Pārtikai paredzētas augļu sulas un daži līdzīgi produkti

P7_TA(2011)0323

Eiropas Parlamenta 2011. gada 6. jūlija rezolūcija par vispusīgu pieeju personas datu aizsardzībai Eiropas Savienībā (2011/2025(INI))

(2013/C 33 E/10)

Eiropas Parlaments,

— ņemot vērā Līgumu par Eiropas Savienības darbību (LESD) un jo īpaši tā 16. pantu,

— ņemot vērā Eiropas Savienības Pamattiesību hartu un jo īpaši tās 7. un 8. pantu, un ņemot vērā Eiropas Cilvēktiesību un pamatbrīvību aizsardzības konvenciju (*ECHR*), īpaši tās 8. pantu par tiesību aizsardzību uz privāto un ģimenes dzīvi un 13. pantu par efektīvas aizsardzības nodrošinājumu,

— ņemot vērā Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti [1],

— ņemot vērā Padomes 2008. gada 27. novembra Pamatlēmumu 2008/977/TI par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās [2],

— ņemot vērā Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regulu (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti [3],

— ņemot vērā Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīvu 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (Direktīva par privāto dzīvi un elektroniskajām komunikācijām) [4],

— ņemot vērā Eiropas Padomes 1981. gada 28. janvāra Konvenciju Nr. 108 Par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi, kura tālāk izstrādāta ar Direktīvu 95/46/EK un tās 2001. gada 8. novembra papildprotokolu par uzraudzības iestādēm un pārrobežu datu plūsmām un Eiropas Padomes Ministru komitejas ieteikumus dalībvalstīm, jo īpaši Ieteikumu Nr. R (87) 15, kas regulē personas datu izmantošanu policijas darbā, Ieteikumu Nr. CM/Rec(2010)13 dalībvalstīm par fizisko personu aizsardzību attiecībā uz personas datu automātisku apstrādi datu profilu veidošanas kontekstā,

— ņemot vērā Pamatnostādnes par elektroniskām personas datu datnēm, kuras 1990. gadā izdevusi ANO Ģenerālā asambleja,

— ņemot vērā Komisijas paziņojumu Padomei, Eiropas Parlamentam, Eiropas Ekonomikas un sociālo lietu komitejai un Reģionu komitejai „Vispusīga pieeja personas datu aizsardzībai Eiropas Savienībā" (COM(2010)0609),

[1] OV L 281, 23.11.1995., 31. lpp.
[2] OV L 350, 30.12.2008., 60. lpp.
[3] OV L 8, 12.1.2001., 1. lpp.
[4] OV L 201, 31.7.2002., 37. lpp.

Trešdiena, 2011. gada 6. jūlijs

— ņemot vērā Padomes secinājumus par Komisijas paziņojumu „Vispusīga pieeja personas datu aizsardzībai Eiropas Savienībā” ([1]),

— ņemot vērā Eiropas Datu aizsardzības uzraudzītāja (E) 2011. gada 14. janvāra atzinumu par Komisijas paziņojumu „Vispusīga pieeja personas datu aizsardzībai Eiropas Savienībā”,

— ņemot vērā 29. panta datu aizsardzības darba grupas un Policijas un tiesiskuma jautājumu darba grupas kopīgi sagatavoto dokumentu apspriedēm ar Eiropas Komisiju par tiesisko regulējumu attiecībā uz pamattiesībām uz personas datu aizsardzību „Privātuma nākotne” ([2]),

— ņemot vērā 29. panta datu aizsardzības darba grupas atzinumu Nr. 8/2010 par piemērojamajiem tiesību aktiem ([3]),

— ņemot vērā iepriekšējās rezolūcijas par datu aizsardzību un rezolūciju par Stokholmas programmu ([4]),

— ņemot vērā Reglamenta 48. pantu,

— ņemot vērā Pilsoņu brīvību, tieslietu un iekšlietu komitejas ziņojumu un Rūpniecības, pētniecības un enerģētikas komitejas, Iekšējā tirgus un patērētāju aizsardzības komitejas, Kultūras un izglītības komitejas un Juridiskās komitejas atzinumus (A7-0244/2011),

A. tā kā Datu aizsardzības direktīva 95/46/EK un Direktīva par ES telekomunikāciju paketi 2009/140/EK atļauj personas datu brīvu apriti iekšējā tirgū;

B. tā kā datu aizsardzības tiesību aktos ES, dalībvalstīs un citur ir izveidojusies juridiska tradīcija, kas jāsaglabā un jāturpina attīstīt;

C. tā kā Datu aizsardzības direktīvas (95/46/EK) pamatprincipi paliek spēkā, bet novērots, ka dalībvalstu pieejas īstenošanai un piemērošanai bijušas atšķirīgas; tā kā Eiropas Savienībai pēc visaptveroša ietekmes novērtējuma jāizstrādā vispārējs, saskaņots, mūsdienīgs augsta līmeņa regulējums, ar kuru varētu efektīvi aizsargāt personas pamattiesības, jo īpaši uz privātumu, kas jebkuros apstākļos spēj aizsargāt privātpersonu personas datus Eiropas Savienībā un aiz tās robežām, lai spētu risināt daudzās problēmas datu aizsardzības jomā, piemēram, tādas, ko radījusi globalizācija, tehnoloģiju attīstība, pieaugusī aktivitāte tiešsaistē, lietojumi, kas saistīti ar aizvien vairākām aktivitātēm un drošības apsvērumi (t. i., cīņa pret terorismu); tā kā šāds datu aizsardzības regulējums var palielināt juridisko noteiktību, samazināt administratīvo slogu, nodrošināt uzņēmējiem līdzvērtīgus konkurences apstākļus, veicināt vienotu digitālo tirgu un veicināt uzticību datu apstrādātāju un izpildiestāžu rīcībai;

([1]) Tieslietu un iekšlietu padomes 3 071. sanāksme Briselē, 2011. gada 24. un 25. februārī, skatīt šeit: http://www.consilium.europa.eu/uedocs/cms_data/docs/pressdata/en/jha/119461.pdf.
([2]) 02356/09/EN WP 168.
([3]) 0836/10/EN WP 179.
([4]) Piemēram: Eiropas Parlamenta 2008. gada 23. septembra nostāja par priekšlikumu Padomes Pamatlēmumam par tādu personas datu aizsardzību, kurus apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās (OV C 8 E, 14.1.2010., 138. lpp); Eiropas Parlamenta 2009. gada 26. marta ieteikums Padomei par drošības un pamatbrīvību stiprināšanu internetā (OV C 117 E, 6.5.2010., 206. lpp.); Eiropas Parlamenta 2009. gada 25. novembra rezolūcija par Komisijas paziņojumu Eiropas Parlamentam un Padomei — brīvības, drošības un tiesiskuma telpa pilsoņu interesēs — Stokholmas programma (OV C 285 E, 21.10.2010., 12 lpp.)

D. tā kā datu aizsardzības noteikumu pārkāpumi var radīt nopietnu apdraudējumu personu pamatbrīvībām un dalībvalstu vērtībām, tāpēc Savienībai un dalībvalstīm jāveic efektīvi pasākumi pret šādiem pārkāpumiem; tā kā šādi pārkāpumi izraisa personu neuzticību, kas kavēs jauno tehnoloģiju atbilstošu izmantojumu, un tā kā personas datu nepareiza un ļaunprātīga izmantošana tādēļ ir sodāma ar atbilstošiem, stingriem un preventīviem sodiem tostarp krimināls odiem;

E. tā kā, nodrošinot pamattiesības uz personas datu aizsardzību, pilnībā jāievēro arī citas Hartā ietvertās pamattiesības un pārējie ES Līgumos noteiktie mērķi, tādi kā tiesības uz vārda brīvību un informāciju un pārskatāmības princips;

F. tā kā LESD 16. pantā noteiktais jaunais tiesiskais pamats kopā ar Pamattiesību hartas 8. pantu, kurā tiesības uz personas datu aizsardzību ir atzītas par autonomām tiesībām un 7. pantu, kurā privātās un ģimenes dzīves neaizskaramība ir atzīta par autonomām tiesībām, pilnībā paredz un atbalsta vispārēju pieeju datu aizsardzībai visās jomās, kurās tiek apstrādāti personas dati, tostarp jomā, uz kuru attiecas policijas un tiesu iestāžu sadarbība krimināllietās, kopējās ārpolitikas un drošības politikas jomā (KĀDP), neskarot konkrētos noteikumus, kas paredzēti LES 39. pantā, un ES iestāžu un struktūru veiktas datu apstrādes jomā;

G. tā kā izvērtējot leģislatīvus risinājumus, ir ļoti svarīgi ņemt vērā vairākus būtiskus aspektus, proti, aizsardzībai jābūt efektīvai, nodrošinātai jebkuros apstākļos un neatkarīgai no politiskajām prioritātēm noteiktā termiņā; tā kā regulējumam jābūt stabilam ilgtermiņā, un, iespējams, var rasties nepieciešamība noteikt ierobežojumus tiesību īstenošanai, taču ierobežojumi jāpiemēro izņēmuma gadījumos, saskaņā ar tiesību aktiem un tiem jābūt pilnīgi nepieciešamiem un samērīgiem un tie nedrīkst ietekmēt pašu tiesību būtiskākos elementus;

H. tā kā datu apkopošana, analīze, apmaiņa un nepareiza izmantošana, kā arī datu profilu veidošanas risks, ko ir veicinājuši tehniskie sasniegumi, ir sasniegusi nepieredzētus apjomus un rada vajadzību izstrādāt stingrus datu aizsardzības noteikumus, piemēram, piemērojamo tiesību aktu un visu ieinteresēto pušu atbildības noteikšanu attiecībā uz ES tiesību aktu datu aizsardzības jomā īstenošanu; tā kā uzņēmumos un tirdzniecībā arvien biežāk tiek lietotas klientu kartes (klubu kartes, atlaižu vai privilēģiju kartes, utt.), kuras izmanto vai var izmantot klientu profilēšanai;

I. tā kā pilsoņi neiepērkas tiešsaistē tikpat droši kā nesaistē, baidoties no identitātes zādzībām un pārredzamības trūkuma attiecībā uz to, kā tiks apstrādāta un izmantota viņu personīgā informācija;

J. tā kā tehnoloģija rada arvien vairāk iespēju izveidot, nosūtīt, apstrādāt un saglabāt personas datus jebkurā laikā un vietā, un daudzos dažādos veidos, un tā kā šajā situācijā ir ļoti svarīgi datu subjektiem saglabāt efektīvu kontroli attiecība uz saviem datiem;

K. tā kā pamattiesības uz datu aizsardzību un privāto dzīvi ietver personu aizsardzību no iespējamas novērošanas un viņu datu ļaunprātīgas izmantošanas, kuru veic valsts vai privātas struktūras;

L. tā kā privātums un drošība ir iespējami un tie abi ir ļoti svarīgi pilsoņiem, tātad nav jāizdara izvēle starp brīvību un drošību;

M. tā kā bērni ir pelnījuši īpašu aizsardzību, jo viņi var neapzināties ar personas datu apstrādi saistītos riskus, sekas, aizsardzības pasākumus un tiesības; tā kā gados jauni cilvēki sociālajos tīklos izpauž savus personas datus un šie sociālie tīkli internetā kļūst arvien izplatītāki;

N. tā kā — lai datu subjekts un valsts datu aizsardzības iestādes varētu efektīvi īstenot kontroli, datu apstrādātājiem jārīkojas pārskatāmi;

O. tā kā ne visi datu apstrādātāji ir tiešsaistes uzņēmumi un tādējādi jauniem datu aizsardzības noteikumiem jāattiecas gan uz tiešsaistes, gan nesaistes vidi, vienlaikus ņemot vērā iespējamās atšķirības starp tiem,

P. tā kā valsts datu aizsardzības iestādes 27 dalībvalstīs pakļaujas ļoti atšķirīgiem noteikumiem, īpaši attiecībā uz to statusu, resursiem un pilnvarām;

Q. tā kā stingrs Eiropas un starptautiskais datu aizsardzības režīms ir nepieciešamais pamats personas datu plūsmai pāri robežām, un tā kā pašreizējās atšķirības datu aizsardzības tiesību aktos un to piemērošanā ietekmē pamattiesības un privātpersonu brīvības, kā arī tiesisko drošību un noteiktību līgumattiecībās, e-komercijas un e-darījumu attīstību, patērētāju uzticēšanos sistēmai, pārrobežu darījumus, pasaules ekonomiku un vienoto Eiropas tirgu; tā kā šajā kontekstā datu apmaiņa ir svarīga, lai nodrošinātu sabiedrisko drošību valsts un starptautiskā līmenī; tā kā nepieciešamība, samērīgums, mērķa ierobežojums, uzraudzība un atbilstīgums ir apmaiņas priekšnoteikumi,

R. tā kā spēkā esošie noteikumi un nosacījumi attiecībā uz personas datu pārsūtīšanu no ES uz trešām valstīm ir noveduši pie tā, ka dažādās dalībvalstīs veidojas atšķirīgas pieejas un prakse; tā kā datu subjekta tiesību pilnīga piemērošana trešās valstīs, uz kurām dati tiek pārsūtīti un kurās tos apstrādā, ir obligāts nosacījums,

Pilnīga vispārējās pieejas pieņemšana

1. ļoti atzinīgi vērtē un atbalsta Komisijas paziņojumu „Vispusīga pieeja personas datu aizsardzībai Eiropas Savienībā" un tās pievēršanos pašreiz spēkā esošā režīma stiprināšanai, ierosinot jaunus principus un mehānismus, kā arī nodrošinot datu aizsardzības saskaņotību un augsta līmeņa standartus jaunajos apstākļos, kurus nosaka Lisabonas līguma stāšanās spēkā (LESD 16. pants) un tas, ka Pamattiesību harta tagad ir saistoša, jo īpaši tās 8. pants;

2. uzsver, ka Direktīvā 95/46/EK izklāstītie standarti un principi ir ideāls sākuma punkts un tos ir jāattīsta tālāk, jāpaplašina un jāpastiprina kā daļu no mūsdienīgām datu aizsardzības tiesībām;

3. uzsver Direktīvas 95/46/EK 9. panta svarīgumu, kurā ir paredzēts pienākums dalībvalstīm noteikt atbrīvojumu no datu aizsardzības noteikumiem, kad personas dati tiek izmantoti vienīgi žurnālistikas nolūkiem vai mākslinieciskās, vai literārās izteiksmes nolūkiem; šajā sakarā aicina Komisiju nodrošināt, lai tiktu saglabāti šie izņēmumi un lai tiktu pieliktas visas pūles izvērtēt nepieciešamību pilnveidot šos izņēmumus, ņemot vērā jebkādus jaunus noteikumus preses brīvības aizsargāšanai;

4. uzsver, ka Direktīvas 95/46/EK tehnoloģiju ziņā neitrālā pieeja jāturpina izmantot kā jauna regulējuma principu;

5. atzīst, ka tehnoloģiju attīstība, no vienas puses, ir radījusi jaunus draudus personas datu aizsardzībai un, no otras puses, ievērojami palielinājusi informācijas tehnoloģiju izmantojumu ikdienas un parasti nekaitīgiem nolūkiem, un ka šīs attīstības dēļ ir nepieciešams pašreizējo datu aizsardzības noteikumu vispusīgs novērtējums, lai nodrošinātu, ka i) noteikumi joprojām nodrošina augstu aizsardzības līmeni, ii) noteikumi joprojām atbilst taisnīgam līdzsvaram starp tiesībām uz personas datu aizsardzību un tiesībām uz vārda brīvību un informāciju, iii) noteikumi nevajadzīgi nekavē personas datu apstrādi ikdienā, kas parasti ir nekaitīga;

6. uzskata, ka ir jāattiecina vispārīgo datu aizsardzības noteikumu piemērošanas joma arī uz policijas un tiesu iestāžu sadarbību, tostarp vietējā līmeņa datu pārstrādes kontekstā, īpaši ņemot vērā tendenci sistemātiski izmantot atkārtoti privātā sektora personas datus tiesībaizsardzības nolūkos, vienlaikus, ja tas demokrātiskā sabiedrībā ir pilnīgi nepieciešams un samērīgi, paredzot īpaši izstrādātus un saskaņotus ierobežojumus konkrētām personas datu aizsardzības tiesībām;

7. uzsver nepieciešamību jaunā regulējuma piemērošanas jomā iekļaut personas datu apstrādi, ko veic Eiropas Savienības iestādes un struktūras, kuru reglamentē Regula (EK) Nr. 45/2001;

8. atzīst, ka noteiktās nozarēs varētu būt nepieciešami uzlaboti papildu pasākumi, lai īpaši noteiktu, kādā veidā uz tām attiecas vispārējā regulējuma vispārīgie principi, kā tas ir noticis e-privātuma direktīvas gadījumā, bet uzstāj, ka noteikumiem, kas attiecināmi uz konkrētām nozarēm, nekādā gadījumā nav jāpazemina aizsardzības līmenis, kuru nodrošina pamata tiesību akti, stingri nosakot izņēmuma, nepieciešamas, leģitīmas un īpaši izstrādātas atkāpes no vispārējiem datu aizsardzības principiem;

9. aicina Komisiju nodrošināt, ka pašreizējā ES datu aizsardzības tiesību aktu pārskatīšanā iekļaus:

— pilnīgu saskaņošanu visaugstākajā līmenī, nodrošinot juridisko noteiktību un vienotu augsta līmeņa indivīdu aizsardzību visos apstākļos;

— to noteikumu tālāku precizēšanu, pamatojoties uz kuriem nosaka piemērojamos tiesību aktus, lai nodrošinātu indivīdiem vienotu aizsardzības līmeni neatkarīgi no tā, kāda ir atbildīgā par datu apstrādi ģeogrāfiskās atrašanās vieta, tostarp gadījumos, kad datu aizsardzība jāīsteno iestādēm vai tiesā;

10. uzskata, ka pārskatītajam datu aizsardzības režīmam, pilnībā realizējot tiesības uz privātumu un datu aizsardzību, ir jāsaglabā iespējami mazāks birokrātiskais un finansiālais slogs un jānodrošina instrumenti, kas rada iespēju konglomerātiem, kas tiek uzskatīti par vienotiem veselumiem, rīkoties kā tādiem, nevis kā daudziem atsevišķiem uzņēmumiem; mudina Komisiju veikt ietekmes novērtējumus un rūpīgi izvērtēt jaunu pasākumu izmaksas;

Indivīdu tiesību stiprināšana

11. aicina Komisiju stiprināt esošos principus un elementus, kā izklāstīts Direktīvā 95/46/EK, uzlabojot to īstenošanu dalībvalstīs, tostarp pārredzamības, datu minimizēšanas un mērķa ierobežojuma principus, apzinātu, iepriekšēju un skaidri izteiktu piekrišanu, ziņošanu par datu aizsardzības pārkāpumiem un datu subjekta piekļuves tiesības datiem, jo īpaši attiecībā uz globālo tiešsaistes vidi;

Trešdiena, 2011. gada 6. jūlijs

12. uzsver, ka piekrišana ir spēkā tikai tad, ja tā ir nepārprotama, apzināta, labprātīgi sniegta un konkrēta, un uzsver, ka ir jāievieš atbilstīgi mehānismi, lai reģistrētu lietotāja piekrišanu vai piekrišanas atsaukšanu, kurai ir jābūt skaidri izteiktai, nevis balstītai uz pieņēmumu;

13. norāda, ka brīvprātīgu piekrišanu darba līgumu jomā nevar pieņemt automātiski;

14. pauž bažas par ļaunprātīgu izmantošanu, kas saistīta ar tiešsaistes paradumorientēto reklāmu, un atgādina, ka Direktīva par privāto dzīvi un elektronisko komunikāciju nosaka, ka ir nepieciešama iepriekšēja skaidri izteikta attiecīgās personas piekrišana sīkdatņu sūtīšanai un turpmākai interneta lietošanas paradumu novērošanai ar mērķi šai privātpersonai piegādāt personalizētu reklāmu;

15. pilnībā atbalsta vispārēja pārredzamības principa ieviešanu, kā arī pārredzamības uzlabošanas tehnoloģiju izmantošanu un ar privāto dzīvi saistītu standartu paziņojumu izstrādi, lai indivīdi varētu kontrolēt savus datus; uzsver, ka informācijai par datu apstrādi jābūt viegli pieejamai un viegli saprotamai un ir jāizmanto skaidra un vienkārša valoda;

16. turklāt uzsver, ka ir svarīgi uzlabot veidus, kā efektīvi izmantojamas un labāk izprotamas piekļuves, labošanas, dzēšanas vai datu bloķēšanas tiesības, kā arī sīki precizēt un kodificēt tā sauktās „tiesības tikt aizmirstam" [1] un datu pārnešanas [2] iespējas, vienlaikus pilnīgu nodrošinot tehnisko un organizatorisko iespēju radīšanu un īstenošanu, lai varētu realizēt šīs tiesības; uzsver, ka indivīdiem jābūt pietiekamai kontrolei pār saviem datiem tiešsaistē, lai viņi varētu izmantot internetu atbildīgi;

17. uzsver, ka pilsoņiem jāspēj realizēt tiesības saistībā ar datiem bez maksas; aicina uzņēmumus atturēties no jebkādiem mēģinājumiem papildus ieviest nevajadzīgus šķēršļus tiesībām piekļūt saviem personas datiem vai tos labot, vai dzēst; uzsver, ka datu subjektam jārada tāds stāvoklis, lai viņš jebkurā laikā varētu uzzināt, kurš un kurus datus ir saglabājis, kad, kādā nolūkā, kādam laika periodam tas ir darīts un kā tie tiek apstrādāti; uzsver, ka datu subjektiem ir jābūt iespējām dzēst, labot vai bloķēt datus, nesaskaroties ar birokrātiskiem šķēršļiem, un viņiem jāsaņem informācija par visiem gadījumiem, kad dati ir nepareizi izmantoti vai vai notikuši to aizsardzības pārkāpumi; turklāt pieprasa panākt, ka dati tiek izpausti pēc attiecīgās personas pieprasījuma un dzēsti vēlākais tad, kad šī persona to pieprasa; uzsver, ka nepieciešams gūt skaidru informāciju par datu subjektu datu aizsardzības līmeni trešās valstīs; uzsver, ka piekļuves tiesības ietver ne tikai pilnīgu piekļuvi apstrādātajiem datiem par sevi, tostarp to avotiem un saņēmējiem, bet arī saprotamu informāciju par datu automatizētā apstrādē ietverto loģiku; uzsver, ka šī informācija kļūs arvien svarīgāka saistībā ar datu profilu veidošanu un datizraci;

18. norāda, ka, ņemot vērā arī sociālo tīklu un integrēto interneta uzņēmējdarbības modeļu arvien lielāko nozīmi, digitālajā jomā svarīgs attīstības virziens ir profilēšana; tādēļ aicina Komisiju ietvert arī normas attiecībā uz profilēšanu, līdztekus skaidri definējot terminus „profils" un „profilēšana";

19. atgādina par nepieciešamību pilnveidot par datu apstrādi atbildīgo personu pienākumus attiecībā uz informācijas sniegšanu datu subjektiem un atzinīgi vērtē Komisijas paziņojumā pievērsto uzmanību izpratnes veicināšanas kampaņām, kas paredzētas plašai sabiedrībai un arī — konkrētāk jauniešiem; uzsver īpašas attieksmes nepieciešamību pret neaizsargātām personām, īpaši bērniem un veciem cilvēkiem; mudina, lai šajās izpratnes veicināšanas kampaņās iesaistītos dažādas ieinteresētās personas un atbalsta Komisijas priekšlikumu par izpratnes veicināšanas pasākumu par datu aizsardzību līdzfinansēšanu no Savienības budžeta; aicina visās dalībvalstīs efektīvi izplatīt informāciju attiecībā uz fizisko un juridisko personu tiesībām un pienākumiem saistībā ar personas datu vākšanu, apstrādi, glabāšanu un pārsūtīšanu;

---

[1] Visiem attiecīgajiem šo tiesību pamatelementiem ir jābūt skaidri un precīzi identificētiem.

[2] Nodrošinot personas datu pārnesamību, tiks veicināta gan iekšējā tirgus, gan interneta netraucēta darbība ar tam raksturīgo atklātumu un savienojamību.

20. atgādina par nepieciešamību īpašā veidā aizsargāt mazāk aizsargātās personas un jo īpaši bērnus, piemēram, nosakot augsta līmeņa datu aizsardzību par pamatprasību un ieviešot piemērotus konkrētus pasākumus viņu personas datu aizsardzībai;

21. uzsver, cik nepieciešami ir datu aizsardzības tiesību akti, lai atzītu īpašo vajadzību aizsargāt bērnus un nepilngadīgos, cita starpā ņemot vērā arvien lielāku interneta un digitālā satura pieejamību bērniem, un uzsver, ka mediju lietotprasmei jākļūst par formālās izglītības sastāvdaļu, lai apmācītu bērnus un nepilngadīgos, kā rīkoties atbildīgi tiešsaistes vidē; tādēļ īpaša uzmanība jāvelta noteikumiem par bērnu datu vākšanu un turpmāku apstrādi, mērķa ierobežojuma principa nostiprināšanu saistībā ar bērnu datiem un to, kādā veidā tiek pieprasīta bērnu piekrišana, kā arī par aizsardzību no paradumorientētās reklāmas ([1]);

22. atbalsta saskaņotāku noteikumu pieņemšanu un garantiju stiprināšanu attiecībā uz jutīgu datu apstrādi, un aicina apsvērt nepieciešamību nodarboties ar jaunām datu kategorijām, piemēram, ģenētiskiem un biometriskiem datiem, jo īpaši ņemot vērā tehnoloģiju (piemēram, mākoņdatošana) un sabiedrības attīstību;

23. uzsver, ka personas datus par lietotāja profesionālo situāciju, kas sniegta viņa darba devējam, nedrīkst publicēt vai pārsūtīt trešajām personām bez attiecīgās personas iepriekšējas piekrišanas;

Iekšējā tirgus aspekta attīstība un datu aizsardzības noteikumu efektīvāka piemērošana

24. atzīmē, ka datu aizsardzībai iekšējā tirgū ir jāiegūst arvien būtiskāka nozīme, un uzsver, ka tiesību uz privāto dzīvi efektīva aizsardzība ir izšķiroši svarīga personu uzticības nodrošināšanai, kas nepieciešams, lai pilnībā realizētu vienota digitālā tirgus izaugsmes iespējas; atgādina Komisijai, ka vienota digitālā tirgus priekšnoteikums ir tas, ka kopējiem principiem un noteikumiem jābūt attiecinātiem gan uz precēm, gan pakalpojumiem, jo pakalpojumi ir nozīmīga digitālā tirgus daļa;

25. atkārto savu aicinājumu Komisijai precizēt noteikumus attiecībā uz piemērojamajām tiesībām personas datu aizsardzības jomā;

26. uzskata, ka jāstiprina atbildīgo par datu apstrādi pienākumi, lai nodrošinātu atbilstību datu aizsardzības tiesību aktiem, cita starpā nosakot proaktīvus mehānismus un procedūras, un šajā sakarībā atzinīgi vērtē citus Komisijas paziņojumā ietvertos norādījumus;

27. atgādina, ka šajā kontekstā īpaša uzmanība ir jāpievērš datu apstrādātājiem, uz kuriem attiecas profesionālā noslēpuma neizpaušanas pienākums, un ka attiecībā uz tiem jāapsver īpašu datu aizsardzības uzraudzības struktūru izveide;

28. atzinīgi vērtē un atbalsta Komisijas apsvērumus ieviest atbildības principu, jo ir ļoti svarīgi nodrošināt, lai datu apstrādātāji rīkotos atbildīgi; vienlaikus aicina Komisiju rūpīgi izvērtēt, kā šādu principu varētu ieviest praksē, un novērtēt tā sekas;

([1]) Ir jāapsver vecuma sliekšņa noteikšana bērniem un vecāku piekrišanas pieprasīšana attiecībā uz to nesasniegušajiem, kā arī jāapsver vecuma apstiprināšanas mehānismi.

Trešdiena, 2011. gada 6. jūlijs

29. atzinīgi vērtē iespēju noteikt obligātu prasību iecelt datu aizsardzības inspektoru uzņēmumos, jo to ES dalībvalstu pieredze, kurās jau ir datu aizsardzības inspektori, pierāda šīs idejas veiksmīgumu; tomēr norāda, ka tas ir rūpīgi jāizvērtē saistībā ar maziem uzņēmumiem un mikrouzņēmumiem un tam nav jārada tiem pārmērīgas izmaksas vai slogs;

30. šajā kontekstā atzinīgi vērtē centienus vienkāršot un saskaņot spēkā esošo paziņošanas sistēmu;

31. uzskata, ka ir izšķiroši svarīgi padarīt privātuma ietekmes novērtējumus obligātus, lai noteiktu riskus saistībā ar privātumu, paredzētu problēmas un piedāvātu proaktīvus risinājumus;

32. uzskata, ka ir ļoti svarīgi, lai datu subjektu tiesības būtu realizējamas; norāda, ka varētu ieviest tiesu prāvu praksi, kas būtu instruments, ar kura palīdzību indivīdi varētu kolektīvi aizstāvēt savas tiesības attiecībā uz datiem un pieprasīt kompensāciju par zaudējumiem, ko sagādājuši datu lietošanas pārkāpumi; tomēr norāda, ka šādā ieviešanā ir jānosaka robežas, lai izvairītos no ļaunprātīgas izmantošanas; prasa, lai Komisija paskaidrotu saistību starp šo paziņojumu par datu aizsardzību un pašreizējo sabiedrisko apspriešanu par kolektīvo tiesisko aizsardzību; tādēļ aicina izveidot kolektīvās tiesiskās aizsardzības mehānismus pret datu aizsardzības noteikumu pārkāpumiem, lai varētu atlīdzināt datu subjektiem nodarītos zaudējumus;

33. uzsver, ka nepieciešama pienācīga saskaņota piemērošana visā ES; aicina Komisiju paredzēt tās tiesību aktu priekšlikumā stingrus un preventīvus sodus, tostarp krimināsodus, par personas datu nepareizu un ļaunprātīgu izmantošanu;

34. mudina Komisiju ieviest sistēmu obligātiem vispārīgiem paziņojumiem par personas datu aizsardzības pārkāpumu, attiecinot to arī uz citām nozarēm, ne vien telekomunikāciju nozari, vienlaikus nodrošinot, ka a) tā nekļūst par ierastu trauksmes signālu sūtīšanu attiecībā uz visa veida pārkāpumiem, bet galvenokārt attiecībā uz tiem, kas var negatīvi ietekmēt indivīdu, b)visi pārkāpumi bez izņēmuma tiek reģistrēti un ir pieejami datu aizsardzības vai citām atbilstošām iestādēm pārbaudei vai izvērtēšanai, tādējādi nodrošinot līdzvērtīgus konkurences apstākļus un vienotu aizsardzību visiem indivīdiem;

35. uzskata, ka jēdzieni „integrēta privātuma aizsardzība" un „privātuma aizsardzība pēc noklusējuma" stiprina datu aizsardzību, un atbalsta to konkrētu piemērošanu un turpmāku izstrādi, kā arī nepieciešamību popularizēt privātuma aizsardzību uzlabojošas tehnoloģijas; šajā saistībā uzsver, ka jebkuras integrētas privātuma aizsardzības īstenošanas pamatā jābūt saprātīgiem un konkrētiem kritērijiem un definīcijām, lai aizsargātu lietotāja tiesības uz privātumu un datu aizsardzību un nodrošinātu juridisko noteiktību, pārredzamību, līdzvērtīgus konkurences apstākļus un brīvu apriti; uzskata, ka integrētas privātuma aizsardzības pamatā vajadzētu būt datu minimizēšanas principam, kas nozīmē, ka visi produkti, pakalpojumi un sistēmas jāizstrādā tādā veidā, lai vāktu, izmantotu un pārsūtītu tikai tos personas datus, kas ir pilnīgi nepieciešami to darbībai;

36. atzīmē, ka mākoņdatošanas attīstība un arvien plašāka izmantošana rada jaunus izaicinājumus attiecībā uz privātumu un personas datu aizsardzību; tādēļ pieprasa precizēt atbildīgo par datu apstrādi, datu apstrādātāju un izvietotāju darbībspējas, lai labāk sadalītu attiecīgo juridisko atbildību un lai nodrošinātu, ka datu subjekti zinātu, kur tiek glabāti viņu dati, kam tie ir pieejami, kas lemj par to izmantošanu, kā arī — kādi dublēšanas un atjaunošanas procesi tiek veikti;

37. tādēļ aicina Komisiju pievērst pienācīgu uzmanību datu aizsardzības jautājumiem saistībā ar mākoņdatošanu, vienlaikus pārskatot Direktīvu 95/46/EK, un nodrošināt, ka datu aizsardzības noteikumi attiecas uz visām ieinteresētajām pusēm, tostarp telekomunikāciju uzņēmumiem un sakaru uzņēmumiem ārpus telekomunikāciju jomas;

38. aicina Komisiju nodrošināt, lai visi interneta operatori uzņemtos atbildību par personas datu aizsardzību, un mudina reklāmas aģentūras un izdevējus iepriekš skaidri informēt interneta lietotājus par jebkuru ar viņiem saistītu datu vākšanu.

39. atzinīgi vērtē tikko parakstīto vienošanos par radiofrekvenču identifikācijas sistēmas (*RFID*) lietojumiem paredzēto privātuma un datu aizsardzības ietekmes novērtējuma sistēmu, kuras mērķis ir aizsargāt patērētāju privātumu pirms *RFID* marķējuma ieviešanas attiecīgajā tirgū;

40. atbalsta centienus turpināt pašregulācijas iniciatīvu, piemēram, rīcības kodeksu attīstīšanu un brīvprātīgu ES sertifikācijas sistēmu izveides apsvēršanu kā papildu soļus likumdošanas pasākumiem, vienlaikus apgalvojot, ka ES datu aizsardzības režīms ir balstīts uz tiesību aktiem, kas nosaka augsta līmeņa garantijas; prasa Komisijai veikt ietekmes novērtējumu par pašregulācijas iniciatīvām kā instrumentu datu aizsardzības noteikumu efektīvākai piemērošanai;

41. uzskata, ka jebkurai sertifikācijas vai marķēšanas sistēmai ir jābūt ar garantētu integritāti un uzticamību, tehnoloģiski neitrālai, atpazīstamai globālā līmenī un viegli pieejamai, lai neradītu pievienošanās šķēršļus;

42. pauž piekrišanu valstu datu aizsardzības iestāžu statusa un pilnvaru turpmākai precizēšanai, stiprināšanai un saskaņošanai, kā arī ES datu aizsardzības noteikumu vienotākas piemērošanas iekšējā tirgū iespēju izpētīšanai; turklāt uzsver, cik nozīmīgi ir nodrošināt saskaņotību starp EDAU, dalībvalstu datu aizsardzības iestāžu un 29. panta darbgrupas pilnvaru īstenošanu;

43. uzsver, ka šajā ziņā jāstiprina 29. panta darba grupas loma un pilnvaras, lai uzlabotu koordināciju un sadarbību starp dalībvalstu datu aizsardzības iestādēm, īpaši attiecībā uz nepieciešamību nodrošināt datu aizsardzības noteikumu vienotu piemērošanu;

44. aicina Komisiju jaunajā tiesiskajā regulējumā precizēt būtiskos nosacījumus attiecībā uz valsts datu aizsardzības iestāžu neatkarību, izslēdzot jebkādu ārēju ietekmi [1]; uzsver, ka valsts datu aizsardzības iestādēm jāpiešķir nepieciešamie līdzekļi un saskaņotas pilnvaras izmeklēt un uzlikt sodus;

Datu aizsardzības stiprināšana pasaules mērogā

45. aicina Komisiju vienkāršot un stiprināt datu starptautiskās pārsūtīšanas procedūras — juridiski saistošus nolīgumus un uzņēmumiem saistošos noteikumus — un, pamatojoties uz iepriekš minētajiem personas datu aizsardzības principiem, formulēt vērienīgus ES pamata datu aizsardzības aspektus, kurus izmantot starptautiskajos nolīgumos; uzsver, ka ES personas datu aizsardzības nolīgumu ar trešām valstīm noteikumiem jānodrošina Eiropas pilsoņiem tāds pats personas datu aizsardzības līmenis kā Eiropas Savienībā;

[1] Saskaņā ar LESD 16. pantu un Hartas 8. pantu.

Trešdiena, 2011. gada 6. jūlijs

46. uzskata, ka vairāk jāprecizē, stingrāk jāīsteno, jāizpilda un jāuzrauga Komisijas pietiekamības novērtēšanas procedūra un rūpīgāk jāizstrādā kritēriji un prasības datu aizsardzības līmeņa novērtēšanai trešā valstī un starptautiskas organizācijas ietvaros, ņemot vērā jauno apdraudējumu privātumam un personas datiem;

47. aicina Komisiju rūpīgi izvērtēt drošā patvēruma principu efektivitāti un pareizu piemērošanu;

48. atzinīgi vērtē Komisijas nostāju par savstarpīgumu attiecībā uz to datu subjektu aizsardzības līmeni, kuru dati tiek piegādāti trešām valstīm, vai turēti tajās; prasa Komisiju veikt izšķirošus pasākumus, lai uzlabotu regulatīvu sadarbību ar trešām valstīm attiecībā uz piemērojamo noteikumu precizēšanu un ES un trešo valstu datu aizsardzības tiesību aktu vienādošanu; prasa Komisiju izvirzīt šo, kā prioritātes programmu atsāktajā Transatlantiskajā ekonomikas padomē;

49. atbalsta Komisijas centienus pastiprināt sadarbību ar trešām valstīm un starptautiskām organizācijām, tostarp Apvienoto Nāciju Organizāciju, Eiropas Padomi un ESAO, kā arī ar standartizācijas organizācijām, piemēram, Eiropas Standartizācijas komiteju (*CEN*), Starptautisko standartizācijas organizāciju (*ISO*), Globālā tīmekļa konsorciju (*W3C*) un Interneta tehnisko uzdevumgrupu (*IETF*); mudina izstrādāt starptautiskus standartus ([1]), vienlaikus nodrošinot saskaņotību starp starptautisko standartu iniciatīvām un patlaban notiekošajiem pārskatīšanas procesiem ES, ESAO un Eiropas Padomē;

*

* *

50. uzdod priekšsēdētājam nosūtīt šo rezolūciju Padomei un Komisijai.

([1]) Skatīt Madrides deklarāciju: Globālie privātuma standarti globālā pasaulē, 2009. gads un Rezolūciju par starptautiskajiem standartiem, kas pieņemta 32. starptautiskās datu aizsardzības un privātuma komisāru konferencē Jeruzalemē 2010. gada 27.-29. oktobrī.

Komisijas darba programmas sagatavošana 2012. gadam

P7_TA(2011)0327

Eiropas Parlamenta 2011. gada 6. jūlija rezolūcija par Komisijas darba programmu 2012. gadam

(2013/C 33 E/11)

Eiropas Parlaments,

— ņemot vērā Komisijas paziņojumu par Komisijas darba programmu 2011. gadam (COM(2010)0623/2),

— ņemot vērā spēkā esošo Pamatnolīgumu par Eiropas Parlamenta un Komisijas attiecībām, jo īpaši tā 4. pielikumu,

— ņemot vērā regulāro dialogu starp visiem Komisijas komisāriem un Parlamenta komitejām un Priekšsēdētāju konferencei iesniegto Komiteju priekšsēdētāju konferences 2011. gada 7. jūnija kopsavilkuma ziņojumu,