den nationella underrättelsetjänsten, även skickat två skrivelser till Justin Antonipillai och Ted Dean vid handelsministeriet, som har översänts till er. Dessa skrivelser innehåller bland annat omfattande redogörelser för de policyer, garantier och begränsningar som gäller för Förenta staterna:s signalspaningsverksamhet. De innehåller dessutom beskrivningar av den insyn som underrättelsemyndigheterna tillhandahåller i dessa frågor. Kommissionen utvärderar för närvarande skölden för skydd av privatlivet, och skrivelserna innehåller information som gör det möjligt att dra slutsatsen att skölden kommer att fungera på lämpligt sätt enligt principerna. Vi är medvetna om att ni i framtiden kan använda information som har offentliggjorts av underrättelsemyndigheterna tillsammans med annan information som underlag för den årliga översynen av skölden för skydd av privatlivet.

På grundval av principerna för skölden för skydd av privatlivet samt åtföljande skrivelser och material, däribland ministeriets åtaganden med avseende på förvaltningen och tillsynen av skölden, är det vår förhoppning att kommissionen kommer att fastställa att skölden för skydd av privatlivet i EU och Förenta staterna ger ett adekvat skydd enligt EU-lagstiftningen och att överföringarna av uppgifter från Europeiska unionen till organisationer som deltar i skölden kommer att fortsätta i framtiden.

Högaktningsfullt,

Ken Hyatt

Bilaga 2

Modell för skiljedomsförfaranden

BILAGA I

I denna bilaga anges de villkor enligt vilka organisationer som har anslutit sig till skölden för skydd av privatlivet är skyldiga att lösa yrkanden genom skiljedom i enlighet med principen om rättsmedel, genomförande och ansvar. Det bindande skiljedomsalternativ som beskrivs nedan är tillämpligt på vissa ”resterande” yrkanden avseende uppgifter som omfattas av skölden för skydd av privatlivet i EU och Förenta staterna. Syftet med detta alternativ är att skapa en snabb, oberoende och rättvis mekanism med valmöjligheter för enskilda personer för att behandla påstådda överträdelser av principerna som eventuella andra instanser inom ramen för skölden inte har löst.

A. **Tillämpningsområde**

Ett skiljedomsalternativ finns tillgängligt för enskilda personer. Syftet är att fastställa om en organisation som har anslutit sig till skölden har brutit mot sina skyldigheter enligt principerna gentemot den enskilde när det gäller ”resterande” yrkanden, och huruvida sådana överträdelser inte har åtgärdats alls eller endast delvis. Detta alternativ finns endast tillgängligt för dessa ändamål. Det är t.ex. inte tillgängligt med avseende på undantag från principerna ([1]) eller när det gäller påståenden om huruvida sköldens skydd är adekvat.

B. **Tillgängliga rättsmedel**

Enligt detta skiljedomsalternativ har arbetsgruppen för skölden för skydd av privatlivet (som består av en eller tre skiljemän beroende på vad som överenskommits av parterna) befogenhet att påföra individuella specifika icke-monetära åtgärder för att avhjälpa skadan (t.ex. tillgång, korrigering, radering eller återlämnande av den enskildes personuppgifter) som är nödvändiga att åtgärda en överträdelse av principerna endast med avseende på denna enskilda person. Dessa befogenheter är de enda skiljenämnden har avseende rättsmedel. När skiljenämnden överväger rättsmedel ska den överväga andra rättsmedel som redan har påförts av andra mekanismer enligt sköldens bestämmelser. Inga andra former av skadestånd, kostnader, avgifter eller andra rättsmedel finns tillgängliga. Varje part betalar sina egna advokatkostnader.

C. **Åtgärder som ska vidtas innan ett ärende tas till skiljenämnden**

En enskild person som beslutar att åberopa skiljedom måste vidta följande åtgärder innan skiljedomsförfarandet inleds: 1) Ta upp den påstådda överträdelsen direkt med organisationen och ge organisationen möjlighet att lösa frågan inom den tidsram som fastställs i avsnitt III.11(d)(i) i principerna, 2) utnyttja den oberoende instanser för handläggning av klagomål enligt principerna, som är kostnadsfri, och 3) via sin dataskyddsmyndighet ta upp frågan med handelsministeriet och ge ministeriet möjlighet att göra sitt bästa för att lösa frågan inom de tidsramar som fastställs i skrivelsen från handelsministeriets utrikeshandelsförvaltning, utan kostnad för den enskilde.

Skiljedomsalternativet kan inte åberopas om den överträdelse av principerna som har begåtts enligt den enskilda personen 1) redan har varit föremål för bindande skiljedom, 2) var föremål för en slutlig dom i ett domstolsförfarande som den enskilde var part i, eller 3) redan har varit föremål för förlikning mellan parterna. Detta alternativ kan inte heller åberopas om en dataskyddsmyndighet i EU 1) är behörig enligt avsnitten III.5 eller III.9 i principerna, eller 2) är behörig att lösa den påstådda överträdelsen direkt med organisationen. Dataskyddsmyndigheters behörighet att lösa samma yrkande mot en personuppgiftsansvarig i EU hindrar i sig inte åberopande av skiljedomsalternativet mot en annan juridisk enhet som inte omfattas av dataskyddsmyndighetens behörighet.

D. **Beslutens bindande karaktär**

En enskild persons beslut att åberopa alternativet med bindande skiljedom är helt frivilligt. Skiljenämndens beslut är bindande för alla parter i skiljedomsförfarandet. När skiljedom åberopas avstår den enskilda personen från alternativet att söka upprättelse i en annan instans, förutom de fall icke-monetära åtgärder för att avhjälpa skadan inte fullständigt avhjälper den påstådda överträdelsen. Åberopande av skiljedom hindrar inte den enskilde från att yrka på andra former av skadeståndsanspråk som finns tillgängliga i domstol.

([1]) Avsnitt I.5 i principerna.

E. **Översyn och verkställighet**

Enskilda personer och organisationer som har anslutit sig till skölden har rätt att begära domstolsprövning och verkställande av skiljedomsbeslut i enlighet med amerikansk lagstiftning, närmare bestämt lagen om federal skiljedom (*Federal Arbitration Act*) ([1]). Sådana ärenden måste tas upp i den federala distriktsdomstol inom vars territoriella behörighetsområde organisationen har sitt huvudsakliga säte.

Syftet med detta skiljedomsalternativ är att lösa individuella tvister. Skiljedomsbesluten är inte avsedda att vara övertygande eller bindande prejudikat i frågor som rör andra parter, inte heller när det gäller framtida skiljedomsförfaranden i domstolar i EU eller Förenta staterna, eller FTC:s förhandlingar.

F. **Skiljenämnd**

Parterna väljer skiljemän från den förteckning över skiljemän som anges nedan.

I enlighet med tillämplig lag kommer Förenta staterna:s handelsministerium och Europeiska kommissionen utarbeta en förteckning med minst 20 skiljemän, som väljs på grundval av oberoende, integritet och sakkunskap. Följande ska gälla för denna process:

Skiljemän

1) kommer att finnas upptagna i förteckningen under en period av tre år, förutom exceptionella omständigheter eller orsaker, med möjlighet till förlängning med en ytterligare treårsperiod,

2) ska inte ta emot instruktioner från eller ha anknytning till någon av parterna eller till någon organisation som är ansluten till skölden för skydd av privatlivet eller till Förenta staterna:s, EU:s eller EU-medlemsstaternas regeringar eller andra statliga myndigheter, offentliga myndigheter eller verkställande myndigheter, och

3) vara behörig att utöva advokatyrket i Förenta staterna och vara expert på amerikansk lagstiftning om integritetsskydd, med sakkunskap om EU:s dataskyddslagstiftning.

G. **Skiljeförfaranden**

I enlighet med tillämplig lag ska handelsministeriet och Europeiska kommissionen, inom sex månader från beslutet om adekvat skyddsnivå, enas om att anta en uppsättning befintliga och väletablerade amerikanska skiljedomsförfaranden (såsom AAA eller JAMS), som ska styra förhandlingarna inför skiljenämnden inom ramen för skölden, enligt följande villkor:

1. Enskilda personer kan inleda ett bindande skiljedomsförfarande enligt de villkor för skiljedomsförfaranden som anges ovan genom att inge ett meddelande till organisationen. Meddelandet ska innehålla en sammanfattning av de åtgärder som vidtagits enligt punkt C för att lösa yrkandet, en beskrivning av den påstådda överträdelsen och, enligt den enskildes val, eventuella styrkande handlingar och annat material och/eller en redogörelse för lagstiftning som är tillämplig på yrkandet.

([1]) Enligt kapitel 2 i lagen om federal skiljedom ”omfattas skiljedomsavtal eller skiljedomar som härrör från ett rättsligt förhållande, oavsett om de är avtalsmässiga eller ej, och betraktas som ett affärsmässigt avtal, en transaktion, ett avtal eller en överenskommelse enligt beskrivningen i [avsnitt 2 i lagen], av konventionen [om erkännande och verkställighet av utländska skiljedomar av den 10 juni 1958, 21 U.S.T. 2519, T.I.A.S. nr 6997 (nedan kallad *New York-konventionen*)].” 9 U.S.C. § 202. I lagen om federal skiljedom föreskrivs vidare att ”ett skiljedomsavtal eller en skiljedom som härrör från ett sådant förhållande och endast rör medborgare i Förenta staterna ska inte anses omfattas av [New York-]konventionen, om inte förhållandet omfattar egendom utomlands, utförande eller verkställande utomlands eller har något annat skäligt förhållande till en eller flera utländska stater”. *Idem*. Enligt kapitel 2 ”kan endera parten i ett skiljedomsförfarande ansöka till alla domstolar som är behöriga enligt detta kapitel om ett beslut som bekräftar skiljedomen mot en annan part i skiljedomsförfarandet. Domstolen ska bekräfta skiljedomen om den inte finner att någon av grunderna för avslag, uppskjutande, erkännande eller verkställighet av skiljedomen som anges i den nämnda [New York-] konventionen är tillämplig”. *Idem*. § 207. I kapitel 2 föreskrivs vidare att ”distriktsdomstolarna i Förenta staterna […] ska ha ursprunglig behörighet för […] talan eller förhandlingar [enligt New York-]konventionen, oavsett tvistebelopp”. *Idem*. § 203.
I kapitel 2 anges även att ”kapitel 1 är tillämpligt på talan och förfaranden som väcks enligt detta kapitel, om inte kapitlet strider mot detta kapitel eller [New York-]konventionen, som ratificerats av Förenta staterna”. *Idem*. § 208. I kapitel 1 föreskrivs å sin sida att ”en skriftlig bestämmelse i […] ett avtal som styrker en affärsmässig transaktion som löses genom skiljedom ska, även om en tvist uppstår om avtalet eller transaktionen eller vid vägran att fullgöra hela eller delar av avtalet eller ett skriftligt avtal om att hänskjuta en befintlig tvist om ett sådant avtal, en sådan transaktion eller en sådan vägran till skiljedom, vara oåterkalleligt och verkställbart, utom när lagliga grunder finns för att häva avtalet”. *Idem*. § 2. I kapitel 1 föreskrivs dessutom att ”varje part i skiljedomsförfarandet får ansöka till den behöriga domstolen om ett beslut som bekräftar skiljedomen, och domstolen måste bevilja ett sådant beslut om skiljedomen inte upphävs, ändras eller korrigeras enligt vad som anges i avsnitten 10 och 11 i lagen [om federal skiljedom]”. *Idem*. § 9.

2. Förfaranden kommer att utarbetas för att säkerställa att den ifrågavarande överträdelsen inte omfattas av dubbla rättsmedel eller förfaranden.

3. FTC kan vidta åtgärder parallellt med skiljedomsförfaranden.

4. Inga företrädare för Förenta staterna, EU, EU-medlemsstater eller andra statliga myndigheter, offentliga myndigheter eller verkställande myndigheter får delta i skiljedomsförfarandet. På den enskildes begäran får dataskyddsmyndigheter i EU endast bistå i utarbetandet av meddelandet, men får inte ges tillgång till framlägganden eller annat material som är relaterat till skiljedomsförfarandet.

5. Platsen för skiljeförfarandet kommer att Förenta staterna, och den enskilda personen kan välja att delta via telefon- eller videoanslutning, som ska tillhandahållas utan kostnad för den enskilde. Den enskilde behöver inte inställa sig personligen.

6. Skiljedomsförfarandet ska genomföras på engelska om inget annat överenskoms av parterna. På motiverad begäran, och med beaktande av om den enskilda personen företräds av en advokat, kommer både tolkning vid skiljedomsförfarandet och översättning av materialet att tillhandahållas utan kostnad för den enskilde, om inte skiljenämnden finner att detta med tanke på de omständigheterna kring förfarandet skulle leda till omotiverade eller oproportionerliga kostnader.

7. Material som lämnas in till skiljenämnden kommer att behandlas konfidentiellt och kommer endast att användas i samband med skiljedomsförfarandet.

8. Enskilda framlägganden kan tillåtas om så är nödvändigt och sådana framlägganden kommer att behandlas konfidentiellt av parterna och kommer endast att användas i samband med skiljedomsförfarandet.

9. Skiljedomsförfaranden bör avslutas inom 90 dagar från den dag då meddelandet inges till organisationen i fråga, om inget annat överenskoms av parterna.

H. **Kostnader**

Skiljemännen bör vidta rimliga åtgärder för att minimera kostnader eller avgifter för skiljeförfaranden.

I enlighet med tillämplig lag kommer handelsministeriet i samråd med Europeiska kommissionen att vidta åtgärder för att inrätta en fond, dit organisationer som är anslutna till skölden för skydd av privatlivet ska betala ett årligt bidrag, delvis baserat på organisationens storlek, som ska täcka kostnaderna för skiljedomsförfarandet, inklusive förlikningsmännens arvoden upp till maximala belopp (”tak”). Fonden kommer att förvaltas av en tredje part, som kommer att rapportera regelbundet om fondens verksamhet. Vid den årliga översynen kommer handelsministeriet och Europeiska kommissionen att granska driften av fonden och undersöka om det är nödvändigt att höja bidragsbeloppen eller taken. De kommer bland annat att överväga antalet skiljedomsförfaranden samt kostnader och tidsåtgång för förfarandena, med en ömsesidig överenskommelse om att organisationer som är anslutna till skölden inte får belastas med överdrivet höga ekonomiska bördor. Advokatkostnader omfattas inte av denna bestämmelse eller någon fond enligt denna bestämmelse.

BILAGA II

ÖVERGRIPANDE PRINCIPER FÖR SKÖLDEN FÖR SKYDD AV PRIVATLIVET I EU OCH FÖRENTA STATERNA UTFÄRDADE AV FÖRENTA STATERNAS HANDELSMINISTERIUM

I. ÖVERSIKT

1. Även om målet för Förenta staterna (nedan kallat *Förenta staterna*) och Europeiska unionen (nedan kallad *EU*) är detsamma, nämligen att stärka integritetsskyddet, har Förenta staterna anammat ett annat tillvägagångssätt i fråga om integritetsskydd än EU. Förenta staterna använder sig av ett sektoriellt tillvägagångssätt som bygger på en blandning av lagstiftning, reglering och självreglering. Mot bakgrund av dessa skillnader, och för ge amerikanska organisationer tillgång till ett tillförlitligt system för överföring av personuppgifter till Förenta staterna från Europeiska unionen samtidigt som det säkerställs att registrerade i EU fortsätter att omfattas av effektiva garantier och skydd enligt EU-lagstiftningen med avseende på behandling av deras personuppgifter när de har överförts till tredjeländer, utfärdar handelsministeriet följande principer för skölden för skydd av privatlivet, inklusive kompletterande principer (tillsammans kallade the *principerna*) i enlighet med sitt lagstadgade bemyndigande att stödja, främja och utveckla den internationella handeln (15 U.S.C. § 1512). Principerna har utarbetats i samråd med Europeiska kommissionen, näringslivet och andra berörda aktörer för att underlätta handel och affärsverksamhet mellan Förenta staterna och EU. De är endast avsedda att tillämpas på de organisationer i Förenta staterna som tar emot personuppgifter från EU och syftet är att dessa organisationer ska uppfylla villkoren för skölden för skydd av privatlivet och således omfattas av Europeiska kommissionens beslut om adekvat skyddsnivå ([1]). Principerna påverkar inte tillämpningen av nationella bestämmelser som genomför direktiv 95/46/EG (nedan kallat *direktivet*) och som gäller vid behandling av personuppgifter i medlemsstaterna. Principerna begränsar inte heller de bestämmelser om respekt för privatlivet som annars är tillämpliga enligt amerikansk lag.

2. För att få överföra personuppgifter från EU inom ramen för skölden för skydd av privatlivet måste organisationen ansluta sig till handelsministeriets principer (eller det organ som ministeriet bestämmer) (nedan kallat *ministeriet*). Det är helt och hållet frivilligt för en organisation att besluta om den vill ansluta sig till skölden för skydd av privatlivet, men det är obligatoriskt att följa bestämmelserna: organisationer som självcertifierar sig hos ministeriet och offentligt förklarar att de följer principerna måste uppfylla dem fullständigt. För att ansluta sig till skölden för skydd av privatlivet måste organisationen a) underställa sig den federala konkurrensmyndigheten (*Federal Trade Commission*, nedan kallad *FTC*), transportministeriets eller ett annat lagstadgat organs utrednings- och verkställighetsbefogenheter, som kommer att säkerställa efterlevnad av principerna (*andra amerikanska lagstadgade organ som är erkända av EU kan inbegripas som en bilaga i framtiden*), b) offentligt förklara att den kommer att följa principerna, c) offentliggöra sin integritetsskyddspolicy i enlighet med dessa principer, och d) genomföra dem fullständigt. En organisations underlåtenhet att iaktta principerna är verkställbar i enlighet med avdelning 5 i *Federal Trade Commission Act*, som förbjuder illojala och bedrägliga handlingar inom ramen för affärsverksamhet eller handlingar som påverkar denna (15 U.S.C. § 45(a)) eller annan lagstiftning eller andra föreskrifter som förbjuder sådana handlingar.

3. Handelsministeriet kommer att upprätthålla och offentliggöra en officiell förteckning över amerikanska organisationer som genom självcertifiering till handelsministeriet har anslutit sig till principerna (nedan kallad förteckningen över organisationer som anslutit sig till skölden). Fördelar i samband med skölden för skydd av privatlivet garanteras från och med det datum då ministeriet för upp organisationen på förteckningen över organisationer som anslutit sig till skölden. Ministeriet kommer att stryka organisationer från förteckningen över organisationer som anslutit sig till skölden som frivilligt drar sig tillbaka från skölden för skydd av privatlivet eller som inte lämnar in sin årliga återcertifiering till ministeriet. Organisationer som stryks från förteckningen över organisationer som anslutit sig till skölden omfattas inte längre av de fördelar som Europeiska kommissionens beslut om adekvat skyddsnivå medför, dvs. att motta personuppgifter från EU. Organisationen måste fortsätta att tillämpa principerna på de personuppgifter som den mottog medan den deltog i skölden för skydd av privatlivet, och årligen bekräfta till ministeriet att den åtar sig att göra detta under hela den tid som den behåller sådana uppgifter. I annat fall måste organisationen återlämna eller radera uppgifterna eller tillhandahålla en ”adekvat” skyddsnivå för uppgifterna genom andra tillåtna medel. Ministeriet kommer även att stryka organisationer som upprepade gånger har överträtt principerna från förteckningen över organisationer som anslutit sig till skölden. Dessa organisationer omfattas inte av de fördelar som skölden för skydd av privatlivet medför och måste återlämna eller radera de personuppgifter som de har mottagit inom ramen för skölden.

4. Ministeriet kommer också att föra och offentliggöra ett officiellt register över amerikanska organisationer som tidigare har lämnat in en självcertifiering till ministeriet, men som har strukits från förteckningen över organisationer som anslutit sig till skölden. Ministeriet kommer att utfärda en tydlig varning om att dessa organisationer inte deltar i skölden för skydd av privatlivet, att en organisation som stryks från förteckningen över organisationer som anslutit sig till skölden inte längre inte kan hävda att den efterlever skölden och att den måste undvika alla uttalanden eller vilseledande metoder som antyder att den deltar i skölden samt att sådana

([1]) Under förutsättning att kommissionens beslut om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna gäller för Island, Liechtenstein och Norge kommer skölden för skydd av privatlivet att omfatta både EU och dessa tre länder. Därför kommer hänvisningarna till EU och dess medlemsstater tolkas som att de även inbegriper Island, Liechtenstein och Norge.

organisationer inte längre är berättigade att omfattas av de fördelar som kommissionens beslut om adekvat skyddsnivå medför, som skulle ge organisationerna rätt att motta personuppgifter från EU. En organisation som fortsätter att hävda att den deltar i skölden för skydd av privatlivet eller gör andra oriktiga utfästelser i samband med skölden efter det att den har strukits från förteckningen över organisationer som anslutit sig till skölden, kan bli föremål för verkställighetsåtgärder av FTC, transportministeriet eller andra verkställande myndigheter.

5. Efterlevnaden av principerna kan begränsas a) till vad som är nödvändigt för att uppfylla krav i fråga om nationell säkerhet, allmänintresset och rättsefterlevnaden, b) av lagar, myndighetsföreskrifter eller rättspraxis som skapar motstridiga skyldigheter eller ger explicita befogenheter, förutsatt att organisationen då den utövar dessa befogenheter kan visa att avvikelsen från principerna begränsar sig till vad som är nödvändigt för att de övergripande legitima intressen som är beroende av dessa befogenheter ska kunna tillgodoses, eller c) om följden av direktivet eller medlemsstaternas lagstiftning är att man tillåter undantag och avvikelser förutsatt att sådana undantag eller avvikelser tillämpas i jämförbara sammanhang. I överensstämmelse med målen om ökat integritetsskydd bör organisationerna sträva efter att genomföra dessa principer öppet och fullt ut, samt även ange i sina planer för integritetsskydd på vilka områden undantag från principerna av skäl angivna i b ovan kommer att göras regelbundet. Av samma skäl förväntas organisationerna, såvida det finns en valmöjlighet enligt principerna och/eller amerikansk lag, välja en högre skyddsnivå om det är möjligt.

6. Organisationerna är skyldiga att tillämpa principerna på alla personuppgifter som överförts inom ramen för skölden för skydd av privatlivet efter sin anslutning till skölden. En organisation som väljer att utsträcka förmånerna i samband med skölden för skydd av privatlivet till att även omfatta personaluppgifter som överförs från EU för att användas i samband med ett anställningsförhållande måste ange detta när den lämnar in sin självcertifiering till handelsministeriet och uppfylla kraven enligt den kompletterande principen om självcertifiering.

7. Amerikansk lag kommer att gälla för frågor som rör tolkning och efterlevnad av principerna och den integritetsskyddspolicy som tillämpas av organisationer anslutna till skölden utom i de fall då sådana organisationer har förbundit sig att samarbeta med dataskyddsmyndigheter i EU. Om inget annat anges ska bestämmelser enligt principerna gälla på de områden de avser.

8. Definitioner:

   a. Personuppgifter: sådana uppgifter om en identifierad eller identifierbar fysisk person som faller inom tillämpningen av direktivet och som mottagits av en organisation i Förenta staterna från Europeiska unionen och är registrerade i någon form.

   b. Behandling av personuppgifter: en åtgärd eller kombination av åtgärder beträffande personuppgifter, oberoende av om de utförs automatiserat eller ej, såsom insamling, registrering, organisering, lagring, bearbetning eller ändring, framtagning, läsning, användning, utlämning eller spridning och radering eller förstöring.

   c. Personuppgiftsansvarig: en person eller organisation som ensam eller tillsammans med andra bestämmer ändamålen och medlen för behandlingen av personuppgifter.

9. Det datum då principerna träder i kraft är datumet för Europeiska kommissionens slutliga godkännande av beslutet om adekvat skyddsnivå.

II. PRINCIPER

1. **Påpekande**

   a. En organisation måste informera enskilda personer om

      i. att den deltar i skölden för skydd av privatlivet och ange en länk eller webbadressen till förteckningen över organisationer som anslutit sig till skölden,

      ii. de typer av personuppgifter som samlas in och, i förekommande fall, de enheter eller dotterföretag till organisationen som också har anslutit sig till principerna,

iii. att den garanterar att alla personuppgifter som mottas från EU inom ramen för skölden omfattas av principerna,

iv. anledningen till att den samlar in och använder uppgifter om dem,

v. hur de kontaktar organisationen om de har frågor eller klagomål, även eventuella relevanta organ i EU som kan besvara sådana frågor eller klagomål,

vi. typ av eller identitet för tredje part som organisationen lämnar ut personuppgifter till och anledningarna till att den gör det,

vii. enskilda personers rätt att få tillgång till sina personuppgifter,

viii. vilka valmöjligheter och tillvägagångssätt som organisationen ger den enskilda personen att begränsa personuppgifternas användning och utlämnande,

ix. det oberoende tvistlösningsorgan som organisationen har utsett för att behandla klagomål och kostnadsfritt tillhandahålla lämpliga rättsmedel till den enskilda personen, och om detta är 1) den arbetsgrupp som har inrättats av dataskyddsmyndigheterna, 2) ett alternativt tvistlösningsorgan som är baserat i EU, eller 3) ett alternativt tvistlösningsorgan baserat i Förenta staterna,

x. som omfattas av de utrednings- och verkställighetsbefogenheter som FCT, transportministeriet eller ett annat amerikanskt behörigt organ har tilldelats,

xi. den enskilda personens möjlighet att, på vissa villkor, kräva ett bindande skiljedomsförfarande,

xii. kravet att lämna ut personuppgifter till följd av en lagstadgad begäran från offentliga myndigheter, även för att uppfylla nationella säkerhets- eller brottbekämpningskrav, och

xiii. dess ansvar vid vidareöverföring till tredje part.

b. Detta meddelande, som ska vara lättbegripligt och lättläst, ska lämnas vid det tillfälle då den enskilde för första gången ombes lämna personuppgifter till en viss organisation eller så snart därefter det är praktiskt möjligt, men i alla händelser innan organisationen använder sådana uppgifter för ett annat ändamål än det för vilket de ursprungligen insamlades eller behandlades av den organisation som överför uppgifterna eller lämnar ut dem till tredje part för första gången.

2. **Valmöjlighet**

a. En organisation ska ge den enskilda personen möjlighet att välja (opt out) om hans eller hennes personuppgifter ska i) lämnas till tredje part, eller ii) användas till ett ändamål som väsentligen skiljer sig från det syfte/de syften för vilka de ursprungligen insamlades eller de enskilda personerna i efterhand har gett sitt tillstånd till. Enskilda personer måste på ett tydligt och lättillgängligt sätt ges möjlighet att utöva denna valmöjlighet.

b. Genom undantag från föregående stycke är det inte nödvändigt att tillämpa principen om valmöjlighet när uppgifter lämnas ut till en tredje part som agerar på organisationens vägnar och därvid utför uppgifter åt organisationen enligt dennas instruktioner. Organisationen ska dock alltid ingå ett avtal med förmedlaren.

c. För känsliga uppgifter (dvs. personuppgifter som rör medicinska förhållanden och hälsa, ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i fackförening eller uppgifter rörande sexualliv) måste organisationerna inhämta ett uttryckligt samtycke (opt in) från de enskilda personerna om uppgifterna kommer att i) lämnas ut till en tredje part, eller ii) användas för ett annat ändamål än det för vilket de ursprungligen samlades in eller de enskilda personerna i efterhand har gett sitt tillstånd till genom att välja (opt in). Om en tredje part anser att personuppgifter är känsliga och behandlar dem därefter ska en organisation som mottagit dessa alltid behandla dem som känsliga.

3. **Ansvar för vidareöverföring**

a. För att organisationer ska få överföra uppgifter till en tredje part i egenskap av personuppgiftsansvariga måste de uppfylla principerna om meddelande och valmöjlighet. Organisationerna måste också ingå ett avtal med den tredje part som agerar som personuppgiftsansvarig om att sådana uppgifter endast får behandlas för begränsade och uttryckligt angivna ändamål som är förenliga med den enskilda personens samtycke och att mottagaren kommer att tillhandahålla samma skyddsnivå som enligt principerna och meddela organisationen om den fastställer att den inte längre kan fullfölja denna skyldighet. Avtalet ska föreskriva att när ett sådant fastställande har gjorts ska den tredje part som agerar som personuppgiftsansvarig upphöra med behandlingen eller vidta andra lämpliga och skäliga korrigeringsåtgärder.

b. För att överföra personuppgifter till en tredje part som agerar som förmedlare ska organisationerna i) endast överföra sådana uppgifter för begränsade angivna ändamål, ii) förvissa sig om att förmedlaren är skyldig att tillhandahålla minst samma integritetsskyddsnivå som krävs i principerna, iii) vidta rimliga och lämpliga åtgärder för att se till att förmedlaren faktiskt behandlar de överförda personuppgifterna på ett sätt som är förenligt med organisationens skyldigheter enligt principerna, iv) kräva att förmedlaren meddelar organisationen om den fastställer att den inte längre kan fullfölja skyldigheten att tillhandahålla samma skyddsnivå som enligt principerna, v) till följd av ett meddelande, inbegripet enligt led iv, vidta skäliga och lämpliga åtgärder för att stoppa och korrigera otillåten behandling, och vi) på begäran lämna en sammanfattning eller en representativ kopia av de relevanta integritetsskyddsbestämmelserna i sitt avtal med förmedlaren till myndigheten.

4. **Säkerhet**

a. Organisationer som skapar, lagrar, använder eller sprider personuppgifter måste vidta rimliga och lämpliga försiktighetsåtgärder för att se till att de inte går förlorade, missbrukas eller utan tillstånd tas fram, utlämnas, förvanskas eller förstörs, med vederbörligt beaktande av riskerna i samband med behandlingen och personuppgifternas natur.

5. **Dataintegritet och ändamålsbegränsning**

a. I enlighet med principerna måste personuppgifter begränsas till de uppgifter som är relevanta för ändamålet med behandlingen ([1]). En organisation får inte behandla personuppgifter på ett sätt som är oförenligt med det ändamål för vilket de samlades in om inte den enskilde i efterhand har gett sitt tillstånd. I den omfattning som krävs för dessa ändamål måste en organisation vidta nödvändiga åtgärder för att se till att personuppgifterna är tillförlitliga för det avsedda ändamålet samt riktiga, fullständiga och aktuella. Organisationerna måste följa principerna så länge som de behåller sådana uppgifter.

b. Uppgifter får endast lagras på ett sätt som identifierar den enskilde eller gör denne identifierbar ([2]) så länge som de uppfyller kravet på ändamål för behandling i den mening som avses i 5a. Denna skyldighet hindrar inte organisationer från att behandla personuppgifter under längre perioder för den tid och i den omfattning sådan behandling skäligen gynnar ändamålen för arkivering i allmänhetens intresse, journalistik, litteratur och konst, vetenskaplig eller historisk forskning och statistisk analys. I dessa fall ska sådan behandling omfattas av de andra principerna och bestämmelserna för skölden. Organisationer bör vidta rimliga och lämpliga åtgärder för att uppfylla denna bestämmelse.

6. **Tillgång**

a. Enskilda ska ha tillgång till de personuppgifter om dem själva som en organisation innehar och ska ha möjlighet att rätta, ändra eller utplåna dessa uppgifter då de är felaktiga eller har behandlats i strid mot principerna, utom då arbetet eller kostnaden för denna tillgång inte står i proportion till risken för den enskildes personliga integritet i ärendet i fråga eller då en annan persons legitima rättigheter skulle kränkas.

([1]) Exempel på förenliga ändamål för behandling kan, beroende på omständigheterna, inbegripa sådana som skäligen kan gynna kundrelationerna, efterlevnad och rättsliga aspekter, revision, säkerhet och bedrägeribekämpning, bevarande eller försvar av organisationens juridiska rättigheter, eller andra ändamål som överensstämmer med en omdömesgill persons förväntningar mot bakgrund av insamlingens sammanhang.

([2]) Om en enskild person i detta sammanhang rimligen kan identifieras av organisationen, eller en tredje part om den skulle ha tillgång till uppgifterna, är den enskilde, med tanke på de metoder för identifiering som rimligen kan komma att användas (med beaktande av bland annat kostnaderna och tidsåtgången för identifiering och den tillgängliga tekniken vid tidpunkten för behandlingen) och i vilken form uppgifterna lagras, att betraktas som ”identifierbar”.

7. **Rättsmedel, genomförande och ansvar**

a. Ett effektivt skydd av den personliga integriteten måste innefatta robusta mekanismer för att se till att principerna följs, att de enskilda personer som drabbats av att principerna inte följts kan vidta rättsliga åtgärder samt att det blir påföljder för den organisation som inte följer principerna. Dessa system ska minst omfatta följande:

i. Enkelt tillgängliga och billiga oberoende instanser för handläggning av klagomål genom vilka varje enskilds klagomål och tvister kan handläggas och lösas utan kostnad för den enskilda personen och genom hänvisning till principerna samt skadestånd tilldelas då tillämpliga lagar eller initiativ inom den privata sektorn så föreskriver.

ii. Uppföljningsförfaranden för att kontrollera att företagens intyg och försäkringar i fråga om deras förfaranden för integritetsskydd är sanna och att förfaranden för integritetsskydd har genomförts såsom angivits, särskilt när det gäller bristande efterlevnad.

iii. Skyldighet att åtgärda problem som uppstår till följd av att principerna inte har efterlevts i de organisationer som har tillkännagivit att de följer dem samt påföljder för dessa organisationer. Påföljderna ska vara tillräckligt stränga för att garantera att organisationerna följer principerna.

b. Organisationer och deras valda oberoende instanser för handläggning av klagomål kommer utan dröjsmål att besvara förfrågningar och ansökningar avseende skölden för skydd av privatlivet från ministeriets informationsavdelning. Alla organisationer måste på lämpligt sätt via informationsavdelningen besvara klagomål rörande överensstämmelse med principerna som hänskjuts från myndigheter i EU-medlemsstaterna. Organisationer som har valt att samarbeta med dataskyddsmyndigheter, inklusive organisationer som behandlar personaluppgifter, måste direkt besvara frågor från sådana myndigheter med avseende på utredning och lösning av klagomål.

c. Organisationer är skyldiga att lösa yrkanden genom skiljedom och uppfylla de villkor som anges i bilaga I, under förutsättning att den enskilda personen har åberopat bindande skiljedom genom att anmäla organisationen i fråga enligt de förfaranden och villkor som anges i bilaga I.

d. I samband med vidare överföring har organisationer som har anslutit sig till skölden för skydd av privatlivet ansvar för behandlingen av de personuppgifter som den mottar inom ramen för skölden, och för vidare överföringar till en tredje part som agerar som förmedlare för organisationens räkning. Organisationer som anslutit sig till skölden är fortfarande skyldiga att följa principerna om deras förmedlare behandlar sådana personuppgifter på ett sätt som inte överensstämmer med principerna, om inte organisationen kan visa att den inte kan hållas ansvarig för den skada som har uppkommit.

e. När en organisation blir föremål för ett rättsligt avgörande från FTC eller en domstol baserat på bristande efterlevnad ska den offentliggöra eventuella avsnitt i efterlevnads- eller bedömningsrapporter som lämnas in till FTC och som är relevanta för skölden, i den utsträckning det är förenligt med sekretesskraven. Ministeriet har inrättat en särskild kontaktpunkt för dataskyddsmyndigheter dit de kan vända sig med eventuella efterlevnadsproblem angående organisationer som har anslutit sig till skölden. FTC kommer att prioritera hänskjutanden om bristande efterlevnad av principerna från ministeriet och EU-medlemsstaterna myndigheter, och kommer i god tid att utbyta information om hänskjutanden med den hänskjutande statliga myndigheten, med förbehåll för befintliga sekretessbegränsningar.

III. KOMPLETTERANDE PRINCIPER

1. **Känsliga uppgifter**

a. En organisation är inte skyldig att inhämta uttryckligt samtycke (opt in) med avseende på känsliga uppgifter när behandlingen är

i. av avgörande betydelse för den registrerade eller annan person,

ii. nödvändig för fastställande av rättsliga yrkanden eller rättsligt försvar,

iii. nödvändig för medicinsk behandling eller diagnos,

iv. utförs inom ramen för berättigad verksamhet hos en stiftelse, en förening eller ett annat icke vinstdrivande organ, som har ett politiskt, filosofiskt, religiöst eller fackligt syfte, förutsatt att behandlingen endast rör sådana organs medlemmar eller personer som på grund av organets ändamål har regelbunden kontakt med detta och uppgifterna inte lämnas ut till tredje part utan den registrerades samtycke,

v. nödvändig för att en organisation ska kunna fullgöra sina förpliktelser på arbetslagstiftningens område,

vi. gäller uppgifter som uttryckligen offentliggörs av den enskilda personen.

2. **Journalistiska undantag**

a. Med tanke på Förenta staterna:s konstitutionella skydd av pressfriheten och direktivets undantag för journalistiskt material ska, när den tryckfrihet som är fastlagd i det första tillägget till Förenta staternas konstitution råkar i konflikt med rätten till skydd för den personliga integriteten, första tillägget styra hur avvägningen mellan dessa intressen ska göras när det gäller medborgare eller företag i Förenta staterna.

b. Personuppgifter som samlas in för publicering, radio- och TV-sändningar eller andra former av offentliggörande av journalistisk stoff, vare sig det används eller inte, samt uppgifter som återfinns i tidigare offentliggjort stoff som sprids från mediers arkiv omfattas inte av kraven enligt sköldens principer.

3. **Sekundärt ansvar**

a. Internetleverantörer, teleföretag eller andra organisationer är inte ansvariga enligt sköldens principer när de på en annan organisations vägnar endast överför, dirigerar, växlar eller cachar uppgifter som strider mot bestämmelserna. I likhet med direktivet skapar sköldens principer inte något sekundärt ansvar. När en organisation endast kanaliserar uppgifter som överförts av tredje man och inte bestämmer ändamålet eller sättet för behandlingen av personuppgifterna, är den inte ansvarig.

4. **Utförande av företagsbesiktningar och revisioner**

a. Den verksamhet som bedrivs av revisorer och investeringsbanker kan medföra att personuppgifter behandlas utan den enskilda personens samtycke eller vetskap. Detta är tillåtet enligt principerna om meddelande, valmöjlighet och tillgång enligt beskrivningen nedan.

b. Publika aktiebolag och företag som ägs av nära familjemedlemmar, inklusive organisationer som har anslutit sig till skölden för skydd av privatlivet, genomgår regelbundna revisioner. Sådana revisioner, särskilt om de rör utredningar av eventuella förseelser, kan äventyras om resultaten lämnas ut för tidigt. På samma sätt måste en organisation som har anslutit sig till skölden och är involverad i eventuella fusioner eller uppköp utföra eller genomgå en företagsbesiktning. Detta medför ofta insamling och behandling av personuppgifter, såsom information om ledande befattningshavare och andra nyckelpersoner. Om sådan information lämnas ut i förtid kan detta hindra transaktionen eller till och med utgöra en överträdelse av tillämplig aktielagstiftning. Investeringsbanker och jurister som utför företagsbesiktningar eller revisorer som utför revisioner får utan den enskilda personens vetskap behandla uppgifter endast i den omfattning och under den tid som det är nödvändigt för att lagstadgade krav ska kunna uppfyllas eller det allmänna intresset tillgodoses, och under andra förhållanden där en tillämpning av dessa principer skulle skada organisationens rättmätiga intressen. Sådana rättmätiga intressen är övervakningen av att en organisation uppfyller sina lagstadgade förpliktelser och sin redovisningsskyldighet, liksom behovet av sekretess i samband med eventuella förvärv, fusioner, samriskföretag eller andra liknande arrangemang som genomförs av investeringsbanker eller revisorer.

5. **Dataskyddsmyndigheternas roll**

a. Organisationerna kommer att fullgöra sitt åtagande att samarbeta med europeiska dataskyddsmyndigheter enligt beskrivningen nedan. Enligt sköldens principer ska organisationer i Förenta staterna som tar emot personuppgifter från EU förbinda sig att på lämpligt sätt sörja för att principerna efterlevs. Närmare bestämt ska deltagande organisationer, enligt principen om rättsmedel, genomförande och ansvar, säkerställa följande: a.i) tillhandahålla möjlighet för de personer som uppgifterna berör att få sin sak prövad, a.ii) tillhandahålla uppföljningsrutiner för att kontrollera att de försäkringar de gjort om sina integritetsskyddsrutiner är sanningsenliga och a.iii) förplikta sig att lösa problem som beror på att principerna inte följs och ta konsekvenserna i form av påföljder i förekommande fall. En organisation kan uppfylla förpliktelserna enligt punkterna a.i och a.iii i principen om rättsmedel, genomförande och ansvar om den iakttar de krav på samarbete med dataskyddsmyndigheterna som anges här.

b. En organisation förpliktar sig att samarbeta med dataskyddsmyndigheterna genom att i sin skrivelse om självcertifiering avseende skölden till handelsministeriet (*se* den kompletterande principen om självcertifiering) förklara att den

i. väljer att uppfylla de krav som anges i punkterna a.i och a.iii i principen om rättsmedel genomförande och ansvar genom att förbinda sig att samarbeta med dataskyddsmyndigheterna,

ii. kommer att samarbeta med dataskyddsmyndigheterna vid handläggning av klagomål som inges inom ramen för skölden för skydd av privatlivet, och

iii. kommer att rätta sig efter dataskyddsmyndigheternas rekommendationer om dessa finner att organisationen måste vidta särskilda åtgärder för att den ska anses följa sköldens principer; detta omfattar korrigerande åtgärder och gottgörelse till enskilda som drabbats av att principerna inte följs, och att den skriftligen till dataskyddsmyndigheterna kommer att bekräfta att sådana åtgärder har vidtagits.

c. Dataskyddsmyndigheternas arbetsgrupper

i. Dataskyddsmyndigheternas samarbete sker i form av information och rekommendationer på följande sätt:

1. Dataskyddsmyndigheternas rekommendationer avges via en informell särskild arbetsgrupp, bestående av dataskyddsmyndigheter inrättad på europeisk nivå. Denna arbetsgrupp ska bland annat hjälpa till med att se till att ett enhetligt och konsekvent tillvägagångssätt tillämpas.

2. Arbetsgruppen ska avge rekommendationer till berörda amerikanska organisationer om olösta klagomål från enskilda rörande hanteringen av personuppgifter som har överförts från EU inom ramen för skölden för skydd av privatlivet. Dessa rekommendationer ska vara utformade på ett sätt som säkerställer att sköldens principer tillämpas korrekt och ska innehålla uppgifter om den gottgörelse till den enskilda personen som dataskyddsmyndigheterna anser är lämplig.

3. Arbetsgruppen ska avge sådana rekommendationer i ärenden som hänskjutits till den av berörda organisationer och/eller som svar på klagomål som inkommer direkt från enskilda och rör organisationer som har förbundit sig att samarbeta med dataskyddsmyndigheterna i samband med skölden. Gruppen ska uppmuntra och vid behov hjälpa enskilda att först och främst använda de interna förfaranden för handläggning av klagomål som organisationen erbjuder.

4. Rekommendationer kommer först att avges efter det att båda parter i en tvist har givits en rimlig möjlighet att inkomma med synpunkter och förete eventuella bevis. Arbetsgruppen ska avge sina rekommendationer så snabbt som möjligt inom ramen för korrekt handläggning av ärendet. Normalt gäller att gruppen ska ha som målsättning att avge sina rekommendationer inom 60 dagar efter det att den mottagit ett klagomål eller ett ärende hänskjutits för handläggning, och om möjligt ännu snabbare.

5. Arbetsgruppen kommer att offentliggöra hur den handlagt klagomål som inkommit, om den anser att detta är lämpligt.

6. Arbetsgruppens rekommendationer innebär inga åligganden vare sig för arbetsgruppen själv eller för enskilda dataskyddsmyndigheter.

ii. Organisationer som väljer detta alternativ för tvistlösning måste i enlighet med ovanstående förbinda sig att följa dataskyddsmyndigheternas rekommendationer. Om en organisation inte följer dessa rekommendationer inom 25 dagar efter det att rekommendationerna avgetts och inte har någon tillfredsställande förklaring till förseningen, ska arbetsgruppen underrätta organisationen om sin avsikt att hänskjuta ärendet till antingen den amerikanska federala konkurrensmyndigheten (*Federal Trade Commission*), transportministeriet eller annan federal myndighet/ett annat offentligt organ i Förenta staterna som har lagstadgad behörighet att vidta tvingande åtgärder mot bedrägliga metoder och missvisande information eller som kan fastställa att en allvarlig överträdelse har skett av samarbetsavtalet, som därmed ska anses ogiltigt. I det senare fallet ska den särskilda arbetsgruppen underrätta handelsministeriet så att förteckningen över organisationer som anslutit sig till skölden kan ändras på motsvarande sätt. Underlåtenhet att fullgöra förpliktelsen att samarbeta med dataskyddsmyndigheterna kan liksom underlåtenhet att följa sköldens principer leda till att åtal väcks för bedrägligt beteende enligt avdelning 5 i den amerikanska lagen om osann utsaga (*False Statements Act*) eller liknande regelverk.

d Organisationer som vill att dess förmåner enligt skölden för skydd av privatlivet ska omfatta personaluppgifter som överförs från EU inom ramen för ett anställningsförhållande måste förbinda sig att samarbeta med dataskyddsmyndigheterna med avseende på sådana uppgifter (se den kompletterande principen om personaluppgifter).

e Organisationer som väljer detta alternativ påförs en årsavgift som är avsedd att täcka kostnaderna för den särskilda arbetsgruppens verksamhet. Dessutom kan organisationerna påföras de eventuella översättningskostnader som uppstår under arbetsgruppens behandling av klagomål eller ärenden som hänskjutits till den. Årsavgiften ska uppgå till högst 500 US-dollar och vara lägre för mindre företag.

6. **Självcertifiering**

a. Förmåner i samband med skölden för skydd av privatlivet garanteras från och med det datum då ministeriet för upp organisationen på förteckningen över organisationer som anslutit sig till skölden.

b. Organisationer som vill ansluta sig till skölden för skydd av privatlivet genom självcertifiering måste till ministeriet lämna in en självcertifiering, som ska vara undertecknad av en person i ansvarig ställning på den organisations vägnar som ansluter sig till skölden. Denna skrivelse ska innehålla åtminstone följande uppgifter:

i. Organisationens namn, postadress, e-postadress, telefon- och faxnummer.

ii. En beskrivning av den del av organisationens verksamhet som rör personuppgifter som tas emot från EU.

iii. En beskrivning av organisationens integritetsskyddspolicy för sådana personuppgifter, vilken ska omfatta

1. om organisationen har en offentlig webbplats, relevant webbadress där dess policy för integritetsskydd finns tillgänglig, eller om organisationen inte har en offentlig webbplats, en angivelse av var dess policy för integritetsskydd finns tillgänglig för allmänheten,

2. det datum den trädde i kraft,

3. en kontaktpunkt för handläggningen av klagomål, ansökningar om åtkomst och andra frågor som kan uppstå inom ramen för skölden,

4. det särskilda lagstadgade organ som är behörigt för att behandla eventuella yrkanden som riktas mot organisationen avseende illojala eller bedrägliga metoder och överträdelser av lagstiftning eller andra föreskrifter som reglerar integritetsfrågor (och anges i principerna eller i framtida bilagor till dessa),

5. namn på eventuella program för integritetsskydd som organisationen deltar i,

6. kontrollmetod (t.ex. intern eller genom tredje part (se den kompletterande principen om kontroll, och

7. den oberoende instans som handlägger olösta klagomål,

c. Om organisationen vill att de fördelar som skölden för skydd av privatlivet innebär ska omfatta personaluppgifter som överförs från EU för att användas inom ramen för anställningsförhållandet, kan detta tillåtas om det finns en tillsynsmyndighet som anges i principerna eller i en framtida bilaga till principerna och som är behörig att behandla klagomål som för organisationen och gäller behandling av sådana personaluppgifter. Dessutom ska organisationen ange detta i sin självcertifiering och förklara att den förbinder sig att samarbeta med berörda EU-myndigheter i enlighet med de kompletterande principerna om personaluppgifter och dataskyddsmyndigheternas roll, beroende på vilken som är tillämplig, samt att den kommer att följa dessa myndigheters rekommendationer. Organisationen ska också lämna en kopia av sin integritetsskyddspolicy avseende personaluppgifter till ministeriet och ange var integritetsskyddspolicyn finns tillgänglig för berörda anställda.

d. Handelsministeriet kommer att hålla en förteckning över alla organisationer som lämnar in självcertifieringar, varigenom fördelarna med skölden för skydd av privatlivet garanteras. Förteckningen kommer att uppdateras i överensstämmelse med de skrivelser om återcertifiering som inkommer varje år och de anmälningar som erhålls i enlighet med den kompletterande principen om tvistlösning och verkställighet. Sådana skrivelser om självcertifiering ska skickas in minst en gång om året. I annat fall stryks organisationen från förteckningen över organisationer som anslutit sig till skölden och de fördelar som skölden innebär kan inte längre åberopas. Såväl förteckningen som de skrivelser om självcertifiering som organisationer skickar in kommer att offentliggöras. Alla organisationer som ministeriet för upp på förteckningen ska även i sin relevanta integritetsskyddspolicy förklara att de följer sköldens principer. Om organisationens integritetsskyddspolicy finns tillgänglig online ska

den innehålla en hyperlänk till ministeriets webbplats för sköldén för skydd av privatlivet och en hyperlänk till ett klagomålsformulär som den oberoende instansen för handläggning av klagomål har gjort tillgängligt för att utreda olösta klagomål.

e. Principerna om integritetsskydd blir omedelbart tillämpliga vid certifiering. Principerna kommer att påverka kommersiella förbindelser med tredje parter, och organisationer som certifierar sin anslutning till sköldén för skydd av privatlivet under de första två månaderna efter ramens ikraftträdande ska därför bringa befintliga kommersiella förbindelser med tredje parter i överensstämmelse med principen om ansvar för vidareöverföring så snart som möjligt, och i alla händelser senast nio månader från det datum då de certifierade sin anslutning till sköldén. Under den mellanliggande perioden ska organisationerna om de överför uppgifter till en tredje part i) tillämpa principerna om meddelande och valmöjlighet, och ii) om personuppgifter överförs till en tredje part som agerar som förmedlare, försäkra sig om att förmedlaren är skyldig att tillhandahålla åtminstone samma skyddsnivå som den som krävs enligt principerna.

f. Organisationerna måste säkerställa att alla personuppgifter som mottas från EU inom ramen för sköldén omfattas av principerna. Åtagandet att följa sköldens principer gäller utan tidsbegränsning för de personuppgifter som organisationen mottagit under den tid som organisationen åtnjuter fördelarna med sköldén. Åtagandet innebär att organisationen kommer att fortsätta att tillämpa principerna på dessa uppgifter under hela den tid som organisationen lagrar, behandlar eller lämnar ut uppgifterna, även om organisationen av någon anledning lämnar sköldén. En organisation som drar sig tillbaka från sköldén för skydd av privatlivet men vill behålla sådana uppgifter, måste årligen till ministeriet bekräfta sitt åtagande att fortsätta att tillämpa principerna eller tillhandahålla en ”adekvat” skyddsnivå för uppgifterna genom andra tillåtna medel (t.ex. genom ett avtal som fullständigt avspeglar kraven i de relevanta standardavtalsbestämmelser som antagits av Europeiska kommissionen). I annat fall måste organisationen återlämna eller radera uppgifterna. En organisation som drar sig tillbaka från sköldén måste avlägsna eventuella hänvisningar från relevanta offentliggjorda integritetsskyddspolicyer som antyder att organisationerna fortsätter att aktivt delta i sköldén för skydd av privatlivet och omfattas av dess förmåner.

g. En organisation som till följd av fusion eller uppköp kommer att upphöra som separat juridisk person ska anmäla detta i förväg till handelsministeriet. I denna anmälan ska det även anges om den förvärvande enheten eller den enhet som uppstår genom fusionen i) kommer att fortsätta att vara bunden av sköldens principer enligt den lagstiftning som styr uppköpet eller fusionen, eller ii) väljer självcertifiering för anslutning till sköldens principer eller inför andra garantier, t.ex. ett skriftligt avtal som säkrar anslutningen till sköldens principer. Om varken alternativ i eller ii är tillämpligt ska samtliga personuppgifter som erhållits inom ramen för sköldén omedelbart raderas.

h. En organisation som av någon anledning lämnar sköldén för skydd av privatlivet måste avlägsna alla förklaringar som antyder att organisationen fortsätter att delta i sköldén eller omfattas av dess förmåner. Om certifieringsmärkningen för sköldén används måste även den avlägsnas. Vid missvisande information till allmänheten om en organisations anslutning till sköldén kan FTC eller annan federal instans väcka åtal. Oriktiga utfästelser till ministeriet kan leda till åtal i enlighet med den amerikanska lagen om osann utsaga (*False Statements Act*, 18USC § 1001).

7. **Kontroll**

a. Organisationerna måste tillämpa uppföljningsförfaranden för att kontrollera att de försäkringar de gjort om sina integritetsskyddsrutiner inom ramen för sköldén för skydd av privatlivet är sanningsenliga och att dessa integritetsskyddsrutiner tillämpas enligt vad som framförts och i överensstämmelse med sköldens principer.

b. För att kraven på kontroll enligt principen om rättsmedel, genomförande och ansvar ska uppfyllas måste organisationen kontrollera sådana försäkringar antingen genom egenkontroll eller externa granskningar.

c. Om man väljer en sådan egenkontroll måste förfarandet visa att organisationens offentliggjorda integritetsskyddspolicy avseende personuppgifter som erhålls från EU är korrekt, heltäckande och offentliggjord på ett tydligt sätt, att den tillämpas fullt ut och att den är tillgänglig för insyn. Organisationen måste också visa att dess integritetsskyddspolicy överensstämmer med sköldens principer, att enskilda personer informeras om eventuella interna arrangemang för handläggning av klagomål och om det oberoende system genom vilket de kan inge klagomål, att det finns förfaranden för utbildning av personal av tillämpning av denna policy och att man vidtar disciplinära åtgärder om policyn inte följs samt att organisationen har interna förfaranden att genomföra

återkommande objektiva granskningar för att kontrollera att ovanstående efterlevs. En rapport om egenkontrollen måste undertecknas av en person i ansvarig ställning eller en annan behörig representant vid företaget minst en gång om året och göras tillgänglig på konsumentens begäran eller inom ramen för en undersökning eller ett klagomål över att bestämmelserna inte efterlevts.

d. Om organisationerna väljer en extern granskning, ska en sådan granskning visa att organisationens integritetsskyddspolicy avseende personuppgifter som erhålls från EU överensstämmer med sköldens principer och att den tillämpas. Metoderna för granskning kan utan begränsning omfatta revision, slumpmässiga kontroller, användandet av "lockbeten", eller i tillämpliga fall användandet av tekniska verktyg. En rapport om att en extern granskning har genomförts ska undertecknas av granskaren eller av en person i ansvarig ställning eller en annan behörig representant vid företaget. Detta ska ske minst en gång om året och rapporten ska göras tillgänglig på begäran av konsumenterna eller inom ramen för ett överklagande.

e. Organisationerna ska dokumentera sina integritetsskyddsrutiner inom ramen för skölden för skydd av privatlivet och på begäran göra dessa dokumentationer tillgängliga (i samband med en undersökning eller klagomål över att bestämmelserna inte följs) för det oberoende organ som svarar för handläggning av klagomål eller till den myndighet som har ansvar för frågor om illojala metoder och bedrägligt beteende. Organisationerna måste också utan dröjsmål besvara förfrågningar och andra ansökningar om information från ministeriet rörande organisationens anslutning till principerna.

8. **Tillgång**

a. Principen om tillgång i praktiken

i. Enligt sköldens principer är rätten till tillgång grundläggande för integritetsskyddet. I synnerhet medger den enskilda personer att kontrollera om de uppgifter som finns om dem är korrekta. Principen om tillgång innebär att enskilda personer har rätt att

1. få bekräftelse på om organisationer behandlar uppgifter som rör dem eller inte ([1]),

2. har meddelat dem sådana uppgifter så att de kan kontrollera att de är riktiga och att behandlingen är laglig, och

3. få uppgifterna korrigerade, ändrade eller raderade om de är felaktiga eller behandlas i strid mot principerna.

ii. Enskilda behöver inte motivera sin förfrågan om att få ta del av sina personuppgifter. Då organisationerna tillmötesgår enskildas förfrågan om tillgång bör de först låta sig ledas av bakgrunden till förfrågningen. Till exempel om en förfrågan om tillgång är vagt formulerad eller väldigt omfattande kan en organisation inleda en dialog med den enskilde för att ta reda på varför förfrågan gjorts och för att lättare kunna hitta lämpliga uppgifter. Organisationen kan ta reda på vilken del eller vilka delar av organisationen den enskilde hade kontakt med eller vilka slags uppgifter (eller vilket användningsområde) som ligger till grund för förfrågan.

iii. I överensstämmelse med själva principen bakom tillgång bör organisationerna alltid visa sin goda vilja när det gäller att ge tillgång till uppgifter. Om t.ex. vissa uppgifter behöver skyddas och lätt kan skiljas från övriga personuppgifter som det begärs tillgång till ska organisationen bearbeta de skyddade uppgifterna och göra de icke-konfidentiella uppgifterna tillgängliga. Om en organisation beslutar att i vissa fall begränsa tillgången till uppgifter, ska organisationen lämna en förklaring till den enskilda person som ansökt om att få tillgång till uppgifterna om varför man kommit fram till detta beslut och ange en kontaktpunkt för ytterligare frågor.

b. Börda eller kostnad för att ge tillgång till personuppgifter

i. Rätten till tillgång till personuppgifter får begränsas i undantagsfall om legitima rättigheter för en annan person än den enskilda personen skulle kränkas eller om bördan eller kostnaden för att ge tillgång till personuppgifter inte står i proportion till riskerna för den enskilda personens integritet. Kostnader och arbetsinsats är viktiga faktorer som man bör ta hänsyn till, men de avgör inte huruvida det är rimligt att bevilja tillgång till uppgifter.

([1]) Organisationen bör besvara frågor från enskilda om ändamålen med behandlingen, de berörda personuppgiftskategorierna och mottagarna eller mottagarkategorierna till vilka personuppgifterna utlämnas.

ii. Om personuppgifterna till exempel används för att fatta beslut som är av stor betydelse för den enskilde (t.ex. i samband med avslag eller beviljande av viktiga förmåner, som försäkring, lån eller arbete), måste organisationen i överensstämmelse med övriga bestämmelser i dessa kompletterande principer lämna ut uppgifter även om detta är svårt eller innebär höga kostnader. Om det inte rör sig om känsliga uppgifter eller om dessa inte används för att fatta beslut som är av stor betydelse för den enskilde, utan är lättillgängliga och det inte innebär några stora kostnader att få fram dessa, måste organisationen göra dessa uppgifter tillgängliga.

c. Konfidentiella uppgifter om affärsverksamhet

i. Konfidentiella uppgifter om affärsverksamhet är uppgifter som en organisation har vidtagit åtgärder för att skydda från insyn och där insynen skulle vara till fördel för en konkurrent på marknaden. Organisationer kan neka eller begränsa tillgång om det skulle innebära att man genom att göra uppgifterna fullständigt tillgängliga avslöjar organisationens egna konfidentiella uppgifter om affärsverksamhet, t.ex. slutsatser eller klassificeringar av marknadsföring som utarbetas av organisationen, eller en annan organisations konfidentiella uppgifter om affärsverksamhet där dessa uppgifter omfattas av ett avtalsreglerat sekretesskrav.

ii. I fall då vissa konfidentiella uppgifter om affärsverksamhet lätt kan skiljas från övriga personuppgifter som det begärs tillgång till ska organisationen bearbeta de konfidentiella uppgifterna om affärsverksamhet och göra de icke-konfidentiella uppgifterna tillgängliga.

d. Organisation av databaser

i. Tillgången kan ges genom att en organisation lämnar ut de relevanta personuppgifterna till den enskilda personen och det är inte nödvändigt att han eller hon får tillgång till organisationens databas.

ii. Tillgång behöver bara medges i den mån en organisation lagrar personuppgifterna. Tillgångsprincipen innebär inte att organisationerna är skyldiga att hålla kvar, upprätthålla, omorganisera eller omstrukturera register med personuppgifter.

e. Begränsad tillgång

i. Eftersom organisationerna alltid måste visa sin goda vilja när det gäller att ge enskilda personer tillgång till sina personuppgifter är de omständigheter under vilka organisationerna kan begränsa tillgång begränsade, och alla skäl till begränsad tillgång måste vara specifika. Precis som enligt direktivet kan en organisation begränsa tillgången till uppgifter om utlämnandet troligtvis kan försvåra skyddet av viktiga offentliga intressen, som nationell säkerhet, försvar eller allmän säkerhet. Dessutom kan tillgång nekas i fall då personuppgifterna uteslutande behandlas för att användas i forskning eller statistik. Andra skäl att neka eller begränsa tillgången till uppgifter kan vara att det annars kan

1. försvåra brottsbekämpning eller civilmål, inklusive förebyggande, utredning eller upptäckt av brottsliga handlingar eller rätten till en rättvis rättegång,

2. utlämnande när andra personers legitima rättigheter eller viktiga intressen skulle kränkas,

3. innebära brott mot rättsliga eller yrkesmässiga privilegier eller skyldigheter,

4. försvåra säkerhetskontroller som gäller anställda eller klagomålsförfaranden eller i samband med turordning när det gäller personplanering och omstrukturering av organisationer,

5. skada den konfidentialitet som kan vara nödvändig i samband med övervakning, inspektion eller reglerande funktioner som tillhör en sund ekonomisk eller finansiell förvaltning, eller i framtida eller pågående förhandlingar som berör organisationen.

ii. Det åligger den organisation som åberopar rätten att göra undantag att bevisa att denna är tillämplig. En motivering till att organisationer begränsar tillgången till uppgifter samt information om en kontaktpunkt för ytterligare undersökningar lämnas till den enskilde.

f. Rätt att få bekräftelse samt uttag av avgifter för att täcka kostnaderna för att erbjuda tillgång

i. En enskild person har rätt att få bekräftelse på huruvida en organisation har personuppgifter som rör honom eller henne. Den enskilde har också rätt att meddelas om personuppgifter som rör honom eller henne. Organisationer kan ta ut en avgift, förutsatt att denna inte är orimligt hög.

ii. Att ta ut en avgift kan vara meningsfullt om man vill förhindra uppenbart överdrivna förfrågningar, särskilt om de är ständigt återkommande.

iii. Tillgång får inte förvägras av kostnadsskäl om den enskilda personen erbjuder sig att stå för kostnaderna.

g. Ständigt återkommande förfrågningar eller okynnesförfrågningar

En organisation kan fastställa rimliga begränsningar vad gäller antalet förfrågningar från en viss person vilka behöver besvaras under en viss period. När dessa begränsningar fastställs ska man ta hänsyn till hur ofta uppgifterna uppdateras, i vilket syfte de används och vilka slags uppgifter det rör sig om.

h. Bedrägliga förfrågningar om tillgång

En organisation är inte skyldig att ge tillgång till uppgifter om den inte erhåller tillräcklig information för att bekräfta identiteten på den person som ansöker om att få tillgång till uppgifterna.

i. Tidsgräns för svar

Organisationerna ska besvara förfrågningar om tillgång inom en rimlig tidsperiod, på ett rimligt sätt och i en form som lätt kan förstås av den enskilde. En organisation som tillhandahåller uppgifter om registrerade vid regelbundna tillfällen kan besvara individuella förfrågningar om tillgång inom ramen för det regelbundna tillhandahållandet av uppgifter om detta inte medför en orimlig försening.

9. **Personaluppgifter**

a. Sköldens omfattning

i. Om en organisation i EU överför personuppgifter som insamlats om de anställda (tidigare eller nuvarande) inom ramen för ett anställningsförhållande till ett moderbolag, en filial eller en oberoende tjänsteleverantör i Förenta staterna ansluten till skölden för skydd av privatlivet, har överföringen de fördelar som skölden innebär. I sådana fall omfattas insamlandet av uppgifterna liksom behandlingen av dessa innan de överförs av lagstiftningen i det EU-land där de samlades in, och om dessa lagar föreskriver villkor eller begränsningar för överföringen måste sådana bestämmelser följas.

ii. Sköldens principer är relevanta endast om enskilt identifierade eller identifierbara register överförs eller görs tillgängliga. Statistikrapportering som bygger på sammanförda sysselsättningsuppgifter som inte innehåller personuppgifter eller användning av uppgifter som avidentifierats innebär inte något problem för integritetsskyddet.

b. Tillämpning av principerna om meddelande och valmöjlighet

i. En organisation i Förenta staterna som har fått uppgifter om anställda från EU inom ramen för skölden för skydd av privatlivet får lämna ut dessa uppgifter till en tredje part eller använda dem för andra ändamål endast i enlighet med principerna om meddelande och valmöjlighet. När en organisation t.ex. har för avsikt att använda personuppgifter som samlats in i samband med ett anställningsförhållande för marknadskommunikation, måste organisationerna i Förenta staterna ge de berörda enskilda den lagstadgade valmöjligheten innan den använder uppgifterna, såvida dessa inte redan tidigare har lämnat sitt samtycke till att uppgifterna används för dessa ändamål. Sådan användning får inte vara oförenlig med de ändamål för vilka personuppgifterna samlades in eller i efterhand ha godkänts av den enskilde. Att en person utnyttjar denna valmöjlighet får inte användas för att begränsa karriärmöjligheter eller för att bestraffa den anställde på något sätt.

ii. Det bör påpekas att vissa allmänt tillämpliga villkor för överföring från en del EU-medlemsstater kan utesluta annan användning av sådana uppgifter även efter det att uppgifterna har överförts till ett land utanför EU och att sådana villkor är bindande.

iii. Dessutom ska arbetsgivare göra rimliga ansträngningar för att tillmötesgå den anställdes önskemål om integritetsskydd. Detta kan t.ex. inbegripa att man begränsar tillgången till personuppgifterna, avidentifierar dem eller inför koder eller pseudonymer om det i förvaltningssyfte inte är nödvändigt att uppge de riktiga namnen.

iv. Om och när det är nödvändigt att undvika inblandning i organisationens personalpolitik, dvs. befordringar, tillsättande av tjänster eller liknande, behöver en organisation inte lämna någon valmöjlighet eller meddelande.

c. Tillämpning av principen om tillgång

Den kompletterande principen om tillgång ger vägledning om vilka orsaker som kan berättiga att en organisation avvisar eller efter en begäran endast ger begränsad tillgång till personaluppgifter. Givetvis måste arbetsgivare i EU handla i enlighet med lokala bestämmelser och se till att anställda inom EU får tillgång till sådana uppgifter som är en lagstadgad rättighet i deras hemländer, oavsett var dessa uppgifter behandlas eller lagras. Enligt skölden ska en organisation som behandlar sådana uppgifter i Förenta staterna samarbeta för att ge tillgång till uppgifterna antingen direkt eller genom arbetsgivaren i EU.

d. Verkställighet

i. I den mån personuppgifterna endast används i samband med ett anställningsförhållande ligger ansvaret för uppgifterna gentemot den anställde hos organisationen i EU. Därmed bör i fall då anställda i EU klagar på att deras rättigheter när det gäller uppgiftsskydd har kränkts och de inte är nöjda med resultatet av förfaranden för intern granskning, klagomål eller överklagande (eller något annat förfarande som avtalats med en fackförening) vända sig direkt till den nationella myndigheten för uppgiftsskydd eller myndigheten med ansvar för arbetsförhållanden inom det område där den berörda personen är anställd. Detta omfattar även fall då det är den organisation i Förenta staterna som mottagit uppgifterna från arbetsgivaren som påstås ha gjort sig skyldig till en felhantering, varvid den innebär en överträdelse av sköldens principer. Detta är det mest effektiva tillvägagångssättet för att hantera ofta förekommande överlappning av rättigheter och skyldigheter som införts genom lokal arbetsrätt, arbetsmarknadsavtal och lagar om uppgiftsskydd.

ii. En organisation i Förenta staterna som är ansluten till skölden för skydd av privatlivet och som använder personaluppgifter om EU-medborgare som överförts från EU i samband med anställningsförhållandet och därvid önskar att överföringen ska omfattas av skölden måste därför samarbeta vid undersökningar som utförs av behöriga myndigheter i EU och följa dessa myndigheters anvisningar i de enskilda fallen.

e. Tillämpning av principen om ansvar för vidare överföring

Om en organisation som deltar i skölden för skydd av privatlivet har tillfälliga anställningsbehov och med avseende på personuppgifter som överförs inom ramen för skölden, såsom flyg- och hotellbokningar eller försäkringstäckning, kan överföringar av personuppgifter för ett fåtal anställda till den personuppgiftsansvarige ske utan att principen om tillgång behöver tillämpas och utan att det är nödvändigt att ingå ett avtal med tredje partens personuppgiftsansvarige, vilket annars krävs enligt principen om ansvar för vidare överföring, på villkor att organisationen uppfyller principerna om meddelande och valmöjlighet.

10. **Obligatoriska avtal om vidare överföring**

a. Behandlingsavtal

i. Det krävs ett avtal, oavsett om den som behandlar uppgifterna är ansluten till skölden för skydd av privatlivet eller inte, när personuppgifter överförs från EU till Förenta staterna endast för behandling.

ii. Personuppgiftsansvariga i EU måste alltid ingå ett avtal om överföring av uppgifter för behandling, oavsett om behandlingen görs inom eller utanför EU, och oavsett om den organisation som behandlar uppgifterna deltar i skölden eller inte. Syftet med avtalet är att se till att den personuppgiftsansvarige

1. endast handlar enligt instruktioner från den personuppgiftsansvarige,

2. vidtar lämpliga tekniska och organisatoriska åtgärder för att skydda personuppgifter från förstöring genom olyckshändelse eller otillåtna handlingar eller förlust genom olyckshändelse samt mot ändringar, otillåten spridning av eller otillåten tillgång till uppgifterna, och vet om vidare överföring är tillåten, och

3. med tanke på behandlingens art, hjälper den personuppgiftsansvarige att svara på begäran om utövande av den registrerades rättigheter.

iii. Eftersom ett adekvat skydd garanteras av alla som är anslutna till skölden för skydd av privatlivet, kan avtal endast för behandling av uppgifter slutas med organisationer som är anslutna till skölden utan att tillstånd behöver begäras i förväg (eller också beviljas sådant tillstånd automatiskt av EU-medlemsstaterna), till skillnad från avtal med mottagare som inte är anslutna till skölden eller inte på annat sätt garanterar ett adekvat skydd.

b. Överföringar inom en kontrollerad grupp av företag eller enheter

Enligt principen om ansvar för vidare överföring krävs inte alltid avtal när personuppgifter överförs mellan två personuppgiftsansvariga inom en kontrollerad grupp av företag eller enheter. Personuppgiftsansvariga inom en kontrollerad grupp av företag eller enheter kan basera sådana överföringar på andra instrument, t.ex. bindande företagsregler på EU-nivå eller andra koncerninterna instrument (t.ex. efterlevnads- och kontrollprogram) och på så vis se till att skyddet av personuppgifter fortsätter att gälla enligt principerna. Vid sådana överföringar förblir organisationer som deltar i skölden ansvariga för efterlevnaden av principerna.

c. Överföringar mellan personuppgiftsansvariga

För överföringar mellan personuppgiftsansvariga måste den mottagande personuppgiftsansvarige inte vara en organisation som deltar i skölden för skydd av personuppgifter och måste inte ha utsett en oberoende instans för handläggning av klagomål. En organisation som deltar i skölden måste ingå ett avtal med den mottagande tredje partens personuppgiftsansvarige som ger samma skyddsnivå som enligt skölden. Kravet att den mottagande personuppgiftsansvarige ska vara en organisation som deltar i skölden för skydd av personuppgifter och att den ska utse en oberoende instans för handläggning av klagomål gäller dock inte, på villkor att tredje parten tillhandahåller en motsvarande instans.

11. **Tvistlösning och genomförande**

a. Kraven för genomförandet av skölden för skydd av privatlivet fastställs i principerna om rättsmedel, genomförande och ansvar. Hur kraven som uppställs i principens punkt a.ii ska uppfyllas framgår av den kompletterande principen om kontroll. Denna kompletterande princip omfattar punkterna a.i och a.iii, som båda innehåller krav på oberoende instanser för handläggning av klagomål. Dessa instanser kan ha olika former men de måste uppfylla kraven enligt principen om rättsmedel, genomförande och ansvar. Organisationerna kan uppfylla kraven på något av följande sätt: i) Den kan följa ett program för integritetsskydd som utarbetats inom den privata sektorn och i vilket sköldens principer inlemmats. I programmet ska det ingå effektiva metoder för kontroll av efterlevnaden av det slag som beskrivs i principen om rättsmedel, genomförande och ansvar. ii) Den kan förbinda sig att rätta sig efter lagstadgade tillsynsmyndigheter eller andra offentliga tillsynsorgan som handlägger individuella klagomål och tillhandahåller tvistlösning. iii) Den kan förbinda sig att samarbeta med dataskyddsmyndigheter inom Europeiska unionen eller deras bemyndigade ombud.

b. Denna förteckning är inte ämnad att vara uttömmande utan snarare belysande. Den privata sektorn kan utarbeta andra metoder för genomförande, förutsatt att de uppfyller kraven enligt principen om rättsmedel, genomförande och ansvar samt de kompletterande principerna. Observera att de villkor som anges i principen

om rättsmedel, genomförande och ansvar gäller utöver kravet om att tvistlösningsmodeller ska tillhandahålla lösningar som kan verkställas enligt avsnitt 5 i *Federal Trade Commission Act*, som förbjuder illojala och bedrägliga handlingar, eller liknande regelverk som förbjuder sådana handlingar.

c. För att säkerställa överensstämmelse med sina åtaganden gentemot skölden för skydd av privatlivet och för att stödja förvaltningen av programmet måste organisationerna och deras oberoende instanser för handläggning av klagomål lämna information om skölden på ministeriets begäran. Organisationerna måste dessutom på lämpligt sätt via informationsavdelningen besvara klagomål rörande överensstämmelse med principerna som hänskjuts av dataskyddsmyndigheterna via ministeriet. I svaret bör organisationerna ange om klagomålet är berättigat och om så är fallet, hur organisationen kommer att rätta till problemet. Ministeriet kommer att skydda sekretessen för den information det mottar i enlighet med amerikansk lag.

d. Instanser för handläggning av klagomål

i. Konsumenterna bör uppmuntras att först inge klagomål till den berörda organisationen innan de vänder sig till oberoende instanser för behandling av klagomål. Organisationerna måste svara konsumenten inom 45 dagar från det att klagomålet mottagits. Att en sådan instans kan anses vara oberoende kan särskilt visas genom opartiskhet, öppenhet i fråga om dess sammansättning och finansiering och genom styrkt erfarenhet. Enligt principen om rättsmedel, genomförande och ansvar ska de rättsmedel som enskilda utnyttja vara lättillgängliga och kunna utnyttjas utan kostnad för den enskilde. Tvistlösningsorganen ska undersöka varje klagomål från enskilda som inte är klart ogrundat eller oseriöst. Detta är inget hinder för att den organisation som tillhandahåller instansen för handläggning av klagomål ställer upp kriterier för vilka som kan tas upp till behandling; sådana kriterier ska dock vara klara och rimliga (t.ex. undanta klagomål som faller utanför programmets räckvidd eller som bör tas upp i ett annat sammanhang) och får inte leda till att uppdraget, nämligen att reda ut berättigade klagomål, försvåras. Organisationen som tillhandahåller instansen för handläggning av klagomål bör dessutom på ett lättillgängligt och uttömmande sätt informera de enskilda om förfarandet för tvistlösning när dessa lämnar in ett klagomål. Sådan information bör, i enlighet med sköldens principer, innehålla en upplysning om vilka regler till skydd för privatlivet som tillämpas av organisationen som tillhandahåller rättsmedlet. De bör även samarbeta vid framtagandet av t.ex. standardformulär för besvär så att handläggningen av ärendena underlättas.

ii. Oberoende instanser för handläggning av klagomål måste på sina offentliga webbplatser lägga ut information om sköldens principer och de tjänster de tillhandahåller inom ramen för skölden. Denna information ska omfatta 1) information om eller en länk till de krav som gäller för oberoende instanser för handläggning av klagomål enligt skölden, 2) en länk till ministeriets webbplats för skölden, 3) en förklaring om att deras tvistlösningstjänster enligt skölden är kostnadsfria för enskilda personer, 4) en beskrivning av hur klagomål i samband med skölden kan inges, 5) tidsfrister för handläggning av klagomål i samband med skölden, och 6) en beskrivning av möjliga lösningar.

iii. Oberoende instanser för handläggning av klagomål ska offentliggöra en årsrapport med sammanställd statistik om sina tvistlösningstjänster. Årsrapporten ska innehålla 1) totalt antal klagomål rörande skölden som mottagits under rapporteringsåret, 2) typer av mottagna klagomål, 3) åtgärder för att förbättra tvistlösningens kvalitet, t.ex. handläggningstid för klagomål, och 4) resultat av mottagna klagomål, särskilt antal och typer av vidtagna åtgärder och beslutade påföljder.

iv. Såsom anges i bilaga I finns ett skiljedomsalternativ tillgängligt för enskilda personer. Syftet är att fastställa om en organisation som har anslutit sig till skölden har brutit mot sina skyldigheter enligt principerna gentemot den enskilde när det gäller ”resterande” yrkanden, och huruvida sådana överträdelser inte har åtgärdats alls eller endast delvis. Detta alternativ finns endast tillgängligt för dessa ändamål. Det är t.ex. inte tillgängligt med avseende på undantag från principerna ([1]) eller när det gäller påståenden om huruvida sköldens skydd är adekvat. Enligt detta skiljedomsalternativ har arbetsgruppen för skölden för skydd av privatlivet (som består av en eller tre skiljemän beroende på vad som överenskommits av parterna) befogenhet att påföra individuella specifika icke-monetära åtgärder för att avhjälpa skadan (t.ex. tillgång, korrigering, radering eller återlämnande av den enskildes personuppgifter) som är nödvändiga att åtgärda en överträdelse av principerna endast med avseende på denna enskilda person. Enskilda personer och organisationer som har anslutit sig till skölden har rätt att begära domstolsprövning och verkställande av skiljedomsbeslut i enlighet med amerikansk lagstiftning, närmare bestämt lagen om federal skiljedom (*Federal Arbitration Act*).

([1]) Avsnitt I.5 av principerna

e. Gottgörelse och påföljder

Gottgörelse som ett organ för tvistlösning beslutat om ska leda till att de negativa effekter som blivit följden av att reglerna inte efterlevts i möjligaste mån rättas till av den ansvariga organisationen och att all behandling av personuppgifter i framtiden sker i överensstämmelse med principerna samt, i tillämpliga fall, att all behandling av personuppgifter om den person som inlämnat klagomålet kommer att upphöra. Påföljderna måste vara tillräckligt kännbara för att borga för att organisationen kommer att följa principerna i framtiden. Ett flertal olika sanktionsmöjligheter av varierande svårighetsgrad kommer att göra det möjligt för organet för tvistlösning att välja en rimlig påföljd beroende på hur allvarligt fallet är. Det kan röra sig om offentliggörande av konstateranden om att organisationen inte följt principerna och om kravet att radera berörda uppgifter ([1]). Andra tänkbara påföljder är upphävande av organisationens status som ansluten till principerna, skadestånd för personer som drabbats av att reglerna inte efterlevts eller förbudsförelägganden. Privata organ för tvistlösning eller självreglering ska anmäla fall där en organisation som är ansluten till skölden underlåter att rätta sig efter deras beslut till domstol eller i förekommande fall de statliga myndigheter som är behöriga att fatta beslut i ärendet samt att även informera ministeriet.

f. Åtgärder från FTC:s sida

FTC har förbundit sig att göra en förhandsprövning av mottagna klagomål rörande bristande efterlevnad av principerna enligt i) organ för självreglering på integritetskyddets område och andra oberoende tvistlösningsorgan, ii) EU-medlemsstater, och iii) ministeriet, för att fastlägga om avsnitt 5 i FTC-lagen, som förbjuder illojala och bedrägliga handlingar eller metoder, har överträtts. Om FTC har skäl att anta att det har skett en överträdelse av avdelning 5, kan myndigheten utverka ett förvaltningsbeslut som förbjuder de handlingar som klagomålet avser eller inge ett klagomål till den federala underrätten, som kan resultera i ett federalt domstolsbeslut. Detta omfattar falska påståenden om anslutning till sköldens principer eller deltagande i skölden som framförs av organisationer som antingen inte längre är upptagna på förteckningen över organisationer som anslutit sig till skölden eller aldrig har lämnat in en självcertifiering till ministeriet. Konkurrensmyndigheten kan utverka böter för överträdelse av ett förvaltningsbeslut eller inleda civilrättsliga eller straffrättsliga förhandlingar om överträdelse av ett federalt domstolsbeslut. Konkurrensmyndigheten underrättar ministeriet om varje sådan åtgärd. Ministeriet anmodar andra statliga myndigheter att meddela ministeriet det slutliga avgörandet i varje sådant hänskjutet ärende liksom andra beslut och domar som gäller efterlevnad av sköldens principer.

g. Upprepad överträdelse av principerna

i. Om en organisation upprepade gånger överträder principerna, förlorar den sin rätt att omfattas av de fördelar skölden för skydd av privatlivet medför. Ministeriet kommer att stryka organisationer som upprepade gånger har överträtt principerna från förteckningen över organisationer som anslutit sig till skölden, och organisationerna måste återlämna eller radera de personuppgifter som de har mottagit inom ramen för skölden.

ii. Upprepad överträdelse av principerna föreligger när en organisation som har lämnat in en självcertifiering till ministeriet vägrar att efterleva ett slutligt avgörande från ett organ för självreglering på integritetskyddets område, ett oberoende tvistlösningsorgan eller ett regeringsorgan, eller där ett sådant organ finner att en organisation så ofta gör sig skyldig till överträdelser att det inte längre är rimligt att tro på organisationens försäkran att den följer principerna. I sådana fall måste organisationen snarast meddela ministeriet dessa fakta. Underlåtenhet att göra detta kan leda till enligt den amerikanska lagen om osann utsaga (*False Statements Act*) (18 U.S.C. § 1001). En organisations tillbakadragande från ett organ för självreglering på integritetskyddets område eller ett oberoende tvistlösningsorgan innebär inte att den befrias från sin skyldighet att uppfylla principerna, och detta skulle utgöra en upprepad överträdelse.

iii. Vid en anmälan om upprepade överträdelser kommer ministeriet att stryka organisationen i fråga från förteckningen över organisationer som har anslutit sig till skölden, oavsett om anmälan mottagits från organisationen själv, från ett organ för självreglering på integritetskyddets område eller ett annat oberoende tvistlösningsorgan eller från en statlig myndighet, dock först sedan de gett den berörda organisationen en möjlighet att inom trettio dagar gå i svaromål. I den förteckning över organisationer som har anslutit sig till

([1]) Organen för tvistlösning kan själva välja de påföljder de anser rimliga. De berörda uppgifternas känslighet är ett kriterium som bör beaktas vid bedömningen av om uppgifterna behöver raderas. Ett annat kriterium är om en organisation har samlat in, använt eller publicerat information på ett sätt som uppenbart strider mot sköldens principer.

skölden som förs av ministeriet kommer det att klargöras vilka organisationer som omfattas av de fördelar som skölden medför och vilka organisationer som inte gör det.

iv. En organisation som ansöker om att få delta i ett privat organ för självreglering med målsättningen att kvalificera sig för skölden för skydd av privatlivet måste till detta organ överlämna all information om tidigare deltagande i skölden.

12. **Valmöjlighet – Tidsfrister när man undanber sig direktmarknadsföring**

a. Allmänt sett är syftet med principen om valmöjlighet att se till att personuppgifter används och vidarebefordras på ett sätt som överensstämmer med den enskildes förväntningar och val. Därför ska en enskild person när som helst kunna välja att undanbe sig att personuppgifter används för direktmarknadsföring, med förbehåll för rimliga tidsgränser för organisationen så att den t.ex. får tid på sig att verkställa den enskildes val. En organisation får också begära de uppgifter som krävs för att bekräfta identiteten hos den som undanber sig direktmarknadsföring. I Förenta staterna kan de enskilda utöva denna möjlighet med hjälp av ett centralt system som det amerikanska direktreklamförbundets tjänst (*Direct Marketing Association*) *Mail Preference Service*. Organisationer som deltar i denna tjänst bör göra de konsumenter som inte vill ta emot direktreklam uppmärksamma på att tjänsten finns. Under alla omständigheter ska den enskilda personen ges möjlighet att på ett lättillgängligt och billigt sätt utöva denna möjlighet.

b. På samma sätt får en organisation använda personuppgifter i samband med viss direktmarknadsföring, om det är orimligt svårt att erbjuda den enskilde möjlighet att undanbe sig direktmarknadsföring innan uppgifterna används. För detta krävs att organisationen samtidigt och utan dröjsmål (eller när som helst, på begäran) ger den enskilde möjlighet att (utan kostnad för den enskilde) undanbe sig ytterligare direktmarknadsföring, och att organisationen rättar sig efter den enskildes önskemål.

13. **Reseinformation**

a. Uppgifter om flygbokningar och andra uppgifter i anslutning till resor, t.ex. om frequent flyer-program, hotellbokningar och särskilda behov, t.ex. måltidskrav av religiösa skäl eller behov på grund av funktionshinder, får överföras till organisationer belägna utanför EU vid flera olika omständigheter. Enligt artikel 26 i direktivet får personuppgifter överföras ”till ett tredje land som inte har en adekvat skyddsnivå i den mening som avses i artikel 25.2” förutsatt att i) det är nödvändigt för att tillhandahålla tjänster som konsumenten begär eller fullgöra ett avtal, t.ex. ett frequent flyer-avtal, eller ii) att konsumenten otvetydigt samtyckt till överföringen. Amerikanska organisationer som omfattas av sköldens principer ger adekvat skydd för personuppgifter, och får därför ta emot uppgifter från EU utan att uppfylla dessa villkor eller andra villkor i artikel 26 i direktivet. Eftersom sköldens principer har särskilda regler för känsliga uppgifter, får sådana uppgifter (som exempelvis samlats in för att betjäna funktionshindrade passagerare) ingå i överföringar till organisationer som deltar i skölden. Under alla omständigheter måste dock den organisation som överför uppgifterna följa lagen i den EU-medlemsstat den verkar i, vilket bl.a. kan innebära särskilda villkor för behandling av känsliga uppgifter.

14. **Farmaceutiska och medicinska produkter**

a. Tillämpning av EU-medlemsstaternas lagstiftning eller sköldens principer

EU-medlemsstaternas lagstiftning tillämpas vid insamling av personuppgifter och vid all den bearbetning, som äger rum före överförandet till Förenta staterna. Sköldens principer tillämpas på uppgifterna först sedan de överförts till Förenta staterna. Uppgifter som används för läkemedelsforskning eller för andra ändamål ska när så befinns lämpligt avidentifieras.

b. Kommande vetenskaplig forskning

i. Personuppgifter som framkommit vid specificerade medicinska och farmaceutiska forskningar och undersökningar spelar ofta en framträdande roll vid kommande vetenskaplig forskning. När personuppgifter som samlats in för en forskningsstudie överförs till en amerikansk organisation som deltar i skölden för skydd av privatlivet kan organisationen använda uppgifterna för ny vetenskaplig forskning efter att först ha meddelat detta och tillhandahållit lämpliga valmöjligheter. I meddelandet ska upplysningar ges om varje kommande specificerad användning av dessa uppgifter såsom periodisk uppföljning, undersökningar inom närliggande områden eller marknadsföring.

ii. Det underförstås att all framtida användning av dessa uppgifter inte kan specificeras, emedan ny användning av forskningsrön kan uppstå ur förnyad förståelse av ursprungliga rön, nya upptäckter och framsteg inom medicinen samt utvecklingen inom folkhälsa och hälsovårdslagstiftning. Där så befinns lämpligt, ska följaktligen meddelandet innehålla en förklaring av huruvida personuppgifter får användas vid sådan framtida medicinsk och farmakologisk forskningsverksamhet som inte kan förutses. Om användningen inte är förenlig med de(t) allmänna forskningssyfte(n) vartill personuppgifterna ursprungligen insamlats, eller vartill den enskilde sedermera samtyckt, måste nytt samtycke inhämtas.

c. Tillbakadragande från ett kliniskt försök

Deltagare får när som helst besluta sig för eller uppmanas att dra sig ur ett kliniskt försök. Alla personuppgifter som samlats in före utträdet får emellertid fortsätta att bearbetas tillsammans med de övriga uppgifter som insamlats för användning i det kliniska försöket, om detta klargjordes för deltagaren i meddelandet då han/hon samtyckte till att delta.

d. Överföringar för kontroll- och övervakningsändamål

Läkemedels- och sjukvårdsutrustningsföretag har tillstånd att lämna personuppgifter från kliniska försök som genomförts i EU till tillsynsmyndigheter i Förenta staterna för kontroll- och övervakningsändamål. Liknande överföringar till andra intresserade än tillsynsmyndigheter, såsom produktionsanläggningar och övriga forskare, är tillåten enligt principerna om meddelande och valmöjlighet.

e. Blindtest

i. För att säkerställa objektivitet kan vid många kliniska försök varken deltagare eller forskningsledare få tillgång till uppgifter om vilken behandling som varje deltagare erhåller. Om så skulle ske skulle undersökningens giltighet och dess resultat kunna äventyras. Deltagare i sådana kliniska försök (s.k. blindtest) behöver inte beredas tillgång till uppgifter om sin behandling under försöket, om denna inskränkning förklarats när deltagaren började delta i försöket, och om avslöjande av sådana uppgifter skulle äventyra forskningsförsökets integritet.

ii. Samtycke till att delta i försöket medför under dessa betingelser rimligen ett avstående från rätten till tillgång. När försöket avslutats, och resultaten analyserats, kommer deltagarna att få tillgång till uppgifterna om sig själva, om de fordrar det. De ska i första hand begära dem av den läkare eller annan sjukvårdsproducent som inom ramen för det kliniska försöket behandlat dem eller i andra hand av den sponsrande organisationen.

f. Produktsäkerhet och effektivitetskontroll

Läkemedels- eller sjukvårdsutrustningsföretag måste inte tillämpa sköldens principer när det gäller principerna om meddelande, ansvar för vidare överföring och tillgång i sin strävan efter produktsäkerhet och effektivitets-kontroll, inklusive rapporter om negativa effekter och spårande av patienter/försökspersoner som använder vissa mediciner eller viss medicinsk utrustning, om anslutningen till principerna inverkar på efterlevnaden av

lagstadgade krav. Detta gäller både rapporter från t.ex. sjukvårdsproducenter till läkemedels- och sjukvårdsutrustningsföretag och rapporter från läkemedels- och sjukvårdsutrustningsföretag till regeringsorgan som *Food and Drug Administration*.

g. Kodade uppgifter

Forskningsrön kodas alltid inledningsvis av ansvarig forskningsledare för att enskilda försökspersoners identitet inte ska avslöjas. De läkemedelsföretag som sponsrar sådan forskning får inte tillgång till kodnyckeln. Den enda kodnyckeln finns endast hos forskaren, för att han eller hon under vissa omständigheter ska kunna identifiera försökspersonen (t.ex. om medicinsk uppföljning erfordras). En överföring från EU till Förenta staterna av uppgifter som kodats på detta sätt utgör inte en överföring av personuppgifter som omfattas av sköldens principer.

15. **Offentliga register och allmänt tillgängliga uppgifter**

a. En organisation måste tillämpa sköldens principer om säkerhet, dataintegritet och ändamålsbegränsning samt rättsmedel, genomförande och ansvar på personuppgifter från allmänt tillgängliga källor. Dessa principer ska tillämpas på personuppgifter som samlas in från offentliga register, dvs. register som hålls av myndigheter och enheter på olika nivåer och är tillgängliga för allmänheten.

b. Det är inte nödvändigt att tillämpa principerna om meddelande, valmöjlighet och ansvar för vidare överföring på allmänt tillgängliga uppgifter, förutsatt att de inte kombineras med icke offentliga uppgifter och att alla villkor för att ta del av uppgifterna som fastställts av behörig myndighet följs. Det är i allmänhet inte heller nödvändigt att tillämpa principerna om meddelande, valmöjlighet och ansvar för vidare överföring på allmänt tillgängliga uppgifter, om inte den som överför uppgifterna från EU anger att uppgifterna omges av restriktioner så att det krävs att principerna för det aktuella ändamålet tillämpas av organisationen. Organisationer har inget ansvar för hur sådana uppgifter används av dem som erhåller uppgifterna från offentligt material.

c. Om en organisation befinns ha uppsåtligt offentliggjort personuppgifter i strid med principerna så att den eller andra kunnat utnyttja dessa undantag, ska den inte längre anses uppfylla kraven för att omfattas av sköldens förmåner.

d. Det är inte nödvändigt att tillämpa principen om tillgång på allmänt tillgängliga uppgifter, förutsatt att de inte kombineras med andra personuppgifter (förutom små mängder personuppgifter som används för att indexera eller organisera allmänt tillgängliga uppgifter). Alla villkor för att ta del av uppgifterna som fastställts av behörig myndighet måste dock följas. Om offentliga registeruppgifter kombineras med andra icke-offentliga registeruppgifter (andra än de som särskilt framhållits ovan), måste organisationen däremot ge tillgång till alla sådana uppgifter om dessa inte omfattas av andra legitima undantag.

e. På samma sätt som med uppgifter från offentliga register är det inte nödvändigt att ge tillgång till uppgifter som redan finns tillgängliga för den stora allmänheten så länge dessa inte kombinerats med icke-offentliga uppgifter. Organisationen som bedriver verksamhet med att sälja offentliga uppgifter kan ta ut en avgift från organisationer i samband med en förfrågan om tillgång. Enskilda personer kan också få tillgång till uppgifter om sig själva från den organisation som ursprungligen samlade in dessa.

16. **Ansökningar om åtkomst från offentliga myndigheter**

a. För att skapa insyn i offentliga myndigheters lagstadgade ansökningar om åtkomst till personuppgifter kan organisationer som är anslutna till skölden för skydd av privatlivet frivilligt utfärda regelbundna insynsrapporter om det antal ansökningar om åtkomst till personuppgifter som de mottar från offentliga myndigheter för brottsbekämpning eller skäl som rör den nationella säkerheten, i den utsträckning utlämnandet av sådana uppgifter är tillåten enligt tillämplig lagstiftning.

b. Den information som organisationer som är anslutna till skölden lämnar i dessa rapporter kan, tillsammans med information som har offentliggjorts av underrättelsemyndigheterna och annan information, användas som underlag för den årliga gemensamma översynen av sköldens funktion i enlighet med principerna.

c. Avsaknad av meddelande i enlighet med punkt a.xii i principen om meddelande ska inte hindra eller försämra en organisations förmåga att besvara lagliga förfrågningar.

Bilaga I

Modell för skiljedomsförfaranden

I denna bilaga anges de villkor enligt vilka organisationer som har anslutit sig till skölden för skydd av privatlivet är skyldiga att lösa yrkanden genom skiljedom i enlighet med principen om rättsmedel, genomförande och ansvar. Det bindande skiljedomsalternativ som beskrivs nedan är tillämpligt på vissa ”resterande” yrkanden avseende uppgifter som omfattas av skölden för skydd av privatlivet i EU och Förenta staterna. Syftet med detta alternativ är att skapa en snabb, oberoende och rättvis mekanism med valmöjligheter för enskilda personer för att behandla påstådda överträdelser av principerna som eventuella andra instanser inom ramen för skölden inte har löst.

A. **Tillämpningsområde**

Ett skiljedomsalternativ finns tillgängligt för enskilda personer. Syftet är att fastställa om en organisation som har anslutit sig till skölden har brutit mot sina skyldigheter enligt principerna gentemot den enskilde när det gäller ”resterande” yrkanden, och huruvida sådana överträdelser inte har åtgärdats alls eller endast delvis. Detta alternativ finns endast tillgängligt för dessa ändamål. Det är t.ex. inte tillgängligt med avseende på undantag från principerna ([1]) eller när det gäller påståenden om huruvida sköldens skydd är adekvat.

B. **Tillgängliga rättsmedel**

Enligt detta skiljedomsalternativ har arbetsgruppen för skölden för skydd av privatlivet (som består av en eller tre skiljemän beroende på vad som överenskommits av parterna) befogenhet att påföra individuella specifika icke-monetära åtgärder för att avhjälpa skadan (t.ex. tillgång, korrigering, radering eller återlämnande av den enskildes personuppgifter) som är nödvändiga att åtgärda en överträdelse av principerna endast med avseende på denna enskilda person. Dessa befogenheter är de enda skiljenämnden har avseende rättsmedel. När skiljenämnden överväger rättsmedel ska den överväga andra rättsmedel som redan har påförts av andra mekanismer enligt sköldens bestämmelser. Inga andra former av skadestånd, kostnader, avgifter eller andra rättsmedel finns tillgängliga. Varje part betalar sina egna advokatkostnader.

C. **Åtgärder som ska vidtas innan ett ärende tas till skiljenämnden**

En enskild person som beslutar att åberopa skiljedom måste vidta följande åtgärder innan skiljedomsförfarandet inleds: 1) Ta upp den påstådda överträdelsen direkt med organisationen och ge organisationen möjlighet att lösa frågan inom den tidsram som fastställs i avsnitt III.11(d)(i) i principerna, 2) utnyttja den oberoende instanser för handläggning av klagomål enligt principerna, som är kostnadsfri, och 3) via sin dataskyddsmyndighet ta upp frågan med handelsministeriet och ge ministeriet möjlighet att göra sitt bästa för att lösa frågan inom de tidsramar som fastställs i skrivelsen från handelsministeriets utrikeshandelsförvaltning, utan kostnad för den enskilde.

Skiljedomsalternativet kan inte åberopas om den överträdelse av principerna som har begåtts enligt den enskilda personen 1) redan har varit föremål för bindande skiljedom, 2) var föremål för en slutlig dom i ett domstolsförfarande som den enskilde var part i, eller 3) redan har varit föremål för förlikning mellan parterna. Detta alternativ kan inte heller åberopas om en dataskyddsmyndighet i EU 1) är behörig enligt avsnitten III.5 eller III.9 i principerna, eller 2) är behörig att lösa den påstådda överträdelsen direkt med organisationen. Dataskyddsmyndigheters behörighet att lösa samma yrkande mot en personuppgiftsansvarig i EU hindrar i sig inte åberopande av skiljedomsalternativet mot en annan juridisk enhet som inte omfattas av dataskyddsmyndighetens behörighet.

D. **Beslutens bindande karaktär**

En enskild persons beslut att åberopa alternativet med bindande skiljedom är helt frivilligt. Skiljenämndens beslut är bindande för alla parter i skiljedomsförfarandet. När skiljedom åberopas avstår den enskilda personen från alternativet att söka upprättelse i en annan instans, förutom de fall icke-monetära åtgärder för att avhjälpa skadan inte fullständigt avhjälper den påstådda överträdelsen. Åberopande av skiljedom hindrar inte den enskilde från att yrka på andra former av skadeståndsanspråk som finns tillgängliga i domstol.

([1]) Avsnitt I.5 i principerna.

E. **Översyn och verkställighet**

Enskilda personer och organisationer som har anslutit sig till skölden har rätt att begära domstolsprövning och verkställande av skiljedomsbeslut i enlighet med amerikansk lagstiftning, närmare bestämt lagen om federal skiljedom (*Federal Arbitration Act*) ([1]). Sådana ärenden måste tas upp i den federala distriktsdomstol inom vars territoriella behörighetsområde organisationen har sitt huvudsakliga säte.

Syftet med detta skiljedomsalternativ är att lösa individuella tvister. Skiljedomsbesluten är inte avsedda att vara övertygande eller bindande prejudikat i frågor som rör andra parter, inte heller när det gäller framtida skiljedomsförfaranden i domstolar i EU eller Förenta staterna, eller FTC:s förhandlingar.

F. **Skiljenämnd**

Parterna väljer skiljemän från den förteckning över skiljemän som anges nedan.

I enlighet med tillämplig lag kommer Förenta staterna:s handelsministerium och Europeiska kommissionen utarbeta en förteckning med minst 20 skiljemän, som väljs på grundval av oberoende, integritet och sakkunskap. Följande ska gälla för denna process:

Skiljemän

1) kommer att finnas upptagna i förteckningen under en period av tre år, förutom exceptionella omständigheter eller orsaker, med möjlighet till förlängning med en ytterligare treårsperiod,

2) ska inte ta emot instruktioner från eller ha anknytning till någon av parterna eller till någon organisation som är ansluten till skölden för skydd av privatlivet eller till Förenta staterna:s, EU:s eller EU-medlemsstaternas regeringar eller andra statliga myndigheter, offentliga myndigheter eller verkställande myndigheter, och

3) vara behörig att utöva advokatyrket i Förenta staterna och vara expert på amerikansk lagstiftning om integritetsskydd, med sakkunskap om EU:s dataskyddslagstiftning.

G. **Skiljeförfaranden**

I enlighet med tillämplig lag ska handelsministeriet och Europeiska kommissionen, inom sex månader från beslutet om adekvat skyddsnivå, enas om att anta en uppsättning befintliga och väletablerade amerikanska skiljedomsförfaranden (såsom AAA eller JAMS), som ska styra förhandlingarna inför skiljenämnden inom ramen för skölden, enligt följande villkor:

1. Enskilda personer kan inleda ett bindande skiljedomsförfarande enligt de villkor för skiljedomsförfaranden som anges ovan genom att inge ett meddelande till organisationen. Meddelandet ska innehålla en sammanfattning av de åtgärder som vidtagits enligt punkt C för att lösa yrkandet, en beskrivning av den påstådda överträdelsen och, enligt den enskildes val, eventuella styrkande handlingar och annat material och/eller en redogörelse för lagstiftning som är tillämplig på yrkandet.

([1]) Enligt kapitel 2 i lagen om federal skiljedom ”omfattas skiljedomsavtal eller skiljedomar som härrör från ett rättsligt förhållande, oavsett om de är avtalsmässiga eller ej, och betraktas som ett affärsmässigt avtal, en transaktion, ett avtal eller en överenskommelse enligt beskrivningen i [avsnitt 2 i lagen], av konventionen [om erkännande och verkställighet av utländska skiljedomar av den 10 juni 1958, 21 U.S.T. 2519, T.I.A.S. nr 6997 (nedan kallad *New York-konventionen*)].” 9 U.S.C. § 202. I lagen om federal skiljedom föreskrivs vidare att ”ett skiljedomsavtal eller en skiljedom som härrör från ett sådant förhållande och endast rör medborgare i Förenta staterna ska inte anses omfattas av [New York-]konventionen, om inte förhållandet omfattar egendom utomlands, utförande eller verkställande utomlands eller har något annat skäligt förhållande till en eller flera utländska stater”. *Idem*. Enligt kapitel 2 ”kan endera parten i ett skiljedomsförfarande ansöka till alla domstolar som är behöriga enligt detta kapitel om ett beslut som bekräftar skiljedomen mot en annan part i skiljedomsförfarandet. Domstolen ska bekräfta skiljedomen om den inte finner att någon av grunderna för avslag, uppskjutande, erkännande eller verkställighet av skiljedomen som anges i den nämnda [New York-] konventionen är tillämplig”. *Idem*. § 207. I kapitel 2 föreskrivs vidare att ”distriktsdomstolarna i Förenta staterna […] ska ha ursprunglig behörighet för […] talan eller förhandlingar [enligt New York-]konventionen, oavsett tvistebelopp”. *Idem*. § 203.
I kapitel 2 anges även att ”kapitel 1 är tillämpligt på talan och förfaranden som väcks enligt detta kapitel, om inte kapitlet strider mot detta kapitel eller [New York-]konventionen, som ratificerats av Förenta staterna”. *Idem*. § 208. I kapitel 1 föreskrivs å sin sida att ”en skriftlig bestämmelse i […] ett avtal som styrker en affärsmässig transaktion som löses genom skiljedom ska, även om en tvist uppstår om avtalet eller transaktionen eller vid vägran att fullgöra hela eller delar av avtalet eller ett skriftligt avtal om att hänskjuta en befintlig tvist om ett sådant avtal, en sådan transaktion eller en sådan vägran till skiljedom, vara oåterkalleligt och verkställbart, utom när lagliga grunder finns för att häva avtalet”. *Idem*. § 2. I kapitel 1 föreskrivs dessutom att ”varje part i skiljedomsförfarandet får ansöka till den behöriga domstolen om ett beslut som bekräftar skiljedomen, och domstolen måste bevilja ett sådant beslut om skiljedomen inte upphävs, ändras eller korrigeras enligt vad som anges i avsnitten 10 och 11 i lagen [om federal skiljedom]”. *Idem*. § 9.

2. Förfaranden kommer att utarbetas för att säkerställa att den ifrågavarande överträdelsen inte omfattas av dubbla rättsmedel eller förfaranden.

3. FTC kan vidta åtgärder parallellt med skiljedomsförfaranden.

4. Inga företrädare för Förenta staterna, EU, EU-medlemsstater eller andra statliga myndigheter, offentliga myndigheter eller verkställande myndigheter får delta i skiljedomsförfarandet. På den enskildes begäran får dataskyddsmyndigheter i EU endast bistå i utarbetandet av meddelandet, men får inte ges tillgång till framlägganden eller annat material som är relaterat till skiljedomsförfarandet.

5. Platsen för skiljeförfarandet kommer att Förenta staterna, och den enskilda personen kan välja att delta via telefon- eller videoanslutning, som ska tillhandahållas utan kostnad för den enskilde. Den enskilde behöver inte inställa sig personligen.

6. Skiljedomsförfarandet ska genomföras på engelska om inget annat överenskoms av parterna. På motiverad begäran, och med beaktande av om den enskilda personen företräds av en advokat, kommer både tolkning vid skiljedomsförfarandet och översättning av materialet att tillhandahållas utan kostnad för den enskilde, om inte skiljenämnden finner att detta med tanke på de omständigheterna kring förfarandet skulle leda till omotiverade eller oproportionerliga kostnader.

7. Material som lämnas in till skiljenämnden kommer att behandlas konfidentiellt och kommer endast att användas i samband med skiljedomsförfarandet.

8. Enskilda framlägganden kan tillåtas om så är nödvändigt och sådana framlägganden kommer att behandlas konfidentiellt av parterna och kommer endast att användas i samband med skiljedomsförfarandet.

9. Skiljedomsförfaranden bör avslutas inom 90 dagar från den dag då meddelandet inges till organisationen i fråga, om inget annat överenskoms av parterna.

H. **Kostnader**

Skiljemännen bör vidta rimliga åtgärder för att minimera kostnader eller avgifter för skiljeförfaranden.

I enlighet med tillämplig lag kommer handelsministeriet i samråd med Europeiska kommissionen att vidta åtgärder för att inrätta en fond, dit organisationer som är anslutna till skölden för skydd av privatlivet ska betala ett årligt bidrag, delvis baserat på organisationens storlek, som ska täcka kostnaderna för skiljedomsförfarandet, inklusive förlikningsmännens arvoden upp till maximala belopp (”tak”). Fonden kommer att förvaltas av en tredje part, som kommer att rapportera regelbundet om fondens verksamhet. Vid den årliga översynen kommer handelsministeriet och Europeiska kommissionen att granska driften av fonden och undersöka om det är nödvändigt att höja bidragsbeloppen eller taken. De kommer bland annat att överväga antalet skiljedomsförfaranden samt kostnader och tidsåtgång för förfarandena, med en ömsesidig överenskommelse om att organisationer som är anslutna till skölden inte får belastas med överdrivet höga ekonomiska bördor. Advokatkostnader omfattas inte av denna bestämmelse eller någon fond enligt denna bestämmelse.

BILAGA III

Skrivelse från Förenta staterna:s utrikesminister John Kerry

7 juli 2016

Bästa kommissionsledamot Jourová,

Det gläder mig att vi har nått en överenskommelse om skölden för skydd av privatlivet i Europeiska unionen och Förenta staterna. Den kommer att omfatta en ombudsman, genom vilken myndigheter i EU kan lämna in förfrågningar från enskilda personer i EU beträffande Förenta staterna:s signalspaningsmetoder.

Den 17 januari 2014 tillkännagav president Obama viktiga reformer av den amerikanska underrättelseverksamheten som fastställdes i *Presidential Policy Directive* 28 (nedan kallat *PPD-28*). Enligt PPD-28 har jag utsett statssekreterare Catherine A. Novelli, chefssamordnare för internationell it-diplomati, som vår kontaktpunkt för utländska regeringar som vill ta upp frågor angående Förenta staterna:s signalspaningsverksamhet. Utifrån detta har jag inrättat en ombudsmannapost i enlighet med de villkor som anges i bilaga A, som har uppdaterats sedan min senaste skrivelse av den 22 februari 2016. Jag har beslutat att undersekreterare Novelli ska inneha denna funktion. Undersekreterare Novelli är oberoende gentemot den amerikanska Förenta staterna:s underrättelsegemenskapen och rapporterar direkt till mig.

Jag har gett anvisningar åt min personal om att ägna nödvändiga resurser åt ombudsmannaposten, och jag är övertygad om att ombudsmannen kommer att bli en effektiv kanal för att behandla frågor från enskilda personer i EU.

Högaktningsfullt,

John F. Kerry

Bilaga A

Ombudsmannen för skölden för skydd av privatlivet i EU och Förenta staterna när det gäller signalspaning

Som ett erkännande av betydelsen av skölden för skydd av privatlivet i EU och Förenta staterna beskriver detta memorandum förfarandet för att inrätta en ny mekanism med avseende på signalspaning i enlighet med *Presidential Policy Directive* 28 (PPD-28) ([1]).

Den 17 januari 2014 tillkännagav president Obama viktiga reformer av den amerikanska underrättelseverksamheten. I sitt tal förklarade han att ”våra ansträngningar bidrar inte bara till att skydda vår nation, utan även våra vänner och allierade. Våra ansträngningar kan endast bli effektiva om allmänheten i andra länder har förtroende för att Förenta staterna respekterar även deras integritet”. President Obama meddelade att ett nytt presidentdirektiv, PPD-28, skulle utfärdas, där det ”tydligt beskrivs vad vi gör, och inte gör, när det gäller vår utländska signalspaning”.

Enligt avsnitt 4(d) i PPD-28PPD-4 ska utrikesministern utse en chefssamordnare för internationell it-diplomati”, som ska […] fungera som kontaktpunkt för utländska regeringar som vill ta upp frågor angående Förenta staterna:s signalspaningsverksamhet”. Från och med januari 2015 har undersekreterare Catherine A. Novelli tjänstgjort som chefssamordnare.

Detta memorandum innehåller en beskrivning av den nya mekanism som chefssamordnaren kommer att tillämpa för att handlägga förfrågningar om tillgång till uppgifter som överförts från EU till Förenta staterna inom ramen för skölden för skydd av privatlivet rörande nationell säkerhet, standardavtalsklausuler, bindande företagsregler samt ”undantag” ([2]) eller ”möjliga framtida undantag” ([3]) genom förfaranden som fastställts enligt tillämpliga amerikanska lagar och policyer, samt hur sådana förfrågningar ska besvaras.

1. **Ombudsman för skölden för skydd av privatlivet** Chefssamordnaren kommer att fungera som ombudsman för skölden och kommer att utse ytterligare tjänstemän från utrikesdepartementet om så behövs för att hjälpa samordnaren att fullgöra de ansvarsuppgifter som anges i detta memorandum. (Nedan kallas samordnaren och eventuella tjänstemän som fullgör sådana uppgifter *ombudsmannen för skölden*). Ombudsmannen för skölden kommer att föra ett nära samarbete med andra ministeriet och myndigheter med ansvar för att handlägga förfrågningar i enlighet med Förenta staterna:s tillämpliga lagar och policyer. Ombudsmannen är oberoende av underrättelsegemenskapen. Ombudsmannen rapporterar direkt till utrikesministern som ska se till att ombudsmannen utför sina arbetsuppgifter objektivt och fritt från otillbörlig påverkan som kan påverka de svar som ska ges.

2. **Effektiv samordning** Ombudsmannen för skölden kommer att kunna använda och samordna med de tillsynsorgan som beskrivs nedan för att säkerställa att ombudsmannens svar på förfrågningar som lämnas in av det organ som handlägger klagomål från enskilda personer i EU grundas på nödvändig information. När en förfrågan avser

([1]) Under förutsättning att kommissionens beslut om huruvida ett adekvat skydd säkerställs genom skölden för skydd av privatlivet i EU och Förenta staterna gäller för Island, Liechtenstein och Norge kommer skölden för skydd av privatlivet att omfatta både EU och dessa tre länder. Därför kommer hänvisningarna till EU och dess medlemsstater tolkas som att de även inbegriper Island, Liechtenstein och Norge.

([2]) ”Undantag” avser i detta sammanhang en eller flera affärsmässiga överföringar som äger rum enligt följande villkor: a) den registrerade otvetydigt har samtyckt till den planerade överföringen, eller b) överföringen är nödvändig för att fullgöra ett avtal mellan den registrerade och den registeransvarige eller för att på den registrerades begäran genomföra åtgärder som vidtas innan avtalet ingås, eller c) överföringen är nödvändig för att ingå eller fullgöra ett avtal mellan den registeransvarige och tredje man i den registrerades intresse, eller d) överföringen är nödvändig eller följer av lag på grund av viktiga allmänna intressen, eller för att kunna fastställa, göra gällande eller försvara rättsliga anspråk, eller e) överföringen är nödvändig för att skydda intressen som är av avgörande betydelse för den registrerade, eller f) överföringen görs från ett offentligt register som enligt lagar eller andra författningar är avsett att ge allmänheten information och som är tillgängligt antingen för allmänheten eller för var och en som kan styrka ett berättigat intresse, i den utsträckning som de i lagstiftningen angivna villkoren för tillgänglighet uppfylls i det enskilda fallet.

([3]) ”Möjliga framtida undantag” avser i detta sammanhang en eller flera affärsmässiga överföringar som äger rum enligt något av följande villkor, i den utsträckning att villkoret i fråga utgör en laglig grund för överföringar av personuppgifter från EU till Förenta staterna: a) Den registrerade har lämnat sitt uttryckliga samtycke till den föreslagna överföringen efter att ha blivit informerad om eventuella risker med sådana överföringar för den registrerade i avsaknad av ett beslut om adekvat skyddsnivå och lämpliga garantier, eller b) överföringen är nödvändig för att skydda intressen som är av grundläggande betydelse för den registrerade eller en annan person, om den registrerade är fysiskt eller rättsligt oförmögen att lämna sitt samtycke, eller c) vid en överföring till ett tredjeland eller en internationell organisation och inget av övriga undantag eller möjliga framtida undantag är tillämpliga, endast om överföringen inte är repetitiv, endast gäller ett begränsat antal registrerade, är nödvändig för ändamål som rör den personuppgiftsansvariges tvingande berättigade intressen och den registrerades intressen eller rättigheter och friheter inte väger tyngre, och den personuppgiftsansvarige har bedömt samtliga omständigheter kring överföringen av uppgifter och på grundval av denna bedömning vidtagit lämpliga skyddsåtgärder för att skydda personuppgifterna.

övervakningens förenlighet med amerikansk lagstiftning kommer ombudsmannen för skölden att kunna samarbeta med en av de oberoende tillsynsorgan som har utredningsbefogenheter.

a. Ombudsmannen för skölden kommer att föra ett nära samarbete med andra tjänstemän i den amerikanska regeringen, inbegripet lämpliga oberoende tillsynsorgan, för att säkerställa att förfrågningar behandlas och löses i enlighet med tillämpliga lagar och policyer. Ombudsmannen kommer att nära samordna arbetet med den nationella underrättelsetjänsten (*Office of the Director of National Intelligence*, ODNI), justitieministeriet och i förekommande fall andra berörda ministerier och myndigheter när det gäller Förenta staterna:s nationella säkerhet samt generalinspektörer och tjänstemän som ansvarar för lagen om informationsfrihet, medborgerliga friheter och integritetsskydd.

b. Den amerikanska regeringen kommer att tillämpa mekanismer för att samordna och övervaka arbetet med nationella säkerhetsfrågor vid ministerier och myndigheter för att bidra till att säkerställa att ombudsmannen för skölden kan besvara förfrågningar enligt avsnitt 3(b) i den mening som avses i avsnitt 4(e).

c. Ombudsmannen för skölden kan hänskjuta frågor i samband med förfrågningar till styrelsen för tillsyn av personlig integritet och medborgerliga friheter för övervägande.

3. **Inlämnande av förfrågningar**

a. En förfrågan görs inledningsvis till medlemsstaternas tillsynsmyndigheter med ansvar för tillsyn av nationella säkerhetstjänster och/eller offentliga myndigheters behandling av personuppgifter. Förfrågan lämnas till ombudsmannen av ett centraliserat EU-organ (nedan tillsammans kallade *EU-organet för handläggning av klagomål*).

b. EU-organet för handläggning av klagomål kommer att vidta följande åtgärder för att kontrollera att förfrågningarna är fullständiga:

i) Kontrollera den enskilda personens identitet och att personen agerar för egen räkning och inte som företrädare för en statlig eller mellanstatlig organisation.

ii) Se till att förfrågningar görs skriftligen och att de innehåller följande grundläggande information:

— All information som ligger till grund för förfrågan.

— Typ av information eller upprättelse som söks.

— De statliga organ i Förenta staterna som anses vara delaktiga, om några.

— Andra åtgärder som vidtagits för att erhålla den begärda informationen eller upprättelsen och de svar som mottagits till följd av dessa andra åtgärder.

iii) Kontrollera att förfrågan avser uppgifter som skäligen kan anses ha överförts från EU till Förenta staterna inom ramen för skölden för skydd av privatlivet eller enligt standardavtalsklausuler, bindande företagsregler, undantag eller möjliga framtida undantag.

iv) Fastställa att förfrågan inte är oseriös eller görs av okynne eller i ond tro.

c. För att en förfrågan ska behandlas vidare av ombudsmannen för skölden enligt detta memorandum är det inte nödvändigt att bevisa att den amerikanska regeringen faktiskt fått tillgång till personens uppgifter genom sin signalspaningsverksamhet.

4. **Åtaganden att meddela det anmälande individuella EU-organet för handläggning av klagomål**

a. Ombudsmannen för skölden kommer att bekräfta mottagandet av förfrågan från EU-organet för handläggning av klagomål.

b. Ombudsmannen kommer att göra en inledande granskning för att kontrollera att förfrågan har fyllts i enligt avsnitt 3(b). Vid eventuella brister eller frågor kommer ombudsmannen att kontakta det anmälande EU-organet för handläggning av klagomål för att tillsammans med detta hantera och lösa sådana frågor.

c. Om ombudsmannen för att underlätta en lämplig behandling av förfrågan behöver mer information eller om den enskilda person som ursprungligen lämnade in förfrågan måste vidta ytterligare åtgärder kommer ombudsmannen att informera det allmänna EU-organet för handläggning av klagomål om detta.

d. Ombudsmannen kommer att följa förfrågningarnas status och vid behov lämna uppdateringar till det anmälande EU-organet för handläggning av klagomål.

e. När en förfrågan har fyllts i enligt beskrivningen i avsnitt 3 i detta memorandum kommer ombudsmannen utan dröjsmål att svara det anmälande EU-organet för handläggning av klagomål på lämpligt sätt, dock med förbehåll för den ständiga skyldigheten att skydda uppgifter enligt tillämplig lagstiftning och policyer. Ombudsmannen kommer att besvara det anmälande EU-organet för handläggning av klagomål genom att bekräfta i) att klagomålet har utretts på lämpligt sätt, och ii) att amerikanska lagar, regelverk, dekret, presidentdirektiv och myndighetsföreskrifter som anger de begränsningar och garantier som beskrivs i ODNI-skrivelsen har följts, eller vid bristande efterlevnad, att detta har avhjälpts. Ombudsmannen kommer varken att bekräfta eller förneka om den enskilda personen har varit föremål för övervakning eller ange vilka specifika avhjälpande åtgärder som har vidtagits. Såsom beskrivs närmare i avsnitt 5 kommer förfrågningar som rör lagen om informationsfrihet (*Freedom of Information Act*, FOIA, nedan kallad *FOI-lagen*) att behandlas enligt detta regelverk och tillämpliga föreskrifter.

f. Ombudsmannen kommer att kommunicera direkt med EU-organet för handläggning av klagomål, som i sin tur kommer att vara ansvarig för kommunikationen med den enskilda person som lämnar in förfrågan. Om direkt kommunikation ingår i en av de underliggande processer som beskrivs nedan ska sådan kommunikation ske i enlighet med befintliga förfaranden.

g. Åtagandena i detta memorandum ska inte vara tillämpliga på allmänna påståenden om att skölden för skydd av privatlivet i EU och Förenta staterna är oförenlig med EU:s dataskyddskrav. Åtagandena i detta memorandum görs på grundval av ett gemensamt samförstånd mellan Europeiska kommissionen och Förenta staterna:s regering om att det till följd av omfattningen av åtagandena enligt denna mekanism kan uppstå resursbegränsningar, även i fråga om förfrågningar som rör FOI-lagen. Om ombudsmannens fullgörande av sina uppgifter betydligt överskrider tillgängliga resurser och hindrar fullgörandet av dessa åtaganden kommer den amerikanska regeringen att diskutera eventuella justeringar med Europeiska kommissionen som kan vara lämpliga för att lösa situationen.

5. **Förfrågningar om upplysningar** Förfrågningar om tillgång till den amerikanska regeringens register kan inges och behandlas enligt FOI-lagen.

a. Enligt FOI-lagen kan alla personer ansöka om tillgång till federala myndigheters befintliga register, oavsett nationalitet. Denna stadga kodifieras i Förenta staterna:s lagstiftning i 5 U.S.C. § 552. Stadgan samt ytterligare information om FOI-lagen finns på www.FOIA.gov och http://www.justice.gov/oip/foia-resources. Varje myndighet har en överordnad FOI-tjänsteman och informerar på sin offentliga webbplats om hur FOI-förfrågningar ska lämnas in till myndigheten. Myndigheterna har förfaranden för att samråda med varandra om FOI-förfrågningar som omfattar register som innehas av andra myndigheter.

b. Följande kan nämnas som exempel:

i) Den nationella underrättelsetjänsten har inrättat ”ODNI FOIA-portalen” för ODNI: http://www.dni.gov/index.php/about-this-site/foia. Portalen innehåller information om hur man inger ansökan, kontrollerar status för en befintlig förfrågan och hur man kan få tillgång till information som har offentliggjorts a ODNI enligt FOI-lagen. ODNI FOIA-portalen innehåller länkar till andra FOI-webbplatser för enheter inom underrättelsegemenskapen (*The United States Intelligence Community*, IC): http://www.dni.gov/index.php/about-this-site/foia/other-ic-foia-sites.

ii) Justitieministeriets informationskontor tillhandahåller detaljerad information om FOI-lagen: http://www.justice.gov/oip. Detta omfattar inte bara information om hur FOI-ansökningar kan lämnas in till justitieministeriet, utan informationskontoret ger även vägledning till den amerikanska regeringen om hur FOI-kraven ska tolkas och tillämpas.

c. Enligt FOI-lagen omfattas tillgång till statliga register föremål av vissa angivna undantag. Undantagen omfattar begränsningar av tillgång till sekretessbelagd nationell säkerhetsinformation, personuppgifter om tredje parter och information om brottsutredningar, och är jämförbara med de begränsningar som varje EU-medlemsstat har infört i sin lagstiftning om tillgång till information. Dessa begränsningar gäller både amerikaner och utländska medborgare.

d. Tvister om utlämnande av registeruppgifter enligt FOI-lagen kan överklagas i förvaltningsrätten och därefter i federala domstolar. Domstolen är skyldig att göra en ny bedömning om registren förs på lämpligt sätt enligt 5 U. S.C. § 552(a)(4)(B), och kan beordra regeringen att ge tillgång till register. I vissa fall har domstolarna ändrat regeringens beslut om att information bör förbli sekretessbelagd. Skadestånd kan inte utdömas, men domstolarna kan besluta om betalning av advokatarvoden.

6. **Begäran om ytterligare åtgärder** En begäran om en påstådd lagöverträdelse eller ett annat tjänstefel kommer att hänskjutas till lämplig amerikansk regeringsmyndighet, inklusive oberoende tillsynsmyndigheter, som är behöriga att utreda respektive begäran och hantera bristande efterlevnad enligt beskrivningen nedan.

a. Generalinspektörerna är lagstadgat oberoende, har omfattande befogenheter att utföra utredningar, revisioner och granskningar av program, även rörande bedrägeri och missbruk eller överträdelser av lagstiftningen, och kan rekommendera korrigerande åtgärder.

i) Genom lagen om generalinspektörer från 1978, i dess ändrade lydelse, inrättades federala generalinspektörer som oberoende och objektiva befattningar inom de flesta myndigheter. Deras uppgift är att bekämpa slöseri, bedrägeri och missbruk i de respektive myndigheternas program och verksamheter. Varje generalinspektör har ansvar för att utföra revisioner och utredningar av myndighetens program och verksamheter. De står även för ledarskap och samordning och rekommenderar lämpliga åtgärder för verksamheten i syfte att främja ekonomi, effektivitet och ändamålsenlighet samt förebygga och upptäcka bedrägeri och missbruk i myndighetens program och verksamheter.

ii) Varje del av underrättelsegemenskapen har sitt eget generalinspektörskontor, som bland annat ansvarar för övervakning av utländsk underrättelseverksamhet. Ett antal rapporter från generalinspektörer om underrättelseprogram har offentliggjorts.

iii) Följande kan nämnas som exempel:

— *The Office of the Inspector General of the Intelligence Community* (IC IG) inrättades enligt avsnitt 405 i *Intelligence Authorization Act of Fiscal Year 2010* – http://www.gpo.gov/fdsys/pkg/PLAW-111publ259/pdf/PLAW-111publ259.pdf. IC IG ansvarar för att utföra allmänna revisioner, utredningar, kontroller och granskningar av underrättelsegemenskapen och för att hantera och lösa övergripande systemrisker, svagheter och brister i underrättelsegemenskapens uppdrag, med målet att förbättra underrättelsegemenskapens ekonomi och effektivitet. IC IG är bemyndigat att utreda klagomål eller uppgifter om påstådda överträdelser av lagar, regler eller föreskrifter samt slöseri, bedrägeri, maktmissbruk eller betydande eller specifika risker för folkhälsan och allmänhetens säkerhet i samband med den nationella underrättelsetjänstens och/eller underrättelsegemenskapens program och verksamheter. IC IG ger information om hur man kontaktar IC IG direkt för att lämna in en rapport: http://www.dni.gov/index.php/about-this-site/contact-the-ig.

— *The Office of the Inspector General* (OIG) – https://www.justice.gov/ – inom det amerikanska justitieministeriet är en lagstadgad oberoende enhet vars uppdrag är att upptäcka och avhjälpa slöseri, bedrägeri, missbruk och tjänstefel i justitieministeriets program och bland dess personal samt främja ekonomi och effektivitet i programmen. OIG undersöker påstådda överträdelser av straff- och civilrätten av justitieministeriets personal och utför även revisioner och kontroller av justitieministeriets program. OIG är behörigt för alla klagomål rörande tjänstefel som begås av justitieministeriets personal, inklusive *Federal Bureau of Investigation, Drug Enforcement Administration, Federal Bureau of Prisons, U.S. Marshals Service, Bureau of Alcohol, Tobacco, Firearms and Explosives* och *United States Attorneys Offices* samt anställda vid andra avdelningar och kontor inom justitieministeriet. (Det enda undantaget är påståenden om tjänstefel som

begås av justitieministeriets jurister eller brottsbekämpande personal i samband med ministeriets juristers behörighet att utreda, väcka talan eller tillhandahålla juridisk rådgivning, där ansvaret ligger hos ministeriets kontor för yrkesansvar). Enligt avsnitt 1001 i *Förenta staterna Patriot Act*, som undertecknades den 26 oktober 2001, ska generalinspektören granska information och motta klagomål om påstådda överträdelser av de medborgerliga fri- och rättigheterna som begås av justitieministeriets personal. OIG har en offentlig webbplats- https://www.oig.justice.gov – med en ”het linje” för ingivande av klagomål – https://www.oig.justice.gov/hotline/index.htm.

b. Kontor och enheter med ansvar för integritetsskydd och medborgerliga friheter inom den amerikanska regeringen har också relevanta ansvarsuppgifter. Följande kan nämnas som exempel:

i) Enligt avsnitt 803 i lagen om 11 september-kommissionens genomföranderekommendationer från 2007, som kodifierats som 42 U.S.C. § 2000-ee1, ska det finnas tjänstemän med ansvar för integritetsskydd och medborgerliga friheter vid vissa ministerier och myndigheter (inklusive utrikesministeriet, justitieministeriet och ODNI). I avsnitt 803 anges att dessa tjänstemän ska fungera som huvudsakliga rådgivare, för att bland annat se till att ministerier, myndigheter eller andra enheter har lämpliga förfaranden för att handlägg klagomål från enskilda personer som hävdar att ministeriet, myndigheten eller enheten i fråga har kränkt deras integritet eller medborgerliga friheter.

ii) ODNI:s *Civil Liberties and Privacy Office* (ODNI CLPO) leds av ODNI *Civil Liberties Protection Officer*, en befattning som inrättades genom lagen om nationell säkerhet från 1948, i dess ändrade lydelse. ODNI CLPO:s ansvarar bland annat för att se till att policyer och förfaranden vid enheter inom underrättelsegemenskapen har lämpliga skyddsmekanismer för integritet och medborgerliga friheter, och för att granska och utreda klagomål om påstått missbruk eller påstådda kränkningar av de medborgerliga fri- och rättigheterna och integritetsskyddet i ODNI:s program och verksamheter. ODNI CLPO tillhandahåller information till allmänheten på sin webbplats, inklusive anvisningar om hur man inger klagomål: www.dni.gov/clpo. Om ODNI CLPO mottar klagomål om integritetsskydd eller medborgerliga friheter som omfattar underrättelsegemenskapens program och verksamheter kommer det att samordna arbetet med andra enheter inom underrättelsegemenskapen när det gäller hur klagomålet bör behandlas vidare inom denna. Observera att även den nationella säkerhetstjänsten (*National Security Agency*, NSA) har ett kontor för en medborgerliga friheter och integritetsskydd. NSA informerar om sina ansvarsuppgifter på sin webbplats – https://www.nsa.gov/civil_liberties/. Om information tyder på att en myndighet inte efterlever integritetskraven (*t.ex.* ett krav enligt avsnitt 4 i PPD-28) har myndigheterna efterlevnadsmekanismer för att granska och avhjälpa händelsen. Myndigheterna är skyldiga att rapportera fall av bristande efterlevnad enligt PPD-28.

iii) *The Office of Privacy and Civil Liberties* (OPCL) vid justitieministeriet stöder de arbets- och ansvarsuppgifter som åligger ministeriets *Chief Privacy and Civil Liberties Officer* (CPCLO). OPCL:s främsta uppgift är att skydda det amerikanska folkets integritet och medborgerliga friheter genom att granska, tillse och samordna ministeriets verksamhet i samband med integritetsskydd. OPCL ger juridisk rådgivning och vägledning till ministeriets avdelningar, ser till att ministeriet följer integritetskraven, inklusive *Privacy Act* från 1974, integritetsbestämmelserna både i *E-Government Act* från 2002 och *Federal Information Security Management Act* samt förvaltningspolitiska direktiv som utfärdas enligt dessa lagar, utformar och tillhandahåller utbildning om integritetsskydd till ministeriets anställda, bistår CPLCO med att utforma ministeriets integritetspolicy, utarbetar rapporter om integritetsfrågor till presidenten och kongressen och granskar informationshanteringsmetoder för att se till att metoderna överensstämmer med integritetsskyddet och de medborgerliga fri- och rättigheterna. OPCL informerar allmänheten om sina ansvarsuppgifter på http://www.justice.gov/opcl.

iv) Enligt 42 U.S.C. § 2000ee och följande artiklar ska styrelsen för tillsyn av personlig integritet och medborgerliga friheter fortlöpande granska i) policyer och förfaranden samt hur ministerier, myndigheter och enheter i den verkställande grenen genomför dessa policyer och förfaranden när det gäller ansträngningarna att skydda nationen från terrorism för att säkerställa att integriteten och de medborgerliga fri- och rättigheterna är skyddade, och ii) andra åtgärder som vidtas av den verkställande grenen i samband med sådana ansträngningar, för att avgöra huruvida åtgärderna skyddar integriteten och de medborgerliga fri- och rättigheterna på lämpligt sätt och är förenliga med gällande lagar, föreskrifter och policyer för integritetsskydd och medborgerliga friheter. Styrelsen ska motta rapporter och annan information från tjänstemän med ansvar för integritetsskydd och medborgerliga rättigheter och ska vid behov lämna rekommendationer när det gäller deras verksamhet. Genom avsnitt 803 i 11 september-kommissionens genomföranderekommendationer (*Implementing Recommendations of the 9/11 Commission Act of 2007*), som kodifierats som 42 U.S.C. § 2000ee-1, regleras tjänstemän med ansvar för integritetsskydd och medborgerliga rättigheter vid åtta federala myndigheter (inklusive *Secretary of Defense, Secretary of Homeland Security, Director of National Intelligence* och *Director of the Central Intelligence Agency*). Eventuella ytterligare myndigheter som utses av styrelsen för att lämna regelbundna rapporter till styrelsen för tillsyn av personlig integritet och medborgerliga fri- och rättigheter (*Privacy and Civil Liberties Oversight Board*, PCLOB) om klagomål om påstådda överträdelser som mottas av

respektive myndighet, inklusive antal, karaktär och disposition, regleras också av detta avsnitt. Enligt PCLOB:s fullmaktsklausul ska styrelsen motta dessa rapporter och vid behov lämna rekommendationer till tjänstemän med ansvar för integritetsskydd och medborgerliga rättigheter när det gäller deras verksamhet.

BILAGA IV

Skrivelse från den federala konkurrensmyndighetens ordförande Edith Ramirez

7 juli 2016

VIA E-POST

Věra Jourová
Kommissionsledamot med ansvar för rättsliga frågor, konsumentfrågor och jämställdhet
Europeiska kommissionen
Rue de la Loi/Wetstraat 200
1049 Bryssel
BELGIEN

Bästa kommissionär Jourová,

Förenta staterna:s federala konkurrensmyndighet (FTC) uppskattar detta tillfälle ett beskriva hur den genomför den nya skölden för skydd av privatlivet i EU och Förenta staterna (nedan kallad *skölden för skydd av privatlivet* eller *ramen*). Vi anser att skölden för skydd av privatlivet kommer att spela en avgörande roll för att underlätta integritetsskyddade affärsmässiga transaktioner i en alltmer sammankopplad värld. Tack vare skölden kommer företag att kunna bedriva omfattande verksamhet i den globala ekonomin, samtidigt som man säkerställer att EU-konsumenternas integritetsskydd förblir starkt. FTC har länge arbetat för integritetsskydd över gränserna och genomförandet av den nya ramen kommer att vara en viktig prioritering. Nedan följer en redogörelse för konkurrensmyndighetens starka åtagande för integritetsskydd i allmänhet, inklusive vårt genomförande av det ursprungliga safe harbor-programmet, samt ministeriets genomförandestrategi för den nya ramen.

Konkurrensmyndigheten gjorde ett offentligt åtagande om att genomföra safe harbor-programmet för första gången 2000. Vid den tidpunkten skickade myndighetens ordförande Robert Pitofsky en skrivelse till Europeiska kommissionen med en redogörelse för ministeriets åtagande att noggrant genomföra safe harbor-principerna. Konkurrensmyndigheten har fullgjort detta åtagande genom nästan 40 verkställighetsåtgärder, ett stort antal ytterligare utredningar och samarbete med enskilda dataskyddsmyndigheter i EU om frågor av ömsesidigt intresse.

Efter det att Europeiska kommissionen i november 2013 uttryckte farhågor om förvaltningen och genomförandet av safe harbor-programmet inledde konkurrensministeriet och handelsministeriet samråd med tjänstemän från Europeiska kommissionen för att undersöka möjliga sätt att förstärka genomförandet. Medan samråden pågick utfärdade EU-domstolen den 6 oktober 2015 ett beslut i Schrems-målet, som bland annat ogiltigförklarade Europeiska kommissionens beslut om adekvat skyddsnivå för safe harbor-programmet. Efter beslutet fortsatte vi att arbeta nära med handelsministeriet och Europeiska kommissionen i en ansträngning för att stärka integritetsskyddet för enskilda personer i EU. Skölden för skydd av privatlivet är resultatet av dessa pågående förhandlingar. Såsom var fallet med safe harbor-programmet åtar sig FTC härmed att noggrant genomföra den nya ramen. Denna skrivelse formaliserar detta åtagande.

Vi bekräftar särskilt våra åtaganden inom följande fyra centrala områden: 1) Prioritera hänskjutanden och utredningar, 2) hantera falska och bedrägliga påståenden om medlemskap i skölden, 3) fortsatt ordningsövervakning. och 4) ökat engagemang och tillsynssamarbete med EU:s dataskyddsmyndigheter. Nedan följer en närmare beskrivning av dessa åtaganden och relevant bakgrundsinformation om FTC: s roll för att skydda konsumenternas integritet och genomföra safe harbor samt en allmän beskrivning av hur integritetsskyddet fungerar i Förenta staterna ([1]).

I. BAKGRUND

A. **FTC:s GENOMFÖRANDE AV INTEGRITETSSKYDDET OCH DESS POLITISKA ARBETE**

FTC har en omfattande civilrättslig behörighet att främja konsumentskydd och konkurrens på det kommersiella området. Som en del av sitt uppdrag på konsumentskyddsområdet upprätthåller FTC en rad olika lagar för att skydda konsumentuppgifters integritet. Enligt FTC-lagen, den primärlagstiftning som upprätthålls av FTC, förbjuds ”illojala” och

([1]) Ytterligare information om Förenta staterna:s federala och delstatliga integritetslagar ges i bilaga A. Dessutom finns en sammanfattning av våra senaste integritets- och säkerhetsåtgärder på FTC:s webbplats: https://www.ftc.gov/reports/privacy-data-security-update-2015.

”bedrägliga” handlingar eller metoder i eller som påverkar handeln ([1]). Bedrägligt är en handling, ett utelämnande eller en metod som på ett konkret sätt antas kunna vilseleda förnuftiga konsumenter ([2]). En metod är illojal om den framkallar, eller kan antas framkalla, väsentlig skada för konsumenter och skadan varken går att undvika på ett rimligt sätt eller uppvägs av fördelar för konsumenterna eller för konkurrensen ([3]). FTC genomför också särskilda lagar om skydd av information beträffande hälsa, krediter och andra finansiella frågor samt information om barn på nätet, och har utfärdat genomförandeföreskrifter för varje lag.

FTC: s behörighet enligt FTC-lagen gäller frågor ”i eller som påverkar handeln”. FTC är inte behörigt för verkställighetsåtgärder på det straffrättsliga området eller för nationella säkerhetsfrågor. Ministeriet är inte heller behörigt för de flesta andra regeringsåtgärder. Dessutom finns det undantag från FTC behörighet för affärsverksamhet, bland annat beträffande banker, flygbolag, försäkringsbranschen och gemensamma transportverksamheter som bedrivs av telekomleverantörer. FTC är inte heller behörigt för de flesta ideella organisationer, men däremot för falsk välgörenhet eller andra organisationer som faktiskt bedriver sin verksamhet i vinstsyfte. FTC är också behörigt för ideella organisationer som drivs i vinstsyfte för deras vinstdrivande medlemmar, bland annat genom att ge betydande ekonomiska fördelar till dessa medlemmar ([4]). I vissa fall har FTC parallell behörighet med andra brottsbekämpande organ.

Vi har utvecklat starka arbetsrelationer med federala och statliga myndigheter och har ett nära samarbete med dem för att samordna utredningar eller hänskjuta ärenden om så är nödvändigt.

Verkställighet utgör grunden för FTC:s strategi för integritetsskydd. Hittills har FTC tagit upp över 500 ärenden rörande integritetsskydd för konsumentinformation. Ärendena omfattar både offline- och onlineinformation och FTC har bland annat vidtagit verkställighetsåtgärder mot både och stora företag till följd av påståenden om att de inte hanterat känslig konsumentinformation på lämpligt sätt, inte har skyddat konsumenters personuppgifter, att de har spårat konsumenter online på ett bedrägligt sätt, skickat skräppost till konsumenter, installerat spionprogram eller andra sabotageprogram på konsumenters datorer, överträtt regeln om att inte ringa kunder som spärrat sina telefonnummer mot oönskade telefonsamtal och andra telekomregler samt på ett olämpligt sätt samlat in och utbytt konsumentinformation på mobila anordningar. FTC:s brottsbekämpande åtgärder – både i den fysiska och den digitala världen – utgör ett viktigt budskap till företagen om behovet av att skydda konsumenternas integritet.

FTC har också genomfört flera politiska initiativ för att öka konsumenternas integritetsskydd och informera om sitt arbete med att genomdriva reglerna. FTC har stått värd för seminarier och har utfärdat rapporter med rekommendationer om bästa praxis för att främja integritetsskyddet i det mobila ekosystemet, öka insynen i uppgiftsförmedlingsbranschen, maximera fördelarna med stordata och samtidigt begränsa riskerna, särskilt för konsumenter med låg inkomst och missgynnade konsumenter, samt genom att lyfta fram integritets- och säkerhetsföljderna av bland annat ansiktsigenkänning och sakernas internet.

FTC engagerar sig även i upplysningskampanjer som riktas mot konsumenter och företag för att öka effekterna av sitt arbete och politiska initiativ. FTC har använt olika verktyg – publikationer, onlineresurser, seminarier och sociala medier – för att tillhandahålla utbildningsmaterial om många olika frågor, bland annat mobilappar, skydd av barns integritet och datasäkerhet. Nyligen lanserade FTC sitt initiativ ”Start With Security”, med ny vägledning för företag som bygger på tidigare erfarenheter av myndighetens datasäkerhetsärenden samt en rad seminarier landet runt. FTC har dessutom länge varit ledande i konsumentutbildning om grundläggande datorsäkerhet. Förra året hade vår webbplats OnGuard Online och dess spanska motsvarighet, Alerta en Línea, mer än 5 miljoner sidvisningar.

B. **Förenta staterna:s rättsliga skyddsmekanismer till förmån för konsumenter i EU**

Skölden kommer att ingå i Förenta staterna:s allmänna integritetsskyddsram, som skyddar EU-konsumenter på en rad olika sätt.

([1]) 15 U.S.C. § 45(a).
([2]) Se FTC:s policyförklaring om bedrägeri, bifogad till Cliffdale Assocs., Inc., 103 F.T.C. 110, 174 (1984), se https://www.ftc.gov/public-statements/1983/10/ftc-policy-statement-deception.
([3]) Se 15 U.S.C § 45(n); FTC policyförklaring om illojala metoder, bifogad till Int'l Harvester Co., 104 F.T.C. 949, 1070 (1984), se https://www.ftc.gov/public-statements/1980/12/ftc-policy-statement-unfairness.
([4]) Se California Dental Ass'n v. FTC, 526 U.S. 756 (1999).

FTC-lagens förbud mot illojala och bedrägliga handlingar eller metoder begränsas inte till att skydda amerikanska konsumenter från amerikanska företag, eftersom den omfattar metoder som 1) orsakar eller sannolikt kan orsaka förutsebar skada i Förenta staterna, eller 2) omfattar faktiskt bedrägligt beteende i Förenta staterna. FTC kan dessutom använda alla tillgängliga rättsmedel, inklusive upprättelse, för skydd av inhemska konsumenter när de skyddar utländska konsumenter.

FTC:s brottsbekämpande arbete gynnar både amerikanska och utländska konsumenter avsevärt. FTC:s ärenden om verkställande av avsnitt 5 i FTC-lagen har skyddat både inhemska och utländska konsumenters integritet. I ett ärende mot informationsförmedlaren Accusearch hävdade FTC att företagets försäljning av konfidentiella telefonregister till tredje parter utan konsumenternas vetskap eller samtycke utgjorde en illojal affärsmetod som strider mot avsnitt 5 i FTC-lagen. Accusearch sålde information om både amerikanska och utländska konsumenter ([1]). Domstolen beviljade föreläggande mot Accusearch, bland annat med ett förbud mot att marknadsföra eller sälja konsumenters personuppgifter utan skriftligt samtycke om inte uppgifterna lagligen erhållits från allmänt tillgänglig information, och beslutade om återbetalning på nästan 200 000 US-dollar ([2]).

FTC:s uppgörelse med TRUSTe är ett annat exempel. Den säkerställer att konsumenter, även i EU, kan förlita sig på utfästelser som en global självreglerande organisation gör om sin granskning och certifiering av inhemska och utländska onlinetjänster ([3]). Våra åtgärder mot TRUSTe stärker dessutom det självreglerande systemet för integritetsskydd mer allmänt, genom att säkerställa att enheter som spelar en viktig roll i självreglerande system, inklusive gränsöverskridande ramar, blir ansvarsskyldiga.

FTC upprätthåller även andra riktade lagar som skyddar konsumenter utanför Förenta staterna, t.ex. lagen om integritetsskydd för barn online (nedan kallad *COPP-lagen*). Enligt denna lag krävs bland annat att operatörer av webbplatser och onlinetjänster som vänder sig till barn eller webbplatser med allmän publik som vet att de inhämtar personuppgifter från barn under 13 års ålder ska innehålla meddelanden till föräldrar och att föräldrarnas kontrollerbara samtycke ska inhämtas. Förenta staterna-baserade webbplatser och tjänster som omfattas av COPP-lagen och samlar in personuppgifter om utländska barn är skyldiga att följa lagen. Utrikesbaserade webbplatser och onlinetjänster måste också uppfylla lagen om de riktas till barn i Förenta staterna eller om de vet att de inhämtar personuppgifter från barn i Förenta staterna. Förutom de amerikanska federala lagar som upprätthålls av FTC kan vissa andra federala och statliga konsument- och integritetsskyddslagar ge ytterligare fördelar för konsumenter i EU.

C. **Genomförandet av safe harbor**

Som en del av sitt integritets- och skyddsprogram har FTC även strävat efter att skydda EU-konsumenter genom att vidta verkställighetsåtgärder vid överträdelser av safe harbor-principerna. FTC har vidtagit 39 verkställighetsåtgärder: 36 falska certifieringspåståenden, och tre ärenden – mot Google, Facebook och Myspace – som rör påstådda brott mot safe harbor-principerna om integritetsskydd ([4]). Dessa ärenden visar verkställbarheten av certifieringar och återverkningar vid bristande efterlevnad. Beslut om att man måste vara 20 år för att kunna lämna sitt samtycke kräver att Google, Facebook och Myspace genomför omfattande integritetsskyddsprogram som måste vara rimligt utformade för att hantera risker för integritetsskyddet i samband med utveckling och drift av nya och befintliga produkter och tjänster och för att skydda integriteten och sekretessen för personuppgifter. De omfattande integritetsskyddsprogram som krävs enligt dessa avgöranden innehåller bestämmelser om att företagen måste identifiera förutsebara materiella risker och genomföra kontroller för att hantera sådana risker. Företagen måste också göra fortlöpande oberoende bedömningar av sina integritetsskyddsprogram, som ska lämnas in till FTC. Enligt avgörandena är företagen dessutom förbjudna att ge en missvisande bild av sina integritetsskyddsmetoder och sitt eventuella deltagande i integritets- eller säkerhetsprogram. Detta förbud skulle även gälla företagens handlingar och metoder enligt den nya skölden för skydd av privatlivet. FTC kan verkställa dessa avgöranden genom att yrka på civilrättsliga påföljder. Faktum är att Google betalade ett rekordhögt

([1]) *Se* Den kanadensiska dataskyddsombudsmannens kontor, klagomål enligt Pipeda mot Accusearch, Inc., verksamt som Abika.com, https://www.priv.gc.ca/cf-dc/2009/2009_009_0731_e.asp. Den kanadensiska dataskyddsombudsmannens kontor ingav en *amicus curiae* i överklagandet mot FTC:s åtgärd och genomförde en egen utredning, som visade att Accusearchs metoder även kränkte kanadensisk lag.

([2]) *Se FTC mot Accusearch, Inc.*, nr 06CV015D (D. Wyo. 20 december 2007), *aff'd* 570 F.3d 1187 (10 Cir. (2009).

([3]) Se *In the Matter of True Ultimate Standards Everywhere, Inc.*, nr C-4512 (F.T.C. 12 mars 2015) (beslut och avgörande), *se* https://www ftc.gov/system/files/documents/cases/150318trust-edo.pdf.

([4]) Se *In the Matter of Google, Inc.*, nr C-4336 (F.T.C. 13 oktober 2011) (beslut och avgörande), *se* https://www.ftc.gov/news-events/press-releases/2011/03/ftc-charges-deceptive-privacy-practices-googles-rollout-its-buzz; *målet Facebook, Inc.*, nr C-4365 (F.T.C. 27 juli 2012) (beslut och avgörande), *se* https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook; *målet Myspace LLC.*, nr C-4369 (F.T.C. 30 augusti 2012) (beslut och avgörande), *se* https://www.ftc.gov/news- events/press-releases/2012/09/ftc-finalizes-privacy-settlement-myspace.

vite på 22,5 miljoner US-dollar 2012 för att frigöra sig från påståenden om att företaget hade brutit mot dess avgörande. Dessa FTC-avgöranden bidrar således till att skydda över en miljard konsumenter i hela världen, varav hundratals miljoner bor i Europa.

De ärenden som FTC har drivit har även inriktats på falska, bedrägliga eller missvisande påståenden om deltagande i safe harbor. FTC tar sådana påståenden på allvar. I målet FTC mot Karnani väckte FTC t.ex. talan 2011 mot en internetmarknadsförare i Förenta staterna för att personen och dennes företag lurade brittiska konsumenter att tro att företaget var baserat i Storbritannien, bland annat genom att använda domännamn med.uk och hänvisa till den brittiska valutan och det brittiska postsystemet ([1]). När konsumenterna fick produkterna upptäckte de dock att de måste betala oväntade importtullar, att garantierna inte var giltiga i Storbritannien och att de måste betala avgifter för att få ersättning. FTC hävdade också att de svarande vilseledde konsumenterna när det gällde företagets deltagande i safe harbor-programmet. Alla konsumenter som föll offer för detta företag fanns i Storbritannien.

Många av våra andra verkställighetsärenden i fråga om safe harbor omfattade organisationer som hade anslutit sig till safe harbor men inte förnyade sin certifiering, samtidigt som de utgav sig för att vara medlemmar. Såsom diskuteras närmare nedan åtar sig FTC även att behandla falska påståenden om deltagande i skölden för skydd av privatlivet. Dessa strategiska verkställighetsåtgärder kommer att komplettera handelsministeriets utökade åtgärder för att kontrollera efterlevnaden av programmets krav på certifiering och återcertifiering, dess övervakning av att reglerna efterlevs på ett effektivt sätt, bland annat genom frågeformulär till organisationer som deltar i skölden, och ministeriets ökade insatser för att identifiera falska påståenden om medlemskap och missbruk av eventuell certifieringsmärkning ([2]).

II. PRIORITERINGAR AVSEENDE HÄNSKJUTANDEN OCH UTREDNINGAR

Precis som med safe harbor-programmet åtar sig FTC att prioritera hänskjutanden avseende skölden för skydd av privatlivet från EU-medlemsstater. Vi kommer även att prioritera hänskjutanden om bristande efterlevnad av självreglerande riktlinjer rörande skölden för skydd av privatlivet från organ för självreglering på integritetskyddets område och andra oberoende tvistlösningsorgan.

För att underlätta hänskjutanden från EU-medlemsstater enligt ramen arbetar FTC med att ta fram ett standardiserat förfarande för hänskjutanden och kommer också att ge vägledning till EU-medlemsstaterna om den typ av information som bäst hjälper FTC att utreda ett hänskjutande. Som ett led i detta arbete kommer FTC att utse en kontaktpunkt hos myndigheten som kommer att ansvara för hänskjutanden från EU-medlemsstaterna. Det är till mycket stor hjälp om den hänskjutande myndigheten har gjort en preliminär utredning av den påstådda överträdelsen och kan samarbeta med FTC i utredningen.

När ett hänskjutande mottas från en EU-medlemsstat eller en självreglerande organisation kan FTC vidta en rad olika åtgärder för att utreda de frågor som tas upp. FTC kan t.ex. granska det berörda företagets integritetsskyddspolicy, inhämta ytterligare information direkt från företaget eller från tredje parter, följa upp ärendet med den hänskjutande myndigheten, bedöma om det finns ett mönster av överträdelser eller om ett betydande antal konsumenter påverkas, fastställa om hänskjutandet berör frågor som omfattas av handelsministeriets behörighetsområde, i förekommande fall bedöma om upplysningskampanjer riktade till konsumenter och företag skulle vara användbara samt inleda verkställighetsförfaranden.

FTC förbinder sig också att utbyta information om hänskjutanden med hänskjutande myndigheter, bland annat om status för hänskjutanden, enligt lagar och begränsningar om sekretess. I den utsträckning det är möjligt med tanke det antal och de typer av hänskjutanden som mottas kommer den information som lämnas att inbegripa en utvärdering av de hänskjutna frågorna, bland annat en beskrivning av viktiga punkter och eventuella åtgärder som vidtagits för att hantera lagöverträdelser som faller inom FTC:s behörighetsområde. FTC kommer också att ge återkoppling till den hänskjutande myndigheten om de typer av hänskjutanden som mottas. Syftet är att öka effektiviteten i de åtgärder som vidtas för att hantera olagligt beteende. Om en hänskjutande myndighet söker information om statusen för ett visst

([1]) *Se FTC mot Karnani*, nr 2:09-cv-05276 (C.D. Cal. 20 maj 2011) (yrkat slutligt avgörande), *se* https://www ftc.gov/sites/default/files/documents/cases/2011/06/110609karnanistip.pdf;*se även* Lesley Fair, FTC Business Center Blog, *Around the World in Shady Ways*, http://www.business.ftc.gov/blog/2011/06/around-world-shady-ways (9 juni 2011).

([2]) Skrivelse från Ken Hyatt, tillförordnad statssekreterare för internationell handel, *International Trade Administration*, till Věra Jourová, kommissionsledamot med ansvar för rättsliga frågor, konsumentfrågor och jämställdhet.

hänskjutande för att själv inleda ett verkställighetsförfarande kommer FTC att besvara sådana förfrågningar, dock med hänsyn till antalet hänskjutanden under behandling och sekretesskrav och andra lagstadgade krav.

FTC kommer också att föra ett nära samarbete med dataskyddsmyndigheter i EU för att hjälpa till med deras verkställighetsåtgärder. I lämpliga fall skulle detta kunna omfatta informationsutbyte och hjälp med utredningar som genomförs enligt *U.S. Safe WEB Act*, enligt vilken FTC får bistå utländska brottsbekämpande myndigheter om den utländska myndigheten verkställer lagar som förbjuder metoder som väsentligen liknar de förfaranden som är förbjudna enligt de lagar som FTC verkställer ([1]). Som ett led i detta stöd kan FTC utbyta information som erhållits i samband en FTC-utredning, utfärda beslut om obligatoriska vittnesmål för en EU-dataskyddsmyndighets räkning som genomför sin egen utredning och inhämta muntliga vittnesmål från vittnen eller svarande i samband med dataskyddsmyndighetens verkställighetsförfaranden enligt kraven i *U.S. Safe WEB Act*. FTC utövar regelbundet denna befogenhet för att hjälpa andra myndigheter i världen med integritets- och konsumentskyddsmål ([2]).

Förutom att prioritera hänskjutanden i fråga om skölden från EU-medlemsstater och organ för självreglering på integritetskyddets område ([3]), förbinder FTC sig att i förekommande fall utreda eventuella överträdelser av ramen på eget initiativ med hjälp av ett antal olika verktyg.

FTC har haft ett effektivt program för utredning av integritetsskydds- och säkerhetsfrågor i samband med kommersiella organisationer i över ett årtionde. Som en del av dessa utredningar har FTC rutinmässigt undersökt om organisationen i fråga gjorde utfästelser om deltagande i safe harbor. Om organisationen gjorde sådana utfästelser och utredningen avslöjade uppenbara överträdelser av safe harbor-principerna inbegrep FTC i sådana fall överträdelser av safe harbor i sina verkställighetsåtgärder. Vi kommer att fortsätta att tillämpa denna proaktiva strategi enligt den nya ramen. FTC genomför dessutom många utredningar som inte leder till offentliga verkställighetsåtgärder. Många FTC-utredningar avslutas eftersom personalen inte kan påvisa en uppenbar lagöverträdelse. Eftersom FTC:s utredningar inte är offentliga och dessutom är sekretessbelagda händer det ofta att avslutandet av en utredning inte offentliggörs.

De nästan 40 verkställighetsåtgärder i fråga om safe harbor-programmet som inleddes av FTC är ett uttryck för myndighetens åtagande att proaktivt verkställa gränsöverskridande integritetsskyddsprogram. FTC kommer att kontrollera eventuella överträdelser av skölden som ett led i sina regelbundna integritets- och säkerhetsutredningar.

III. HANTERA FALSKA ELLER BEDRÄGLIGA PÅSTÅENDEN OM MEDLEMSKAP I SKÖLDEN FÖR SKYDD AV PRIVATLIVET

Såsom anges ovan kommer FTC att vidta åtgärder mot organisationer som ger missvisande information om sitt deltagande i skölden. FTC kommer att prioritera hänskjutanden från handelsministeriet som rör fall där ministeriet har konstaterat att organisationer påstår att de är medlemmar i skölden eller använder sköldens certifieringsmärkning utan tillstånd.

FTC konstaterar dessutom att om en organisation i sin integritetsskyddspolicy utlovar att den följer sköldens principer och inte registrerar sig eller omregistrerar sig hos handelsministeriet kommer detta sannolikt inte i sig själv att undanta organisationen från verkställighetsåtgärder från FTC:s sida för att genomdriva åtagandena enligt skölden.

([1]) När FTC beslutar om huruvida det ska utöva sin befogenhet enligt *U.S. Safe WEB Act* överväger det bland annat följande aspekter: ”A) Om den hänskjutande myndigheten har samtyckt till eller kommer att tillhandahålla ömsesidig hjälp till FTC, B) huruvida ett verkställande av begäran skulle skada Förenta staternas allmänintresse, och C) huruvida den hänskjutande myndighetens utredning eller verkställighetsförfarande rör handlingar eller metoder som orsakar eller sannolikt kan orsaka skada för ett betydande antal personer.” 15 U.S.C. § 46(j)(3). Denna befogenhet är inte tillämplig på upprätthållandet av konkurrenslagstiftningen.

([2]) Under budgetåren 2012–2015 utövade FTC t.ex. sin befogenhet enligt *U.S. Safe WEB Act* för att dela information till svar på nästan 60 förfrågningar från utländska myndigheter och utfärdade nästan 60 civilrättsliga krav på utredning (motsvarande administrativa förelägganden) för att bistå i 25 utländska utredningar.

([3]) Även om FTC inte löser eller medlar i individuella konsumentklagomål bekräftar FTC att hänskjutanden rörande skölden för skydd av privatlivet från dataskyddsmyndigheter i EU kommer att prioriteras. Dessutom använder FTC klagomål i sin konsumentkontrolldatabas, som många andra brottsbekämpande myndigheter har tillgång till, för att identifiera trender, fastställa verkställighetsprioriteringar och identifiera eventuella luckor i utredningsprioriteringarna. Enskilda i EU kan använda samma klagomålssystem som finns tillgängliga för amerikanska medborgare för att inge klagomål till FTC på http://www.ftc.gov/complaint. När det gäller individuella klagomål rörande skölden bör enskilda i EU dock inge klagomål till dataskyddsmyndigheten i sin medlemsstat eller till ett alternativt tvistlösningsorgan.

IV. ÖVERVAKNING AV BESLUT

FTC bekräftar även sitt åtagande att övervaka verkställighetsbeslut för att säkerställa efterlevnad av skölden för skydd av privatlivet.

FTC kommer att kräva att skölden efterlevs genom en rad lämpliga förbudsbestämmelser i framtida rambeslut från FTC. Detta omfattar förbud mot oriktiga utfästelser angående skölden och andra integritetsskyddsprogram, när dessa ligger till grund för FTC-åtgärden i fråga.

FTC:s ärenden rörande det ursprungliga safe harbor-programmet är vägledande. I de 36 ärendena om falska eller bedrägliga påståenden om deltagande i safe harbor-certifieringen förbjuder varje beslut svaranden att göra missvisande utfästelser om deltagande i safe harbor eller något annat integritetsskydds- eller säkerhetsprogram och kräver att företaget lämnar efterlevnadsrapporter till FTC. I ärenden som omfattade överträdelser av safe harbor-principerna har företagen beordrats att genomföra omfattande integritetsskyddsprogram och inhämta oberoende bedömningar från en tredje part om dessa program vartannat år under en tjugoårsperiod, som de måste lämna till FTC.

Överträdelser av FTC:s administrativa beslut kan leda till vite på upp till 16 000 US-dollar per överträdelse eller 16 000 US-dollar per dag för upprepade överträdelser ([1]). I fall där metoderna påverkar många konsumenter kan beloppet uppgå till miljontals dollar. Varje förordnande omfattar även rapporterings- och efterlevnadskrav. Organisationer som omfattas av ett förordnande måste bevara dokument som visar deras efterlevnad under ett angivet antal år. Förordnandena måste också spridas till anställda som ansvarar för att säkerställa att de efterlevs.

Precis som alla förordnanden övervakar FTC systematiskt efterlevnaden av safe harbor-förordnanden. FTC tar verkställandet av sina förordnanden om integritetsskydd och uppgiftssäkerhet på allvar, och vidtar åtgärder för att verkställa dem om så behövs. Såsom anges ovan betalade t.ex. Google ett vite på 22,5 miljoner US-dollar för att frigöra sig från påståenden om att företaget hade brutit mot sitt FTC-förordnande. FTC kommer genom sina förordnanden att fortsätta att skydda alla konsumenter i världen som samverkar med ett företag, inte bara konsumenter som inger klagomål.

Slutligen kommer FTC att föra en onlineförteckning över företag som omfattas av förordnanden i samband med genomförandet av både safe harbor-programmet och den nya skölden för skydd av privatlivet ([2]). När ett företag blir föremål för ett rättsligt avgörande från FTC eller en domstol på grundval av bristande efterlevnad av principerna ska det, enligt principerna för skölden för skydd av privatlivet, nu dessutom offentliggöra alla avsnitt i efterlevnads- eller bedömningsrapporter som berör skölden som har lämnats in till FTC, i den utsträckning detta är förenligt med lagar och regler om sekretess.

V. SAMARBETE MED DATASKYDDSMYNDIGHETER I EU OCH OM VERKSTÄLLIGHETSÅTGÄRDER

FTC bekräftar den viktiga roll som dataskyddsmyndigheter i EU spelar för efterlevnaden av skölden för skydd av privatlivet, och uppmuntrar till ökat samarbete när det gäller samråd och genomförande. Förutom eventuella samråd med hänskjutande dataskyddsmyndigheter om ärendespecifika frågor förbinder sig FTC att delta i regelbundna möten med de utsedda företrädarna för artikel 29-arbetsgruppen för att diskutera hur det brottsbekämpande samarbetet inom ramen för skölden kan förbättras i allmänhet. FTC kommer också, tillsammans med handelsministeriet, Europeiska kommissionen och företrädarna för artikel 29-arbetsgruppen, att delta i den årliga översynen av skölden för att diskutera dess genomförande.

FTC uppmuntrar även framtagandet av verktyg för att förbättra samarbetet om genomförandet av skölden med dataskyddsmyndigheter i EU samt andra myndigheter med ansvar för integritetsskydd i världen. Tillsammans med berörda verkställande myndigheter i EU och i världen lanserade FTC förra året ett system för tidig varning inom ramen för *Global Privacy Enforcement Network* (nedan kallat *GPEN*), i syfte att utbyta information om utredningar och främja samordning av brottsbekämpande åtgärder. GPEN-systemet för tidig varning kan vara särskilt användbart inom ramen för skölden för skydd av privatlivet. FTC och EU:s dataskyddsmyndigheter kan använda systemet för att samordna utredningar inom ramen för skölden och andra utredningar rörande integritetsskydd, och använda det som en utgångspunkt för informationsutbyte för att skapa ett samordnat och mer effektivt integritetsskydd för konsumenterna. Vi ser fram emot att fortsätta samarbetet med de deltagande EU-myndigheterna för att genomföra GPEN-systemet för

([1]) 15 U.S.C. § 45(m); 16 C.F.R. § 1.98.

([2]) *Se FTC, Business Center, Legal Resources,* https://www.ftc.gov/tips-advice/business-center/legal-resources?type=case&field-consumer-protection-topics-tid=251.

tidig varning mer allmänt och utforma andra verktyg för att förbättra det brottsbekämpande samarbetet när det gäller integritetsskyddsärenden, även ärenden som rör skölden för skydd av privatlivet.

FTC bekräftar härmed sitt åtagande att genomföra den nya skölden för skydd av privatlivet. Vi ser också fram emot att fortsätta samarbetet med våra EU-kolleger när vi tillsammans arbetar för att skydda konsumenternas integritet på båda sidor av Atlanten.

Högaktningsfullt,

Edith Ramirez

Ordförande

Tillägg A

Skölden för skydd av privatlivet i EU och Förenta staterna i sitt sammanhang: en överblick över ramarna för integritet och säkerhet i Förenta staterna

Skyddet som skölden för skydd av privatlivet i EU och Förenta staterna (nedan kallad *skölden*) innebär är en del av det bredare integritetsskydd som det amerikanska rättssystemet i sin helhet medför. För det första har Förenta staterna:s federala konkurrensmyndighet (*U.S. Federal Trade Commission*, nedan kallad *FTC*) ett robust program för integritet och datasäkerhet för kommersiellt bruk som skyddar konsumenter globalt. För det andra har ramarna för skyddet av konsumenternas integritet och säkerheten i Förenta staterna utvecklats betydligt sedan 2000, då Förenta staterna:s och EU:s Safe Harbor-program antogs. Sedan dess har många federala och statliga lagar om integritet och säkerhet antagits, och de offentliga och privata tvisterna för tillämpning av integritetsskyddet har ökat avsevärt i omfattning. Det omfattande amerikanska rättsliga skydd för konsumenternas integritet och säkerhet som gäller kommersiell hantering av uppgifter kompletterar skyddet för enskilda i EU genom den nya ramen.

I. FTC:s ÖVERGRIPANDE INTEGRITETS- OCH SKYDDSPROGRAM

FTC är det huvudsakliga amerikanska konsumentskyddsorganet med inriktning på integritetsfrågor inom den kommersiella sektorn. FTC har befogenhet att väcka åtal vid illojala och bedrägliga handlingar eller metoder som bryter mot konsumenternas integritet samt att genomföra mer riktad integritetslagstiftning för skydd av viss finansiell och hälsorelaterad information, information om barn och information som används för att fatta vissa beslut rörande urval när det gäller kunder.

FTC har erfarenheter utan motstycke när det gäller genomförande av integritetsskydd för konsumenter. FTC:s åtgärder för genomförande har varit riktade mot olagliga metoder både offline och online. FTC har t.ex. vidtagit verkställighetsåtgärder mot välkända företag som Google, Facebook, Twitter, Microsoft, Wyndham, Oracle, HTC och Snapchat, liksom mot mindre kända företag. FTC har stämt företag som enligt uppgift har skickat skräppost till konsumenter, installerat spionprogram på datorer, försummat att säkra konsumenters personuppgifter, spårat konsumenter online på ett bedrägligt sätt, brutit mot barns integritet, samlat in information från konsumenters mobila enheter olagligen och misslyckats med att säkra internetanslutna enheter som använts för att lagra personuppgifter. De beslut som detta har lett till har generellt sett inneburit fortlöpande övervakning av FTC under tjugo års tid, förhindrat ytterligare lagöverträdelser och ålagt företagen omfattande böter för brott mot bestämmelserna ([1]). Viktigt är att FTC:s beslut inte bara skyddar de enskilda personer som kan ha framfört klagomål. De skyddar snarare alla konsumenter som har med företaget att göra, och som då inte behöver vidta åtgärder. I det gränsöverskridande perspektivet har FTC behörighet att skydda konsumenter globalt från metoder som tillämpas i Förenta staterna ([2]).

Hittills har FTC tagit upp mer än 130 fall av skräppost och spionprogram, över 120 fall telemarketing gentemot kunder som spärrat sina telefonnummer mot oönskade telefonsamtal, nästan 60 fall av datasäkerhet, och vidtagit över 100 åtgärder enligt lagen om rättvis kreditrapportering och över 50 åtgärder rörande integritet i allmänhet samt tagit upp nästan 30 fall av brott mot lagen Gramm-Leach-Bliley, samt vidtagit över 20 åtgärder för genomförande av lagen om integritetsskydd för barn online (*Children's Online Privacy Protection Act* – COPPA) ([3]). Utöver dessa fall har FTC också utfärdat och offentliggjort varningsbrev ([4]).

([1]) En enhet som underlåter att följa ett beslut av FTC beläggs med vite på upp till 16 000 US-dollar per överträdelse, eller 16 000 US-dollar per dag om överträdelsen fortsätter. *Se* 15 U.S.C. § 45(l); 16 C.F.R. § 1.98c.

([2]) Kongressen har uttryckligen fastslagit FTC:s befogenhet att tillgripa rättsmedel, inbegripet upprättelse, för handlingar eller metoder som inbegriper utländsk handel som 1) orsakar eller sannolikt kan orsaka förutsebar skada i Förenta staterna, eller 2) omfattar faktiskt bedrägligt beteende i Förenta staterna. *Se* 15 U.S.C. § 45(a)(4).

([3]) Kommissionens fall rörande integritet och datasäkerhet visade ibland att ett företag var involverat i både bedrägliga och illojala metoder; dessa fall innefattade emellanåt också påstådda brott mot flera lagar, t.ex. lagen om rättvis kreditrapportering, lagen Gramm-Leach-Bliley och COPPA.

([4]) *Se t.ex.* federala konkurrensmyndighetens pressmeddelande *FTC Warns Children's App Maker BabyBus About Potential COPPA Violations* (22 december 2014), https://www.ftc.gov/news-events/press- releases/2014/12/ftc-warns-childrens-app-maker-babybus-about-potential-coppa, federala konkurrensmyndighetens pressmeddelande *FTC Warns Data Broker Operations of Possible Privacy Violations* (7 maj 2013), https://www.ftc.gov/news-events/press-releases/2013/05/ftc-warns-data-broker-operations-possible-privacy-violations, federala konkurrensmyndighetens pressmeddelande *FTC Warns Data Brokers That Provide Tenant Rental Histories They May Be Subject to Fair Credit Reporting Act* (3 april 2013), https://www.ftc.gov/news-events/press-releases/2013/04/ftc-warns-data-brokers-provide-tenant-rental-histories-they-may.

Som en del av sitt historiskt sett starka genomförande av integritetsskyddet har FTC också regelbundet letat efter potentiella brott mot safe harbor-programmet. Sedan safe harbor-programmet antogs har FTC på eget initiativ genomfört många utredningar angående efterlevnaden av safe harbor och tagit upp 39 fall med amerikanska företag som brutit mot safe harbor. FTC kommer att fortsätta med sitt proaktiva arbetssätt genom att prioritera genomförandet av den nya ramen.

II. INTEGRITETSSKYDD FÖR KONSUMENTER PÅ FEDERAL OCH STATLIG NIVÅ

Översikten över genomförandet av safe harbor, som finns som bilaga till EU-kommissionens safe harbor-beslut om adekvat skyddsnivå, innehåller en sammanfattning av många av de federala och statliga integritetslagar som gällde när safe harbor-programmet antogs år 2000 ([1]). På den tiden reglerades kommersiell insamling och användning av personuppgifter genom många federala lagar, utöver avsnitt 5 i FTC-lagen, inbegripet lagen om kabelkommunikationer (*Cable Communications Policy Act*), lagen om integritetsskydd för bilförare (*Driver's Privacy Protection Act*), lagen om elektronisk brevhemlighet (*Electronic Communications Privacy Act*), lagen om elektronisk överföring av pengar (*Electronic Funds Transfer Act*), lagen om rättvis kreditrapportering (*Fair Credit Reporting Act*), lagen Gramm-Leach-Bliley, lagen om integritetsskydd för finansiella uppgifter (*Right to Financial Privacy Act*), lagen om konsumentskydd för telefonabonnenter (*Telephone Consumer Protection Act*) och lagen om integritetsskydd i samband med videouthyrning (*Video Privacy Protection Act*). Många av delstaterna hade också motsvarande lagstiftning på dessa områden.

Mycket har hänt sedan 2000, både på federal och statlig nivå, som har medfört starkare skydd av konsumenternas integritet ([2]). På federal nivå t.ex. ändrade FTC COPPA-bestämmelsen 2013 i syfte att införa en rad förbättringar av skyddet av barns personuppgifter. FTC utfärdade också två regler för genomförande av lagen Gramm-Leach-Bliley – "Privacy Rule" och "Safeguards Rule" – som kräver att finansiella institutioner ([3]) lämnar ut information om sina metoder för informationsspridning och att de genomför ett omfattande program för informationssäkerhet för skydd av konsumentinformation. ([4]) På liknande sätt kompletterar lagen om rättvisa och korrekta kredittransaktioner (*Fair and Accurate Credit Transactions Act* – FACTA), som antogs 2003, gamla amerikanska kreditlagar i syfte att fastställa krav för maskering, delning och radering av vissa känsliga finansiella uppgifter. FTC utfärdade ett antal regler inom ramen för FACTA beträffande bl.a. konsumenternas rätt till en årlig kreditrapport utan kostnad, krav på säker radering avseende information om konsumentrapportering, konsumenters rätt att välja att inte få vissa kredit- och försäkringserbjudanden, konsumenters rätt att välja att information som tillhandahålls av ett anknutet företag inte får användas för marknadsföring av dess produkter och tjänster, samt krav för finansiella institutioner och kreditgivare att genomföra program för upptäckt och förebyggande av identitetsstöld. ([5]) Reglerna som utfärdats enligt lagen om rätt till sjukförsäkring och ersättning (*Health Insurance Portability and Accountability Act*) reviderades dessutom 2013, vilket skapade nya garantier om integritet och säkerhet för personuppgifter rörande hälsa. ([6]) Regler för att skydda konsumenter från oönskad telefonförsäljning, automatisk uppringning med uppspelning av inspelade meddelanden (robocalls) och skräppost har också trätt i kraft. Kongressen har också antagit lagar enligt vilka vissa företag som samlar in hälsorelaterad information ska meddela konsumenterna om en överträdelse sker ([7]).

Vissa stater har också varit mycket aktiva för att anta lagar om integritet och säkerhet. Sedan 2000 har 47 stater, Columbiadistriktet, Guam, Puerto Rico och Jungfruöarna antagit lagar enligt vilka företag ska meddela enskilda om brott

([1]) *Se* amerikanska handelsministeriets översikt över genomförandet av safe harbor, https://build.export.gov/main/safeharbor/eu/eg_main_018476.

([2]) För en mer omfattande sammanfattning av det rättsliga skyddet i Förenta staterna, se Daniel J. Solove & Paul Schwartz, *Information Privacy Law* (femte utgåvan 2015).

([3]) Finansiella institutioner har en mycket bred definition enligt lagen Gramm-Leach-Bliley, och omfattar alla företag som på ett avsevärt sätt är engagerade i verksamhet för tillhandahållande av finansiella produkter eller tjänster. Detta inbegriper t.ex. verksamhet för inlösen av checkar, snabblåneföretag, hypotekslånemäklare, långivare som inte är banker, värderingsmän för personlig eller fast egendom samt professionella skatterådgivare.

([4]) Med 2010 års lag om konsumentskydd på det finansiella området (*Consumer Financial Protection Act* – CFPA, Title X Pub. L. 111–203, 124 Stat. (1955, 21 juli 2010) (även kallad *Dodd-Frank Wall Street Reform and Consumer Protection Act*), överfördes den största delen av FTC:s regleringsbefogenheter enligt lagen Gramm-Leach-Bliley till byrån för skydd av konsumenternas finansiella intressen (*Consumer Financial Protection Bureau* – CFPB). FTC fortsätter att vara brottsbekämpande myndighet enligt lagen Gramm-Leach-Bliley samt regleringsmyndighet för *Safeguards Rule* och begränsad regleringsmyndighet enligt *Privacy Rule* när det gäller bilhandlare.

([5]) Enligt CFPA delar kommissionen sin brottsbekämpande roll enligt FCRA med CFPB, men regleringsbefogenheterna är till stor del överförda till CFPB (med undantag av reglerna för *Red Flags* och radering).

([6]) *Se* 45 C.F.R. punkterna 160, 162, 164.

([7]) *Se t.ex.* 2009 års *American Recovery & Reinvestment Act*, Pub. L. nr 111–5, 123 Stat. 115 (2009) och relevanta regler, 45 C.F.R. §§ 164.404–164.414; 16 C.F.R. punkt 318.

mot säkerheten för personuppgifter ([1]). Åtminstone 32 stater och Puerto Rico har lagar om radering av uppgifter, där krav fastställs för när personuppgifter ska förstöras eller raderas ([2]). Ett antal stater har också antagit generella lagar om datasäkerhet. Kalifornien har dessutom antagit olika integritetslagar, däribland en lag enligt vilken företag ska ha integritetspolicyer och offentliggöra sina metoder för icke-spårning (*Do Not Track*) ([3]), en lag kallad ”Shine the Light” som ålägger uppgiftsförmedlare större öppenhet och insyn ([4]), och en lag med krav på en ”raderingsknapp” så att minderåriga kan begära att viss information på sociala media raderas ([5]). Med hjälp av dessa lagar och av andra myndigheter har den federala regeringen och delstatsregeringarna ålagt företag som har brustit i skyddet av integritet och säkerhet med avseende på konsumenternas personuppgifter avsevärda böter ([6]).

Talan som väckts av privatpersoner har också lett till framgångsrika domar och uppgörelser som medfört bättre skydd av integriteten och datasäkerheten för konsumenterna. Under 2015 gick t.ex. Target med på att betala 10 miljoner US-dollar som en del av en uppgörelse med konsumenter som hävdade att deras finansiella personuppgifter hade riskerats genom en omfattande uppgiftsincident. 2013 gick AOL med på att betala 5 miljoner US-dollar i en uppgörelse för att lösa en grupptalan om påstådd oegentlig avidentifiering förknippad med att hundratusentals AOL-medlemmars sökningar lämnats ut. En federal domstol beslutade också att Netflix skulle betala 9 miljoner US-dollar för att ha bevarat historiska uthyrningsdata i strid mot 1988 års lag om integritetsskydd i samband med videouthyrning. Federala domstolar i Kalifornien godkände två separata uppgörelser med Facebook, en om ett belopp på 20 miljoner US-dollar och en annan om ett belopp på 9,5 miljoner US-dollar, rörande företagets insamling, användning och spridning av sina användares personuppgifter. En delstatsdomstol i Kalifornien godkände 2008 en uppgörelse om ett belopp på 20 miljoner US-dollar med LensCrafters efter att företaget olagligen röjt medicinska uppgifter om konsumenter.

I korthet, som denna sammanfattning visar säkerställer Förenta staterna ett omfattande rättsligt skydd av konsumenternas integritet och säkerhet. Den nya skölden för skydd av privatlivet, som innebär ett viktigt skydd för enskilda i EU, kommer att tillämpas mot bakgrund av detta bredare sammanhang där skyddet av konsumenternas integritet och säkerhet även i fortsättningen kommer att vara en viktig prioritering.

([1]) *Se t.ex. National Conference of State Legislatures* – NCSL), *State Security Breach Notification Laws* (4 januari 2016), http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx.

([2]) NCSL, *Data Disposal Laws* (12 januari 2016), se http://www.ncsl.org/research/telecommunications-and-information-technology/data-disposal-laws.aspx.

([3]) *Cal. Bus. & Professional Code* §§ 22575–22579.

([4]) *Cal. Civ. Code* §§ 1798.80–1798.84.

([5]) *Cal. Bus. & Professional Code* §§ 22580–22582.

([6]) *Se* Jay Cline, *U.S. Takes the Gold in Doling Out Privacy Fines*, Computerworld (17 februari, 2014), *Se* http://www.computerworld.com/s/article/9246393/Jay-Cline-U.S.-takes-the-gold-in-doling-out-privacy-fines?taxonomyId=17&pageNumber=1.

BILAGA V

Skrivelse från Anthony Foxx, Förenta staterna:s statssekreterare för transportfrågor

19 februari 2016

Kommissionsledamot Vera Jourová
Europeiska kommissionen
Rue de la Loi/Wetstraat 200
1049 Bryssel
BELGIEN

Ärende: Skölden för skydd av privatlivet i EU och Förenta staterna

Bästa kommissionär Jourová,

Förenta staternas transportministerium (*Department of Transportation*, nedan kallat *ministeriet* eller *DOT*) uppskattar denna möjlighet att beskriva sin roll i genomförandet av skölden för skydd av privatlivet i EU och Förenta staterna. Skölden spelar en avgörande roll för skyddet av personuppgifter som lämnas inom ramen för affärstransaktioner i en alltmer sammankopplad värld. Tack vare skölden kan företag bedriva omfattande verksamhet i den globala ekonomin, samtidigt som man säkerställer att EU-konsumenternas integritetsskydd förblir starkt.

Ministeriet gjorde ett offentligt åtagande om att genomföra safe harbor-programmet för första gången i en skrivelse till Europeiska kommissionen för över 15 år sedan. I den skrivelsen lovade ministeriet att noggrant genomföra safe harbor-principerna. Ministeriet håller fast vid detta åtagande och denna skrivelse formaliserar det åtagandet.

Ministeriet förnyar särskilt sitt åtagande inom följande centrala områden: 1) Prioritera utredningar av påstådda överträdelser av skölden om skydd för privatlivet, 2) vidta lämpliga verkställighetsåtgärder mot organisationer som gör falska eller bedrägliga utfästelser om att de är certifierade enligt skölden, och 3) övervaka och offentliggöra verkställighetsbeslut om överträdelser av skölden. Vi lämnar information om dessa åtaganden och lämpliga bakgrundsfakta om ministeriets roll i skyddet av konsumenternas integritet och genomförandet av skölden.

I. BAKGRUND

A. **Transportministeriets behörighet på integritetsskyddets område**

Ministeriet har ett starkt engagemang när det gäller att säkerställa integritetsskyddet för den information som konsumenter lämnar till flygbolag och biljettförsäljningskontor. Transportministeriets behörighet att vidta åtgärder på området stöds av artikel 49 i *United States Code* 41712, vilken förbjuder flygbolag och biljettförsäljningskontor att tillämpa illojala metoder eller bedrägligt beteende eller illojal konkurrens vid försäljning av lufttransporttjänster som skadar eller kan skada en konsument. Avsnitt 41 712 är utformat efter avsnitt 5 i *Federal Trade Commission Act* (15 U.S.C. 45). Vi tolkar denna lags bestämmelser om illojala eller bedrägliga metoder som att flygbolag eller biljettförsäljningskontor är förbjudna att 1) bryta mot villkoren i sin integritetsskyddspolicy, eller 2) att samla in eller lämna ut personuppgifter på ett sätt som strider mot allmän ordning, är omoraliskt eller orsakar konsumenten väsentlig skada som inte uppvägs av fördelar som konsumenten kan erhålla. Vi tolkar också avsnitt 41712 som ett förbud för flygbolag och biljettförsäljningskontor 1) att bryta mot regler som utfärdats av ministeriet som innebär att vissa förfaranden för integritetsskydd är illojala eller bedrägliga, eller 2) strider mot lagen om integritetsskydd för barn online (nedan kallad *COPP-lagen*) eller FTC:s regler som genomför COPP-lagen. Enligt federal lag har ministeriet exklusiv behörighet att reglera flygbolagens förfaranden för integritetsskydd, och den har delad behörighet med FTC när det gäller biljettförsäljningskontors förfaranden för integritetsskydd vid försäljning av flygbiljetter.

När ett flygbolag eller en försäljare av flygbiljetter offentligt förbinder sig att följa principerna för integritetsskydd enligt skölden för skydd av privatlivet har ministeriet därför rätt att använda sina lagstadgade befogenheter enligt avsnitt 41712 för att säkerställa överensstämmelse med dessa principer. Detta innebär i sin tur att när en passagerare lämnar information till ett flygbolag eller ett biljettförsäljningskontor som har förbundit sig att följa sköldens integritetsskyddsprinciper utgör bristande efterlevnad av detta åtagande från flygbolagets eller biljettförsäljningskontorets sida en överträdelse av avsnitt 41712.

B. **Metoder för verkställande**

Ministeriets tillsynsenhet för luftfart (*Aviation Enforcement and Proceeding*) utreder och väcker åtal i ärenden enligt 49 U.S. C. 4171 2. Tillsynsenheten verkställer det lagstadgade förbudet i avsnitt 41712 mot illojala och bedrägliga metoder, vilket främst sker via förhandlingar, förbereder förbud mot fortsatt verksamhet och utarbetar beslut om bedömningar av vite. Ministeriet får främst kännedom om eventuella överträdelser via klagomål som mottas från enskilda personer, resebyråer, flygbolag samt amerikanska och utländska myndigheter. Konsumenterna kan inge klagomål om integritetsskydd mot flygbolag och biljettförsäljningskontor via ministeriets webbplats ([1]).

Om en rimlig och lämplig lösning inte nås i ett ärende har tillsynsenheten för luftfart befogenhet att inleda verkställighetsförfaranden med en utfrågning för att samla in bevis inför en av ministeriets förvaltningsdomare. Domaren är behörig att utfärda förbud mot fortsatt verksamhet och vite. Överträdelser av avsnitt 41712 kan innebära ett förvaltningsbeslut som förbjuder dessa handlingar och vite på upp till 27 500 US-dollar för varje överträdelse av avsnitt 41 712.

Ministeriet har inte befogenhet att besluta om skadestånd eller ersättningsbelopp till enskilda klagande. Det har dock befogenhet att godkänna uppgörelser till följd av utredningar som genomförts av tillsynsenheten för luftfart som direkt gynnar konsumenterna (t.ex. kontanter, rabattkuponger) som en kvittning av böter som annars skulle betalats till den amerikanska regeringen. Ministeriet har gjort så tidigare och kommer att kunna göra så i samband med sköldens principer när det är befogat. Upprepade överträdelser av avsnitt 41 712 som något flygbolag begår kommer också att ifrågasätta flygbolagets ”compliance disposition” som i flagranta fall kan resultera i att flygbolaget inte längre kan anses ägnat att driva flygverksamhet och kunna förlora sitt tillstånd (economic operating authority).

Hittills har ministeriet dock mottagit relativt få klagomål om påstådda överträdelser av integritetsskyddet om begåtts av biljettförsäljningskontor eller flygbolag. Om sådana klagomål inkommer utreds de enligt de principer som anges ovan.

C. **Transportministeriets rättsliga skyddsmekanismer till förmån för konsumenter i EU**

Enligt avsnitt 41712 är förbudet mot illojala eller bedrägliga metoder vid lufttransport eller försäljning av flygbiljetter tillämpligt på både amerikanska och utländska flygbolag och biljettförsäljningskontor. Ministeriet vidtar ofta åtgärder mot amerikanska och utländska flygbolag med anledning av metoder som påverkar både utländska och amerikanska konsumenter om flygbolaget tillämpade metoden i fråga inom ramen för tillhandahållande av lufttransport till eller från Förenta staterna. Transportministeriet använder alla tillgängliga rättsmedel för att skydda både utländska och amerikanska konsumenter mot illojala eller bedrägliga metoder inom luftfarten som begås av reglerade enheter, och kommer så även att göra i framtiden.

När det gäller flygbolag upprätthåller ministeriet dessutom även andra riktade lagar som skyddar konsumenter utanför Förenta staterna, t.ex. COPP-lagen. Enligt denna lag krävs bland annat att operatörer av webbplatser och onlinetjänster som vänder sig till barn eller webbplatser med allmän publik som vet att de inhämtar personuppgifter från barn under 13 ska innehålla meddelanden till föräldrar och att föräldrarnas kontrollerbara samtycke ska inhämtas. Förenta staterna-baserade webbplatser och tjänster som omfattas av COPP-lagen och samlar in personuppgifter om utländska barn är skyldiga att följa lagen. Utrikesbaserade webbplatser och onlinetjänster måste också uppfylla lagen om de riktas till barn i Förenta staterna eller om de vet att de inhämtar personuppgifter från barn i Förenta staterna. Om amerikanska eller utländska flygbolag som bedriver verksamhet i Förenta staterna överträder COPP-lagen är ministeriet behörigt att vidta verkställighetsåtgärder.

II. GENOMFÖRANDET AV SKÖLDEN FÖR SKYDD AV PRIVATLIVET

Om ministeriet mottar klagomål om påstådda överträdelser rörande flygbolag eller biljettförsäljningskontor som har valt att delta i skölden kommer det att vidta följande åtgärder för att noggrant genomföra sköldens bestämmelser:

([1]) http://www.transportation.gov/airconsumer/privacy-complaints.

A. **Prioritera utredningar av påstådda överträdelser**

Tillsynsenheten för luftfart kommer att utreda varje klagomål om påstådda överträdelser av skölden (inklusive klagomål som mottas från dataskyddsmyndigheter i EU) och vidta verkställighetsåtgärder om det finns bevis för överträdelser. Tillsynsenheten kommer dessutom att samarbeta med FTC och handelsministeriet och prioritera utredningar av påståenden om att reglerade enheter inte följer de åtaganden om integritetsskydd som de gjort inom ramen för skölden.

När ministeriets tillsynsenhet mottar klagomål med påståenden om överträdelser av skölden kan den vidta en rad olika åtgärder inom ramen för sin utredning. Tillsynsenheten kan t.ex. granska biljettförsäljningskontorets eller flygbolagets policy för integritetsskydd, inhämta information från dem eller från tredje parter, följa upp ärendet med den hänskjutande myndigheten och bedöma om det finns ett mönster av överträdelser eller om ett avsevärt antal konsumenter påverkas. Dessutom kommer den att fastställa om ärendet rör frågor som hör till handelsministeriets eller FTC:s behörighetsområden, bedöma om upplysningskampanjer riktade till konsumenter och företag skulle vara användbara samt i förekommande fall inleda verkställighetsförfaranden.

Om ministeriet får kännedom om eventuella överträdelser av skölden som begås av biljettförsäljningskontor kommer det att samordna sina åtgärder i ärendet med FTC. Vi kommer också informera FTC och handelsministeriet om resultatet av eventuella verkställighetsåtgärder i fråga om skölden.

B. **Hantera falska eller bedrägliga påståenden om medlemskap i skölden för skydd av privatlivet**

Ministeriet vidhåller sitt åtagande att utreda överträdelser av sköldens bestämmelser, inklusive falska eller bedrägliga påståenden om medlemskap i programmet. Vi kommer att prioritera hänskjutanden från handelsministeriet som rör fall där ministeriet har konstaterat att organisationer påstår att de är medlemmar i skölden eller använder sköldens certifieringsmärkning utan tillstånd.

Vi konstaterar dessutom att om en organisation i sin integritetsskyddspolicy utlovar att den följer sköldens väsentliga principer och inte registrerar sig eller omregistrerar sig hos handelsministeriet kommer detta sannolikt inte i sig själv att undanta organisationen från verkställighetsåtgärder från transportministeriets sida för att genomdriva dessa åtaganden.

C. **Övervakning samt offentliggörande av verkställighetsbeslut angående överträdelser av bestämmelserna för skölden för skydd av privatlivet**

Ministeriets tillsynsenhet för luftfart vidhåller även sitt åtagande att vid behov övervaka verkställighetsbeslut för att säkerställa efterlevnad av skölden för skydd av privatlivet. Om tillsynsenheten utfärdar ett beslut om att ett flygbolag eller biljettförsäljningskontor i framtiden ska upphöra med och avstå från överträdelser av skölden för skydd av privatlivet samt av avsnitt 41712, kommer den att övervaka enhetens efterlevnad av bestämmelsen om upphörande och avstående i beslutet. Tillsynsenheten kommer dessutom att se till att beslut i ärenden som rör skölden finns tillgängliga på dess webbplats.

Vi ser fram emot ett fortsatt samarbete med våra federala partner och EU-aktörer i frågor som rör skölden för skydd av privatlivet.

Jag hoppas denna information är till nytta för er. Har ni frågor eller behöver ytterligare information står jag till ert förfogande.

Högaktningsfullt,

Anthony R. Foxx

Transportminister

BILAGA VI

Skrivelse från chefsjurist Robert Litt
Office of the Director of National Intelligence

22 februari 2016

Justin S. Antonipillai
Jurist
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Biträdande minister
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Bäste herr Antonipillai och herr Dean,

Under de senaste två och ett halvt åren har Förenta staterna inom ramen för förhandlingarna om skölden för skydd av privatlivet i EU och Förenta staterna lämnat utförlig information om hur den amerikanska underrättelsegemenskapens signalspaningsverksamhet fungerar. Informationen rör bland annat gällande regelverk, tillsyn på flera nivåer av signalspaningsverksamheten, den omfattande insynen i dessa verksamheter och det övergripande skyddet av integriteten och de medborgerliga fri- och rättigheterna, och syftet är att hjälpa Europeiska kommissionen att avgöra om dessa skyddsmekanismer är adekvata, eftersom de rör undantaget för nationell säkerhet i sköldens principer. Detta dokument utgör en sammanfattning av den information som har lämnats.

I. PPD-28 OCH GENOMFÖRANDET AV DEN AMERIKANSKA SIGNALSPANINGSVERKSAMHETEN

Den amerikanska underrättelsegemenskapen samlar in utländska underrättelseuppgifter på ett noggrant kontrollerat sätt och i strikt efterlevnad av amerikanska lagar. Verksamheten är föremål för tillsyn på flera nivåer, som inriktas på viktiga utländska och nationella säkerhetsprioriteringar. Den amerikanska underrättelsetjänstens insamling av underrättelseuppgifter styrs av en mosaik av lagar och politiska direktiv, inklusive den amerikanska konstitutionen, lagen om underrättelseverksamhet och övervakning utomlands (50 U.S.C. § 1801 och följande artiklar) (*Foreign Intelligence Surveillance Act*, nedan kallad *FISA*), dekret 12333 och dess genomförandeförfaranden, presidentdirektiv och ett stort antal förfaranden och riktlinjer som godkänts av FISA-domstolen och justitieministern, och som fastställer ytterligare regler som begränsar insamling, lagring, användning och spridning av utländska underrättelseuppgifter ([1]).

a. **Översikt av PPD 28**

I januari 2014 höll president Barack Obama ett tal där han beskrev ett antal reformer av Förenta staterna:s signalspaningsverksamhet. Presidenten utfärdade också *Presidential Policy Directive 28* (nedan kallat *PPD-28*) rörande dessa verksamheter ([2]). Presidenten betonade att den amerikanska signalspaningsverksamheten inte bara bidrar till att skydda vårt land och våra friheter, utan även andra länders säkerhet och friheter, även EU-medlemsstaterna, som använder information som inhämtas av de amerikanska underrättelsetjänsterna för att skydda sina egna medborgare.

I PPD-28 anges en uppsättning principer och krav som gäller för all amerikansk signalspaningsverksamhet och för alla personer, oavsett nationalitet eller plats. Lagen innehåller i synnerhet vissa krav på förfaranden förinsamling, lagring och spridning av personuppgifter om personer som inte är amerikanska medborgare och som inhämtats inom ramen för Förenta staterna:s signalspaningsverksamhet. Dessa krav anges närmare nedan, men i en sammanfattning.

— I PPD-28 upprepas att Förenta staterna:s uppgiftsinsamling via signalspaning endast sker enligt de metoder som godkänns i lagstiftning, dekret eller andra presidentdirektiv.

([1]) Ytterligare information om Förenta staterna:s utländska underrättelseverksamhet har lagts ut på nätet och finns tillgänglig för allmänheten via ODNI:s offentliga webbplats *IC On the Record* (www.icontherecord.tumblr.com) som syftar till att främja ökad insyn för allmänheten i regeringens underrättelseverksamhet.
([2]) *Se* https://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities.

— I PPD-28 fastställs förfaranden för att säkerställa att signalspaningsverksamhet endast genomförs för att främja legitima och godkända nationella säkerhetsändamål.

— Lagen kräver också att integritetsskydd och medborgerliga friheter ska integreras i planeringen av insamling av uppgifter via signalspaning. Förenta staterna samlar inte in underrättelseuppgifter för att undertrycka eller bestraffa kritik eller avvikande åsikter, för att skada personer på grundval av etniskt ursprung, ras, kön, sexuell läggning eller religion, eller för att ge amerikanska företag och amerikanska affärssektorer kommersiella konkurrensfördelar.

— Enligt PPD-28 ska uppgiftsinsamling via signalspaning anpassas till ändamålet och signalspaningsuppgifter som samlas in i bulk får endast användas för särskilt angivna ändamål.

— Lagen föreskriver dessutom att underrättelsegemenskapen ska införa förfaranden som är ”skäligen utformade för att minimera spridning och lagring av personuppgifter som samlats in via signalspaningsverksamheter”. Vissa skyddsmekanismer som gäller för amerikanska medborgares personuppgifter utsträcks även till att omfatta personuppgifter för medborgare i andra länder.

— Myndighetens förfaranden för att genomföra PPD-28 har antagits och offentliggjorts.

Det står klar att de förfaranden och skyddsmekanismer som anges i detta dokument är tillämpliga på skölden för skydd av privatlivet. När uppgifter överförs till företag i Förenta staterna enligt skölden, i själva verket på alla sätt, kan de amerikanska underrättelsetjänsterna endast ansöka om att få tillgång till dessa uppgifter om begäran uppfyller FISA eller görs enligt en av de lagstadgade bestämmelserna i *National Security Letter*, som diskuteras nedan ([1]). Utan att varken bekräfta eller förneka medierapporter om påståenden om att den amerikanska underrättelsegemenskapen samlar in uppgifter från transatlantiska kabelanslutningar medan uppgifterna överförs till Förenta staterna vill vi förklara följande: om den amerikanska underrättelsegemenskapen skulle samla in uppgifter från transatlantiska kabelanslutningar skulle den göra detta enligt de begränsningar och garantier som anges häri, inklusive kraven i PPD-28.

b. **Begränsningar av insamlingen**

I PPD-28 fastställs ett antal viktiga allmänna principer som reglerar insamlingen av uppgifter via signalspaning:

— Insamling av uppgifter via signalspaning måste vara godkänd enligt lag eller ske med presidentens tillstånd, och måste genomföras i enlighet med konstitutionen och lagstiftningen.

— Integritetsskyddet och de medborgerliga fri- och rättigheterna måste vara integrerade överväganden i planeringen av signalspaningsverksamhet.

— Signalspaningsuppgifter samlas endast in när det finns ett giltigt ändamål som rör utländska underrättelser eller kontraspionage.

— Förenta staterna samlar inte in signalspaningsuppgifter för att undertrycka eller bestraffa kritik och avvikande åsikter.

— Förenta staterna samlar inte signalspaningsuppgifter för att skada personer på grundval av etniskt ursprung, ras, kön, sexuell läggning eller religion.

— Förenta staterna samlar inte signalspaningsuppgifter för att ge amerikanska företag och amerikanska affärssektorer kommersiella konkurrensfördelar.

— Förenta staterna:s signalspaningsverksamhet måste *alltid* anpassas till ändamålet, med hänsyn till tillgången till andra informationskällor. Detta innebär bland annat att insamling av uppgifter via signalspaning när så är möjligt sker på ett riktat sätt, dvs. uppgifterna samlas inte in i bulk.

Kravet att signalspaningsverksamheten ska ”anpassas till ändamålet” rör metoderna för att samla in signalspaningsuppgifter samt vilka uppgifter som faktiskt samlas in. När underrättelsegemenskapen avgör om signalspaningsuppgifter

([1]) Brottsbekämpande myndigheter eller tillsynsmyndigheter kan begära information från företag för utredningsändamål i Förenta staterna enligt bestämmelser som gäller för andra straff- och civilrättsliga myndigheter och tillsynsmyndigheter som inte omfattas av denna skrivelse, som begränsas till myndigheter med ansvar för den nationella säkerheten.

bör samlas in måste den t.ex. överväga om andra informationskällor finns tillgängliga, inklusive diplomatiska eller offentliga källor, och prioritera insamling via dessa kanaler, när så är lämpligt och möjligt. Underrättelsegemenskapens policyer bör dessutom kräva att insamlingen när så är möjligt bör inriktas på specifika utländska underrättelsemål eller frågor genom användning av urvalsfaktorer (t.ex. specifika anläggningar, urvalstermer och identifierare).

Det är viktigt att se den information som lämnas till kommissionen i ett helhetsperspektiv. Besluten om vad som är ”möjligt” eller ”genomförbart” lämnas inte till enskilda personers godtycke, utan är föremål för de policyer som underrättelsetjänsterna har utfärdat enligt PPD-28 – som har offentliggjorts – och de andra processer som beskrivs där ([1]). Såsom anges i PPD-28 utgör uppgiftsinsamling via signalspaning insamling som ”på grund av tekniska eller operativa överväganden” sker utan användning av urvalsfaktorer (t.ex. särskilda identifierare, urvalstermer osv.) I detta avseende bekräftas i PPD-28 att underrättelsegemenskapens organisationer måste samla in signalspaningsuppgifter i bulk under vissa omständigheter för att identifiera nya eller framväxande hot och annan mycket viktig säkerhetsinformation som ofta är dold i det stora och komplexa globala kommunikationssystemet. Lagen bekräftar även att insamling av uppgifter via signalspaning i bulk väcker farhågor rörande integritetsskydd och medborgerliga friheter. Enligt PPD-28 ska därför underrättelsegemenskapen prioritera alternativ som möjliggör riktad signalspaning i stället för insamling av uppgifter i bulk. Underrättelsegemenskapens organisationer bör därför genomföra riktad signalspaningsverksamhet i stället för att samla in uppgifter i bulk när så är möjligt ([2]). Dessa principer garanterar att undantaget för insamling i bulk inte får företräde framför den allmänna regeln.

När det gäller begreppet ”skälighet” är det en grundsten i amerikansk lagstiftning. Det innebär att underrättelsegemenskapens organisationer inte ska vidta teoretiskt möjliga åtgärder, utan i stället ska balansera insatserna när det gäller att skydda legitima intressen rörande integritetsskydd och medborgerliga friheter med signalspaningsverksamhetens praktiska behov. Även här har byråernas policyer offentliggjorts och visar att begreppet ”skäligt utformad för att minimera spridning och lagring av personuppgifter” inte undergräver den allmänna regeln.

PPD-28 föreskriver även att signalspaningsuppgifter som samlas in i bulk får användas för sex särskilda ändamål: upptäcka och motverka vissa utländska makters aktiviteter, terrorismbekämpning, åtgärder för att motverka masspridning, it-säkerhet, upptäcka och motverka hot mot Förenta staterna:s eller allierade makters arméer och bekämpa transnationella kriminella hot, inklusive kringgående av sanktioner. Presidentens nationella säkerhetsrådgivare kommer i samarbete med direktören för den nationella underrättelseverksamheten (*Director for National Intelligence*) att se över dessa tillåtna användningsområden för signalspaningsuppgifter som samlas in i bulk för att se om de behöver ändras. DNI kommer att göra denna förteckning allmänt tillgänglig i största möjliga utsträckning med tanke på den nationella säkerheten. Detta utgör en viktig och öppen begränsning av möjligheten att samla in signalspaningsuppgifter i bulk.

De organisationer inom underrättelsegemenskapen som genomför PPD-28 har dessutom förstärkt befintliga analysmetoder och normer för att granska signalspaning som inte tidigare utvärderats ([3]). Analytikerna måste omstrukturera sina frågor eller använda andra söktermer eller söktekniker för att säkerställa att de är lämpliga för att identifiera underrättelseinformation som är relevant för en tillåten utländsk underrättelseverksamhet eller brottsbekämpande verksamhet. I detta syfte måste underrättelsegemenskapens organisationer inrikta sina personundersökningar på de kategorier av signalspaningsinformation som motsvarar lagkrav i fråga om utländska underrättelseuppgifter eller brottsbekämpande verksamheter, för att undvika att personuppgifter används för andra verksamhetstyper än de tillåtna verksamheterna.

Det är viktigt att betona att all insamling i bulk av internetkommunikation som den amerikanska underrättelsegemenskapen utför genom signalspaning bedrivs inom en liten del av internet. Genom att använda riktade frågor enligt beskrivningen ovan säkerställer man dessutom att endast de uppgifter som anses ha ett eventuellt värde som underrättelseuppgifter undersöks av analytikerna. Syftet med dessa begränsningar är att skydda alla personers integritet och medborgerliga friheter, oavsett nationalitet och bostadsort.

([1]) *Se* www.icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties#ppd-28. Genom dessa förfaranden genomförs de koncept för målinriktning och anpassning som diskuteras i denna skrivelse på ett särskilt sätt för varje organisation inom underrättelsegemenskapen.

([2]) För att nämna ett exempel anges i NSA:s genomförandeförfaranden för PPD-28 att ”när så är möjligt ska insamling ske genom ett eller flera urvalstermer så att den inriktas på specifika utländska underrättelsemål (t.ex. en viss känd internationell terrorist eller terroristgrupp) eller specifika utländska underrättelsefrågor (t.ex. spridning av massförstörelsevapen av en utländsk makt eller dess ombud).”

([3]) *Se* http://www.dni.gov/files/documents/1017/PPD-28_Status_Report_Oct_2014.pdf.

Förenta staterna har detaljerade förfaranden för att se till att signalspaningsverksamhet endast används för att främja den nationella säkerheten. Varje år fastställer presidenten nationens främsta prioriteringar för insamling av utländska underrättelseuppgifter på grundval av ett omfattande formellt förfarande mellan berörda myndigheter. DNI ansvarar för att omsätta dessa prioriteringar för underrättelseverksamheten i ”prioriteringsramen för nationell underrättelseverksamhet (*National Intelligence Priorities Framework*), eller NIPF. Detta förfarande mellan berörda ministerier har förstärkts genom PPD-28 för att säkerställa att alla underrättelseprioriteringar som underrättelsegemenskapen har ställt upp granskas och godkänns av politiska beslutsfattare på hög nivå. Underrättelsegemenskapens direktiv 204 (nedan kallat *ICD*) ger ytterligare vägledning om NIPF och uppdaterades i januari 2015 för att inbegripa kraven i PPD-28 ([1]). Även om NIPF är sekretessbelagd offentliggörs information om specifika amerikanska prioriteringar för utländska underrättelseuppgifter varje år i DNI:s offentliga *Worldwide Threat Assessment*, som även finns tillgänglig på ODNI:s webbplats.

NIPF:s prioriteringar är relativt allmänt hållna. De omfattar frågor som kontroll av utländska motståndares kärntekniska och ballistiska robotkapacitet, effekter av korruption inom ramen för drogkarteller och människorättsliga överträdelser i vissa länder. De gäller inte bara för signalspaning, utan för all underrättelseverksamhet. Den organisation som ansvarar för att omsätta NIPF:s prioriteringar i insamling av signalspaningsuppgifter i praktiken benämns *National Signals Intelligence Committee*, eller SIGCOM. SIGCOM arbetar under ledning av direktören för NSA, som genom dekret 12333 utses som ”funktionell chef för signalspaning”, med ansvar för att övervaka och samordna underrättelsegemenskapens signalspaningsverksamhet, och står i sin tur under översyn av både försvarsministern och DNI. SIGCOM består av företrädare för alla tjänster inom underrättelsegemenskapen. När Förenta staterna fullständigt genomför PPD-28 kommer även andra ministerier och myndigheter med politiskt intresse av signalspaning vara fullständigt representerade i SIGCOM.

Alla amerikanska ministerier och myndigheter som använder utländska underrättelseuppgifter kan lämna förfrågningar om insamling till SIGCOM. SIGCOM granskar dessa förfrågningar, kontrollerar att de är förenliga med NIPF och tilldelar dem en prioritetsnivå med hjälp av t.ex. följande kriterier:

— Kan signalspaning ge värdefull information i detta fall eller finns det bättre eller mer kostnadseffektiva informationskällor för att tillgodose behovet, t.ex. bilder eller information från öppna källor?

— Hur viktigt är detta informationsbehov? Om förfrågningen prioriteras högt av NIPF blir den ofta en viktig signalspaningsprioritering.

— Vilken typ av signalspaning kan användas?

— Är insamlingen så anpassad som möjligt? Bör det finnas tidsbegränsningar, geografiska begränsningar eller andra begränsningar?

De amerikanska signalspaningsbestämmelserna kräver även uttryckligt övervägande av andra faktorer, nämligen följande:

— Är målet för insamlingen eller den använda insamlingsmetoden särskilt känsliga? Om så är fallet krävs en bedömning av höga beslutsfattare.

— Kommer insamlingen att medföra en omotiverad risk för integritetsskyddet och de medborgerliga fri- och rättigheterna, oavsett nationalitet?

— Krävs ytterligare garantier för spridning och lagring för att skydda integriteten eller nationella säkerhetsintressen?

I slutet av processen använder utbildad NSA-personal de prioriteringar som godkänts av SIGCOM för att undersöka och fastställa särskilda urvalstermer, t.ex. telefonnummer eller e-postadresser, som förväntas bidra till att samla in utländska underrättelseuppgifter som tillgodoser dessa prioriteringar. Alla urvalstermer måste granskas och godkännas innan de förs in i NSA:s insamlingssystem. Om och när insamlingen genomförs beror även delvis på ytterligare överväganden,

([1]) Se http://www.dni.gov/files/documents/ICD/ICD%20204%20National%20Intelligence%20Priorities%20Framework.pdf.

såsom tillgång till tillräckliga insamlingsresurser. Denna process säkerställer att målen för den amerikanska signalspaningsinsamlingen avspeglar giltiga och viktiga behov av utländska underrättelseuppgifter. När insamlingen väl sker enligt FISA, NSA och andra myndigheter gäller dessutom ytterligare begränsningar som godkänts av domstolen för övervakning av utländsk underrättelseinformation (*Foreign Intelligence Surveillance Court*). Kort sagt kan varken NSA eller någon annan amerikansk underrättelsetjänst på egen hand bestämma vilka uppgifter de ska samla in.

Sammantaget säkerställer denna process att alla amerikanska underrättelseprioriteringar fastställs av höga beslutsfattare som är bäst lämpade att fastställa Förenta staterna:s behov av utländska underrättelseuppgifter, och att beslutsfattarna inte bara beaktar det eventuella värdet av insamlingen, utan även de risker som är förknippade med denna, inklusive risker för integritetsskyddet, nationella ekonomiska intressen och utländska förbindelser.

När det gäller uppgifter som överförs till Förenta staterna enligt skölden för skydd av privatlivet, och trots att Förenta staterna varken kan bekräfta eller förneka användningen av särskilda underrättelsemetoder eller operationer, gäller kraven i PPD-28 för all signalspaningsverksamhet som utförs av Förenta staterna, oavsett typ av insamlade uppgifter eller vilken källa de kommer från. De begränsningar och garantier som gäller för insamling av uppgifter genom signalspaning gäller dessutom för signalspaningsuppgifter som samlas in för alla godkända ändamål, vilket omfattar både utländska förbindelser och nationella säkerhetssyften.

De förfaranden som beskrivs ovan visar ett tydligt åtagande att förhindra godtycklig och slumpartad insamling av signalspaningsuppgifter och att genomföra principen om skälighet – från högsta regeringsnivå. Genomförandeförfarandena enligt PPD-28 och ministeriets förfaranden klargör nya och befintliga begränsningar av och beskriver mer detaljerat för vilka ändamål Förenta staterna samlar in och använder signalspaningsuppgifter. Syftet med dessa förfaranden är att garantera att signalspaningsverksamheten även i fortsättningen endast kommer att genomföras för att främja legitima mål för insamling av utländska underrättelseuppgifter.

c. **Begränsningar av lagring och spridning av uppgifter**

Enligt avsnitt 4 i PPD-28 ska uttryckliga begränsningar gälla för alla tjänster inom underrättelsegemenskapen när det gäller lagring och spridning av personuppgifter för personer som inte är amerikanska medborgare och som samlas in genom signalspaning. Begränsningarna är jämförbara med de som gäller för amerikanska medborgare. Dessa regler har inbegripits i varje underrättelsetjänsts förfaranden. De offentliggjordes i februari 2015 och finns allmänt tillgängliga. För att kunna lagra och sprida personuppgifter i form av utländska underrättelseuppgifter måste informationen röra ett godkänt underrättelsekrav, vilket fastställs i den NIPF-process som beskrivs ovan, skäligen kunna anses utgöra bevis på ett brott, eller uppfylla någon av de andra reglerna för lagring av amerikanska personuppgifter enligt avsnitt 2.3 i dekret 12333.

Information som inte omfattas av sådana krav får lagras i högst fem år, om inte DNI uttryckligen fastställer att fortsatt lagring är i Förenta staterna:s nationella säkerhetsintresse. Underrättelsegemenskapens organisationer måste således radera personuppgifter för personer som inte är amerikanska medborgare och som har samlats in genom signalspaning fem år efter insamlingen om inte informationen t.ex. bedöms vara relevant för ett godkänt krav rörande utländska underrättelseuppgifter eller om DNI, efter att ha övervägt vad ODNI:s *Civil Liberties Protection Officer* och andra myndigheters tjänstemän med ansvar för integritetsskydd och medborgerliga friheter anser, fastställer att fortsatt lagring är ett nationellt säkerhetsintresse.

Dessutom innehåller nu alla myndigheters policyer för genomförandet av PPD-28 ett uttryckligt krav om att information om en person inte får spridas bara för att personen inte är amerikansk medborgare, och ODNI har utfärdat ett direktiv till alla organisationer i underrättelsegemenskapen ([1]) om detta krav. Underrättelsegemenskapens personal är uttryckligen skyldiga att överväga integritetsintressen för personer som inte är EU-medborgare när de utarbetar och förmedlar underrättelserapporter. Signalspaning som riktas mot en utländsk persons rutinmässiga aktiviteter anses inte utgöra utländska underrättelseuppgifter som kan spridas eller lagras permanent endast på grundval av detta faktum, om spaningen inte på annat sätt motsvarar ett godkänt krav rörande utländska underrättelseuppgifter. Detta innebär en viktig begränsning till svar på Europeiska kommissionens farhågor om den breda definitionen av utländska underrättelseuppgifter i dekret 12333.

([1]) Intelligence Community Directive (ICD) 203, se http://www.dni.gov/files/documents/ICD/ICD%20203%20Analytic%20Standards.pdf.

d. **Efterlevnad och tillsyn**

Det amerikanska systemet för övervakning av utländska underrättelseuppgifter omfattas av ett strikt tillsynssystem med flera nivåer för att säkerställa efterlevnad av tillämpliga lagar och förfaranden, bland annat för insamling, lagring och spridning av personuppgifter för personer som inte är amerikanska medborgare och som samlats in genom signalspaning enligt PPD-28. Följande aspekter är relevanta i detta sammanhang:

— Underrättelsegemenskapen sysselsätter tusentals personer som arbetar med tillsynsuppgifter. Bara NSA har över 300 anställda som arbetar med efterlevnadsuppgifter, och andra underrättelsetjänster har också tillsynskontor. Justitieministeriet utövar dessutom en omfattande tillsyn av underrättelseverksamheten och även försvarsministeriet arbetar med tillsyn.

— Varje del av underrättelsegemenskapen har sitt eget generalinspektörskontor, som bland annat ansvarar för övervakning av utländsk underrättelseverksamhet. Generalinspektörerna är lagstadgat oberoende, har omfattande befogenheter att utföra utredningar, revisioner och granskningar av program, även rörande bedrägeri och missbruk eller överträdelser av lagstiftningen, och kan rekommendera korrigerande åtgärder. Generalinspektörens rekommendationer är visserligen inte bindande, men rapporter offentliggörs ofta, och lämnas i alla händelser till kongressen. Detta omfattar uppföljningsrapporter om korrigerande åtgärder som rekommenderats i tidigare rapporter men som ännu inte vidtagits. Kongressen informeras således om eventuell bristande efterlevnad och kan utöva påtryckningar, även genom budgetmedel, för att uppnå korrigerande åtgärder. Ett antal rapporter från generalinspektörer om underrättelseprogram har offentliggjorts ([1]).

— ODNI:s *Civil Liberties and Privacy Office* (CLPO) har ansvar för att säkerställa att underrättelsegemenskapen fungerar på ett sätt som främjar den nationella säkerheten, samtidigt som de medborgerliga fri- och rättigheterna och integritetsskyddet främjas ([2]). Andra organisationer i underrättelsegemenskapen har egna tjänstemän med ansvar för integritetsskydd.

— Styrelsen för tillsyn av personlig integritet och medborgerliga fri- och rättigheter (*Privacy and Civil Liberties Oversight Board*, PCLOB), ett oberoende lagstadgat organ, ansvarar för att analysera och granska program och policyer för terrorismbekämpning, inbegripet användning av signalspaning, för att se till att integriteten och de medborgerliga fri- och rättigheterna skyddas på lämpligt sätt. Styrelsen har utfärdat flera offentliga rapporter om underrättelseverksamhet.

— Såsom diskuteras närmare nedan är domstolen för övervakning av utländsk underrättelseinformation, en domstol som består av oberoende federala domare, ansvarig för tillsyn och efterlevnad när det gäller insamling av uppgifter genom signalspaning som genomförs enligt FISA.

— Slutligen har kongressen, särskilt representanthusets och senatens kommittéer för underrättelseverksamhet respektive domstolsväsendet, omfattande tillsynsansvar när det gäller all amerikansk underrättelseverksamhet, inbegripet Förenta staterna:s signalspaning.

Förutom dessa formella tillsynsmekanismer har underrättelsegemenskapen infört ett antal mekanismer för att säkerställa att den uppfyller begränsningarna av insamling enligt ovan. Detta gäller t.ex. följande:

— Tjänstemännen är skyldiga att validera signalspaningsbehoven varje år.

— NSA kontrollerar signalspaningsmålen under insamlingsprocessen för att fastställa om signalspaningen faktiskt ger värdefulla utländska underrättelseuppgifter som motsvarar prioriteringarna, och stoppar insamlingen om målen inte uppfylls. Ytterligare förfaranden säkerställer regelbundna granskningar av urvalstermerna.

([1]) *Se t.ex.* rapporten från justitieministeriets generalinspektör *A Review of the Federal Bureau of Investigation's Activities Under Section 702 of the Foreign Intelligence Surveillance Act of 2008* (september 2012),https://oig.justice.gov/reports/2016/o1601a.pdf.

([2]) Se www.dni.gov/clpo.

— På grundval av en rekommendation från en oberoende granskningsgrupp som utsetts av president Barack Obama har DNI inrättat en ny mekanism för att övervaka insamlingen och spridningen av signalspaningsuppgifter som är särskilt känsliga på grund av målets karaktär eller använd insamlingsmetod. Syftet är att se till att insamlingen och spridningen överensstämmer med beslutsfattarnas avgöranden.

— Slutligen genomför ODNI årliga granskningar av underrättelsegemenskapens resursfördelning mot NIPF:s prioriteringar och underrättelseuppdraget i helhet. Granskningen omfattar bedömningar av värdet av alla typer av insamling av underrättelseuppgifter, inklusive signalspaning, och man undersöker både bakåt – hur framgångsrik har underrättelsegemenskapen varit när det gäller att uppnå målen? – och framåt – vad krävs i framtiden? På så sätt säkerställs att signalspaningsresurserna används för de viktigaste nationella prioriteringarna.

Såsom framgår av denna omfattande översikt beslutar inte underrättelsegemenskapen på egen hand om vilka samtal den ska lyssna till, försöker inte samla in allt och arbetar inte utan kontroll. Verksamheten inriktas på prioriteringar som fastställs av beslutsfattare genom en process som regeringen är delaktig i, och kontrolleras av NSA och ODNI, justitieministeriet och försvarsministeriet.

PPD-28 innehåller också många andra bestämmelser för att säkerställa att personuppgifter som samlas in genom signalspaning skyddas, oavsett nationalitet. PPD-28 föreskriver t.ex. datasäkerhet, tillgång och kvalitetssäkringsförfaranden för att skydda personuppgifter som samlas in genom signalspaning samt obligatorisk utbildning för att se till att personalen förstår sitt ansvar att skydda personuppgifter, oavsett nationalitet. Lagen föreskriver dessutom ytterligare tillsyns- och efterlevnadsmekanismer. Det handlar bland annat om regelbundna revisioner och granskningar av metoderna för att skydda personuppgifter som ingår i signalspaningsuppgifter, som utförs av tjänstemän med ansvar för tillsyns- och efterlevnadsfrågor. Dessutom granskas myndigheternas efterlevnad av förfarandena för att skydda sådan information.

PPD-28 föreskriver dessutom att viktiga efterlevnadsfrågor som berör personer som inte är amerikanska medborgare behandlas på hög regeringsnivå. Om ett allvarligt efterlevnadsproblem uppstår som omfattar personuppgifter som samlats in genom signalspaning måste detta problem, förutom eventuella ytterligare rapporteringskrav, omedelbart rapporteras till DNI. Om det rör sig om personuppgifter för en person som inte är amerikansk medborgare kommer DNI i samråd med utrikesministern och chefen för den relevanta organisationen inom underrättelsegemenskapen att avgöra om det är nödvändigt att vidta åtgärder för att meddela den berörda utländska regeringen i enlighet med källskyddet samt skyddet av metoder och amerikansk personal. Enligt PPD-28 har utrikesministern dessutom utsett en högt uppsatt tjänsteman, statssekreterare Catherine Novelli, som kontaktperson för utländska regeringar som har frågor om Förenta staterna:s signalspaningsverksamhet. Detta engagemang på hög nivå är ett exempel på den amerikanska regeringens ansträngningar under de senaste åren för att skapa förtroende för de olika överlappande bestämmelserna om integritetsskydd som finns både för amerikanska och utländska medborgare.

e. **Sammanfattning**

Förenta staterna:s förfaranden för att samla in, lagra och sprida utländska underrättelseuppgifter omfattas av ett starkt integritetsskydd för alla personuppgifter, oavsett personens nationalitet. Dessa processer säkerställer särskilt att vår underrättelsegemenskap inriktar sig på sitt nationella säkerhetsuppdrag enligt tillämpliga lagar, dekret och presidentdirektiv och skyddar information från otillåten åtkomst,användning och utlämnande. Verksamheten är föremål för granskning och tillsyn på flera nivåer, bland annat av kongressens tillsynskommittéer. PPD-28 och dess genomförandeförfaranden representerar våra ansträngningar för att utvidga vissa minimeringsprinciper och andra viktiga dataskyddsprinciper till att omfatta alla personuppgifter, oavsett personens nationalitet. Personuppgifter somsamlas in genom Förenta staterna:s signalspaning omfattas av principerna och kraven i den amerikanska lagstiftningen och presidentdekret, inbegripet de skyddsmekanismer som anges i PPD-28. Dessa principer och krav säkerställer att alla människor behandlas med värdighet och respekt, oavsett nationalitet och bostadsort, och erkänner att alla personer har legitima integritetsintressen när det gäller behandlingen av deras personuppgifter.

II. LAGEN OM UNDERRÄTTELSEVERKSAMHET OCH ÖVERVAKNING UTOMLANDS – AVSNITT 702

Insamling enligt avsnitt 702 i lagen om underrättelseverksamhet och övervakning utomlands ([1]) är inte ”slumpartad massinsamling”, utan är snävt inriktad på insamling av utländska underrättelseuppgifter om individuellt identifierade legitima mål, är uttryckligen godkänd av lagstadgade myndigheter och är föremål för både oberoende rättslig tillsyn och noggrann granskning och tillsyn inom den verkställande makten och kongressen. Insamling enligt avsnitt 702 anses utgöra signalspaning som omfattas av kraven i PPD-28 ([2]).

Insamling enligt avsnitt 702 är en av de mest värdefulla underrättelsekällorna, och skyddar både Förenta staterna och våra europeiska partner. Omfattande information om genomförandet och tillsynen av avsnitt 702 finns allmänt tillgänglig. Sekretessen för många rättsliga yrkanden, domstolsbeslut och tillsynsrapporter rörande programmet har hävts och lagts ut på ODNI:s webbplats för offentliggörande, www.icontherecord.tumblr.com. Avsnitt 702 har dessutom analyserats grundligt av styrelsen för tillsyn av personlig integritet och medborgerliga fri- och rättigheter (PCLOB) i en rapport som finns på https://www.pclob.gov/library/702-Report.pdf ([3]).

Avsnitt 702 antogs som en del av FISA-ändringsakten från 2008 ([4]), efter en bred offentlig debatt i kongressen. Enligt avsnitt 702 godkänns inhämtande av utländska underrättelseuppgifter genom målsökning av personer som inte är amerikanska medborgare och som befinner sig utanför Förenta staterna, med obligatorisk assistans från amerikanska telekomtjänstleverantörer. Avsnitt 702 bemyndigar även justitieministern och DNI – två regeringstjänstemän som utses av presidenten och bekräftas av senaten – att utfärda årliga certifieringar till FISA-domstolen ([5]). I dessa certifieringar anges specifika kategorier av utländska underrättelseuppgifter som ska samlas in, t.ex. uppgifter i samband med terrorismbekämpning eller massförstörelsevapen, som måste falla inom de kategorier av utländska underrättelseuppgifter som fastställs i FISA-lagen ([6]). Styrelsen för tillsyn av personlig integritet och medborgerliga friheter har fastställt att ”sådana begränsningar tillåter *inte* obegränsad insamling av information om utlänningar” ([7]).

Certifieringarna ska också innehålla förfaranden för ”målinriktning” och ”minimering”, som ska granskas och godkännas av FISA-domstolen ([8]). Förfarandena för målinriktning är utformade för att se till att insamling endast sker på de sätt som är godkända enligt lag och att de faller inom certifieringens tillämpningsområde. Minimeringsförfarandena är avsedda att begränsa inhämtande, spridning och lagring av information om amerikanska medborgare, men innehåller även bestämmelser som ger ett väsentligt skydd av information som tillhör icke-amerikanska medborgare, vilket beskrivs nedan. Såsom beskrivs ovan föreskriver presidenten i PPD-28 att underrättelsegemenskapen ska tillhandahålla ytterligare skyddsmekanismer för personuppgifter om utländska medborgare, och dessa skyddsmekanismer gäller för information som samlas in enligt avsnitt 702.

När domstolen har godkänt förfarandena för målinriktning och minimering enligt avsnitt 702 anses insamlingen inte ske i bulk eller vara slumpartad, utan”inriktas enbart på specifika personer som det har fattats ett individuellt beslut om”, enligt vad styrelsen för tillsyn av personlig integritet och medborgerliga friheter har förklarat ([9]). Insamlingen riktas genom användning av individuella urvalsfaktorer, såsom e-postadresser eller telefonnummer, som enligt den amerikanska

([1]) 50 U.S.C. § 1881a.

([2]) Förenta staterna kan också inhämta domstolsbeslut enligt andra bestämmelser i FISA för framtagande av uppgifter, inklusive uppgifter som överförts enligt skölden för skydd av privatlivet. Se 50 U.S.C. § 1801 och följande artiklar. Avdelningarna I och III i FISA. Enligt dessa bestämmelser krävs domstolsbeslut för elektronisk övervakning respektive fysiska kontroller (förutom i nödsituationer) och det ska alltid finnas en trolig orsak till att anse att målet är en utländsk makt eller ett ombud för en utländsk makt. Enligt avdelning IV i FISA kan användningen av ”pen register”och ”trap and trace”-anordningar tillåtas enligt domstolsbeslut (förutom i nödsituationer) i godkända undersökningar av utländsk underrättelseverksamhet, kontraspionage eller terrorismbekämpning. Enligt avdelning V i FISA får FBI, enligt domstolsbeslut (förutom i nödsituationer) inhämta företagsregister som är relevanta för godkända undersökningar av utländsk underrättelseverksamhet, kontraspionage eller terrorismbekämpning. Såsom diskuteras nedan innehåller *Förenta staterna Freedom Act* ett uttryckligt förbud mot att beslut som godkänner användning av ”pen register” enligt FISA eller företagsregister används för bulkinsamling. Ett krav på ”specifika urvalstermer” har också införts för att se till att dessa befogenheter tillämpas på ett riktat sätt.

([3]) Styrelsen för tillsyn av personlig integritet och medborgerliga fri- och rättigheter, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (2 juli 2014) (nedan kallad *PCLOB-rapporten*).

([4]) *Se* Pub. L. nr 110–261, 122 Stat. 2436 (2008).

([5]) Se 50 U.S.C. § 1881a(a) och (b).

([6]) Idem, § 1801(e).

([7]) Se PCLOB-rapporten, 99.

([8]) Se 50 U.S.C. § 1881a(d) och (e).

([9]) Se PCLOB-rapporten, 111.

underrättelsepersonalens bedömning sannolikt används för att kommunicera utländska underrättelseuppgifter av den typ som omfattas av den certifiering som har lämnats in till domstolen ([1]). Underlaget för valet av mål måste dokumenteras och dokumentationen för varje urvalsfaktor granskas därefter av justitieministeriet ([2]). Den amerikanska regeringen har offentliggjort information som visar att omkring 90 000 enskilda personer omfattades av målinriktning enligt avsnitt 702 under 2014, vilket är en minimal del av världens över tre miljarder internetanvändare ([3]).

Information som samlas in enligt avsnitt 702 är föremål för de domstolsgodkända minimeringsförfarandena, som både skyddar utländska och amerikanska medborgare. De har offentliggjorts ([4]). Kommunikation som har inhämtats enligt avsnitt 702, vare sig den rör utländska eller amerikanska medborgare, lagras t.ex. i databaser med strikt åtkomstkontroll. De kan endast granskas av underrättelsetjänstpersonal som har utbildats i minimeringsförfaranden för integritetsskydd och har fått ett uttryckligt tillstånd om åtkomst för att utföra sina godkända uppgifter ([5]). Användningen av uppgifterna begränsas till identifiering av utländsk underrättelseinformation eller bevis för brott ([6]). Enligt PPD-28 får denna information spridas endast om det finns ett giltigt ändamål som rör utländska underrättelseuppgifter eller brottsbekämpning; enbart det faktum att en av parterna i kommunikationen inte är amerikansk medborgare räcker inte ([7]). Minimeringsförfarandena och PPD-28 föreskriver dessutom begränsningar av hur data med långtidsvärde som inhämtats enligt avsnitt 702 får lagras ([8]).

Tillsynen enligt avsnitt 702 är omfattande och utförs av samtliga tre grenar av vår regering. De myndigheter som genomför lagen har inrättat interna granskningsförfaranden i flera skikt, bland annat genom oberoende generalinspektörer och tekniska kontroller av åtkomst till uppgifterna. Justitieministeriet och ODNI granskar och undersöker noggrant tillämpningen av avsnitt 702 för att kontrollera att lagens bestämmelser efterlevs. Myndigheterna har också en oberoende skyldighet att rapportera eventuella fall av bristande efterlevnad. Sådana rapporter utreds och alla fall av bristande efterlevnad rapporteras till domstolen för övervakning av utländsk underrättelseinformation, presidentens styrelse för tillsyn av underrättelseverksamheten och kongressen, och åtgärdas på lämpligt sätt ([9]). Hittills har inga fall av medvetna försök att bryta mot lagen eller kringgå lagkrav förekommit ([10]).

FISA domstolen spelar en viktig roll i genomförandet av avsnitt 702. Den består av oberoende federala domare som tjänstgör vid FISA-domstolen under en sjuårsperiod. Precis som alla federala domare är de dock domare på livstid. Såsom anges ovan måste domstolen granska de årliga certifieringarna och förfarandena för målinriktning och minimering för att kontrollera att de är förenliga med lagstiftningen. Såsom även nämns ovan är regeringen dessutom skyldig att omedelbart rapportera fall av bristande efterlevnad till domstolen ([11]). Sekretessen för flera domstolsyttranden har hävts, vilket visar på domstolens mycket höga nivå av rättslig kontroll och oberoende när den granskar sådana ärenden.

Domstolens noggranna förfaranden har beskrivits av dess före detta ordförande i ett brev till kongressen, som har offentliggjorts ([12]). Till följd av *Förenta staterna Freedom Act*, som beskrivs nedan, är nu domstolen uttryckligen bemyndigad att utse en extern jurist som oberoende advokat för integritetsskydd i ärenden med nya eller viktiga juridiska frågor ([13]). Denna grad av deltagande av ett lands oberoende rättsväsende i utländska underrättelseverksamheter som riktas mot personer som varken är medborgare i landet eller bor inom dess gränser är ovanligt, om inte unikt, och bidrar till att säkerställa att insamling enligt avsnitt 702 sker inom lagliga gränser.

([1]) *Idem*.

([2]) *Idem* 8. 50 U.S.C. § 1881a(l); *se även* rapporten från *NSA Director of Civil Liberties and Privacy, NSA's Implementation of Foreign Intelligence Surveillance Act Section 702* (nedan kallad *NSA-rapporten*) s. 4, http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([3]) Director of National Intelligence *2014 Transparency Report, se* http://icontherecord.tumblr.com/transparency/odni_transparencyreport_cy2014.

([4]) Minimeringsförfarandena finns tillgängliga på http://www.dni.gov/files/documents/ppd-28/2014%20NSA%20702%20Minimization%20Procedures.pdf ("NSA Minimization Procedures"); http://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf; och http://www.dni.gov/files/documents/ppd-28/2014%20CIA%20702%20Minimization%20Procedures.pdf.

([5]) Se NSA rapporten, s. 4.

([6]) Se t.ex. NSA:s minimeringsförfaranden, s. 6.

([7]) Underrättelsetjänsternas PPD-28-förfaranden,se http://icontherecord.tumblr.com/ppd-28/2015/privacy-civil-liberties.

([8]) Se NSA:s minimeringsförfaranden, avsnitt 4 i PPD-28.

([9]) Se 50 U.S.C. § 1881(l), *se även* PCLOB-rapporten, s. 66–76.

([10]) Se dokumentet *Semiannual Assessment of Compliance with Procedures and Guidelines Issues Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, inlämnad av justitieministern och Director of National Intelligence, s. 2–3, http://www.dni.gov/files/documents/Semiannual%20Assessment%20of%20Compliance%20with%20procedures%20and%20guidelines%20issued%20pursuant%20to%20Sect%20702%20of%20FISA.pdf.

([11]) Regel 13 i arbetsordningen för domstolen för övervakning av utländsk underrättelseinformation, se http://www.fisc.uscourts.gov/sites/default/files/FISC%20Rules%20of%20Procedure.pdf.

([12]) Skrivelse från Reggie B. Walton till Patrick J. Leahy av den 29 juli 2013, se http://fas.org/irp/news/2013/07/fisc-leahy.pdf.

([13]) Se avsnitt 401 i *Förenta staterna Freedom Act*, P.L. s. 114–123.

Kongressen utövar tillsyn genom lagstadgade rapporter till kommittéerna för underrättelseverksamhet och rättsväsendet samt genom regelbundna genomgångar och utfrågningar. Det handlar bland annat om en halvårsrapport från justitieministern om tillämpningen av avsnitt 702 och eventuella fall av bristande efterlevnad ([1]) en separat halvårsbedömning av justitieministern och DNI om efterlevnaden av förfarandena för målinriktning och minimering samt efterlevnaden av de förfaranden som har tagits fram för att se till att insamlingen sker för ett godkänt ändamål i fråga om utländska underrättelseuppgifter ([2]) och en årsrapport från underrättelsetjänsternas chefer, för att säkerställa att insamlingen enligt avsnitt 702 fortsätter att ge utländska underrättelseuppgifter ([3]).

Sammanfattningsvis är insamling enligt avsnitt 702 godkänd enligt lag och är föremål för tillsyn på flera nivåer samt rättslig övervakning och tillsyn. Enligt ett tidigare sekretessbelagt yttrande från FISA-domstolen ”sker insamlingen inte i bulk eller på ett slumpartat sätt utan genom […] enligt noggrant övervägda beslut om målinriktning av individuell [kommunikation]” ([4]).

III. FÖRENTA STATERNA FREEDOM ACT

Genom *Förenta staterna Freedom Act*, som undertecknades i juni 2015, genomfördes väsentliga förändringar av den amerikanska underrättelsetjänsten och andra myndigheter med ansvar för nationell säkerhet. Dessutom ökades allmänhetens insyn i dessa myndigheter och FISA-domstolens beslut, vilket beskrivs nedan ([5]). Lagen säkerställer att våra anställda inom underrättelsetjänsten och de brottsbekämpande myndigheterna har de befogenheter som krävs för att skydda nationen, samtidigt som enskilda personers integritet skyddas på lämpligt sätt i utövandet av dessa befogenheter. Lagen stärker integritetsskyddet och de medborgerliga fri- och rättigheterna och ökar insynen.

Lagen förbjuder bulkinsamling av register, både beträffande amerikanska och utländska medborgare, enligt flera bestämmelser i FISA eller via nationella säkerhetsskrivelser (*National Security Letters*), en form av lagstadgade administrativa föreläggande) ([6]). Förbudet gäller särskilt telefonmetadata rörande samtal mellan personer i och personer utanför Förenta staterna, och skulle även omfatta dessa myndigheters insamling av information inom ramen för skölden för skydd av privatlivet. Enligt lagen ska regeringen basera eventuella ansökningar om tillgång till register inom ramen för dessa befogenheter på ”specifika urvalstermer”, dvs. termer som specifikt identifierar en person, kontonummer, adresser eller personliga anordningar, på ett sätt som begränsar omfattningen av den information som söks i största möjliga utsträckning ([7]). Detta innebär en ytterligare garanti för att information för underrättelsesyften är exakt fokuserad och riktad.

Genom lagen genomfördes dessutom betydande ändringar av förfarandena vid FISA-domstolen, för att både öka insynen och ge ytterligare garantier för integritetsskydd. Såsom anges ovan inrättas en ständig arbetsgrupp av säkerhetsgodkända advokater genom lagen. Advokaterna har sakkunskap om integritetsskydd och medborgerliga friheter, insamling av underrättelseuppgifter, kommunikationsteknik eller andra relevanta områden, och kan kallas till domstolen i egenskap av sakkunniga i mål som omfattar viktiga eller nya lagtolkningar. Advokaterna har befogenheter att framföra juridiska argument för att öka skyddet av enskilda personers integritet och medborgerliga friheter, och har tillgång till all information, inklusive sekretessbelagd information, som domstolen anser att de behöver för att fullgöra sina uppgifter ([8]).

Lagen bygger även på den unika insyn som den amerikanska regeringen ger i underrättelseverksamheten genom att kräva att DNI, i samråd med justitieministern, antingen ska häva sekretessen för eller offentliggöra en öppen sammanfattning av varje beslut, föreläggande eller yttrande som utfärdas av FISA-domstolen eller revisionsdomstolen för utländsk underrättelseinformation (*Foreign Intelligence Surveillance Court of Review*), och som innehåller en viktig redogörelse för eller tolkning av lagbestämmelser.

([1]) Se 50 U.S.C. § 1881f.
([2]) Se idem § 1881a(l)(1).
([3]) Se idem § 1881a(l)(3). En del av dessa rapporter är sekretessbelagda.
([4]) Mem. Yttrande och beslut, 26 (FISC 2014), se http://www.dni.gov/files/documents/0928/FISC%20Memorandum%20Opinion%20and%20Order%2026%20August%202014.pdf.
([5]) Se *Förenta staterna Freedom Act of 2015*, Pub. L. nr 114–23, § 401, 129 Stat. 268.
([6]) Se idem §§ 103, 201, 501. Nationella säkerhetsskrivelser godkänns enligt en rad olika lagar och ger FBI tillåtelse att inhämta information i kreditrapporter, finansiella register samt elektroniska abonnent- samt transaktionsregister från vissa typer av företag, i de enda syftet att skydda nationen mot internationell terrorism eller hemlig underrättelseverksamhet. Se 12 U.S.C. § 3414, 15 U.S.C. §§ 1681u-1681v, 18 U.S.C. § 2709. FBI använder vanligen nationella säkerhetsskrivelser för att samla in viktig ”innehållslös” information i de tidiga faserna av terrorismbekämpning och kontraspionage, t.ex. identiteten för en abonnent av ett konto som kan ha kommunicerat med agenter för en utländsk terroristgrupp som Islamiska staten. Personer som omfattas av nationella säkerhetsskrivelser har rätt att bestrida detta i domstol. *Se* 18 U.S.C. § 3511.
([7]) *Se idem*.
([8]) *Se idem* § 401.

Lagen föreskriver dessutom att omfattande information ska offentliggöras om FISA-insamling och förfrågningar enligt nationella säkerhetsskrivelser. Förenta staterna måste varje år till kongressen och allmänheten lämna ut information om antalet FISA-förelägganden och certifieringar som har sökts och beviljats, uppskattningar av antalet utländska medborgare och amerikanska medborgare som är föremål för och påverkas av övervakning och antalet utnämningar av advokater i egenskap av sakkunniga ([1]). Enligt lagen ska regeringen dessutom rapportera till allmänheten om antalet nationella säkerhetsskrivelser med förfrågningar om både utländska och amerikanska medborgare ([2]).

När det gäller insyn i företag föreskriver lagen en rad olika alternativ för företagens rapportering till allmänheten om det sammanlagda antalet FISA-förelägganden eller nationella säkerhetsskrivelser som de mottar från regeringen samt om antalet kundkonton som omfattas av dessa förelägganden ([3]). Flera företag har redan lämnat ut sådana uppgifter, vilka visar att antalet ansökningar om tillgång till kunders register är begränsat.

Dessa företags insynsrapporter visar att den amerikanska underrättelsetjänstens förfrågningar endast omfattar en minimal del av uppgifterna. Ett stort företags senaste insynsrapport visar t.ex. att de förfrågningar om uppgifter för nationella säkerhetssyften som det mottog (enligt FISA eller nationella säkerhetsskrivelser) berörde färre än 20 000 av företagets konton, vid en tidpunkt då företaget hade minst 400 miljoner abonnenter. Med andra ord berörde samtliga förfrågningar om uppgifter för nationella säkerhetssyften mindre än 0,005 procent av företagets abonnenter. Även om samtliga förfrågningar skulle ha gällt safe harbor-uppgifter, vilket naturligtvis inte är fallet, är det uppenbart att förfrågningarna är riktade och lämpliga till omfattningen, och att de varken utgör bulkinsamling eller är slumpartade.

I de fall bestämmelserna om utfärdande av nationella säkerhetsskrivelser redan begränsade de omständigheter under vilka skrivelsens mottagare kunde vara förhindrad att lämna ut informationen föreskriver lagen dessutom att sådana sekretesskrav måste ses över regelbundet. Mottagarna av nationella säkerhetsskrivelser ska meddelas när fakta inte längre stöder ett sekretesskrav och förfaranden för hur mottagarna kan bestrida sekretesskrav införs ([4]).

Sammanfattningsvis är de viktiga förändringar av de amerikanska underrättelsemyndigheterna som införs genom *Förenta staterna Freedom Act* ett tydligt bevis de stora ansträngningar som Förenta staterna har gjort för att prioritera skyddet av personuppgifter, integritetsskydd, medborgerliga friheter och insyn i alla amerikanska underrättelsemetoder.

IV. INSYN OCH ÖPPENHET

Förutom den insyn som föreskrivs i *Förenta staterna Freedom Act* tillhandahåller den amerikanska underrättelsegemenskapen en stor mängd ytterligare information till allmänheten, och föregår därigenom med gott exempel när det gäller insyn i dess underrättelseverksamheter. Underrättelsegemenskapen har offentliggjort många av sina policyer, förfaranden, beslut från domstolen för övervakning av utländsk underrättelseinformation och annat material för vilket sekretessen har hävts, vilket ger mycket stor insyn i verksamheten. Dessutom lämnar underrättelsegemenskapen ut betydligt mer statistik om hur regeringen tillämpas sina befogenheter för uppgiftsinsamling av nationella säkerhetsskäl. Den 22 april 2015 utfärdade underrättelsegemenskapen sin andra årsrapport med statistik över hur ofta regeringen tillämpar dessa viktiga befogenheter. ODNI också har offentliggjort en uppsättning konkreta insynsprinciper ([5]) på sin webbplats och på *IC On the Record* samt en genomförandeplan där principerna omsätts i konkreta och mätbara initiativ ([6]). I oktober 2015 beslutade *Director of National Intelligence* att varje underrättelsetjänst ska utse en tjänstemän med ansvar för insyn i underrättelseverksamheten inom sitt behörighetsområde, med uppgift att främja insyn och leda insynsinitiativ ([7]). Dessa tjänstemän kommer att föra ett nära samarbete med varje underrättelsetjänsts tjänsteman med ansvar för insyn och medborgerliga friheter för att se till att insyn, integritetsskydd och medborgerliga friheter fortsätter att prioriteras högt.

([1]) *Se idem* § 602.
([2]) *Se idem*.
([3]) *Se idem* § 603.
([4]) Se idem §§ 502 (f)–503.
([5]) *Se* http://www.dni.gov/index.php/intelligence-community/intelligence-transparency-principles.
([6]) *Se* http://www.dni.gov/files/documents/Newsroom/Reports%20and%20Pubs/Principles%20of%20Intelligence%20Transparency%20Implementation%20Plan.pdf.
([7]) Se idem.

Ett exempel på dessa ansträngningar är att NSA:s *Chief Privacy and Civil Liberties Officer* har hävt sekretessen för och lämnat ut flera rapporter under de senaste åren, bland annat rapporter om verksamheter enligt avsnitt 702 i dekret 12333 och *Förenta staterna Freedom Act* ([1]). Underrättelsegemenskapen samarbetar dessutom med styrelsen för tillsyn av personlig integritet och medborgerliga fri- och rättigheter, kongressen och amerikanska intresseorganisationer på integritetsskyddets område för att ge ytterligare insyn i Förenta staterna:s underrättelseverksamhet, när så är möjligt och förenligt med skyddet av känsliga underrättelsekällor och metoder. Sammantaget är Förenta staterna:s underrättelseverksamhet lika öppen som eller öppnare än andra nationers underrättelseverksamheter, och medger så stor insyn som möjligt med tanke på behovet av att skydda känsliga källor och metoder.

Sammanfattning av den omfattande insynen i Förenta staterna:s underrättelseverksamhet:

— Underrättelsegemenskapen har offentliggjort och lagt ut tusentals sidor av domstolsyttranden och myndighetsförfaranden om specifika förfaranden och krav för vår underrättelseverksamhet. Vi har också offentliggjort rapporter om underrättelsetjänsternas efterlevnad av tillämpliga begränsningar.

— Högt uppsatta tjänstemän inom underrättelsetjänsten gör regelbundet offentliga uttalanden om sina organisationers roller och verksamheter, inklusive beskrivningar av de efterlevnadssystem och garantier som styr deras arbete.

— Underrättelsegemenskapen har offentliggjort ett stort antal ytterligare dokument om underrättelseverksamheten enligt lagen om informationsfrihet.

— Presidenten utfärdade PPD-28, som föreskriver ytterligare begränsningar av våra underrättelseverksamheter, och ODNI har utfärdat två offentliga rapporter om genomförandet av dessa begränsningar.

— Underrättelsegemenskapen har nu en lagstadgad skyldighet att offentliggöra viktiga rättsliga yttranden som utfärdas av FISA-domstolen eller sammanfattningar av sådana yttranden.

— Regeringen är skyldig att årligen rapportera om hur ofta den utnyttjar vissa nationella säkerhetsmyndigheter, och även företagen får utfärda sådana rapporter.

— Styrelsen för tillsyn av personlig integritet och medborgerliga friheter har utfärdat flera detaljerade offentliga rapporter om underrättelseverksamhet, och kommer att fortsätta att göra så även i framtiden.

— Underrättelsegemenskapen lämnar en stor mängd sekretessbelagd information till kongressens tillsynskommittéer.

— DNI har utfärdat insynsprinciper som styr underrättelsegemenskapens verksamhet.

Denna omfattande insyn kommer att upprätthållas i framtiden. All information som har offentliggjorts kommer naturligtvis även att finnas tillgänglig för handelsministeriet och Europeiska kommissionen. Den årliga översyn som genomförs av handelsministeriet och Europeiska kommissionen om genomförandet av skölden för skydd av privatlivet kommer att ge kommissionen möjlighet att diskutera eventuella frågor som uppstår om ny offentliggjord information och andra frågor i samband med skölden och dess genomförande, och ministeriet kan efter eget gottfinnande be företrädare för andra myndigheter, inklusive underrättelsegemenskapen, att delta i översynen. Detta är naturligtvis utöver den mekanism som PPD-28 föreskriver för att EU-medlemsstaterna ska kunna ta upp övervakningsrelaterade frågor med en utsedd tjänsteman från utrikesdepartementet.

V. RÄTTSMEDEL

Amerikansk lagstiftning föreskriver en rad olika rättsmedel för enskilda personer som har varit föremål för olaglig elektronisk övervakning för nationella säkerhetssyften. Enligt FISA begränsas inte rätten att söka upprättelse i amerikanska domstolar till amerikanska medborgare. En enskild person som har grunder för att väcka talan har

([1]) *Se* https://www.nsa.gov/civil_liberties/_files/nsa_report_on_section_702_program.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf; https://www.nsa.gov/civil_liberties/_files/UFA_Civil_Liberties_and_Privacy_Report.pdf.

rättsmedel till sitt förfogande för att bestrida olaglig elektronisk övervakning enligt FISA. Enligt FISA kan t.ex. personer som har varit föremål för olaglig elektronisk övervakning stämma tjänstemän vid den amerikanska regeringen personligen och begära skadestånd och advokatarvoden. *Se* 50 U.S.C. § 1810. Enskilda personer som har grunder för att väcka talan kan även åberopa civilrättsliga grunder för skadestånd mot Förenta staterna, inklusive rättegångskostnader, om uppgifter om dem som har erhållits genom elektronisk övervakning enligt FISA har använts eller lämnats ut på ett olagligt och medvetet sätt. *Se* 18 U.S.C. § 2712. Om regeringen har för avsikt att använda eller lämna ut information som har erhållits eller härletts från elektronisk övervakning av en förfördelad person enligt FISA mot den personen i rättsliga eller administrativa förfaranden i Förenta staterna, måste den informera domstolen och den berörda personen om sin avsikt på förhand. Den berörda personen kan därefter bestrida övervakningens laglighet och kräva att informationen sekretessbeläggs. *Se* 50 U.S.C. § 1806. Slutligen föreskriver FISA även straffrättsliga påföljder för enskilda personer som avsiktligen deltar i olaglig elektronisk övervakning under falska lagliga förespeglingar, eller som avsiktligen använder eller lämnar ut information som erhållits från olaglig övervakning. *Se* 50 U.S.C. § 1809.

EU-medborgare har även andra sätt att väcka talan mot amerikanska regeringstjänstemän för olaglig användning av eller åtkomst till uppgifter från regeringens sida, även mot regeringstjänstemän som bryter mot lagen i samband med olaglig åtkomst till eller användning av information för att främja nationella säkerhetssyften. Enligt lagen om datorbedrägeri (*Computer Fraud and Abuse Act*) förbjuds avsiktlig otillåten åtkomst (eller överskridande av tillåten åtkomst) för att inhämta information från finansinstitut, den amerikanska regeringens datorsystem eller datoråtkomst via internet samt hot om att skada skyddade datorer för utpressning eller bedrägeri. *Se* 18 U.S.C. § 1030. Alla personer, oavsett nationalitet, som lider skada eller förlust till följd av överträdelser av denna lag kan stämma lagöverträdaren (inklusive regeringstjänstemän) för att få skadestånd och begära föreläggande eller andra motsvarande rättsmedel enligt avsnitt 1030(g) oavsett om straffrättsligt åtalande har väckts, på villkor att agerandet åtminstone omfattar en av de olika omständigheter som anges i lagen. Lagen om elektronisk brevhemlighet (*Electronic Communications Privacy Act* – ECPA) reglerar regeringens åtkomst till lagrade elektroniska meddelanden samt transnationella register och abonnentuppgifter som innehas av utomstående kommunikationsleverantörer.*Se* 18 U.S.C. §§ 2701–2712. Enligt ECPA kan förfördelade personer stämma regeringstjänstemän för oavsiktlig och olaglig åtkomst till lagrade uppgifter. ECPA gäller alla personer, oavsett medborgarskap, och förfördelade personer kan beviljas skadestånd och få advokatkostnader betalda. Lagen om integritetsskydd för finansiella uppgifter (*Right to Financial Privacy Act* – RFPA) begränsar den amerikanska regeringens åtkomst till bankers och mäklarföretags register över enskilda kunder. *Se* 12 U.S.C. §§ 3401–3422. Enligt FRPA kan en bank eller ett mäklarföretag stämma den amerikanska regeringen för att få lagstadgat skadestånd för olaglig åtkomst till kundregister, och om sådan olaglig åtkomst befinns vara avsiktlig inleds automatiskt en utredning om eventuella disciplinära åtgärder mot berörda regeringsanställda. *Se* 12 U.S.C. § 3417.

Slutligen föreskriver lagen om informationsfrihet (*Freedom of Information Act* – FOIA) att alla personer kan ansöka om åtkomst till federala myndighetsregister rörande vilken fråga som helst, med undantag för vissa kategorier av uppgifter. *Se* 5 U.S.C. § 552(b). Undantagen omfattar begränsningar av tillgång till sekretessbelagd nationell säkerhetsinformation, personuppgifter för andra enskilda personer och information om brottsutredningar, och är jämförbara med de begränsningar som nationerna har infört i sina egna lagar om tillgång till information. Dessa begränsningar gäller både amerikaner och utländska medborgare. Tvister om utlämnande av registeruppgifter enligt FOI-lagen kan överklagas i förvaltningsrätten och därefter i federala domstolar. Domstolen är skyldig att göra en ny bedömning om registren förs på lämpligt sätt enligt 5 U.S.C. § 552(a)(4)(B), och kan beordra regeringen att ge tillgång till register. I vissa fall har domstolarna ändrat regeringens beslut om att information bör förbli sekretessbelagd ([1]). Skadestånd kan inte utdömas, men domstolarna kan besluta om betalning av advokatarvoden.

VI. SLUTSATSER

Förenta staterna bekräftar att landet i sin signalspaning och andra underrättelseverksamheter måste beakta att alla människor ska behandlas med värdighet och respekt, oavsett nationalitet och bostadsort, och erkänner att alla personer har legitima integritetsintressen när det gäller behandlingen av deras personuppgifter. Förenta staterna använder endast signalspaning för att främja sina nationella säkerhets- och utrikespolitiska intressen och för att skydda sina medborgare och sina allierades medborgare från skada. Underrättelsegemenskapen bedriver kort sagt ingen godtycklig övervakning av någon, inte heller av vanliga EU-medborgare. Insamling av uppgifter genom signalspaning sker endast enligt vederbörligt godkännande och i strikt efterlevnad av dessa begränsningar, efter övervägande av eventuella alternativa källor, även

([1]) *Se t.ex. New York Times mot Department of Justice*, 756 F.3d 100 (2d Cir. 2014), *American Civil Liberties Union mot CIA*, 710 F.3d 422 (D.C. Cir. 2014).

diplomatiska och politiska källor, och på ett sätt som prioriterar lämpliga och genomförbara alternativ. Om så är praktiskt möjligt sker signalspaning endast genom insamling som inriktas på specifika utländska underrättelsemål och genom användning av urvalsfaktorer.

Förenta staterna: s politik i detta avseende bekräftas i PPD-28. Inom denna ram har de amerikanska underrättelsetjänsterna inte rättsliga befogenheter, resurser, teknisk kapacitet eller någon önskan om att fånga upp hela världens kommunikationer. Underrättelsetjänsterna läser inte alla människors e-post i Förenta staterna eller i världen. I enlighet med PPD-28 tillhandahåller Förenta staterna ett starkt skydd för utländska medborgares personuppgifter som samlas in genom signalspaning. I största möjliga överensstämmelse med den nationella säkerheten omfattar detta policyer och förfaranden för att minimera lagring och spridning av utländska medborgares personuppgifter, jämförbart med det skydd som amerikanska medborgare åtnjuter. Såsom diskuteras ovan saknar det omfattande tillsynssystemet enligt avsnitt 702 i FISA motstycke i världen. Avslutningsvis bidrar de omfattande ändringarna av Förenta staterna:s lagstiftning om underrättelseverksamhet som anges i *Förenta staterna Freedom Act* och de ODNI-ledda initiativen för att främja insyn i underrättelseverksamheten stort till att förbättra integritetsskyddet och de medborgerliga fri- och rättigheterna för alla enskilda personer, oavsett nationalitet.

Högaktningsfullt,

Robert S. Litt

den 21 juni 2016

Justin S. Antonipillai
Jurist
U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Ted Dean
Biträdande minister
International Trade Administration
1401 Constitution Avenue, N.W.
Washington, DC 20230

Bäste herr Antonipillai och herr Dean,

Jag skriver för att ge ytterligare information om hur Förenta staterna genomför bulkinsamling av signalunderrättelser. Som förklaras i fotnot 5 i *Presidential Policy Directive 28* (PPD-28) avser ”bulkinsamling” inhämtning av en relativt stor mängd signalunderrättelser under omständigheter där underrättelsegemenskapen inte kan använda en identifierare som är förknippad med ett specifikt mål (till exempel e-postadress eller telefonnummer) för att rikta insamlingen. Det innebär dock inte att denna typ av insamling är någon ”slumpartad massinsamling”. Enligt PPD-28 ska också signalspaningen i så stor utsträckning som möjligt anpassas till ändamålet. För att underlätta denna uppgift vidtar underrättelsegemenskapen åtgärder för att säkerställa att de uppgifter som ska samlas in, även om vi inte kan använda målspecifika identifierare, sannolikt innehåller utländska underrättelser som motsvarar de krav som amerikanska beslutsfattare har fastställt i enlighet med det förfarande jag redogjort för i min tidigare skrivelse, och minimerar mängden insamlad information som inte är relevant.

Underrättelsegemenskapen kan t.ex. bli ombedd att inhämta signalunderrättelser om verksamheten inom en terroristgrupp i en region i ett land i Mellanöstern som tros planera attacker mot västeuropeiska länder, men kanske inte känner till namn, telefonnummer, e-postadresser eller andra specifika identifierare hos de personer som är förknippade med denna terroristgrupp. Vi kan välja att rikta in oss på denna grupp genom insamling av meddelanden till och från denna region för ytterligare kontroll och analys i syfte att identifiera den kommunikation som rör gruppen. Därvid skulle underrättelsegemenskapen sträva efter att avgränsa insamlingen så mycket som möjligt. Detta skulle betraktas som ”bulkinsamling” eftersom användningen av urvalsfaktorer inte är möjlig, men det är ingen ”slumpartad massinsamling”; den är snarare riktad så precist som möjligt.

Även när målinriktning genom användning av särskilda urvalsfaktorer inte är möjlig samlar Förenta staterna alltså inte in alla meddelanden från alla kommunikationsanläggningar överallt i världen, utan använder filter och andra tekniska hjälpmedel för att inrikta sin insamling på de anläggningar som sannolikt innehåller meddelanden av värde som utländska underrättelseuppgifter. Därvid berör Förenta staternas signalspaningsverksamhet endast en bråkdel av den kommunikation som sker över internet.

Eftersom ”bulkinsamling” medför en större risk för att irrelevanta meddelanden samlas in, som anges i min tidigare skrivelse, begränsar PPD-28 underrättelsegemenskapens användning av signalunderrättelser som samlats in på detta sätt till sex bestämda ändamål. PPD-28, och myndigheternas policyer för genomförande av PPD-28, begränsar också lagringen och spridningen av personuppgifter som erhållits genom signalspaning, oberoende av om uppgifterna har samlats in genom bulkinsamling eller målinriktad insamling, och oberoende av den enskilde personens nationalitet.

Underrättelsegemenskapens ”bulkinsamling” är således inte någon ”slumpartad massinsamling”, utan innebär att metoder och verktyg används för att filtrera insamlingen i syfte att rikta den mot material som uppfyller beslutsfattarnas krav för utländska underrättelseuppgifter och samtidigt minimera insamlingen av irrelevant information, och innefattar stränga

regler för att skydda den irrelevanta information som eventuellt inhämtas. De policyer och förfaranden som beskrivs i denna skrivelse gäller för all bulkinsamling av signalspaningsuppgifter, inklusive bulkinsamling av meddelanden till och från Europa, utan att bekräfta eller förneka huruvida sådan insamling sker.

Ni har också begärt mer information avseende styrelsen för tillsyn av personlig integritet och medborgerliga fri- och rättigheter (*Privacy and Civil Liberties Oversight Board* – PCLOB) samt om generalinspektörer, och deras befogenheter. PCLOB är en oberoende myndighet inom den verkställande makten. Medlemmarna i styrelsen, som består av fem ledamöter från båda partierna, utses av presidenten och godkänns av senaten ([1]). Varje styrelseledamot har en mandatperiod på sex år. Styrelsens ledamöter och personal har säkerhetsgodkännande för att till fullo kunna utöva sina lagstadgade skyldigheter och ansvar ([2]).

PCLOB:s uppgift är att se till att den federala regeringens insatser för att förhindra terrorism vägs mot behovet att skydda den personliga integriteten och de medborgerliga fri- och rättigheterna. Styrelsen har två grundläggande ansvarsområden – tillsyn och rådgivning. PCLOB fastställer sin egen dagordning och bestämmer vilka insatser för tillsyn eller rådgivning som den önskar vidta.

I sin *tillsynsroll* granskar och analyserar PCLOB den verkställande maktens åtgärder för att skydda landet mot terrorism, och ser till att behovet av sådana åtgärder vägs mot behovet av att skydda den personliga integriteten och de medborgerliga fri- och rättigheterna ([3]). PCLOB:s senaste tillsyn omfattade övervakningsprogram som genomförts i enlighet med avsnitt 702 i FISA ([4]). För närvarande gör PCLOB en översyn av den underrättelseverksamhet som bedrivs i enlighet med dekret 12333 ([5]).

I sin *rådgivande* funktion säkerställer PCLOB att frihetsaspekterna beaktas på rätt sätt vid utarbetandet och genomförandet av lagar, regler och politik som rör insatser för att skydda landet mot terrorism ([6]).

För att styrelsen ska kunna utföra sitt uppdrag har den lagstadgad tillgång till alla relevanta myndighetsregister, rapporter, revisioner, inspektioner, handlingar, skrivelser och rekommendationer samt till annat relevant material, inklusive sekretessbelagd information enligt lag ([7]). Dessutom får styrelsen intervjua, ta emot uttalanden från eller ta upp offentliga vittnesmål från tjänstemän eller anställda inom den verkställande makten ([8]). Styrelsen kan dessutom skriftligen begära att justitieministern på styrelsens vägnar utfärdar förelägganden för att tvinga parter utanför den verkställande makten att tillhandahålla relevant information ([9]).

Slutligen har PCLOB lagstadgade krav på offentlig insyn. Detta inbegriper att hålla allmänheten underrättad om sin verksamhet genom offentliga utfrågningar och genom att göra sina rapporter allmänt tillgängliga, i möjligaste mån på ett sätt som är förenligt med skyddet av sekretessbelagd information ([10]). PCLOB har dessutom skyldighet att rapportera när ett organ under den verkställande makten underlåter att följa dess rekommendationer.

Generalinspektörer inom underrättelsegemenskapen genomför revisioner, inspektioner och översyner av program och aktiviteter inom underrättelsegemenskapen för att identifiera och åtgärda systemrisker, svagheter och brister. Dessutom utreder generalinspektörerna klagomål eller information om påstådda överträdelser av lagar, regler eller föreskrifter, eller

([1]) 42 U.S.C. 2000ee(a), (h).
([2]) 42 U.S.C. 2000ee(k).
([3]) 42 U.S.C. 2000ee(d)(2).
([4]) *Se* https://www.pclob.gov/library.html#oversightreports.
([5]) *Se* https://www.pclob.gov/events/2015/may13.html.
([6]) 42 U.S.C. 2000ee(d)(1); *se även* PCLOB:s *Advisory Function Policy and Procedure, Policy 2015–004*, https://www.pclob.gov/library/Policy-Advisory_Function_Policy_Procedure.pdf.
([7]) 42 U.S.C. 2000ee(g)(1)(A).
([8]) 42 U.S.C. 2000ee(g)(1)(B).
([9]) 42 U.S.C. 2000ee(g)(1)(D).
([10]) 42 U.S.C. 2000eee(f).

dålig förvaltning, slöseri med resurser, maktmissbruk, eller om underrättelsegemenskapens program och verksamhet innebär betydande och konkret fara för folkhälsan och säkerheten. Generalinspektörernas oberoende ställning är en viktig komponent för att säkerställa objektivitet och integritet i rapporter, resultat och rekommendationer som de ligger bakom. Några av de viktigaste komponenterna för att säkerställa generalinspektörernas oberoende omfattar förfarandet för utnämning och entledigande av dem, separata myndigheter för de operativa delarna, för budget och för personal, och krav om dubbel rapportering till cheferna inom den verkställande maktens organ och till kongressen.

Kongressen inrättade ett oberoende generalinspektörskontor hos varje organ under den verkställande makten, inklusive varje organisation inom underrättelsegemenskapen ([1]). Till följd av att *Intelligence Authorization Act for Fiscal Year 2015* antogs utses nästan alla generalinspektörer med tillsyn över en organisation inom underrättelsegemenskapen av presidenten och godkänns av senaten, bl.a. justitiedepartementet, *Central Intelligence Agency*, nationella säkerhetsmyndigheten och underrättelsegemenskapen ([2]). Dessa generalinspektörer är dessutom fast anställda tjänstemän, utan partianknytning, som bara kan entledigas av presidenten. Även om Förenta staterna:s konstitution föreskriver att presidenten ska ha befogenhet att entlediga generalinspektörer har den sällan utnyttjats, och kräver dessutom att presidenten lämnar en skriftlig motivering till detta till kongressen 30 dagar i förväg ([3]). Detta förfarande för utnämning av generalinspektörer garanterar att det inte förekommer någon otillbörlig påverkan från den verkställande maktens tjänstemän vid urval, utnämning eller entledigande av en generalinspektör.

För det andra har generalinspektörerna omfattande lagstadgade befogenheter att genomföra revisioner, utredningar och granskningar av den verkställande maktens program och insatser. Utöver den tillsyn av utredningar och granskningar som krävs enligt lag har generalinspektörerna stort utrymme att tillämpa tillsynsbefogenheten för att själva välja program och verksamhet för granskning ([4]). Vid utövandet av denna befogenhet garanterar lagen att generalinspektörerna har oberoende resurser för att utföra sina uppgifter, inbegripet befogenhet att anställa sin egen personal och separat dokumentera sina budgetförslag till kongressen ([5]). Lagen säkerställer att generalinspektörerna har tillgång till den information de behöver för att utföra sina uppgifter. Detta omfattar befogenheten att ha direkt tillgång till myndighetens alla register och information om myndighetens program och verksamhet oavsett klassificering, befogenheten att förelägga om information och handlingar, och befogenheten att ta upp ed ([6]). I begränsade fall får en chef för ett organ under den verkställande makten förbjuda en generalinspektörs verksamhet, till exempel om en generalinspektörs revision eller undersökning avsevärt skulle strida mot Förenta staterna:s nationella säkerhetsintressen. Att denna behörighet utövas är extremt ovanligt och kräver att organets chef underrättar kongressen inom 30 dagar om skälen för utövandet av den ([7]). *Director of National Intelligence* har aldrig utnyttjat denna behörighet till begränsning för någon generalinspektörsverksamhet.

För det tredje ansvarar generalinspektörerna för att hålla båda cheferna för verkställande maktens organ och kongressen fullt informerade genom rapporter om bedrägerier och andra allvarliga problem, missbruk och brister i fråga om dessa organs program och verksamhet ([8]). Dubbel rapportering stärker generalinspektörernas oberoende genom att ge insyn i förfarandena för generalinspektörernas tillsyn och ge cheferna för organen möjlighet att genomföra rekommendationer avseende generalinspektörerna innan kongressen kan vidta lagstiftande åtgärder. Generalinspektörerna är till exempel enligt lag skyldiga att utarbeta halvårsvisa rapporter som beskriver sådana problem och vilka korrigerande åtgärder som hittills vidtagits ([9]). Organ under den verkställande makten tar generalinspektörernas konstateranden och

([1]) Avsnitten 2 och 4 i *Inspector General Act* från 1978, i dess ändrade lydelse (nedan kallad *lagen om generalinspektörer*); avsnitt 103H(b) och (e) i *National Security Act* från 1947, i dess ändrade lydelse (nedan kallad *lagen om nationell säkerhet*); avsnitt 17(a) i *Central Intelligence Act* (nedan kallad *CIA-lagen*).

([2]) *Se* Pub. L. nr 113–293, 128 Stat. 3990, (19 december 2014). Endast generalinspektörer för Försvarets underrättelsetjänst (*Defense Intelligence Agency*) och nationella byrån för geospatiala underrättelser utses inte av presidenten; generalinspektörerna inom DOD och underrättelsegemenskapen har emellertid konkurrerande behörighet för dessa organ.

([3]) Avsnitt 3 i lagen om generalinspektörer från 1978, i dess ändrade lydelse, avsnitt 103H(c) i lagen om nationell säkerhet, och avsnitt 17(b) i CIA-lagen.

([4]) *Se* avsnitt 4(a) och 6(a)(2) i lagen om generalinspektörer från 1947, avsnitt 103H(e) och (g)(2)(A) i lagen om nationell säkerhet, avsnitt 17 (a) och (c) i CIA-lagen.

([5]) Avsnitt 3(d), 6(a)(7) och 6(f) i lagen om generalinspektörer, avsnitt 103H(d), (i), (j) och (m) i lagen om nationell säkerhet, avsnitt 17(e)(7) och (f) i CIA-lagen.

([6]) Avsnitt 6(a)(1), (3), (4), (5), och (6) i lagen om generalinspektörer, avsnitt 103H(g)(2) i lagen om nationell säkerhet, avsnitt 17(e)(1), (2), (4), och (5) i CIA-lagen.

([7]) *Se t.ex.* avsnitt 8(b) och 8E(a) i lagen om generalinspektörer, avsnitt 103H(f) i lagen om nationell säkerhet, avsnitt 17(b) i CIA-lagen.

([8]) Avsnitt 4(a)(5) i lagen om generalinspektörer, avsnitt 103H(a)(b)(3) och (4) i lagen om nationell säkerhet, avsnitt 17(a)(2) och (4) i CIA-lagen.

([9]) Avsnitt 2(3), 4(a) och 5 i lagen om generalinspektörer, avsnitt 103H(k) i lagen om nationell säkerhet, avsnitt 17(d) i CIA-lagen. Generalinspektören vid justitiedepartementet gör sina offentliggjorda rapporter tillgängliga på följande internetadress: http://oig.justice.gov/reports/all.htm. Likaså gör generalinspektören för underrättelsegemenskapen sina halvårsvisa rapporter allmänt tillgängliga på https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

rekommendationer på allvar och generalinspektörerna kan ofta återspegla organens godtagande och genomförande av generalinspektörernas rekommendationer i dessa och andra rapporter till kongressen, och i vissa fall till allmänheten ([1]). Utöver denna struktur med dubbla generalinspektörsrapporter är generalinspektörerna också ansvariga för att ledsaga visselblåsare inom den verkställande makten till lämplig tillsynskommitté i kongressen för att avslöja påstådda bedrägerier, slöseri eller missbruk inom den verkställande maktens program och verksamhet. Identiteten på dem som trätt fram är skyddad från den verkställande makten, som skyddar visselblåsare mot eventuella förbjudna personalåtgärder eller åtgärder för säkerhetsgodkännande som vidtagits som vedergällning för rapportering till generalinspektörerna ([2]). Eftersom visselblåsare ofta är källorna bakom generalinspektörernas utredningar blir generalinspektörernas tillsyn effektivare i och med möjligheten att rapportera till kongressen utan påverkan från den verkställande makten. På grund av detta oberoende kan generalinspektörerna främja ekonomi, effektivitet och ansvarsskyldighet inom den verkställande maktens organ med objektivitet och integritet.

Avslutningsvis har kongressen inrättat*Council of Inspectors General on Integrity and Efficiency*. Detta råd utvecklar bland annat generalinspektörernas standarder för revisioner, undersökningar och utvärderingar, främjar fortbildning, och har rätt att pröva påståenden om tjänstefel bland generalinspektörerna, vilket fungerar som ett kritiskt öga på generalinspektörerna, som anförtrotts övervakningen av alla andra ([3]).

Jag hoppas att denna information kan vara till nytta.

Med vänlig hälsning
Robert S. Litt
Chefsjurist

([1]) Avsnitt 2(3), 4(a) och 5 i lagen om generalinspektörer, avsnitt 103H(k) i lagen om nationell säkerhet, avsnitt 17(d) i CIA-lagen. Generalinspektören vid justitiedepartementet gör sina offentliggjorda rapporter tillgängliga på följande internetadress: http://oig.justice.gov/reports/all.htm. Likaså gör generalinspektören för underrättelsegemenskapen sina halvårsvisa rapporter allmänt tillgängliga på https://www.dni.gov/index.php/intelligence-community/ic-policies-reports/records-requested-under-foia#icig.

([2]) Avsnitt 7 i lagen om generalinspektörer, avsnitt 103H(g)(3) i lagen om nationell säkerhet, avsnitt 17(e)(3) i CIA-lagen.

([3]) Avsnitt 11 i lagen om generalinspektörer.

BILAGA VII

Skrivelse från Bruce Swartz, biträdande justitieminister och rådgivare för internationella frågor vid Förenta staterna:s justitieministerium

19 februari 2016

Justin S. Antonipillai
Rådgivare
U.S. Department of Commerce
1401 Constitution Ave., NW
Washington, DC 20230

Ted Dean
Biträdande minister
International Trade Administration
1401 Constitution Ave., NW
Washington, DC 20230

Bäste herr Antonipillai och herr Dean,

Denna skrivelse ger en kortfattad översikt av de främsta utredningsverktyg som används för att erhålla affärsuppgifter och annan information i register från företag i Förenta staterna för ändamål som rör brottsbekämpning och allmänintresset (civilt och lagstadgat), inbegripet de åtkomstbegränsningar som anges av dessa myndigheter ([1]). Dessa rättsprocesser är icke-diskriminerande eftersom de används för att erhålla information från företag i Förenta staterna, även från företag som självcertifierar sig via skölden för skydd av privatlivet i EU och Förenta staterna, oavsett den registrerades nationalitet. Företag som är föremål för rättsprocesser i Förenta staterna kan dessutom bestrida detta i domstol enligt vad som diskuteras nedan ([2]).

Det fjärde tillägget till Förenta staterna:s konstitution är särskilt relevant för offentliga myndigheters beslagtagande av uppgifter. Där anges följande: ”Folkets rätt att vara säkra i sina personer, hus, dokument och ägodelar mot oskälig husrannsakan och gripande ska ej överträdas och inga rannsaknings- eller arresteringsorder ska utgå, utom på skälig grund, understödd av ed eller försäkran, och med en noggrann beskrivning av den plats som ska rannsakas och de personer som ska gripas eller föremål som ska beslagtas.” Förenta staterna:s konstitution, tillägg IV. Såsom Förenta staterna:s högsta domstol förklarade i målet Berger mot State of New York, ”är det grundläggande syftet med detta tillägg, vilket domstolen har bekräftat i oräkneliga beslut, att skydda enskilda personers integritet och säkerhet mot godtyckliga kränkningar från regeringstjänstemäns sida”. 388 U.S. 41, 53 (1967) (*citat från målet Camara mot Mun. Court of San Francisco*, 387 U.S. 523, 528 (1967)). Enligt det fjärde tillägget är tjänstemän vid brottsbekämpande myndigheter i regel skyldiga att inhämta en husrannsakningsorder från en domare innan de gör en husrannsakan inom ramen för nationella brottsutredningar. Se Katz mot United States, 389 U.S. 347, 357 (1967). När kravet på husrannsakningsorder inte gäller är statliga åtgärder enligt det fjärde tillägget föremål för ett ”skälighetstest”. Det garanteras alltså i konstitutionen att den amerikanska regeringen inte har gränslösa eller godtyckliga befogenheter att beslagta privatuppgifter.

Brottsbekämpande myndigheter på det straffrättsliga området:

Federala åklagare, som är tjänstemän vid justitieministeriet, och federala utredare, inklusive tjänstemän från *Federal Bureau of Investigation* (FBI), en brottsbekämpande myndighet inom justitieministeriet, får tvinga företag i Förenta staterna att lämna ut handlingar och annan registerinformation för brottsutredningar via olika typer av obligatoriska rättsprocesser,

([1]) Denna översikt omfattar inte de utredningsverktyg inom ramen för den nationella säkerheten som används av de brottsbekämpande myndigheterna i utredningar om terrorism och andra utredningar som rör den nationella säkerheten, inklusive nationella säkerhetsskrivelser (*National Security Letters*) för viss registerinformation i kreditrapporter, finansiella register och elektroniska abonnent- och transaktionsregister, *se* 12 U.S.C. § 3414, 15 U.S.C. § 1681u, 15 U.S.C. § 1681v, 18 U.S.C. § 2709, och för elektronisk övervakning, husrannsakningsorder, företagsregister och annan insamling av kommunikation i enlighet med lagen om underrättelseverksamhet och övervakning utomlands, se 50 U.S.C. § 1801 och följande.

([2]) I denna skrivelse diskuteras federal brottsbekämpande verksamhet och federala tillsynsmyndigheter. Lagöverträdelser utreds av staterna och behandlas i deras domstolar. Statliga brottsbekämpande myndigheter använder generellt beslut och förelägganden som utfärdas enligt statlig lag på samma sätt som beskrivs här, men statliga rättsprocesser kan skyddas genom staternas konstitutioner, som har företräde framför den amerikanska konstitutionen. Det lagstadgade statliga skyddet måste åtminstone motsvara det skydd som den amerikanska konstitutionen ger, inklusive men inte begränsat till det fjärde tillägget.

inklusive förelägganden från åtalsjuryn, administrativa förelägganden och husrannsakningsorder, och kan inhämta andra meddelanden genom federal avlyssning i brottsbekämpande syfte samt befogenheter att utföra ”pen register”.

Förelägganden från åtalsjury eller rättegångsförelägganden: Straffrättsliga förelägganden används till stöd för riktade brottbekämpningsutredningar. Ett föreläggande från en åtalsjury är en officiell begäran som utfärdas av en åtalsjury (vanligen på begäran av en federal åklagare) för att stödja åtalsjuryns utredning av en misstänkt överträdelse av straffrätten. Åtalsjuryer är domstolens utredande gren och utses av en domare eller en fredsdomare. Ett föreläggande kan innehålla krav på att en viss person ska vittna under en rättegång eller ta fram eller tillhandahålla företagsregister, elektroniskt lagrad information eller andra materiella ting. Informationen måste vara relevant för utredningen och föreläggandet får inte vara orimligt på grund av att det är för allmänt utformat eller betungande. Mottagaren kan bestrida föreläggandet enligt dessa grunder. Se Fed. R. Crim. s. 17. Under begränsade omständigheter får rättegångsförelägganden rörande handlingar användas efter det att målet har avgjorts av juryn.

Befogenheter avseende administrativa förelägganden: Befogenheter avseende administrativa förelägganden får utövas i straff- eller civilrättsliga utredningar. Inom brottsbekämpningen är användningen av administrativa förelägganden för att ta fram eller tillhandahålla företagsregister, elektroniskt lagrad information eller andra materiella ting tillåten enligt flera federala lagar i utredningar som rör bedrägerier inom hälsovården, övergrepp mot barn, skydd av säkerhetstjänsterna, ärenden rörande kontrollerade ämnen och generalinspektörens utredningar som omfattar regeringsmyndigheter. Om regeringen vill verkställa ett administrativt föreläggande i domstol kan mottagare av ett administrativt föreläggande, precis som mottagare av ett föreläggande från en åtalsjury, hävda att föreläggandet är orimligt på grund av att det är för allmänt utformat eller betungande.

Domstolsbeslut om ”pen register”och ”trap and trace”-anordningar: Enligt straffrättens bestämmelser om ”pen register”och ”trap and trace”-anordningar kan brottsbekämpande myndigheter ansöka om domstolsbeslut för att inhämta innehållslös information i realtid om uppringda telefonnummer, koppling av telefonsamtal, adresser och signaler rörande ett telefonnummer eller en e-postadress om det säkerställs att den information som lämnas är relevant för en pågående brottsutredning. *Se* 18 U.S.C. §§ 3121–3127. Olaglig användning eller installation av en sådan anordning utgör ett federalt brott.

Lagen om elektronisk brevhemlighet, 1986 (*Electronic Communications Privacy Act* – ECPA): Regeringens tillgång till abonnentuppgifter, trafikdata och lagrat innehåll i meddelanden som innehas av internet- och telefonföretag och andra utomstående tjänsteleverantörer regleras av ytterligare bestämmelser i avdelning II i lagen om elektronisk brevhemlighet, som även kallas lagen om lagrade meddelanden (*Stored Communications Act* – SCA), 18 U.S.C. §§ 2701–2712. I lagen om lagrade meddelanden fastställs ett system för obligatoriska rättigheter avseende integritetsskydd som begränsar brottsbekämpande myndigheters tillgång till uppgifter utöver vad som krävs enligt konstitutionell rätt från kunder och abonnenter till internetleverantörer. Lagen föreskriver ett ökat integritetsskydd beroende på hur inkräktande insamlingen är. För abonnentregisterinformation måste de brottsbekämpande myndigheterna inhämta ett föreläggande för att få tillgång till IP-adresser och deras tidsmarkeringar samt faktureringsinformation. För de flesta andra typer av lagrad innehållslös information, såsom e-postrubriker utan ämnesrad, måste brottsbekämpande myndigheter anföra särskilda fakta inför domstol som visar att den begärda informationen är relevant och väsentlig för en pågående brottsutredning. För att få tillgång till lagrat innehåll i elektroniska meddelanden måste de brottsbekämpande myndigheterna i allmänhet inhämta en rannsakningsorder från en domare som grundas på en rimlig orsak att anse att kontot i fråga innehåller bevis på brott. Lagen om lagrade meddelanden föreskriver även skadestånd och straffrättsliga påföljder.

Domstolsbeslut om övervakning enligt den federala avlyssningslagen: Brottsbekämpande myndigheter kan dessutom fånga upp trådmeddelanden, muntliga meddelanden eller elektroniska meddelanden i realtid för brottsutredningssyften enligt den federala avlyssningslagen. *Se* 18 U.S.C. §§ 2510–2522. Denna befogenhet får endast utövas enligt ett domstolsbeslut där en domare bland annat finner att det finns en rimlig orsak att anse att avlyssning eller elektronisk

övervakning kommer att ge bevis för ett federalt brott eller uppgift om var en person som är på flykt från åtal uppehåller sig. Lagen föreskriver skadestånd och straffrättsliga påföljder för överträdelser av avlyssningsbestämmelserna.

Husrannsakan – regel 41: Brottsbekämpande åtgärder kan fysiskt genomsöka platser i Förenta staterna om de får tillstånd från en domare. Den brottsbekämpande myndigheten måste visa för domaren att det finns en ”rimlig grund” för att ett brott har begåtts eller står i begrepp att begås och att föremål som har samband med brottet sannolikt finns på den plats som anges i husrannsakan. Denna befogenhet används ofta när polisen måste göra en fysisk genomsökning av en plats på grund av risken för att bevis kan förstöras om ett föreläggande eller en annat beslut om att producera bevis delges företaget. Se Förenta staterna:s konstitution, tillägg IV (diskuteras närmare ovan), Fed. R. Crim. s. 41. Föremålet för en husrannsakan kan vidta åtgärder för att häva ordern om den är för allmänt hållen, trakasserande eller har erhållits på olämpligt sätt. En förfördelad person som har giltiga skäl kan vidta åtgärder för att upphäva eventuella bevis som påträffats till följd av en olaglig husrannsakan. Se Mapp mot Ohio, 367 U.S. 643 (1961).

Amerikanska justitieministeriets riktlinjer och policyer: Förutom dessa konstitutionella, lagstadgade och regelbaserade begränsningar av regeringens tillgång till uppgifter har justitieministern utfärdat riktlinjer med ytterligare begränsningar av brottsbekämpande myndigheters tillgång till uppgifter, som även föreskriver integritetsskydd och skydd av de medborgerliga fri- och rättigheterna. T.ex. justitieministerns riktlinjer för FBI:s verksamhet (september 2008) (nedan kallade *justitieministerns FBI-riktlinjer*), se http://www.justice.gov/archive/opa/docs/guidelines.pdf, begränsar användningen av undersökningsmetoder för sökning av information förknippad med utredningar som omfattar federala brott. Enligt riktlinjerna ska FBI använda utredningsmetoder som inkräktar så lite som möjligt, med tanke på följderna för integritetsskyddet och de medborgerliga fri- och rättigheterna samt eventuellt skadat förtroende. I riktlinjerna påpekas dessutom att ”det är självklart att FBI måste genomföra sina utredningar och andra verksamheter på ett lagligt och rimligt sätt som respekterar friheten och integritetsskyddet och bidrar till att undvika onödigt inkräktande i laglydiga människors liv”. Se justitieministerns FBI-riktlinjer, s. 5. FBI har genomfört dessa riktlinjer genom vägledningen *FBI Domestic Investigations and Operations Guide* (DIOG), se https://vault.fbi.gov/FBI%20Domestic%20Investigations%20and%20Operations%20Guide%20(DIOG), en omfattande handbok med detaljerade begränsningar av användningen av utredningsverktyg samt vägledning för att säkerställa att de medborgerliga fri- och rättigheterna och integritetsskyddet respekteras i alla utredningar. Ytterligare regler och förfaranden som föreskriver begränsningar av federala åklagares utredningar anges i ***United States Attorneys' Manual*** (USAM), finns även på nätet: http://www.justice.gov/usam/united-states-attorneys-manual.

Civila myndigheter och tillsynsmyndigheter (allmänhetens intresse):

Det finns även avsevärda begränsningar av civila myndigheters och tillsynsmyndigheters (dvs. ”allmänintresset”) tillgång till uppgifter som innehas av företag i Förenta staterna. Myndigheter med samhälls- och tillsynsansvar kan utfärda förelägganden till företag för att inhämta företagsregister, elektroniskt lagrad information eller andra konkreta föremål. Dessa myndigheter omfattas av begränsningar i utövandet av sin administrativa eller civila befogenhet att utfärda förelägganden, inte bara av sina egna regler, utan även genom oberoende rättslig granskning av förelägganden innan ett eventuellt rättsligt verkställande. Se t.ex. Fed. R. Civ. s. 45. Myndigheter kan endast begära åtkomst till uppgifter som är relevanta för frågor som omfattas av deras tillsynsbefogenhet. En person som mottar ett administrativt föreläggande kan dessutom bestrida verkställandet av detta i domstol genom att lägga fram bevis för att myndigheten inte har agerat enligt grundläggande skälighetsnormer, vilket har diskuterats tidigare.

Det finns andra rättsliga grunder för företag att bestrida administrativa myndigheters förfrågningar om åtkomst till uppgifter som grundas på den bransch som företaget är verksamt i och vilka typer av uppgifter som de innehar. Finansinstitut kan t.ex. bestrida administrativa förelägganden om tillgång till vissa typer av information genom att hävda att de strider mot lagen om banksekretess och dess genomförandeföreskrifter. *Se* 31 U.S.C. § 5318, 31 C.F.R. del X. Andra företag kan hänvisa till lagen om rättvis kreditrapportering, se 15 U.S.C. § 1681b eller en samling andra branschspecifika lagar. Om en myndighet missbrukar sin befogenhet att utfärda förelägganden kan myndigheten eller dess tjänstemän bli skadeståndsskyldiga. *Se t.ex. Right to Financial Privacy Act*, 12 U.S.C. §§ 3401–3422. Domstolar i Förenta staterna är därför väktare mot olämpliga lagstadgade förfrågningar och utövar oberoende tillsyn av federala myndigheters verksamhet.

Avslutningsvis måste administrativa myndigheters eventuella lagstadgade befogenheter att fysiskt beslagta register som tillhör företag i Förenta staterna inom ramen för en administrativ genomsökning uppfylla kraven i fjärde tillägget. Se See mot City of Seattle, 387 U.S. 541 (1967).

Slutsats

All brottsbekämpande verksamhet och tillsynsverksamhet i Förenta staterna måste uppfylla tillämplig lagstiftning, inklusive Förenta staterna:s konstitution, lagar, regler och föreskrifter. Sådana verksamheter måste också överensstämma med tillämpliga riktlinjer, bland annat justitieministerns riktlinjer för federal brottsbekämpningsverksamhet. Den rättsliga ram som beskrivs ovan begränsar amerikanska brottsbekämpnings- och tillsynsmyndigheters möjligheter att erhålla information från företag i Förenta staterna, vare sig informationen rör amerikanska eller utländska medborgare, och föreskriver dessutom rättslig granskning av eventuella regeringsförfrågningar om uppgifter enligt dessa befogenheter.

Högaktningsfullt,

Bruce C. Swartz

Vice justitieminister och rådgivare för internationella frågor