Jurnalul Oficial al Uniunii Europene

C 463

Anul 59

Ediția în limba română

Comunicări și informări

13 decembrie 2016

Cuprins

RO

[1] Text cu relevanță pentru SEE

[1] Text cu relevanță pentru SEE

ALTE ACTE

Comisia Europeană

II

(Comunicări)

COMUNICĂRI PROVENIND DE LA INSTITUȚIILE, ORGANELE ȘI ORGANISMELE UNIUNII EUROPENE

COMISIA EUROPEANĂ

Nonopoziție la o concentrare notificată

(Cazul M.8260 – DCNS/SPI/DCNS Energies)

(Text cu relevanță pentru SEE)

(2016/C 463/01)

La 5 decembrie 2016, Comisia a decis să nu se opună concentrării notificate menționate mai sus și să o declare compatibilă cu piața internă. Prezenta decizie se bazează pe articolul 6 alineatul (1) litera (b) din Regulamentul (CE) nr. 139/2004 al Consiliului [1]. Textul integral al deciziei este disponibil doar în limba franceză și va fi făcut public după ce vor fi eliminate orice secrete de afaceri pe care le-ar putea conține. Va fi disponibil:

— pe site-ul internet al Direcției Generale Concurență din cadrul Comisiei, în secțiunea consacrată concentrărilor (http://ec.europa.eu/competition/mergers/cases/). Acest site internet oferă diverse facilități care permit identificarea deciziilor de concentrare individuale, inclusiv întreprinderea, numărul cazului, data și indexurile sectoriale;

— în format electronic, pe site-ul internet EUR-Lex (http://eur-lex.europa.eu/homepage.html?locale=ro), cu numărul de document 32016M8260. EUR-Lex permite accesul online la legislația europeană.

[1] JO L 24, 29.1.2004, p. 1.

Nonopoziție la o concentrare notificată

(Cazul M.8268 – Norinco/Delphi's Mechatronics Business)

(Text cu relevanță pentru SEE)

(2016/C 463/02)

La 2 decembrie 2016, Comisia a decis să nu se opună concentrării notificate menționate mai sus și să o declare compatibilă cu piața internă. Prezenta decizie se bazează pe articolul 6 alineatul (1) litera (b) din Regulamentul (CE) nr. 139/2004 al Consiliului [1]. Textul integral al deciziei este disponibil doar în limba engleză și va fi făcut public după ce vor fi eliminate orice secrete de afaceri pe care le-ar putea conține. Va fi disponibil:

— pe site-ul internet al Direcției Generale Concurență din cadrul Comisiei, în secțiunea consacrată concentrărilor (http://ec.europa.eu/competition/mergers/cases/). Acest site internet oferă diverse facilități care permit identificarea deciziilor de concentrare individuale, inclusiv întreprinderea, numărul cazului, data și indexurile sectoriale;

— în format electronic, pe site-ul internet EUR-Lex (http://eur-lex.europa.eu/homepage.html?locale=ro), cu numărul de document 32016M8268. EUR-Lex permite accesul online la legislația europeană.

[1] JO L 24, 29.1.2004, p. 1.

IV

(Informări)

INFORMĂRI PROVENIND DE LA INSTITUȚIILE, ORGANELE ŞI ORGANISMELE UNIUNII EUROPENE

CONSILIU

Aviz în atenția persoanelor care fac obiectul măsurilor restrictive prevăzute în Decizia 2010/788/PESC a Consiliului, astfel cum a fost modificată prin Decizia (PESC) 2016/2231 a Consiliului, și în Regulamentul (CE) nr. 1183/2005 al Consiliului, astfel cum a fost modificat prin Regulamentul (UE) 2016/2230 privind adoptarea de măsuri restrictive împotriva Republicii Democratice Congo

(2016/C 463/03)

Informațiile de mai jos sunt aduse la cunoștința persoanelor care figurează în anexa II la Decizia 2010/788/PESC a Consiliului [1] și în anexa Ia la Regulamentul (CE) nr. 1183/2005 al Consiliului [2] de instituire a anumitor măsuri speciale împotriva Republicii Democratice Congo.

Consiliul Uniunii Europene a decis că persoanele care figurează în anexele menționate anterior ar trebui incluse pe lista persoanelor și entităților care fac obiectul măsurilor restrictive prevăzute în Decizia 2010/788/PESC și în Regulamentul (CE) nr. 1183/2005 de instituire a anumitor măsuri speciale împotriva Republicii Democratice Congo. Motivele pentru desemnarea persoanelor respective sunt prezentate în rubricile corespunzătoare din anexele menționate.

Se atrage atenția persoanelor în cauză asupra posibilității de a prezenta o cerere autorităților competente ale statului sau statelor membre relevante, astfel cum se precizează pe site-urile web menționate în anexa II la Regulamentul (CE) nr. 1183/2005 al Consiliului, pentru a obține o autorizație de a utiliza fonduri înghețate pentru nevoi esențiale sau pentru plăți specifice (cf. articolul 3 din regulament).

Persoanele în cauză pot trimite Consiliului, înainte de 1 octombrie 2017, o cerere însoțită de documente doveditoare, solicitând reanalizarea deciziei pe baza căreia au fost incluse pe listele menționate anterior, la următoarea adresă:

Consiliul Uniunii Europene
Secretariatul General
DG C 1C
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-mail: sanctions@consilium.europa.eu

Orice observație primită va fi luată în considerare în vederea reexaminării următoare a Consiliului, în conformitate cu articolul 9 din Decizia 2010/788/PESC.

Se atrage atenția persoanelor în cauză asupra posibilității de a contesta decizia Consiliului în fața Tribunalului Uniunii Europene, în conformitate cu condițiile stabilite la articolul 275 paragraful al doilea și la articolul 263 paragrafele al patrulea și al șaselea din Tratatul privind funcționarea Uniunii Europene.

---

[1] JO L 336, 21.12.2010, p. 30.
[2] JO L 193, 23.7.2005, p. 1.

Aviz în atenția persoanelor vizate care fac obiectul măsurilor restrictive prevăzute în Regulamentul (CE) nr. 1183/2005 al Consiliului de instituire a anumitor măsuri speciale împotriva persoanelor ale căror acțiuni încalcă embargoul asupra armelor impus Republicii Democratice Congo

(2016/C 463/04)

În conformitate cu articolul 12 din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([1]), se atrage atenția persoanelor vizate asupra următoarelor informații:

Temeiul juridic al acestei operațiuni de prelucrare îl reprezintă Regulamentul (CE) nr. 1183/2005 al Consiliului ([2]).

Controlorul acestei operațiuni de prelucrare este Consiliul Uniunii Europene, reprezentat de Directorul general al DG C (Afaceri Externe, extindere și protecție civilă) a Secretariatului General al Consiliului, iar departamentul însărcinat cu operațiunea de prelucrare este Unitatea 1C din cadrul DG C, care poate fi contactată la următoarea adresă:

Consiliul Uniunii Europene
Secretariatul General
DG C 1C
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-mail: sanctions@consilium.europa.eu

Scopul operațiunii de prelucrare este stabilirea și actualizarea listei persoanelor care fac obiectul măsurilor restrictive prevăzute în Regulamentul (CE) nr. 1183/2005.

Persoanele vizate sunt persoanele fizice care îndeplinesc criteriile de includere pe listă, conform prevederilor regulamentului respectiv.

Datele cu caracter personal colectate cuprind datele necesare identificării corecte a persoanei în cauză, expunerea de motive și orice alte date conexe.

Datele cu caracter personal colectate pot fi partajate, dacă este necesar, cu Serviciul European de Acțiune Externă și cu Comisia.

Fără a aduce atingere restricțiilor prevăzute la articolul 20 alineatul (1) literele (a) și (d) din Regulamentul (CE) nr. 45/2001, se va răspunde la cererile de acces, precum și la cererile de rectificare sau la obiecții în conformitate cu secțiunea 5 din Decizia 2004/644/CE a Consiliului ([3]).

Datele cu caracter personal vor fi păstrate timp de cinci ani din momentul în care persoana vizată a fost eliminată de pe lista persoanelor care fac obiectul înghețării activelor sau din momentul în care măsura a expirat, sau pe durata procedurilor judiciare, în cazul în care acestea au demarat.

Persoanele vizate pot sesiza Autoritatea Europeană pentru Protecția Datelor în conformitate cu Regulamentul (CE) nr. 45/2001.

([1]) JO L 8, 12.1.2001, p. 1.
([2]) JO L 193, 23.7.2005, p. 1.
([3]) JO L 296, 21.9.2004, p. 16.

Aviz în atenția persoanelor cărora li se aplică măsurile restrictive prevăzute în Decizia 2011/72/PESC a Consiliului și în Regulamentul (UE) nr. 101/2011 al Consiliului privind măsuri restrictive împotriva anumitor persoane, entități și organisme având în vedere situația din Tunisia

(2016/C 463/05)

Următoarele informații sunt aduse la cunoștința persoanelor care figurează în anexa la Decizia 2011/72/PESC a Consiliului [1] și în anexa I la Regulamentul (UE) nr. 101/2011 al Consiliului [2] privind măsuri restrictive împotriva anumitor persoane, entități și organisme având în vedere situația din Tunisia.

Consiliul intenționează să reînnoiască măsurile restrictive prevăzute în Decizia 2011/72/PESC. Consiliul deține la dosar anumite elemente noi privind toate persoanele care figurează pe lista din anexa la Decizia 2011/72/PESC și din anexa I la Regulamentul (UE) nr. 101/2011. Persoanele vizate sunt informate cu privire la faptul că pot depune o cerere adresată Consiliului pentru a obține informațiile care le privesc, înainte de 18 decembrie 2016, la următoarea adresă:

Consiliul Uniunii Europene
Secretariatul General
DG C 1C
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-mail: sanctions@consilium.europa.eu

Orice observații primite vor fi luate în considerare în scopul reexaminării periodice de către Consiliu, în conformitate cu articolul 5 din Decizia 2011/72/PESC și cu articolul 12 alineatul (4) din Regulamentul (UE) nr. 101/2011.

---

[1] JO L 28, 2.2.2011, p. 62.
[2] JO L 31, 5.2.2011, p. 1.

Aviz în atenția persoanelor cărora li se aplică măsurile restrictive prevăzute în Regulamentul (UE) nr. 101/2011 al Consiliului privind măsuri restrictive împotriva anumitor persoane, entități și organisme având în vedere situația din Tunisia

(2016/C 463/06)

În conformitate cu articolul 12 din Regulamentul (CE) nr. 45/2001 al Parlamentului European și al Consiliului ([1]), se atrage atenția persoanelor vizate asupra următoarelor informații:

Temeiul juridic al acestei operațiuni de prelucrare îl reprezintă Regulamentul (UE) nr. 101/2011 al Consiliului ([2]).

Controlorul acestei operațiuni de prelucrare este Consiliul Uniunii Europene, reprezentat de directorul general al DG C (Afaceri Externe, Extindere și Protecție Civilă) a Secretariatului General al Consiliului, iar departamentul însărcinat cu operațiunea de prelucrare este Unitatea 1C din cadrul DG C, care poate fi contactată la următoarea adresă:

Consiliul Uniunii Europene
Secretariatul General
DG C 1C
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-mail: sanctions@consilium.europa.eu

Scopul operațiunii de prelucrare este stabilirea și actualizarea listei persoanelor care fac obiectul măsurilor restrictive în conformitate cu Regulamentul (UE) nr. 101/2011.

Persoanele vizate sunt persoanele fizice care îndeplinesc criteriile de includere pe listă, conform prevederilor regulamentului respectiv.

Datele cu caracter personal colectate cuprind datele necesare identificării corecte a persoanei în cauză, expunerea de motive și orice alte date conexe.

Datele cu caracter personal colectate pot fi partajate, dacă este necesar, cu Serviciul European de Acțiune Externă și cu Comisia.

Fără a aduce atingere restricțiilor prevăzute la articolul 20 alineatul (1) literele (a) și (d) din Regulamentul (CE) nr. 45/2001, se va răspunde la cererile de acces, precum și la cererile de rectificare sau la obiecții în conformitate cu secțiunea 5 din Decizia 2004/644/CE a Consiliului ([3]).

Datele cu caracter personal vor fi păstrate timp de cinci ani din momentul în care persoana vizată a fost eliminată de pe lista persoanelor care fac obiectul înghețării activelor sau din momentul în care măsura a expirat, sau pe durata procedurilor judiciare, în cazul în care acestea au demarat.

Persoanele vizate pot sesiza Autoritatea Europeană pentru Protecția Datelor în conformitate cu Regulamentul (CE) nr. 45/2001.

([1]) JO L 8, 12.1.2001, p. 1.
([2]) JO L 31, 5.2.2011, p. 1.
([3]) JO L 296, 21.9.2004, p. 16.

Aviz în atenția unei persoane căreia i se aplică măsurile restrictive prevăzute în Decizia 2014/119/PESC a Consiliului și în Regulamentul (UE) nr. 208/2014 al Consiliului privind măsuri restrictive împotriva anumitor persoane, entități și organisme având în vedere situația din Ucraina

(2016/C 463/07)

Următoarele informații sunt aduse la cunoștința domnului Viktor Ivanovych Ratushniak al cărui nume figurează în anexa la Decizia 2014/119/PESC a Consiliului [1] și în anexa I la Regulamentul (UE) nr. 208/2014 al Consiliului [2] privind măsuri restrictive împotriva anumitor persoane, entități și organisme având în vedere situația din Ucraina.

În urma reexaminării listei persoanelor desemnate în Decizia 2014/119/PESC și în Regulamentul (UE) nr. 208/2014, Consiliul intenționează să reînnoiască măsurile din actele respective.

Consiliul intenționează să mențină măsurile restrictive împotriva persoanei sus-menționate. Prin urmare, persoana sus-menționată este informată că poate transmite Consiliului o cerere pentru a obține elementele pe care Consiliul le deține la dosarul privind desemnarea sa, înainte de 19 decembrie 2016, la următoarea adresă:

Consiliul Uniunii Europene
Secretariatul General
DG C 1C
Rue de la Loi/Wetstraat 175
1048 Bruxelles/Brussel
BELGIQUE/BELGIË

E-mail: sanctions@consilium.europa.eu

În acest sens, se atrage atenția persoanei vizate asupra reexaminării periodice de către Consiliu a listei persoanelor desemnate în Decizia 2014/119/PESC și în Regulamentul (UE) nr. 208/2014. Pentru ca observațiile să fie analizate la următoarea revizuire, acestea ar trebui prezentate până la 13 ianuarie 2017.

[1] JO L 66, 6.3.2014, p. 26.
[2] JO L 66, 6.3.2014, p. 1.

COMISIA EUROPEANĂ

Rata de schimb a monedei euro [1]

12 decembrie 2016

(2016/C 463/08)

1 euro =

	Moneda	Rata de schimb		Moneda	Rata de schimb
USD	dolar american	1,0596	CAD	dolar canadian	1,3918
JPY	yen japonez	122,69	HKD	dolar Hong Kong	8,2211
DKK	coroana daneză	7,4371	NZD	dolar neozeelandez	1,4793
GBP	lira sterlină	0,83900	SGD	dolar Singapore	1,5145
SEK	coroana suedeză	9,7445	KRW	won sud-coreean	1 237,73
CHF	franc elvețian	1,0772	ZAR	rand sud-african	14,5441
ISK	coroana islandeză		CNY	yuan renminbi chinezesc	7,3225
NOK	coroana norvegiană	8,9498	HRK	kuna croată	7,5335
BGN	leva bulgărească	1,9558	IDR	rupia indoneziană	14 121,82
CZK	coroana cehă	27,027	MYR	ringgit Malaiezia	4,6750
HUF	forint maghiar	314,02	PHP	peso Filipine	52,720
PLN	zlot polonez	4,4530	RUB	rubla rusească	64,8661
RON	leu românesc nou	4,5073	THB	baht thailandez	37,764
TRY	lira turcească	3,7269	BRL	real brazilian	3,5953
AUD	dolar australian	1,4174	MXN	peso mexican	21,4472
			INR	rupie indiană	71,4485

[1] *Sursă*: rata de schimb de referință publicată de către Banca Centrală Europeană.

AUTORITATEA EUROPEANĂ PENTRU PROTECȚIA DATELOR

Rezumatul avizului Autorității Europene pentru Protecția Datelor privind eficacitatea aplicării legii în economia societății digitale

(Textul integral al prezentului aviz poate fi consultat în limbile engleză, franceză și germană pe site-ul AEPD www.edps.europa.eu)

(2016/C 463/09)

Prelucrarea informațiilor cu caracter personal este indispensabilă pentru serviciile bazate pe internet. Strategia Uniunii Europene privind piața unică digitală recunoaște potențialul tehnologiilor și al serviciilor bazate pe date de a servi drept catalizator pentru creșterea economică. Serviciile de acest tip prestate pe internet au ajuns să depindă de urmărirea – adesea disimulată – a persoanelor, care nu sunt în general conștiente de natura și amploarea acestei urmăriri. Societățile comerciale care domină aceste piețe ar putea fi în măsură să le blocheze accesul la piață noilor participanți, care le fac concurență prin factori benefici din punctul de vedere al drepturilor și intereselor persoanelor, și ar putea impune clauze și condiții inechitabile, care să exploateze în mod abuziv consumatorii. Dezechilibrul care crește vizibil dintre furnizorii de servicii pe internet și consumatori ar putea să reducă diversitatea opțiunilor, capacitatea de inovare și calitatea elementelor de protecție a vieții private. Acest dezechilibru poate conduce și la creșterea prețului efectiv – în ceea ce privește divulgarea datelor cu caracter personal – cu mult mai mult decât ar fi de așteptat pe piețe perfect competitive.

În 2014, AEPD a emis un aviz preliminar privind viața privată și competitivitatea în epoca bazelor de date de dimensiuni foarte mari. În pofida unor sinergii evidente în ceea ce privește aspecte precum transparența, simțul răspunderii, diversitatea opțiunilor și bunăstarea generală, am observat tendința ca normele UE privind protecția datelor, protecția consumatorilor, aplicarea legilor antitrust și controlul concentrărilor economice să fie aplicate izolat unele de altele. Prin urmare, am lansat o dezbatere pe tema modalității de a aplica obiectivele și standardele UE într-o manieră mai holistică. În acest nou aviz se argumentează că Strategia privind piața unică digitală oferă ocazia unei abordări coerente și se actualizează avizul preliminar din 2014, adresându-se instituțiilor UE câteva recomandări practice pentru remedierea situației. Avizul abordează îngrijorarea crescândă față de faptul că o concentrare pe piețele digitale ar putea dăuna intereselor oamenilor, în calitate de persoane vizate și de consumatori.

Instituțiile și organismele UE, precum și autoritățile naționale atunci când aplică legislația UE, au obligația de a respecta drepturile și libertățile prevăzute în Carta drepturilor fundamentale a Uniunii Europene. Mai multe dintre aceste dispoziții, printre care dreptul la viață privată și la protecția datelor cu caracter personal, libertatea de exprimare și nediscriminarea, sunt periclitate de comportamentul normativ și de standardele care predomină în prezent în spațiul cibernetic. Uniunea Europeană dispune deja de suficiente instrumente pentru a combate distorsiunile pieței care acționează împotriva intereselor persoanelor și ale societății în general. Este posibil ca o serie de practici de pe piețele digitale să încalce două sau mai multe cadre juridice aplicabile, fiecare bazat pe noțiunea de „corectitudine". Asemenea mai multor studii din ultimele luni, facem apel la mai mult dialog, la învățarea lecțiilor și chiar la o colaborare între cei care stabilesc normele de comportament în mediul digital. De asemenea, subliniem necesitatea ca UE să creeze – atât online, cât și offline – condiții propice pentru drepturile și libertățile stipulate în cartă.

Prin urmare, prezentul aviz recomandă stabilirea unui mecanism digital de schimb de informații pentru aplicarea legii în sectorul digital al UE, o rețea voluntară de organisme de reglementare care fac schimb de informații, în mod voluntar și în limitele lor de competență, cu privire la posibilele abuzuri din ecosistemul digital și la cea mai bună metodă de abordare a acestora. La acest mecanism ar trebui să se adauge orientări de aplicare coerentă a normelor de protecție a persoanelor de către autoritățile de reglementare. De asemenea, recomandăm ca instituțiile UE care colaborează cu experți externi să exploreze posibilitatea de a crea un spațiu comun pe internet, în care persoanele să poată interacționa fără a fi urmărite, în conformitate cu carta. În sfârșit, recomandăm actualizarea normelor de aplicare a controalelor concentrărilor economice de către autorități în vederea unei mai bune protecții a vieții private, a informațiilor cu caracter personal și a libertății de exprimare în mediul online.

I. ÎN DESCHIDEREA DEZBATERII

1. Contextul și structura prezentului aviz

Avizul nostru preliminar privind „viața privată și competitivitatea în epoca bazelor de date de dimensiuni foarte mari" din 2014 (denumit în continuare „avizul preliminar") a comparat cadrele legislative ale UE privind protecția datelor,

concurența și consumatorii și a ajuns la concluzia că există câteva sinergii evidente în contextul piețelor digitale ([1]). Am adresat instituțiilor UE câteva recomandări provizorii, care au fost îmbunătățite în urma unui atelier de lucru găzduit de AEPD în iunie 2014 ([2]), printre care:

1. să înțeleagă mai bine „valoarea" datelor cu caracter personal pe piețele digitale și să revizuiască metodologiile de analiză a pieței, în special a serviciilor prestate pe internet și promovate ca „gratuite", cu o analiză retrospectivă sau ex-post a impactului deciziilor de aplicare a legii;

2. să analizeze modalități de încurajare a tehnologiilor care protejează viața privată pentru a obține un avantaj competitiv;

3. să revizuiască legislația UE în contextul relevanței sale pentru piețele digitale ale secolului al XXI-lea;

4. să gândească etape practice în vederea cooperării între autorități, inclusiv a unui dialog mai strâns și a unor investigații comune.

VI. **CONCLUZIE**

Drepturile omului au fost concepute ca mijloc de protecție a persoanelor împotriva ingerinței statului. Politica antitrust își are rădăcinile în deciziile politice de stopare a puterii abuzive de monopol, în beneficiul societății în ansamblu. Drepturile consumatorilor au apărut ca un bastion împotriva comercianților abuzivi.

Oportunitățile create de bazele de date de dimensiuni foarte mari în sensul stimulării productivității și a conectivității ar trebui să fie însoțite de măsuri de protecție a informațiilor conținute în ele. În ultimii ani, UE a demonstrat excelente calități de lider în încercarea de a stimula o întrecere înspre atingerea celor mai înalte standarde de protejare a vieții private în mediul digital. Regulamentul general privind protecția datelor reprezintă un act normativ de referință pentru protejarea datelor cu caracter personal în economia digitală. Pentru ca economia și societatea digitală să se bazeze pe valorile Uniunii Europene, UE poate valorifica chiar mai mult instrumentele disponibile pentru a asigura existența unor produse și servicii care nu afectează viața privată și care respectă drepturile fundamentale. Mai multă transparență, tratament echitabil, posibilitate efectivă de a alege, neblocarea accesului la piață pentru modelele care nu urmăresc utilizatorii – toate acestea sunt obiective întru totul compatibile și complementare.

Strategia privind piața unică digitală îi oferă Uniunii Europene ocazia potrivită de a se îndrepta spre aceste obiective într-o manieră coerentă. Aplicarea efectivă a normelor existente în dreptul UE prezintă o importanță capitală. Considerăm că recomandările noastre pentru crearea unui mecanism digital de schimb de informații, combinat cu o abordare mai holistică a concentrărilor și cu promovarea unui spațiu comun bazat pe valorile UE, ar constitui importanți pași înainte. Într-un moment în care legile privind protecția datelor și dreptul la viață privată proliferează în întreaga lume, acest mecanism ar trebui să fie o platformă pentru construirea unor punți mai mari către alte regiuni ale lumii, permițând un grad mai înalt de dialog și de cooperare cu toate țările care se confruntă cu aceeași provocare digitală.

Acesta nu reprezintă cuvântul final în discuția de față. AEPD intenționează să faciliteze în continuare discuțiile și să ajute la eliminarea fragmentărilor care împiedică protejarea intereselor și drepturilor persoanelor.

Adoptat la Bruxelles, 23 septembrie 2016.

Giovanni BUTTARELLI

Autoritatea Europeană pentru Protecția Datelor

([1]) Avizul preliminar al AEPD „Viața privată și competitivitatea în epoca bazelor de date de dimensiuni foarte mari, interacțiunea dintre protecția datelor, legea concurenței și protecția consumatorilor în economia digitală", martie 2014.

([2]) „Raportul atelierului de lucru privind viața privată, consumatorii, concurența și bazele de date de dimensiuni foarte mari, 2 iunie 2014"; https://secure.edps.europa.eu?EDPSWEB/webdav/site/mySite/shared/Documents/consultation/Big%20data

Rezumatul avizului Autorității Europene pentru Protecția Datelor privind sistemele de management al datelor cu caracter personal

(Textul integral al prezentului aviz poate fi consultat în limbile engleză, franceză și germană pe site-ul AEPD www.edps.europa.eu)

(2016/C 463/10)

Acest aviz explorează conceptul tehnologiilor și al ecosistemelor care vizează autorizarea persoanelor fizice în ceea ce privește controlul asupra dezvăluirii datelor cu caracter personal („sisteme de management al informațiilor cu caracter personal" sau „SMICP" pe scurt).

Viziunea noastră implică crearea unei noi realități, în care persoanele fizice să își gestioneze și să își controleze identitatea online. Scopul nostru este de a transforma sistemul actual centrat pe furnizor într-un sistem centrat pe om, unde persoanele fizice să fie protejate contra procesării ilegale a datelor și contra urmăririi și tehnicilor intruzive de creare a profilurilor, care vizează eludarea principiilor referitoare la protejarea datelor principale.

Această nouă realitate va fi facilitată de cardul modernizat de reglementare al UE și de posibilitățile oferite de aplicarea viguroasă și comună de către toate autoritățile de reglementare și supervizare relevante.

Regulamentul general privind protecția datelor (RGPD) consolidează și modernizează cadrul de reglementare astfel încât să rămână eficient în era Big Data prin sporirea încrederii persoanelor fizice în mediul online și în Piața Unică Digitală. Noile reguli, inclusiv cele referitoare la transparența sporită și drepturile puternice de acces și portabilitatea datelor, contribuie la posibilitatea utilizatorilor de a își controla mai bine propriile date și poate de asemenea oferi o contribuție la piețe mai eficiente pentru datele cu caracter personal, în beneficiul consumatorilor și al companiilor.

Recent am emis un aviz referitor la aplicarea efectivă a drepturilor fundamentale în era volumelor mari de date. Aceasta subliniază condițiile actuale ale pieței și practicile comerciale care creează obstacole pentru exercitarea efectivă a drepturilor persoanelor fizice la protecția datelor personale și alte drepturi fundamentale și apeluri pentru intensificarea aplicării concentrate și consecvente a legilor privind concurența, protecția consumatorilor și protecția datelor cu caracter personal. Sperăm ca această aplicare sporită va contribui la crearea condițiilor de piață în care serviciile favorabile confidențialității să se poată dezvolta. Abordarea din acest aviz vizează consolidarea drepturilor fundamentale în lumea noastră digitală și, în același timp, deschiderea de noi oportunități pentru dezvoltarea de către companii a unor servicii inovatoare, bazate pe date cu caracter personal, construite pe încredere reciprocă. SMICP promite să ofere nu numai o arhitectură tehnică și organizare pentru managementul datelor, ci și cadre de încredere și, ca urmare, modele alternative de afaceri pentru culegerea și procesarea datelor cu caracter personal în era volumelor mari de date, într-un mod care să respecte mai mult legea europeană privind protecția datelor.

În această aviz, descriem pe scurt ce sunt SMICP, care sunt problemele pe care își propun să le rezolve și cum. Apoi, analizăm modul în care contribuie la o protecție mai bună a datelor cu caracter personal și care sunt provocările cu care se confruntă. În final, identificăm modalități de a dezvolta oportunitățile oferite. Pentru dezvoltarea noilor modele de afaceri în domeniul protecției datelor, pot fi necesare stimulente suplimentare pentru furnizorii de servicii care le oferă. Ar trebui explorat îndeosebi, care dintre inițiativele în materie de politică ar putea motiva operatorii să accepte această modalitate de furnizare a datelor. Mai mult, o inițiativă a serviciilor publice de a accepta SMICP ca sursă de date în locul culegerii directe a acestora, ar putea fi cântări foarte mult în acceptarea SMICP.

Arhitectura emergentă a SMICP, ce vizează restabilirea controlului persoanelor fizice și al consumatorului în ceea ce privește propriile date cu caracter personal, merită considerație suplimentară, asistență și cercetare ulterioară în vederea contribuției la un mod sustenabil și etic de utilizare a volumelor mari de date și în vederea implementării efective a principiilor recent adoptatului RGPD.

I. SMICP: PARTAJAREA DATELOR, BENEFICII ALE PARTAJĂRII?

1. Condițiile actuale pentru procesarea datelor cu caracter personal sunt adesea injuste pentru persoanele fizice ale căror date sunt procesate. Condițiile legale și instrumentele tehnice fac ca exercitarea drepturilor persoanelor fizice să fie dificilă și permit operatorilor să își limiteze responsabilitatea. Brokerii de date, rețelele de publicitate, furnizorii de rețele sociale și alți jucători corporativi au dosare din ce în ce mai complete despre persoanele fizice participante la societatea digitală de azi și persoanele fizice pierd controlul asupra amprentelor digitale pe care le lasă în urmă. Persoanele fizice care adesea, independent de voința și fără cunoștința lor, sunt vizate de jucători care le

stabilesc profilul și le evaluează, se simt neajutorate și trebuie autorizate să preia controlul asupra propriilor identități. Chiar și atunci când li se transmite formal un tip de „notificare" și posibilitatea de a „fi de acord" cu termenii și condițiile generale, persoanele fizice se găsesc adesea într-un sistem conceput pentru a maximiza monetizarea datelor personale, care nu oferă persoanelor fizice posibilitatea reală de alegere sau control.

2. Comunicarea Comisiei Europene privind volumul mare de date ([1]) stabilește un plan de măsuri care vizează datele personale și protecția consumatorilor. Acest lucru încurajează în mod specific folosirea „spațiilor de date cu caracter personal", ca locuri sigure și securizate, centrate pe utilizator, pentru stocarea datelor cu caracter personal, care pot oferi posibilitatea altora să acceseze aceste date. Împărtășim părerea că instrumentele digitale inovatoare și modelele de afaceri bazate pe autorizarea persoanelor fizice, ar trebui încurajate. Acestea pot permite persoanelor fizice să beneficieze de o astfel de partajare a datelor, adică să participe la utilizarea și distribuirea informațiilor cu caracter personal.

3. În avizul nostru privind „Răspunsul la provocările volumelor mari de date" ([2]) am argumentat faptul că ar trebui să completăm obligația legală a aprobării eficiente cu un control real, practic asupra informațiilor cu caracter personal. Am argumentat faptul că *„în locul unei poveri administrative, furnizarea drepturilor de acces poate deveni o caracteristică a serviciului furnizat clientului"*, iar organizațiile bazate pe exploatarea volumelor mari de date ar trebui *„să fie pregătite să împartă averea creată prin procesarea datelor cu caracter personal cu acele persoane fizice ale căror date le procesează"*. În acest context, am menționat faptul că *„depozitele de date cu caracter personal ar putea fi de folos în ceea ce privește adresarea preocupărilor privind pierderea controlului asupra datelor cu caracter personal de către persoana fizică"*. Regulamentul general privind protecția datelor (RGPD), adoptat recent ([3]) a consolidat cerințele legale pentru consimțământ ([4]) și a introdus principii moderne, eficiente de protecție a datelor prin concept și implicit ([5]), precum și un drept nou legat de portabilitatea datelor ([6]). Pentru ca noul cadru general de protecție a datelor să-și îndeplinească promisiunea, avem nevoie de instrumente care să le permită persoanelor fizice să își exercite drepturile într-un mod convenabil, favorabil utilizatorului.

4. Acest aviz explorează noi tehnologii și ecosisteme care vizează autorizarea persoanelor fizice în ceea ce privește controlul asupra culegerii și partajării datelor cu caracter personal. Vom face referire la acest concept ca „sistemul de management al informațiilor cu caracter personal" („SMICP") ([7]). Conceptul SMICP oferă o nouă abordare conform căreia persoanele fizice sunt deținătoarele propriilor informații cu caracter personal. Se poate crea o schimbare a paradigmei în managementul și procesarea datelor cu caracter personal, cu consecințe sociale și economice. În schimb, arhitectura actuală a serviciilor online este caracterizată de un număr mic de furnizori de servicii, care domină piața prin monetizarea datelor cu caracter personal ale utilizatorilor în schimbul serviciilor „gratuite". Aceasta este adesea însoțită de un dezechilibru al puterii, unde clientul se confruntă cu o abordare de tipul „acceptă sau refuză" și de o asimetrie informatică între furnizorii de servicii și utilizatori, cu lipsă totală sau parțială de transparență pentru persoanele fizice în ceea ce privește lucrurile care se întâmplă cu datele lor personale.

5. Ideea de bază din spatele conceptului SMCIP este transformarea sistemului actual centrat pe furnizor într-un sistem centrat pe persoane fizice, capabil să gestioneze și să-și controleze identitatea online ([8]). În principiu, persoanele fizice ar trebui să poată decide dacă și cu cine partajează informațiile cu caracter personal și în ce scopuri, pentru cât timp și să le urmărească și să decidă să le retragă dacă se dorește acest lucru. Merită explorată modul în care SMCIP ar putea ajuta în ceea ce privește adresarea preocupărilor referitoare la pierderea controlului individual asupra datelor cu caracter personal, subliniat ca una dintre preocupările cheie referitoare la volumele mari de date ([9]).

([1]) Comunicarea COM(2014) 442 final privind o economie prosperă antrenată de date: https://ec.europa.eu/digital-single-market/en/news/communication-data-driven-economy

([2]) Avizul AEPD 7/2015. https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2015/15-11-19_Big_Data_EN.pdf A se vedea secțiunea 3, pentru alte detalii.

([3]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1).

([4]) A se vedea, printre altele, articolul 6 alineatul (1) litera (a), articolele 7 și 8 și expunerea de motive 42-43 RGPD.

([5]) Articolul 25 RGPD.

([6]) Articolul 20 RGPD.

([7]) Conceptele corelate includ „magazinele de date cu caracter personal", „spații pentru date cu caracter personal" sau „seifuri de date cu caracter personal". În acest aviz, vom folosi termenul „SMCIP", deoarece pare să descrie cel mai bine conceptul într-o manieră generală și ușor de înțeles. Așa cum este folosită în acest aviz, abrevierea „SMCIP" se poate referi fie la singular, fie la plural: sistem de management al informațiilor cu caracter personal sau sisteme de management al informațiilor cu caracter personal.

([8]) A se vedea expunerea de motive 7 RGPD: „Persoanele fizice ar trebui să aibă control asupra propriilor date cu caracter personal". A se vedea, de exemplu, Doc Searls, *Economia de intenție: când clientul preia controlul* (Boston, Harvard Business Review Press, 2012).

([9]) A se vedea, de exemplu, Ira S. Rubinstein, *Volumul mare de date: sfârșitul confidențialității sau un nou început? Legea internațională privind confidențialitatea datelor*, 2013, vol. 3, nr. 2.

6. Această abordare vizează consolidarea drepturilor fundamentale în lumea noastră digitală și, în același timp, deschiderea de noi oportunități pentru dezvoltarea de către companii a unor servicii inovatoare, bazate pe date cu caracter personal, construite pe încredere reciprocă. SMCIP promit să ofere o nouă arhitectură și organizare tehnică pentru managementul datelor, care va dezvolta cadre generale de încredere. Acestea speră să faciliteze modele alternative de afaceri pentru culegerea și procesarea datelor cu caracter personal în era volumelor mari de date, într-un mod care respectă mai mult legea europeană privind protecția datelor.

7. În această aviz, descriem pe scurt ce sunt SMICP, care sunt problemele pe care își propun să le rezolve și cum ([1]). Analizăm modul în care contribuie la o protecție mai bună a datelor cu caracter personal și care sunt provocările cu care se confruntă. În final, identificăm modalități de a dezvolta oportunitățile oferite.

IV. CONCLUZII ȘI ETAPELE URMĂTOARE

4.1. Către aplicarea completă a oportunităților RGPD

54. Așa cum s-a menționat mai sus, legiuitorul UE a adoptat un pachet de reforme privind protecția datelor cu caracter personal, care consolidează și modernizează cadrul general de reglementare, astfel încât să rămână în vigoare în era volumelor mari de date.

55. Noul RGPD, inclusiv cel referitor la transparența sporită și drepturile puternice de acces și portabilitatea datelor, ar trebui să ajute persoanele fizice să-și controleze mai bine propriile date și poate de asemenea oferi o contribuție la piețe mai eficiente pentru datele cu caracter personal, în beneficiul consumatorilor și al companiilor deopotrivă.

56. Codurile de conduită și schemele de certificare, în forma specificată pentru RGPD sunt instrumente privilegiate, care conferă vizibilitate specifică și un rol tehnologiei și produselor ca – la fel ca SMCIP – pot servi la implementarea mai eficientă a legii privind protecția datelor, la nivel practic.

57. Însă, SMCIP se confruntă cu dificultatea globală de penetrare a pieței dominată de serviciile online, bazate pe modele de afaceri și arhitecturi tehnice în care persoanele fizice nu au control asupra datelor, așa cum se explică în secțiunea 3.9. Trecerea la o situație în care persoanele fizice au posibilitatea efectivă de a da acces unui furnizor de servicii la unele date din SMCIP, în loc să furnizeze direct datele prestatorului de servicii, va necesita stimulente suplimentare pentru prestatorii de servicii. Comisia poate folosi inițiativele anunțate privind fluxurile de date și proprietatea datelor ([2]) pentru a explora care inițiative suplimentare de politici ar putea motiva operatorii de date să accepte acest mod de furnizare a datelor. Mai mult, o inițiativă a serviciilor publice de guvernare electronică, de a accepta SMCIP ca sursă de date în locul culegerii directe a acestora, ar putea fi cântări foarte mult în acceptarea SMCIP.

58. Această analiză ar putea fi completată de măsuri care să vizeze stabilirea unor fundații tehnice, sociale și economice, inclusiv eforturi de standardizare, stimulente economice și favorizarea de proiecte de cercetare și pilot.

59. Uniunea Europeană și administrațiile publice ale statelor membre și proiectele cofinanțate de acestea, sunt primele locuri unde ar trebui testată, favorizată și realizată această schimbare de perspectivă.

4.2. Susținerea SMICP și tehnologia subiacentă către protecția eficientă a datelor

60. Deși este esențială, o bună reglementare nu este suficientă în sine. Așa cum am menționat în avizul nostru privind „Răspunsul la provocările volumelor mari de date” ([3]), companiile și celelalte organizații care depun multe eforturi pentru a găsi căi inovatoare de utilizare a datelor cu caracter personal, care cu aceeași atitudine inovatoare, să pună în aplicare principiile protecției datelor.

([1]) A se vedea, de exemplu, raportul privind magazinele de date cu caracter personal, al Universității Cambridge pentru Comisia Europeană: https://ec.europa.eu/digital-single-market/en/news/study-personal-data-stores-conducted-cambridge-university-judge-business-school

([2]) Comunicare: „Industria europeană de digitalizare – Culegerea beneficiilor complete ale unei Piețe Digitale Unice” http://europa.eu/rapid/press-release_MEMO-16-1409_en.htm

([3]) Avizul AEPD 7/2015, citat mai sus.

61. Contribuția tehnologiei la modelul SMICP este fundamentală. SMICP poate servi la protecția datelor testate prin abordări conceptuale și tehnologii care să le susțină. Subiectele relevante de cercetare, unde sunt necesare asistența și investițiile adecvate, includ: managementul identității, interoperabil și favorabil confidențialității; mecanisme de autorizare; interoperabilitatea datelor; securitatea datelor și mecanisme pentru aplicarea automată a „contractelor" încheiate în persoanele fizice și celelalte părți. Toate acestea sunt influențate de criptografie și codificare și sunt amplificate de disponibilitatea puterii de calcul ieftine. Asistența decisivă a factorilor de decizie, cum ar fi Comisia, în ceea ce privește cercetarea de bază și cea aplicată în aceste domenii ale tehnologiei, este necesară în această etapă inițială, pentru a nu pierde oportunitățile curente.

62. Pentru a favoriza cercetarea, dezvoltarea și implementarea în piață în domeniul SMICP, recomandăm planificarea de către Comisie a posibilelor sinergii cu alte domenii ale strategiei Pieței Digitale Unice, cum ar fi Cloud Computing și Internetul obiectelor. Astfel, s-ar putea desfășura proiecte pilot și s-ar putea testa interacțiunea serviciilor de tip cloud și IoT cu SMICP.

4.3. **Cum va face AEPD să progreseze această dezbatere**

63. AEDP are drept scop contribuția la încurajarea eforturilor private și publice în direcția subliniată mai sus. Vom continua să facilităm discuțiile, inclusiv prin organizarea de evenimente/seminare de exemplu, vizând identificarea, încurajarea și promovarea celor mai bune practici pentru a mări transparența și controlul utilizatorului și pentru a explora oportunitățile oferite de SMICP. Vom continua de asemenea să facilităm lucrările la Rețeaua de Inginerie pentru Confidențialitatea pe internet (RICI) ca o platformă de cunoștințe interdisciplinare pentru ingineri și experți în confidențialitate. În acest context, vom continua să oferim o platformă dezvoltatorilor și promotorilor SMICP, pentru a beneficia de schimburi de experiență cu specialiști din alte domenii tehnologice și de protecție a datelor.

Adoptat la Marrakesh, 20 octombrie 2016.

Giovanni BUTTARELLI

Autoritatea Europeană pentru Protecția Datelor

Rezumatul avizului Autorității Europene pentru Protecția Datelor privind cel de-al doilea pachet UE cu privire la frontierele inteligente

(Textul integral al prezentului aviz poate fi consultat în limbile engleză, franceză și germană pe site-ul AEPD www.edps.europa.eu)

(2016/C 463/11)

REZUMAT

Organul legislativ al Uniunii are în vedere de mult timp instituirea unui sistem de intrare/ieșire (EES) care să înregistreze intrările și ieșirile resortisanților țărilor terțe pe teritoriul Uniunii Europene. Comisia a adoptat trei propuneri ca parte a primului pachet privind frontierele inteligente în 2013; colegiuitorii au manifestat preocupări serioase, motiv pentru care nu s-a ajuns la un acord referitor la pachet. Ulterior, Comisia a lansat un exercițiu de validare a conceptului ca răspuns la aceste preocupări și a lansat, în acest an, un al doilea pachet privind frontierele inteligente, de această dată compus din două propuneri revizuite.

AEPD a analizat cu atenție aceste propuneri și emite recomandări care vin în sprijinul legiuitorului pentru a garanta conformitatea deplină a cadrului juridic aplicabil sistemului EES cu dreptul UE privind protecția datelor și a vieții private, în special cu articolele 7 și 8 din Carta drepturilor fundamentale a Uniunii Europene.

AEPD admite necesitatea unor sisteme de informare coerente și eficiente pentru frontiere și securitate. Aceste propuneri vin într-un moment esențial, în care UE se confruntă cu provocări serioase în acest domeniu. Cu toate acestea, AEPD subliniază caracterul semnificativ și potențial invaziv al prelucrării propuse a datelor cu caracter personal în cadrul EES care, prin urmare, trebuie să fie luată în considerare în conformitate cu articolele 7 și 8 din Cartă. Se vor evalua necesitatea și proporționalitatea sistemului EES, atât la nivel global, luând în considerare sistemele informatice deja existente la scară largă în UE, cât și, în mod special, în cazul specific al acestor resortisanți ai țărilor terțe care sunt vizitatorii legali ai UE. AEPD ia act de faptul că datele EES vor fi prelucrate în două scopuri diferite, pe de o parte, pentru gestionarea frontierelor și în scopuri de facilitare și, pe de altă parte, în scopul aplicării legii. AEPD recomandă în mod insistent specificarea clară a diferenței dintre aceste obiective în întreaga propunere EES din 2016, deoarece aceste scopuri implică un impact diferit asupra drepturilor la viață privată și la protecția datelor.

Deși consideră oportună atenția acordată problemelor legate de confidențialitatea și protecția datelor exprimate anterior și îmbunătățirile în propunerile revizuite, AEPD manifestă îngrijorări serioase în ceea ce privește mai multe aspecte ale propunerii EES, care ar trebui să fie mai bine justificată sau chiar reanalizată de către legiuitor, în special:

— perioada de păstrare a datelor EES de cinci ani. AEPD ia act de faptul că necesitatea de păstrare a datelor referitoare la persoanele care depășesc termenul legal de ședere ar trebui să fie mai bine demonstrată și că un termen de păstrare de cinci ani a tuturor datelor cu caracter personal stocate în EES pare să fie disproporționat;

— colectarea imaginii faciale a persoanelor care călătoresc pe bază de viză, care este deja stocată în VIS;

— necesitatea de a asigura accesul autorităților de aplicare a legii la datele EES, care nu este susținută suficient de dovezi convingătoare;

— condiție preliminară de furnizare a amprentei digitale, aplicabilă persoanei vizate, în exercitarea drepturilor sale de acces, rectificare și/sau ștergere a datelor sale cu caracter personal, care ar putea constitui un obstacol important în calea exercitării efective a acestor drepturi.

Avizul prevede în continuare recomandări suplimentare în ceea ce privește protecția datelor și a vieții private, care ar trebui să fie luate în considerare în procesul legislativ, inclusiv securitatea sistemului.

I. INTRODUCERE ȘI CONTEXT

1. Comisia și-a anunțat pentru prima oară intenția de a construi un sistem european de intrare/ieșire cu scopul de a controla intrările și ieșirile resortisanților țărilor terțe în/din teritoriul Uniunii Europene în 2008 ([1]). La momentul respectiv, AEPD și-a exprimat observațiile preliminare ([2]) pe acest subiect și apoi a evidențiat aspecte specifice în avizul său din iulie 2011 ([3]). Comisia și-a elaborat în continuare punctul de vedere într-o comunicare ([4]) denumită *Frontiere inteligente – opțiuni și calea de urmat* din octombrie 2011, la care grupul de lucru „Articolul 29" a făcut observații ([5]). De asemenea, AEPD și-a oferit contribuția la o masă rotundă comună cu diferite părți interesate ([6]).

2. În februarie 2013, Comisia a adoptat trei propuneri ca parte a primului pachet privind frontierele inteligente: o propunere de instituire a unui sistem de intrare/ieșire ([7]) (denumită în continuare „Propunerea EES din 2013"), o propunere de instituire a unui program de înregistrare a călătorilor ([8]) (denumită în continuare „Propunerea RTP din 2013") și o propunere de modificare a Codului frontierelor Schengen ([9]) pentru a introduce aceste modificări în mod corespunzător. Pachetul a primit imediat critici din partea ambilor colegiuitori, ca urmare a problemelor tehnice, operaționale și a preocupărilor referitoare la costuri, precum și în ceea ce privește protecția datelor importante. În același an, AEPD a furnizat primele sale recomandări concrete cu privire la cele trei propuneri sub forma unui aviz ([10]). Grupul de lucru „Articolul 29" a emis, de asemenea, un aviz ([11]) la care AEPD a contribuit, care punea sub semnul întrebării însăși necesitatea unui sistem de intrare/ieșire.

3. Ca răspuns la aceste preocupări, la începutul anului 2014, Comisia a anunțat lansarea unui exercițiu de validare a conceptului care constă din două etape: mai întâi, un studiu tehnic ([12]) și un studiu privind costurile ([13]) în vederea identificării celor mai potrivite opțiuni și soluții pentru a pune în aplicare frontierele inteligente, urmate de un proiect-pilot, în cursul anului 2015 ([14]), condus de Agenția Europeană pentru Gestionarea Operațională a Sistemelor Informatice la Scară Largă în Spațiul de Libertate, Securitate și Justiție (denumită în continuare „eu-LISA"), cu scopul de a testa diferitele opțiuni identificate. În paralel, în iulie 2015 Comisia a lansat o consultare publică de trei luni ([15]) pentru a colecta punctele de vedere și opiniile cetățenilor și ale organizațiilor, la care a contribuit și AEPD ([16]).

4. La 6 aprilie 2016, Comisia a lansat un al doilea pachet privind frontierele inteligente ([17]). De data aceasta, se propune un singur sistem: sistemul de intrare/ieșire (denumit în continuare „EES"). Comisia a decis să-și revizuiască

([1]) Comunicarea Comisiei din 13 februarie 2008 privind „Pregătirea următoarelor etape ale gestionării frontierelor în Uniunea Europeană" COM(2008) 69 final.
([2]) Observațiile preliminare ale AEPD din 3 martie 2008 pe baza a trei comunicări privind gestionarea frontierelor.
([3]) Avizul AEPD din 7 iulie 2011 referitor la comunicarea privind migrația.
([4]) Comunicarea Comisiei din 25 octombrie 2011 privind „Frontierele inteligente - opțiuni și calea de urmat", COM(2011) 680 final.
([5]) Grupul de lucru „Articolul 29" a prezentat observații cu privire la Comunicarea Comisiei privind frontierele inteligente într-o scrisoare adresată Comisarului Malmström din 12 iunie 2012.
([6]) Rezumatul Mesei rotunde AEPD privind pachetul frontiere inteligente și implicațiile asupra protecției datelor, Bruxelles, 10 aprilie 2013, este disponibil la adresa: http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/EDPS/PressNews/Events/2013/13-04-10_Summary_smart_borders_final_EN.pdf
([7]) Propunerea de Regulament al Parlamentului European și al Consiliului de instituire a sistemului de intrare/ieșire (EES) pentru înregistrarea datelor de intrare și de ieșire ale resortisanților țărilor terțe care trec frontierele externe ale statelor membre ale Uniunii Europene, COM(2013) 95 final.
([8]) Propunerea de Regulament al Parlamentului European și al Consiliului de instituire a unui program de înregistrare a călătorilor, COM(2013) 97 final.
([9]) Propunerea de Regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (CE) nr. 562/2006 în ceea ce privește utilizarea sistemului de intrare/ieșire (EES) și a programului de înregistrare a călătorilor (RTP), COM(2013) 96 final.
([10]) Avizul AEPD din 18 iulie 2013 privind Propunerile pentru un Regulament de instituire a unui sistem de intrare/ieșire (EES) și a unui Regulament de instituire a unui program de înregistrare a călătorilor (RTP).
([11]) Avizul 05/2013 al grupului de lucru „Articolul 29" din 6 iunie 2013 privind frontierele inteligente.
([12]) Studiul tehnic privind frontierele inteligente – raport final din octombrie 2014 este disponibil la adresa: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_technical_study_en.pdf
([13]) Studiul tehnic privind frontierele inteligente - Analiza costurilor din octombrie 2014 este disponibil la adresa: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/docs/smart_borders_costs_study_en.pdf
([14]) Raport final privind proiectul-pilot Frontiere inteligente al eu-LISA din decembrie 2015 este disponibil la adresa: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/smart-borders/index_en.htm
([15]) Consultarea publică a Comisiei privind frontierele inteligente este disponibilă la adresa: http://ec.europa.eu/dgs/home-affairs/what-is-new/public-consultation/2015/consulting_0030_en.htm
([16]) Observațiile formale ale AEPD din 3 noiembrie 2015 cu privire la Consultarea publică a Comisiei privind frontierele inteligente.
([17]) Comunicatul de presă este disponibil la: http://europa.eu/rapid/press-release_IP-16-1247_en.htm

Propunerea EES din 2013 și Propunerea din 2013 de modificare a Codului frontierelor Schengen, însă își va retrage Propunerea RTP din 2013. În prezent, pachetul privind frontierele inteligente este alcătuit din:

— un comunicat privind „Sistemele informatice mai solide și mai inteligente pentru securitatea la frontiere” ([1]);

— o propunere de Regulament al Parlamentului European și al Consiliului de instituire a sistemului de intrare/ieșire pentru înregistrarea datelor de intrare și de ieșire și a datelor referitoare la refuzul intrării în ceea ce îi privește pe resortisanții țărilor terțe care trec frontierele externe ale statelor membre ale Uniunii Europene, de stabilire a condițiilor de acces la EES în scopul asigurării respectării legii și de modificare a Regulamentului (CE) nr. 767/2008 și a Regulamentului (UE) nr. 1077/2011 ([2]) (denumită în continuare „Propunerea EES din 2016”); și

— o propunere de Regulament al Parlamentului European și al Consiliului de modificare a Regulamentului (UE) 2016/399 ([3]) cu privire la utilizarea sistemului de intrare/ieșire ([4]) (denumită în continuare „Propunerea de modificare a Codului Frontierelor Schengen din 2016”).

5. În plus, cele două propuneri sunt însoțite de o evaluare a impactului ([5]) detaliată.

6. Pachetul Frontiere inteligente a luat un nou avânt în urma crizei migrației actuale și a atacurilor teroriste recente din Europa. Președinția neerlandeză și președinția slovacă au anunțat că intenționează să lucreze intens la pachet pentru a se ajunge la un acord politic până la sfârșitul anului 2016 ([6]).

7. AEPD salută faptul că a fost consultată neoficial de către Comisie înainte de adoptarea noilor propuneri. De asemenea, autoritatea consideră oportună buna cooperare ([7]) dintre DG Afaceri Interne și AEPD pe durata procesului de reînnoire a primului pachet Frontiere inteligente.

IV. **CONCLUZIE**

90. AEPD consideră oportună activitatea întreprinsă de Comisie în Propunerea EES din 2016 pentru abordarea preocupărilor legate de protecția datelor manifestate cu privire la pachetul Frontiere inteligente din 2013. Unele dintre recomandările și observațiile AEPD din avizul anterior cu privire la pachet au fost luate în considerare în mod corespunzător, de exemplu, în ceea ce privește introducerea unor proceduri de rezervă în caz de imposibilitate tehnică sau defecțiune a sistemului.

91. AEPD consideră oportune eforturile Comisiei de a justifica necesitatea instituirii sistemului EES, însă face recomandări majore legate direct de proporționalitatea acesteia, pentru a asigura conformitatea deplină a EES cu condiția prealabilă esențială a articolului 52 alineatul (1) din Cartă, conform căreia aceasta trebuie să fie atât necesară, cât și proporțională. AEPD subliniază că necesitatea și proporționalitatea sistemului EES vor fi evaluate atât la nivel global, luând în considerare sistemele informatice deja existente la scară largă în UE, cât și, în special, în cazul specific al acestor resortisanți ai țărilor terțe care sunt vizitatori legali ai UE. AEPD consideră că o perioadă de păstrare de cinci ani a tuturor datelor cu caracter personal stocate în EES ar trebui să fie pe deplin justificată. De asemenea, aceasta subliniază faptul că următoarele aspecte ale Propunerii EES din 2016 ar trebui să fie mai bine justificate și susținute de dovezi convingătoare: colectarea imaginii faciale a persoanelor care călătoresc pe bază de viză, perioada de păstrare de cinci ani pentru persoanele care depășesc termenul legal de ședere, precum și nevoia de acces a autorităților de aplicare a legii la datele EES. *Quod non*, aceste aspecte ar trebui să fie reanalizate de către organul legislativ al Uniunii.

92. Mai mult, având în vedere interferența largă cu drepturile fundamentale la viață privată și protecția datelor resortisanților țărilor terțe, AEPD consideră că EES ar trebui să rămână un instrument de gestionare a frontierelor special conceput în acest scop. Prin urmare, diferența dintre obiectivele declarate ale EES, adică dintre obiectivele principale ale gestionării frontierelor și ale facilitării și obiectivul secundar de aplicare a legii ar trebui să fie introdusă în mod clar și reflectată în întreaga Propunere EES din 2016, în special în ceea ce privește articolele 1 și 5.

([1]) Comunicarea Comisiei din 6 aprilie 2016 privind „Sistemele informatice mai solide și mai inteligente pentru securitatea la frontiere”, COM(2016) 205 final.
([2]) COM(2016) 194 final.
([3]) Regulamentul (UE) 2016/399 al Parlamentului European și al Consiliului din 9 martie 2006 cu privire la Codul Uniunii privind regimul de trecere a frontierelor de către persoane (Codul Frontierelor Schengen) (JO L 77, 23.3.2016, p. 1).
([4]) COM(2016) 196 final.
([5]) Documentul de lucru al Serviciilor Comisiei din 6 aprilie 2016 privind „Evaluarea impactului privind instituirea unui sistem UE de intrare/ieșire care însoțește Propunerea EES din 2016 și Propunerea din 2016 de modificare a Codului Frontierelor Schengen”, SWD(2016) 115 final (denumită în continuare „evaluarea impactului”).
([6]) http://data.consilium.europa.eu/doc/document/ST-8485-2016-INIT/en/pdf
([7]) În 2015 au avut loc două ateliere, între DG Afaceri Interne și AEPD, care abordează aspecte privind frontierele inteligente: un atelier la data de 20 martie, dedicat în special elaborării propunerilor privind frontierele inteligente, și un atelier interactiv, la data de 21 septembrie 2015, privind considerațiile referitoare la protecția datelor și confidențialitatea în politicile privind migrația și afacerile interne, în cursul căruia s-au abordat și propunerile din 2013 privind frontierele inteligente; a se vedea procesul-verbal al atelierului din 20 martie 2015, în anexa 16 la evaluarea impactului.

93. În plus, AEPD își exprimă preocuparea în ceea ce privește cerința aplicabilă tuturor persoanelor vizate referitoare la furnizarea de amprente digitale, indiferent de circumstanțe, pentru depunerea oricărei cereri de acces, rectificare și ștergere a datelor lor cu caracter personal. Acest lucru ar putea crea un obstacol important în calea exercitării efective a dreptului de acces, o garanție importantă pentru persoana vizată, prevăzut la articolul 8 alineatul (2) din Carta UE.

94. Alte recomandări ale AEPD din prezentul aviz se referă la următoarele aspecte și articole:

— Este necesară detalierea articolului 14, astfel încât, în cazul în care imaginile faciale ale resortisanților țărilor terțe sunt obținute pe loc, fotografiile să atingă un nivel minim de calitate, iar articolul 33 ar trebui să precizeze faptul că Comisia va furniza informații detaliate cu privire la modul de a ajunge la nivelul de calitate necesar pentru imaginile faciale obținute pe loc.

— Este necesară modificarea articolului 15 alineatul (3), astfel încât să se precizeze ce informații pot fi colectate, stocate și utilizate de către autoritățile de frontieră atunci când acestea solicită clarificări suplimentare cu privire la motivele pentru imposibilitatea temporară de a furniza amprente digitale.

— Articolul 39 ar trebui să prevadă necesitatea stringentă a unei coordonări între eu-LISA și statele membre în ceea ce privește asigurarea securității EES.

— Se impune clarificarea responsabilităților de securitate în propunere, în cazul interconectării programelor naționale de facilitare ale statelor membre la EES. Noul articol 8e din Codul Frontierelor Schengen ar trebui să precizeze necesitatea asigurării securității în urma unei evaluări adecvate a riscurilor de securitate a informațiilor și să descrie măsurile de securitate necesare.

— Propunerea ar trebui să precizeze în mod clar că eu-LISA este responsabilă pentru securitatea serviciului web, securitatea datelor cu caracter personal pe care le conține și procesul de transmitere a datelor cu caracter personal din sistemul central în serviciul web.

— Articolul 44 alineatul (1) ar trebui modificat pentru a include următoarele în informațiile comunicate persoanelor vizate: perioada de păstrare care se aplică datelor respective, dreptul persoanelor care depășesc termenul legal de ședere de a-și șterge datele cu caracter personal în cazul în care furnizează dovada că depășirea perioadei de ședere a fost cauzată de evenimente imprevizibile și grave și o explicație a faptului că datele EES vor fi accesate în scopuri de gestionare a frontierelor și de facilitare.

— Articolul 46 alineatul (1) ar trebui să stabilească un termen strict armonizat de răspuns la cererile de acces, care să nu depășească câteva luni.

— Articolul 9 alineatul (2) ar trebui modificat cu o descriere clară a garanțiilor care să asigure atenția adecvată acordată datelor referitoare la copii, persoanele în vârstă și persoanele cu handicap.

— Articolul 57 ar trebui să fie modificat și să impună eu-LISA dezvoltarea de funcționalități care să permită statelor membre, Comisiei, eu-LISA și Frontex extragerea automată a statisticilor necesare în mod direct din sistemul central EES, fără a fi nevoie de un depozitar suplimentar.

— Propunerea ar trebui să prezinte AEPD informațiile și resursele corespunzătoare, astfel încât noile sale responsabilități în calitate de supraveghetor al viitorului EES să poată fi realizate în mod eficient și eficace.

— Articolul 28 alineatul (2) ar trebui să prevadă un termen strict pentru a verificarea *ex post* de către autoritățile de control a condițiilor de acces la datele EES în scopul aplicării legii, în caz de urgență.

— Articolul 28 alineatul (3) ar trebui modificat pentru a impune cerința ca autoritățile desemnate și autoritatea de control să nu facă parte din aceeași organizație.

95. AEPD insistă asupra necesității de a aborda aceste chestiuni dintr-o perspectivă globală. AEPD încurajează legiuitorul să-și exercite în continuare punerea în corespondență a diferitelor baze de date în contextul frontierelor și a migrației, o mai bună coordonare și evitarea suprapunerilor între diferitele sisteme, respectând în același timp pe deplin standardele de protecție a datelor și în relațiile sale cu țările terțe.

Adoptat la Bruxelles, 21 septembrie 2016.

Giovanni BUTTARELLI

Autoritatea Europeană pentru Protecția Datelor

V

(Anunțuri)

PROCEDURI REFERITOARE LA PUNEREA ÎN APLICARE A POLITICII ÎN DOMENIUL CONCURENȚEI

COMISIA EUROPEANĂ

Notificare prealabilă a unei concentrări

(Cazul M.8288 – Permira/Schustermann & Borenstein)

Caz care poate face obiectul procedurii simplificate

(Text cu relevanță pentru SEE)

(2016/C 463/12)

1. La data de 6 decembrie 2016, Comisia Europeană a primit, în temeiul articolului 4 din Regulamentul (CE) nr. 139/2004 al Consiliului ([1]), o notificare a unei concentrări propuse prin care întreprinderea Permira Holdings Limited („Permira", Guernsey), acționând indirect prin intermediul fondurilor pe care le gestionează ori cărora le oferă consiliere, dobândește, în sensul articolului 3 alineatul (1) litera (b) din Regulamentul privind concentrările economice, controlul asupra întregii întreprinderi Schustermann & Borenstein Holding GmbH („S & B", Germania), prin achiziționare de acțiuni.

2. Activitățile economice ale întreprinderilor respective sunt:

— în cazul întreprinderii Permira: fond de investiții în societăți necotate în diverse sectoare;

— în cazul întreprinderii S & B: comerțul cu amănuntul de articole de modă pe internet (www.bestsecret.com) și trei magazine fizice, situate în Austria și Germania.

3. În urma unei examinări prealabile, Comisia Europeană constată că tranzacția notificată ar putea intra sub incidența Regulamentului privind concentrările economice. Cu toate acestea, nu se ia o decizie finală în această privință. În conformitate cu Comunicarea Comisiei privind o procedură simplificată de analiză a anumitor concentrări în temeiul Regulamentului (CE) nr. 139/2004 al Consiliului ([2]), trebuie precizat că acest caz poate fi tratat conform procedurii prevăzute în comunicare.

4. Comisia Europeană invită părțile terțe interesate să îi prezinte eventualele observații cu privire la operațiunea propusă.

Observațiile trebuie primite de către Comisia Europeană în termen de cel mult 10 zile de la data publicării prezentei. Observațiile pot fi trimise Comisiei Europene, cu numărul de referință M.8288 – Permira/Schustermann & Borenstein, prin fax (+32 22964301), prin e-mail, la adresa COMP-MERGER-REGISTRY@ec.europa.eu, sau prin poștă, la următoarea adresă:

Commission Européenne
Direction générale de la concurrence
Greffe des concentrations
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

([1]) JO L 24, 29.1.2004, p. 1 („Regulamentul privind concentrările economice").
([2]) JO C 366, 14.12.2013, p. 5.

Notificare prealabilă a unei concentrări

(Cazul M.8259 – Groupe H.I.G./Guillaume Dauphin/Ecore)

Caz care poate face obiectul procedurii simplificate

(Text cu relevanță pentru SEE)

(2016/C 463/13)

1. La data de 1 decembrie 2016, Comisia Europeană a primit, în temeiul articolului 4 din Regulamentul (CE) nr. 139/2004 al Consiliului ([1]), o notificare a unei concentrări propuse prin care întreprinderile Guillaume Dauphin și H.I.G. Capital LLC („Groupe H.I.G.", Statele Unite) dobândesc, în sensul articolului 3 alineatul (1) litera (b) din Regulamentul privind concentrările economice, controlul în comun asupra întreprinderii Ecore B.V. („Ecore", Țările de Jos) care, în prezent, se află sub controlul unic al întreprinderii Guillaume Dauphin; controlul în comun se va efectua prin vânzare și achiziționare de acțiuni.

2. Activitățile economice ale întreprinderilor respective sunt:

— în cazul întreprinderii Guillaume Dauphin: produce și comercializează, prin intermediul întreprinderii Ecore, materie primă reciclată;

— în cazul întreprinderii Groupe H.I.G.: firmă de investiții în societăți necotate, care deține participații în întreprinderi mici și mijlocii;

— în cazul întreprinderii Ecore: produce și comercializează materie primă reciclată. Întreprinderea Ecore desfășoară, în special, activități de colectare și tratare a deșeurilor și de comercializare a materialelor reciclate, îndeosebi metale feroase. Ecore produce și comercializează, de asemenea, alte materiale reciclate, cum ar fi metale neferoase, hârtie, carton și materiale plastice.

3. În urma unei examinări prealabile, Comisia Europeană constată că tranzacția notificată ar putea intra sub incidența Regulamentului privind concentrările economice. Cu toate acestea, nu se ia o decizie finală în această privință. În conformitate cu Comunicarea Comisiei privind o procedură simplificată de analiză a anumitor concentrări în temeiul Regulamentului (CE) nr. 139/2004 al Consiliului ([2]), trebuie precizat că acest caz poate fi tratat conform procedurii prevăzute în comunicare.

4. Comisia Europeană invită părțile terțe interesate să îi prezinte eventualele observații cu privire la operațiunea propusă.

Observațiile trebuie primite de către Comisia Europeană în termen de cel mult 10 zile de la data publicării prezentei. Observațiile pot fi trimise Comisiei Europene, cu numărul de referință M.8259 – Groupe H.I.G./Guillaume Dauphin/Ecore, prin fax (+32 22964301), prin e-mail, la adresa COMP-MERGER-REGISTRY@ec.europa.eu, sau prin poștă, la următoarea adresă:

Commission européenne
Direction générale de la concurrence
Greffe des concentrations
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

([1]) JO L 24, 29.1.2004, p. 1 („Regulamentul privind concentrările economice").
([2]) JO C 366, 14.12.2013, p. 5.

ALTE ACTE

COMISIA EUROPEANĂ

Comunicare în atenția persoanelor fizice Pak Chun Il, Kim Song Chol, Son Jong Hyok, Kim Se Gon, Ri Won Ho, Jo Yong Chol, Kim Chol Sam, Kim Sok Chol, Chang Chang Ha, Cho Chun Ryong și Son Mun San și a entităților Korea United Development Bank, Ilsim International Bank, Korea Daesong Bank, Singwang Economics and Trading General Corporation, Korea Foreign Technical Trade Center, Korea Pugang Trading Corporation, Korea International Chemical Joint Venture Company, DCB Finance Limited, Korea Taesong Trading Company și Korea Daesong General Trading Corporation, care au fost adăugate pe lista menționată la articolul 6 alineatul (1) din Regulamentul (CE) nr. 329/2007 al Consiliului, care impune o serie de măsuri restrictive specifice împotriva persoanelor, a entităților și a organismelor desemnate de Comitetul de sancțiuni sau de Consiliul de Securitate al Organizației Națiunilor Unite, în conformitate cu punctul (8) litera (d) din Rezoluția 1718 (2006) a Consiliului de Securitate al ONU și cu punctul (8) din Rezoluția 2094 (2013) a Consiliului de Securitate al ONU, în temeiul Regulamentului de punere în aplicare (UE) 2016/2215 al Comisiei

(2016/C 463/14)

(1) Decizia (PESC) 2016/849 a Consiliului [1] îndeamnă Uniunea să înghețe fondurile și resursele economice ale persoanelor și entităților desemnate de Comitetul de sancțiuni sau de Consiliul de Securitate al ONU ca participând în cadrul sau oferind sprijin, inclusiv prin mijloace ilicite, programelor RPDC din domeniul nuclear sau legate de rachete balistice sau altor programe legate de arme de distrugere în masă, ori ale persoanelor sau entităților care acționează în numele acestora sau în conformitate cu instrucțiunile lor, ori ale entităților aflate în proprietatea lor sau controlate de acestea, inclusiv prin mijloace ilicite.

(2) Consiliul de Securitate al ONU a hotărât în Rezoluția sa 2321 din 30 noiembrie 2016 că persoanele fizice Pak Chun Il, Kim Song Chol, Son Jong Hyok, Kim Se Gon, Ri Won Ho, Jo Yong Chol, Kim Chol Sam, Kim Sok Chol, Chang Chang Ha, Cho Chun Ryong și Son Mun San și entitățile Korea United Development Bank, Ilsim International Bank, Korea Daesong Bank, Singwang Economics and Trading General Corporation, Korea Foreign Technical Trade Center, Korea Pugang Trading Corporation, Korea International Chemical Joint Venture Company, DCB Finance Limited, Korea Taesong Trading Company și Korea Daesong General Trading Corporation trebuie adăugate pe lista Comitetului de sancțiuni.

Persoanele și entitățile vizate pot oricând să adreseze o cerere Comitetului Consiliului de Securitate al ONU instituit în temeiul Rezoluției 1718 (2006), însoțită de documente justificative, în scopul reanalizării deciziilor privind includerea lor pe lista ONU. Cererea trebuie trimisă la următoarea adresă:

United Nations – Focal point for delisting
Security Council Subsidiary Organs Branch
Room S-3055 E
New York, NY 10017
UNITED STATES OF AMERICA

Pentru mai multe informații, a se vedea: https://www.un.org/sc/suborg/en/sanctions/delisting

(3) În vederea punerii în aplicare a noilor înscrieri pe listă, Comisia a adoptat Regulamentul de punere în aplicare (UE) 2016/2215 al Comisiei din 8 decembrie 2016 [2], care modifică în consecință anexa IV la Regulamentul (CE) nr. 329/2007 al Consiliului.

Persoanele și entitățile în cauză pot transmite Comisiei Europene observații referitoare la decizia de a le înscrie sau de a le menține pe listă, împreună cu documentele justificative, la următoarea adresă:

Comisia Europeană
"Restrictive measures"
Rue de la Loi/Wetstraat 200
1049 Bruxelles/Brussel
BELGIQUE/BELGIË

[1] JO L 141, 28.5.2016, p. 79.
[2] JO L 334, 9.12.2016, p. 29.

(4) De asemenea, se atrage atenția persoanelor și entităților în cauză asupra posibilității de a introduce la Tribunalul Uniunii Europene o acțiune în contestare privind Regulamentul de punere în aplicare (UE) 2016/2215, în conformitate cu condițiile prevăzute la articolul 263 paragrafele al patrulea și al șaselea din Tratatul privind funcționarea Uniunii Europene.

(5) Nu în ultimul rând, se atrage atenția entităților și persoanelor incluse pe listă asupra posibilității de a adresa o cerere autorităților competente din statul membru (statele membre) relevant(e), care figurează în anexa II la Regulamentul (CE) nr. 329/2007, în vederea obținerii autorizării de a utiliza, pentru nevoi esențiale sau plăți specifice, fonduri și resurse economice înghețate, în conformitate cu dispozițiile articolului 7 din regulamentul menționat anterior.

ISSN 1977-1029 (ediție electronică)
ISSN 1830-3668 (ediție tipărită)

Oficiul pentru Publicații al Uniunii Europene
2985 Luxemburg
LUXEMBURG

RO