Piektdiena, 2021. gada 21. maija

P9_TA(2021)0262

Apvienotās Karalistes nodrošināta pienācīga personas datu aizsardzība

Eiropas Parlamenta 2021. gada 21. maija rezolūcija par Apvienotās Karalistes nodrošinātu pienācīgu personas datu aizsardzību (2021/2594(RSP))

(2022/C 15/23)

Eiropas Parlaments,

— ņemot vērā Eiropas Savienības Pamattiesību hartu (Harta), jo īpaši tās 7., 8., 16., 47. un 52. pantu,

— ņemot vērā Eiropas Savienības Tiesas (EST) 2020. gada 16. jūlija spriedumu lietā C-311/18 – *Data Protection Commissioner* pret *Facebook Ireland Limited, Maximillian Schrems* (spriedums "Schrems II" lietā) ([1]),

— ņemot vērā EST 2015. gada 6. oktobra spriedumu lietā C-362/14 Maximillian Schrems pret Data Protection Commissioner (spriedums "Schrems I" lietā) ([2]),

— ņemot vērā EST 2020. gada 6. oktobra spriedumu lietā C-623/17 *Privacy International* pret *Secretary of State of Foreign and Commonwealth affairs* ([3]),

— ņemot vērā 2014. gada 12. marta rezolūciju par ASV Nacionālās drošības aģentūras novērošanas programmu, novērošanas struktūrām dažādās dalībvalstīs un ietekmi uz ES pilsoņu pamattiesībām un transatlantisko sadarbību tieslietu un iekšlietu jomā ([4]),

— ņemot vērā 2018. gada 5. jūlija rezolūciju par ES un ASV privātuma vairoga nodrošinātās aizsardzības pietiekamību ([5]),

— ņemot vērā 2018. gada 25. oktobra rezolūciju par "Facebook" lietotāju datu izmantošanu, ko veicis uzņēmums "Cambridge Analytica", un ietekmi uz datu aizsardzību ([6]),

— ņemot vērā 2021. gada 20. maija rezolūciju par Eiropas Savienības Tiesas 2020. gada 16. jūlija spriedumu lietā C-311/18 – *Data Protection Commissioner* pret *Facebook Ireland Limited, Maximillian Schrems* (*Schrems II*) ([7]),

— ņemot vērā 2020. gada 26. novembra rezolūciju par ES tirdzniecības politikas pārskatīšanu ([8]),

— ņemot vērā 2020. gada 31. decembra Tirdzniecības un sadarbības nolīgumu starp Eiropas Savienību un Eiropas Atomenerģijas kopienu, no vienas puses, un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, no otras puses ([9]),

— ņemot vērā 2021. gada 28. aprīļa rezolūciju par ES un Apvienotās Karalistes sarunu rezultātiem ([10]),

— ņemot vērā Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulu (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti ([11]) (Vispārīgā datu aizsardzības regula — VDAR),

---

([1]) ECLI:EU:C:2020:559.
([2]) ECLI:EU:C:2015:650.
([3]) ECLI:EU:C:2020:790.
([4]) OV C 378, 9.11.2017., 104. lpp.
([5]) OV C 118, 8.4.2020., 133. lpp.
([6]) OV C 345, 16.10.2020., 58. lpp.
([7]) Pieņemtie teksti, P9_TA(2021)0256.
([8]) Pieņemtie teksti, P9_TA(2020)0337.
([9]) OV L 444, 31.12.2020., 14. lpp.
([10]) Pieņemtie teksti, P9_TA(2021)0141.
([11]) OV L 119, 4.5.2016., 1. lpp.

— ņemot vērā Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Direktīvu (ES) 2016/680 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi, ko veic kompetentās iestādes, lai novērstu, izmeklētu, atklātu noziedzīgus nodarījumus vai sauktu pie atbildības par tiem vai izpildītu krimināLsodus, un par šādu datu brīvu apriti ([12]) (Direktīva par datu aizsardzību tiesībaizsardzības jomā),

— ņemot vērā Eiropas Parlamenta un Padomes Direktīvu 2002/58/EK (2002. gada 12. jūlijs) par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē ([13]),

— ņemot vērā Komisijas 2017. gada 10. janvāra priekšlikumu Eiropas Parlamenta un Padomes regulai par privātās dzīves neaizskaramību un personas datu aizsardzību elektronisko sakaru jomā (COM(2017)0010) un 2017. gada 20. oktobrī pieņemto Eiropas Parlamenta nostāju par to ([14]),

— ņemot vērā Eiropas Datu aizsardzības kolēģijas (EDAK) ieteikumus, tostarp tās 2021. gada 9. marta paziņojumu par E-privātuma regulu un tās 2020. gada 10. novembra Ieteikumu 01/2020 par pasākumiem, kas papildina datu nosūtīšanai nepieciešamo instrumentu izmantošanu, lai nodrošinātu personas datu aizsardzību atbilstoši ES noteiktajam drošības līmenim;

— ņemot vērā 29. panta datu aizsardzības darba grupas 2018. gada 6. februārī pieņemto un EDAK apstiprināto Rokasgrāmatu par pietiekamību,

— ņemot vērā EDAK 2021. gada 2. februāra Ieteikumu 01/2021 par Rokasgrāmatu par pietiekamību saskaņā ar Direktīvu par datu aizsardzību tiesībaizsardzības jomā,

— ņemot vērā lēmumu par aizsardzības līmeņa pietiekamību projektus, ko Komisija publicēja 2021. gada 19. februārī, no kuriem vienu pieņēma, pildot VDAR ([15]), bet otru, pildot Direktīvu par datu aizsardzību tiesībaizsardzības jomā ([16]),

— ņemot vērā EDAK 2021. gada 13. aprīļa atzinumus Nr. 14/2021 un Nr. 15/2021 par Eiropas Komisijas īstenošanas lēmuma projektu saskaņā ar Direktīvu (ES) 2016/680 par personas datu pienācīgu aizsardzību Apvienotajā Karalistē,

— ņemot vērā Eiropas Cilvēktiesību konvenciju (ECTK) un Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi, kā arī tās grozījumu protokolu ("Konvencija 108+"), kurā Apvienotā Karaliste ir līgumslēdzēja puse,

— ņemot vērā Eiropas Parlamenta un Padomes 2011. gada 16. februāra Regulu (ES) Nr. 182/2011, ar ko nosaka normas un vispārīgus principus par dalībvalstu kontroles mehānismiem, kuri attiecas uz Komisijas īstenošanas pilnvaru izmantošanu,

— ņemot vērā Reglamenta 132. panta 2. punktu,

— ņemot vērā Pilsoņu brīvību, tieslietu un iekšlietu komitejas rezolūcijas priekšlikumu,

A. tā kā spēja nosūtīt personas datus pāri robežām var būt ļoti nozīmīgs inovācijas, produktivitātes un ekonomiskās konkurētspējas virzītājspēks, un tai ir izšķiroša nozīme, īstenojot efektīvu sadarbību cīņā pret pārrobežu organizēto un smago noziedzību, kā arī cīņā pret terorismu, kas arvien vairāk ir atkarīga no personas datu apmaiņas;

B. tā kā spriedumā "Schrems I" lietā EST norādīja, ka izlūkošanas iestāžu neselektīva piekļuve elektronisko sakaru saturam ir Hartas 7. pantā paredzēto tiesību uz komunikācijas konfidencialitāti būtības pārkāpums un ka Amerikas Savienotās Valstis nenodrošina pietiekamus tiesiskās aizsardzības līdzekļus pret masveida novērošanu ārpus ASV dzīvojošām personām, tādējādi pārkāpjot Hartas 47. pantu;

([12]) OV L 119, 4.5.2016., 89. lpp.
([13]) OV L 201, 31.7.2002., 37. lpp.
([14]) A8-0324/2017.
([15]) Projekts Komisijas īstenošanas lēmumam, kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Regulu (ES) 2016/679, par personas datu aizsardzības pietiekamību Apvienotajā Karalistē.
([16]) Projekts Komisijas īstenošanas lēmumam, kas pieņemts saskaņā ar Eiropas Parlamenta un Padomes Direktīvu (ES) 2016/680, par personas datu aizsardzības pietiekamību Apvienotajā Karalistē,

Piektdiena, 2021. gada 21. maija

C. tā kā Apvienotā Karaliste ierasti ir bijusi svarīga daudzu ES dalībvalstu tirdzniecības partnere, kā arī tuva sabiedrotā drošības jomā; tā kā, neraugoties uz Apvienotās Karalistes izstāšanos no Eiropas Savienības, ES un Apvienotajai Karalistei būtu jāsaglabā šī ciešā sadarbība, jo tā būs izdevīga abām pusēm;

D. tā kā Eiropas uzņēmumiem ir vajadzīga juridiskā skaidrība un noteiktība, jo spēja nosūtīt personas datus pāri robežām kļūst arvien svarīgāka visu veidu uzņēmumiem, kas piegādā preces un sniedz pakalpojumus starptautiskā mērogā; tā kā ir ļoti svarīgi attiecībā uz Apvienoto Karalisti pieņemt lēmumu par aizsardzības līmeņa pietiekamību saskaņā ar VDAR, jo daudziem Eiropas uzņēmumiem ir tirdzniecības darījumi pāri Lamanšam, jo īpaši ņemot vērā to, ka kopš *Brexit* stāšanās spēkā vēl ir pagājis salīdzinoši neilgs laiks un datu plūsmas Savienībā nav tikušas pakļautas ierobežojumiem; tā kā, ja netiks pieņemts stabils aizsardzības līmeņa pietiekamības satvars, pastāv risks, ka var tikt traucēta personas datu pārrobežu nosūtīšana starp ES un Apvienoto Karalisti komerciālos nolūkos, kā arī rasties lielas atbilstības nodrošināšanas izmaksas;

E. tā kā Tirdzniecības un sadarbības nolīgums (TSN) ietver vairākus papildu aizsardzības pasākumus un nosacījumus attiecīgo personas datu apmaiņai tiesībaizsardzības kontekstā, tā kā sarunas par personas datu plūsmām notika paralēli sarunām par TSN, bet līdz pārejas perioda beigām (2020. gada 31. decembrim) tās vēl nebija pabeigtas; tā kā TSN kā pagaidu risinājums tika iekļauta pārejas klauzula ar nosacījumu, ka Apvienotā Karaliste apņemas nemainīt savu pašreizējo personas datu aizsardzības režīmu, lai nodrošinātu, ka datu plūsmas starp Apvienoto Karalisti un ES turpinās līdz lēmuma par aizsardzības līmeņa pietiekamību pieņemšanai; tā kā sākotnējais četru mēnešu periods ir pagarināts un beigsies 2021. gada jūnija beigās;

F. tā kā novērtējums, ko Komisija veica, pirms nākt klajā ar īstenošanas lēmuma priekšlikumu, bija nepilnīgs un neatbilda prasībām, ko EST izvirzījusi pietiekamības novērtējumiem, kā uzsvēra EDAK savos atzinumos par aizsardzības līmeņa pietiekamību, kuros tā iesaka Komisijai dziļāk izvērtēt Apvienotās Karalistes tiesību aktu un prakses konkrētus aspektus attiecībā uz datu lielapjoma vākšanu, izpaušanu ārvalstīs un starptautiskiem nolīgumiem izlūkdatu apmaiņas, tiesībaizsardzības nolūkos savāktās informācijas papildu izmantošanas un tiesu komisāru neatkarības jomā;

G. tā kā Komisija nav ņēmusi vērā dažus Apvienotās Karalistes tiesību aktu un/vai prakses aspektus, kā rezultātā ir izstrādāti īstenošanas lēmumu projekti, kas ir pretrunā ES tiesību aktiem; tā kā VDAR 45. pantā ir noteikts, ka "izvērtējot aizsardzības līmeņa pietiekamību, Komisija jo īpaši ņem vērā… attiecīgos tiesību aktus, gan vispārējos, gan nozaru, tostarp attiecībā uz sabiedrisko drošību, aizsardzību, valsts drošību un krimināltiesībām un publisko iestāžu piekļuvi personas datiem, kā arī šādu tiesību aktu, datu aizsardzības noteikumu, dienesta noteikumu un drošības pasākumu īstenošanu, tostarp noteikumus par personas datu tālāku nosūtīšanu uz citu trešo valsti vai starptautisko organizāciju, kurus ievēro minētajā valstī vai minētajā starptautiskajā organizācijā, judikatūru" un "starptautiskās saistības, ko ir uzņēmusies attiecīgā trešā valsts vai starptautiskā organizācija, vai citi pienākumi, kas izriet no juridiski saistošām konvencijām vai instrumentiem, kā arī no tās dalības daudzpusējās vai reģionālās sistēmās, jo īpaši saistībā ar personas datu aizsardzību", kas ietver tādus citās jomās noslēgtus starptautiskus nolīgumus, kuri attiecas uz piekļuvi datiem vai informācijas kopīgošanu, un ka tāpēc šādi starptautiski nolīgumi ir jāizvērtē;

H. tā kā EST spriedumā "Schrems I" lietā nepārprotami norādīja: "pārbaudot trešās valsts nodrošināto aizsardzības līmeni, Komisijai ir pienākums izvērtēt no vietējiem tiesību aktiem vai starptautiskajām saistībām izrietošo un minētajā valstī piemērojamo noteikumu saturu, kā arī praksi, kas tiek īstenota, lai nodrošinātu atbilstību minētajiem noteikumiem, jo saskaņā ar Direktīvas 95/46/EK 25. panta 2. punktu Komisijai ir jāņem vērā visi apstākļi, kas saistīti ar personas datu nosūtīšanu uz trešām valstīm" (75. punkts);

I. tā kā saskaņā ar Līgumiem izlūkdienestu darbība un informācijas kopīgošana ar trešām valstīm neietilpst ES tiesību aktu darbības jomā attiecībā uz dalībvalstīm, jo šie faktori ir ietverti trešo valstu nodrošinātā personas datu aizsardzības līmeņa novērtējuma tvērumā, kā to apstiprinājusi EST savos spriedumos lietā "Schrems I" un "Schrems II";

J. tā kā datu aizsardzības standarti balstās ne tikai uz spēkā esošajiem tiesību aktiem, bet arī uz šo aktu piemērošanu praksē, un tā kā Komisija, gatavojot savu lēmumu, novērtēja tikai tiesību aktus, nevis to reālo piemērošanu praksē;

K. tā kā Komisija pašlaik atzīst, ka pienācīgu aizsardzības līmeni saskaņā ar VDAR nodrošina 12 valstis, un ir nesen noslēgusi sarunas ar Korejas Republiku šajā jomā; tā kā Apvienotā Karaliste ir pirmā valsts, kurai Komisija ierosina piešķirt pietiekama datu aizsardzības līmeņa statusu saskaņā ar Direktīvu par datu aizsardzību tiesībaizsardzības jomā;

L. tā kā Apvienotās Karalistes gadījums no visiem iepriekšējiem aizsardzības līmeņa pietiekamības novērtējumiem atšķiras ar to, ka tiek vērtēta bijusī ES dalībvalsts, kura ir iekļāvusi VDAR noteikumus savos tiesību aktos un turklāt ir paredzējusi, ka pēc pārejas perioda beigām tiks piemēroti visi no ES tiesībām atvasinātie valsts tiesību akti, tostarp tie tiesību akti, ar kuriem transponē Direktīvu par datu aizsardzību tiesībaizsardzības jomā,

I. **VISPĀRĪGĀ DATU AIZSARDZĪBAS REGULA**

Vispārīgi apsvērumi

1. atzīmē, ka Apvienotā Karaliste ir parakstījusi ECTK un Eiropas Padomes Konvenciju par personu aizsardzību attiecībā uz personas datu automātisko apstrādi; sagaida, ka Apvienotā Karaliste nodrošinās tādu pašu datu aizsardzības minimuma satvaru, neraugoties uz tās izstāšanos no Eiropas Savienības;

2. atzinīgi vērtē Apvienotās Karalistes apņemšanos ievērot demokrātiju un tiesiskumu un aizsargāt un savā teritorijā nodrošināt, ka tiek ievērotas pamattiesības, piemēram, ECTK noteiktās pamattiesības, tostarp augsta līmeņa datu aizsardzība; atgādina, ka tas ir obligāts priekšnosacījums ES sadarbībai ar Apvienoto Karalisti; atgādina, ka, neraugoties uz to, ka ECTK 8. pants par tiesībām uz privāto dzīvi ir daļa no Apvienotās Karalistes tiesību aktiem saskaņā ar *Human Rights Act 1998* (1998. gada Likums par cilvēktiesībām), kā arī saskaņā ar paražu tiesībām, kā nosaka jaunais delikts par privātās dzīves informācijas ļaunprātīgu izmantošanu, valdība balsoja pret centieniem tiesības uz datu aizsardzību noteikt kā pamattiesības;

3. norāda, ka ES datu pārvaldībā ir izvēlējusies ievērot uz cilvēktiesībām orientētu pieeju, izstrādājot VDAR paredzētos stingros datu aizsardzības noteikumus, un tāpēc ir ļoti nobažījies par Apvienotās Karalistes premjerministra publiskajiem paziņojumiem, kuros deklarēts, ka Apvienotā Karaliste centīsies atteikties no ES datu aizsardzības noteikumiem un veidos savus "suverēnus" kontroles mehānismus šajā jomā; uzskata, ka Apvienotās Karalistes 2020. gada Valsts datu stratēģija nozīmē pāreju no personas datu aizsardzības uz plašāku datu izmantošanu un kopīgošanu, kas neatbilst VDAR noteiktajiem taisnīguma, datu minimizēšanas un mērķa ierobežojuma principiem; norāda, ka EDAK savos atzinumos par aizsardzības līmeņa pietiekamību uzsvēra, ka tas varētu radīt riskus saistībā ar to personas datu aizsardzību, kas tiktu nosūtīti no ES;

4. norāda, ka pamatoti lēmumi par aizsardzības līmeņa pietiekamību ievērojami veicina privātpersonu pamattiesību aizsardzību un juridisko noteiktību uzņēmumiem; tomēr uzsver, ka lēmumiem par aizsardzības līmeņa pietiekamību, kas balstīti uz nepilnīgiem novērtējumiem un kam neseko Komisijas veikta pienācīga izpildes nodrošināšana, var būt pretējs efekts, ja tos apstrīd tiesā;

5. norāda, ka novērtējums, ko Komisija veica, pirms nākt klajā ar īstenošanas lēmuma priekšlikumu, bija nepilnīgs un neatbilda prasībām, ko EST izvirzījusi pietiekamības novērtējumiem, kā uzsvēra EDAK savos atzinumos par aizsardzības līmeņa pietiekamību, kuros tā iesaka Komisijai dziļāk izvērtēt Apvienotās Karalistes tiesību aktu un prakses konkrētus aspektus attiecībā uz datu lielapjoma vākšanu, izpaušanu ārvalstīs un starptautiskiem nolīgumiem izlūkdatu apmaiņas, tiesībaizsardzības nolūkos savāktās informācijas papildu izmantošanas un tiesu komisāru neatkarības jomā;

VDAR izpildes nodrošināšana

6. pauž bažas par to, ka Apvienotā Karaliste pat tad, kad tā vēl bija ES dalībvalsts, VDAR izpildi nenodrošināja pietiekamā apmērā un bieži to pat nenodrošināja vispār; jo īpaši norāda uz Apvienotās Karalistes Informācijas komisāra biroja (*Information Commissioner's Office* (*ICO*)) pienācīgu izpildes pasākumu trūkumu pagātnē; kā uz piemēru norāda uz to, ka *ICO* sakarā ar sūdzību par reklāmu tehnoloģijām sarīkoja divus pasākumus ar ieinteresēto personu piedalīšanos, sagatavoja ziņojumu ("Update Report on Adtech" — "Aktualizētais ziņojums par reklāmu tehnoloģijām") un pauda atziņu, ka "šķiet, ka reklāmu tehnoloģiju nozarei ir nenopietna attieksme pret datu aizsardzības prasībām", bet pēc tam to slēdza,

nekādi neizmantojot savas izpildes nodrošināšanas pilnvaras ([17]); pauž bažas par to, ka izpildes nodrošināšanas pasākumu neveikšana ir strukturāla problēma, kā izklāstīts ICO regulatīvo pasākumu politikas dokumentā, kurā nepārprotami norādīts, ka "lielākajā daļā gadījumu birojs savas pilnvaras izmantos tikai smagākajos informācijas tiesību ievērošanas pienākumu pārkāpumu gadījumos. Tie parasti ir saistīti ar apzinātām, tīšām vai nolaidīgām darbībām vai atkārtotiem informācijas tiesību ievērošanas pienākumu pārkāpumiem, ar kuriem personām tiek nodarīts kaitējums vai zaudējumi"; uzsver — praksē tas nozīmē, ka šīs nostājas dēļ liels skaits datu aizsardzības tiesību aktu pārkāpumu Apvienotajā Karalistē nav novērsti;

7. pieņem zināšanai Apvienotās Karalistes Valsts datu stratēģiju, kurā pēdējie atjauninājumi pieņemti 2020. gada 9. decembrī un kurā pausts, ka notiks pāreja no personas datu aizsardzības uz datu plašāku izmantošanu un kopīgošanu lielākā mērogā; norāda, ka stratēģijā paustā nostāja "datu neizpaušana var negatīvi ietekmēt sabiedrību" nav saderīga ar VDAR un primārajos tiesību aktos ietvertajiem datu minimizēšanas un izmantošanas mērķa ierobežojuma principiem;

8. ņem vērā, ka Konstitucionālo jautājumu komiteja 2004. gadā ([18]) un Apvienotās Karalistes parlamenta Sabiedrisko lietu komiteja 2014. gadā ([19]) ieteica aizsargāt *ICO* neatkarību, paredzot, ka turpmāk to vairs neieceļ digitālo plašsaziņas līdzekļu un sporta ministrs, bet ka tā ir parlamentam pakļauta parlamenta amatpersona; pauž nožēlu par to, ka šis ieteikums nav izpildīts;

Datu apstrāde imigrācijas kontroles nolūkā

9. konstatē, ka Apvienotās Karalistes datu aizsardzības tiesību aktos ir paredzēta atkāpe no dažiem tādiem fundamentāliem datu aizsardzības tiesību un principu aspektiem kā piekļuves tiesības un datu subjektu tiesības zināt, ar kādām struktūrām viņu dati ir tikuši kopīgoti, ja šāda aizsardzība "apdraudētu efektīvu imigrācijas kontroli" ([20]); uzsver, ka atbrīvojuma izmantošanas uzraudzība ir jāveic un tā pareizība jānodrošina saskaņā ar standartiem, kas paredzēti Rokasgrāmatā par pietiekamību, kurā prasīts ņemt vērā gan praksi, gan principus, norādot, ka "jāņem vērā ne tikai to noteikumu saturs, kurus piemēro uz trešo valsti nosūtītajiem personas datiem, bet arī sistēma, kas ieviesta, lai nodrošinātu šādu noteikumu iedarbīgumu"; atzīst, ka šo atbrīvojumu, kas ir pieejams visiem datu pārziņiem Apvienotajā Karalistē, ir apstiprinājusi *ICO* un tiesa, uz to var atsaukties tikai katrā gadījumā atsevišķi un to var piemērot nepieciešamā un samērīgā veidā; atgādina nesen atklāto informāciju, saskaņā ar ko Iekšlietu ministrijai ir tikuši iesniegti 17 780 piekļuves pieprasījumi saistībā ar ministrijas apstrādātajiem datiem par 146,75 miljoniem datu subjektu laikposmā no 2018. gada 1. aprīļa līdz 2019. gada 31. martam, un ka 2020. gadā Iekšlietu ministrija atbrīvojumu imigrācijas kontroles apsvērumu dēļ piemēroja vairāk nekā 70 % no datu subjektu pieprasījumiem; uzsver, ka pat tajos gadījumos, kad Iekšlietu ministrija izmantoja minēto atbrīvojumu, piekļuve informācijai netika pilnībā liegta, bet ierobežota, sniedzot piekļuvi tikai rediģētiem dokumentiem;

10. norāda, ka šis atbrīvojums tagad attiecas uz ES pilsoņiem, kuri uzturas vai plāno uzturēties Apvienotajā Karalistē; ir ļoti nobažījies, ka ar šo atbrīvojumu tiek izslēgtas nozīmīgas iespējas garantēt pārskatatbildību un tiesisko aizsardzību, un uzsver, ka šādi netiek nodrošināta pietiekama aizsardzība;

([17]) *Lomas, N.*, "*UK's ICO faces legal action after closing adtech complaint with nothing to show for it*", *TechCrunch*, Sanfrancisko, 2020.

([18]) Īpašās Konstitucionālo jautājumu komitejas septītais ziņojums, ko Pārstāvju palāta publicēja 2006. gada 13. jūnijā. Tā 108. punkts ir šāds: "Uzskatām, ka būtu ievērojami labāk, ja Informācijas komisārs par savu darbu būtu tieši atbildīgs parlamenta priekšā un ja tā darbību finansētu parlaments, un iesakām izskatīt šādu iespēju, kad radīsies izdevība grozīt attiecīgos tiesību aktus."

([19]) Valsts pārvaldes komitejas ziņojums "Who's accountable? Relationships between Government and arm's-length bodies" ("Kurš ir atbildīgs? Valdības un pakļautības iestāžu attiecības"), ko Pārstāvju palāta publicēja 2014. gada 4. novembrī. Tā 64. punkts ir šāds: "Informācijas komisāram un Karaliskajai cietumu inspekcijai vajadzētu būt lielākai neatkarībai no valdības, un par savu darbu tiem būtu jāziņo parlamentam. Informācijas komisāram, Civildienesta ierēdņu iecelšanas komisāram un Sabiedriskās dzīves standartu komitejas priekšsēdētājam būtu jākļūst par parlamenta amatpersonām tāpat kā Ombudam parlamentārajos un veselības aprūpes pakalpojumu jautājumos un Valsts kontrolierim."

([20]) "*Open Rights Group*" 2021. gada 3. marta paziņojums presei "*Documents reveal controversial Immigration Exemption used in 70 % of access requests to Home Office*" ("Dokumenti liecina par to, ka atbrīvojums imigrācijas kontroles apsvērumu dēļ 2020. gadā piemērots vairāk nekā 70 % no datu subjektu pieprasījumiem Iekšlietu ministrijai").

11. atkārto savas nopietnās bažas par datu subjektu tiesību izņēmumiem Apvienotās Karalistes imigrācijas politikā; atkārto savu nostāju, proti — lai būtu iespējams pieņemt pamatotu lēmumu par aizsardzības līmeņa pietiekamību, vispirms ir jāgroza personas datu apstrādei piemērojamais atbrīvojums imigrācijas kontroles nolūkos — ko tas jau vairākkārt ir paudis, tostarp 2020. gada 12. februāra rezolūcijā par ierosinātajām pilnvarām sarunās par jaunu partnerību ar Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti ([21]) un Pilsoņu brīvību, tieslietu un iekšlietu komitejas 2021. gada 5. februāra atzinumā ([22]); aicina Komisiju censties panākt atbrīvojuma imigrācijas nolūkos atcelšanu vai reformu, kuras rezultātā atbrīvojums un tā izmantošana sniegtu pietiekamas garantijas datu subjektiem un nepārkāptu no trešās valsts gaidītos standartus;

Masveida novērošana

12. atgādina par trauksmes cēlēja *Edward Snowden* atklāto ASV un Apvienotās Karalistes veikto masveida novērošanu; atgādina, ka Apvienotās Karalistes programma "Tempora", ko vada Valdības sakaru galvenā mītne (*GCHQ*), pārtver sakarus reāllaikā, izmantojot optiskās šķiedras maģistrālos interneta kabeļus, un reģistrē datus, lai tos vēlāk varētu apstrādāt un pārmeklēt; atgādina, ka šāda sakaru satura un metadatu masveida novērošana notiek neatkarīgi no tā, vai pastāv kādas konkrētas aizdomas vai mērķa dati;

13. atgādina, ka EST savos spriedumos lietā "Schrems I" un "Schrems II" secināja, ka masveida piekļuve privāto sakaru saturam skar tiesību uz privātumu būtību un ka šādos gadījumos vairs nav jāveic nepieciešamības vai samērīguma pārbaude; uzsver, ka šie principi attiecas uz datu nosūtīšanu uz trešām valstīm, kas nav ASV, tostarp Apvienoto Karalisti;

14. atgādina par savu 2014. gada 12. marta rezolūciju, kurā konstatēts, ka Apvienotās Karalistes izlūkošanas aģentūras *GCHQ* īstenotās neselektīvās un nepamatojoties uz aizdomām veiktās masveida novērošanas programmas nav saderīgas ar nepieciešamības un proporcionalitātes principu demokrātiskā sabiedrībā un nenodrošina pietiekamu aizsardzību atbilstīgi ES datu aizsardzības tiesību aktiem; atzīst, ka Apvienotā Karaliste kopš tā laika ir būtiski pārveidojusi savus uzraudzības tiesību aktus un ieviesusi aizsardzības pasākumus, kas pārsniedz Eiropas Savienības Tiesas (EST) spriedumā "*Schrems II*" ([23]) noteiktos nosacījumus un lielākās daļas dalībvalstu uzraudzības tiesību aktos paredzētos aizsardzības pasākumus; īpaši atzinīgi vērtē to, ka tiek nodrošināta pilnīga piekļuve efektīvai tiesiskajai aizsardzībai; atgādina, ka ANO īpašais referents jautājumos par tiesībām uz privātumu ir atzinīgi novērtējis stingros aizsardzības pasākumus, kas ieviesti ar 2016. gada Likumu par izmeklēšanas pilnvarām (*IPA*) attiecībā uz nepieciešamību, proporcionalitāti un tiesu iestādes sniegtu neatkarīgu atļauju;

15. atgādina, ka Eiropas Cilvēktiesību tiesa 2018. gada septembrī apstiprināja, ka Apvienotās Karalistes masveida datu pārtveršanas un saglabāšanas programmas, tostarp "Tempora", bija "nelikumīgas un nesaderīgas ar demokrātiskai sabiedrībai nepieciešamajiem nosacījumiem" ([24]);

16. uzskata par nepieņemamu to, ka lēmumu par aizsardzības līmeņa pietiekamību projektos nav ņemts vērā ierobežojumu trūkums attiecībā uz Apvienotās Karalistes lielapjoma datu vākšanas pilnvaru izmantošanu vai Apvienotās Karalistes un ASV izlūkošanas operāciju reālo izmantošanu, ko atklātībā cēlis *Edward Snowden*, tostarp šādus apsvērumus:

a) ne ICO, ne tiesas reāli nepārrauga, kā tiek izmantots Apvienotās Karalistes Likumā par datu aizsardzību paredzētais atbrīvojums nacionālās drošības apsvērumu dēļ;

b) Apvienotās Karalistes lielapjoma datu vākšanas pilnvaru ierobežojumi nav paredzēti pašā likumā, kā to prasa EST, bet atstāti izpildvaras ziņā, paredzot "cieņpilnas" tiesas kontroles iespējas;

([21]) Pieņemtie teksti, P9_TA(2020)0033.

([22]) Pilsoņu brīvību, tieslietu un iekšlietu komitejas atzinums par to, lai Savienības vārdā noslēgtu Tirdzniecības un sadarbības nolīgumu starp Eiropas Savienību un Eiropas Atomenerģijas kopienu, no vienas puses, un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti, no otras puses, un Nolīgumu starp Eiropas Savienību un Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti par drošības procedūrām klasificētas informācijas apmaiņai un aizsardzībai, LIBE_AL(2021)680848.

([23]) Eiropas Savienības Tiesas 2020. gada 16. jūlija spriedums lietā C-311/18 *Data Protection Commissioner* pret *Facebook Ireland Limited* un *Maximillian Schrems*, ECLI:EU:C:2020:559.

([24]) Eiropas Cilvēktiesību tiesas 2018. gada 13. septembra spriedums lietā *Big Brother Watch* u.c. pret Apvienoto Karalisti, pieteikumi Nr. 58170/13, 62322/14, 24960/15.

Piektdiena, 2021. gada 21. maija

c) "sekundāro datu" (metadatu) apraksts lēmumu projektos ir ļoti maldinošs, un tajā nav pieminēts, ka šādi dati var būt ļoti atklājoši un privātumu aizskaroši, un ka tiem tiek veikta sarežģīta automātiska analīze (kā to konstatēja ES Tiesa spriedumā *Digital Rights Ireland* lietā ([25])), bet saskaņā ar Apvienotās Karalistes tiesību aktiem metadati netiek pilnvērtīgi aizsargāti pret Apvienotās Karalistes izlūkošanas aģentūru nepamatotu piekļuvi, lielapjoma vākšanu un uz MI balstītu analīzi;

d) "Five Eyes" aģentūras, jo īpaši *GCHQ* un Nacionālā drošības aģentūra (*NSA*) praksē kopīgo visus izlūkošanas datus;

turklāt norāda, ka attiecībā uz ASV uz Apvienotās Karalistes pilsoņiem attiecas daži neoficiāli aizsardzības pasākumi, par kuriem vienojušās *GCHQ* un *NSA*; pauž lielas bažas par to, ka šie aizsardzības pasākumi neaizsargās ES pilsoņus vai iedzīvotājus, kuru dati var tikt nosūtīti tālāk un kopīgoti ar NSA;

17. aicina dalībvalstis slēgt nolīgumus par nespiegošanu ar Apvienoto Karalisti un aicina Komisiju izmantot kontaktus ar Apvienotās Karalistes partneriem, lai informētu, ka gadījumā, ja Apvienotās Karalistes uzraudzības tiesību akti un prakse netiks mainīti, vienīgais iespējamais risinājums, lai veicinātu lēmumu par aizsardzības līmeņa pietiekamību pieņemšanu, būtu noslēgt ar dalībvalstīm nolīgumus par nespiegošanu;

Tālākpārsūtīšana

18. stingri uzsver to, ka *European Union (Withdrawal) Act 2018* (2018. gada Akts par Eiropas Savienību (izstāšanos)) paredz, ka EST judikatūra, kas izstrādāta pirms pārejas perioda beigām, kļūs par "saglabātajām ES tiesībām", kas tādējādi būs Apvienotajai Karalistei juridiski saistoša; norāda, ka Apvienotajai Karalistei, kad tā novērtē citu trešo valstu pietiekamību, ir saistoši EST spriedumā "Schrems I" un "Schrems II" lietā definētie principi un nosacījumi; pauž bažas par to, ka Apvienotās Karalistes tiesas tomēr vairs nepiemēros Hartu; norāda, ka Apvienotā Karaliste vairs nav EST — augstākās instances, kura var interpretēt Hartu — jurisdikcijā;

19. norāda, ka Apvienotās Karalistes noteikumi par personas datu kopīgošanu saskaņā ar *Digital Economy Act 2017* (2017. gada Likums par digitālo ekonomiku) un par pētniecības datu tālāku nosūtīšanu acīmredzami nav "būtībā līdzvērtīgi" VDAR noteikumiem, kā interpretējusi EST;

20. ir nobažījies par to, ka Apvienotā Karaliste sev ir piešķīrusi tiesības atzīt, vai citas trešās valstis vai teritorijas nodrošina pienācīgu datu aizsardzību neatkarīgi no tā, vai ES ir atzinusi, ka attiecīgā trešā valsts vai teritorija nodrošina šādu aizsardzību; atgādina, ka Apvienotā Karaliste jau ir paziņojusi, ka Gibraltārs nodrošina šādu aizsardzību, kaut gan ES to nav izdarījusi; ir ļoti nobažījies par to, ka ar lēmumu par Apvienotās Karalistes pietiekamību piešķirtais statuss varētu radīt situāciju, kurā tiek apieti ES noteikumi par tālāku nosūtīšanu uz valstīm vai teritorijām, kurās saskaņā ar ES tiesību aktiem netiek garantēta pietiekama aizsardzība;

21. pieņem zināšanai, ka 2021. gada 1. februārī Apvienotā Karaliste nosūtīja pieprasījumu pievienoties Visaptverošajai un progresīvajai Klusā okeāna valstu partnerībai (*CPTTP*), jo īpaši, lai "gūtu labumu no moderniem digitālās tirdzniecības noteikumiem, kas ļauj notikt datu brīvai apritei starp dalībniekiem, likvidē nevajadzīgus šķēršļus uzņēmumiem (utt.)"; ar bažām konstatē, ka *CPTTP* ir vienpadsmit dalībnieki un ka attiecībā uz astoņiem no tiem Eiropas Savienība nav pieņēmusi lēmumu par aizsardzības līmeņa pietiekamību; pauž nopietnas bažas par ES pilsoņu un iedzīvotāju personas datu iespējamu tālāku nosūtīšanu uz šīm valstīm, ja tiks pieņemts lēmums par Apvienotās Karalistes aizsardzības līmeņa pietiekamību ([26]);

([25]) Tiesas 2014. gada 8. aprīļa spriedums *Digital Rights Ireland Ltd* pret *Minister for Communications, Marine and Natural Resources* u. c. un *Kärntner Landesregierung* un citi, apvienotās lietas C-293/12 un C-594/12, ECLI:EU:C:2014:238.

([26]) Apvienotās Karalistes Starptautiskās tirdzniecības departamenta 2021. gada 30. janvāra paziņojums presei "UK applies to join huge Pacific free trade area CPTPP" ("Apvienotā Karaliste iesniedz pieteikumu dalībai lielajā Klusā okeāna brīvās tirdzniecības zonā *CPTPP*").

22. pauž nožēlu par to, ka Komisija nav novērtējusi to, kāda ietekme un riski varētu būt nolīgumam par visaptverošu ekonomisko partnerību starp Lielbritānijas un Ziemeļīrijas Apvienoto Karalisti un Japānu, kurā ir noteikumi par personas datiem un datu aizsardzības;

23. ir nobažījies par to, ka tad, ja Apvienotā Karaliste turpmākajos tirdzniecības nolīgumos, cita starpā ASV un Apvienotās Karalistes tirdzniecības nolīgumos, iekļaus noteikumus par datu nosūtīšanu, var tikt apdraudēts VDAR paredzētais aizsardzības līmenis;

II. **DIREKTĪVA PAR DATU AIZSARDZĪBU TIESĪBAIZSARDZĪBAS JOMĀ**

24. uzskata, ka Apvienotā Karaliste ir pirmā valsts, par kuru Komisija ir ierosinājusi pieņemt lēmumu par aizsardzības līmeņa pietiekamību saskaņā ar Direktīvu (ES) 2016/680;

25. norāda uz Apvienotās Karalistes nolīgumu ar ASV par pārrobežu piekļuvi datiem ([27]), saskaņā ar ASV *CLOUD Act*, kas atvieglo datu nosūtīšanu tiesībaizsardzības nolūkos; pauž lielas bažas par to, ka tas ASV iestādēm ļaus nepamatoti piekļūt ES pilsoņu un iedzīvotāju personas datiem; piekrīt EDAK bažām par to, ka ES un ASV jumta nolīgumā ([28]) paredzētie aizsardzības pasākumi, ko piemēro *mutatis mutandis*, varētu neatbilst kritērijiem par skaidriem, precīziem un pieejamiem noteikumiem attiecībā uz piekļuvi personas datiem, vai arī tajos šādi aizsardzības pasākumi varētu nebūt pietiekami nostiprināti, lai tos varētu uzskatīt par iedarbīgiem un izmantojamiem saskaņā ar Apvienotās Karalistes tiesību aktiem;

26. atgādina, ka EST spriedums Lietā Nr. C-623/17 ir jāinterpretē tādējādi, ka tas nepieļauj tādus valsts tiesību aktus, kuri ļauj valsts iestādei pieprasīt elektronisko sakaru pakalpojumu sniedzējiem veikt vispārēju un nediferencētu informācijas par datplūsmu un atrašanās vietu nosūtīšanu valsts drošības un izlūkošanas aģentūrām valsts drošības aizsardzības nolūkā;

27. norāda, ka EST šajā lietā nosprieda, ka lielapjoma datu vākšana, kas Apvienotajā Karalistē veikta saskaņā ar *Regulation of Investigatory Powers Act 2000* (2000. gada Likums par izmeklēšanas pilnvaru regulējumu), ir nelikumīga; norāda, ka minētais regulējums ir aizstāts ar *Investigatory Powers Act 2016* (*IPA 2016*, 2016. gada Likums par izmeklēšanas pilnvarām), lai stiprinātu nepieciešamības un proporcionalitātes principus; norāda, ka *IPA 2016* attiecībā uz informācijas pārtveršanu paredz tiesu uzraudzību un dod personām iespēju piekļūt saviem datiem un iesniegt sūdzības *Investigatory Powers Tribunal* (Izmeklēšanas pilnvaru tiesā); tomēr pauž nožēlu par to, ka *IPA 2016* joprojām ļauj veikt lielapjoma datu saglabāšanas praksi;

28. pauž bažas par nesenajiem ziņojumiem, kuros minēts, ka masveida datu vākšanas un saglabāšanas shēma ir daļa no izmēģinājuma, ko Apvienotās Karalistes Iekšlietu ministrija īsteno saskaņā ar *IPA 2016*;

29. atgādina, ka Eiropas Parlaments 2020. gada 12. februāra rezolūcijā uzsvēra, ka "Apvienotajai Karalistei nevar būt tieša piekļuve ES informācijas sistēmu datiem un tā nevar līdzdarboties ES aģentūru pārvaldības struktūrās brīvības, drošības un tiesiskuma telpā, savukārt jebkādai informācijas, tostarp personas datu, apmaiņai ar Apvienoto Karalisti būtu jāpiemēro stingri aizsardzības, revīzijas un pārraudzības nosacījumi, tostarp personas datu aizsardzības līmenis, kas līdzvērtīgs tam, kāds paredzēts ES tiesību aktos"; pieņem zināšanai trūkumus, kas konstatēti saistībā ar to, kā Apvienotā Karaliste īstenoja datu aizsardzības tiesību aktus, kamēr tā vēl bija ES dalībvalsts; atgādina, ka Apvienotā Karaliste savulaik saglabāja un uzturēja Šengenas Informācijas sistēmas (*SIS*) datu kopiju; sagaida, ka Apvienotās Karalistes tiesībaizsardzības iestādes, veicot personas datu apmaiņu nākotnē, pilnībā ievēros piemērojamos noteikumus; atgādina, ka Apvienotā Karaliste saglabā piekļuvi dažām ES tiesībaizsardzības datubāzēm saskaņā ar principu "atbilst/neatbilst" un ka tai ir juridiski liegta piekļuve sistēmai *SIS*;

([27]) Nolīgums starp Lielbritānijas un Ziemeļīrijas Apvienotās Karalistes valdību un Amerikas Savienoto Valstu valdību (2019. gada 3. oktobris) par piekļuvi elektroniskajiem datiem smagu noziegumu apkarošanas nolūkā.

([28]) Nolīgums starp Amerikas Savienotajām Valstīm un Eiropas Savienību par personas informācijas aizsardzību saistībā ar noziedzīgu nodarījumu novēršanu, izmeklēšanu un atklāšanu, kā arī saukšanu pie kriminālatbildības par tiem, OV L 336, 10.12.2016., 3. lpp.

Piektdiena, 2021. gada 21. maija

30. pauž bažas par 2021. gada janvārī atklāto informāciju par to, ka no kāda Apvienotās Karalistes Valsts policijas datora tika izdzēsti 400 000 sodāmības reģistra ierakstu; uzsver, ka tas nerosina uzticību Apvienotās Karalistes centieniem aizsargāt tiesībaizsardzības nolūkos nepieciešamos datus;

31. norāda, ka lēmuma par aizsardzības līmeņa pietiekamību projektā ir rūpīgi izvērtētas katras tādas Apvienotās Karalistes iestādes tiesības, kura saskaņā ar valsts tiesību aktiem ir pilnvarota pārtvert un saglabāt personas datus valsts drošības apsvērumu dēļ; tāpēc atzinīgi vērtē arī to, ka sīki izstrādāti pārraudzības ziņojumi par iestādēm, kas atbild par izlūkdienestu darbību, sniedz informāciju par Apvienotās Karalistes pašreizējo uzraudzības praksi; aicina Komisiju turpināt novērtēt un uzraudzīt tos datu pārraides veidus, uz kuriem attiecas Apvienotās Karalistes datu saglabāšanas un likumīgas pārtveršanas pilnvaras;

32. norāda, ka ES un Apvienotās Karalistes Tirdzniecības un sadarbības nolīgumā (TSN) ir sadaļas par DNS, pirkstu nospiedumu un transportlīdzekļu reģistrācijas datu apmaiņu, pasažieru datu reģistra (PDR) datu nosūtīšanu un apstrādi, sadarbību operatīvās informācijas jomā un sadarbību ar Eiropolu un Eurojust, kas būs piemērojamas neatkarīgi no tā, vai tiks pieņemts lēmums par aizsardzības līmeņa pietiekamību; tomēr atgādina par bažām, kas paustas Pilsoņu brīvību, tieslietu un iekšlietu komitejas 2021. gada februāra atzinumā par TSN attiecībā uz tādu personas datu īpašu izmantošanu un ilgāku glabāšanu, kas Apvienotajai Karalistei nodoti saskaņā ar TSN sadaļām attiecībā uz Prīmes līgumu un PDR, kas neatbilst dalībvalstu praksei datu izmantošanas un saglabāšanas jomā; atgādina par tiesībām celt prasību EST, lai pārliecinātos par ierosinātā starptautiskā nolīguma likumību un jo īpaši tā saderību ar pamattiesību aizsardzību ([29]);

Secinājumi

33. aicina Komisiju apliecināt ES uzņēmumiem, ka lēmums par aizsardzības līmeņa pietiekamību nodrošinās stabilu, pietiekamu un uz nākotni orientētu juridisko pamatu datu nosūtīšanai; uzsver, cik svarīgi ir nodrošināt, ka šis lēmums par aizsardzības līmeņa pietiekamību tiks uzskatīts par pieņemamu gadījumā, ja to izskatīs EST, un uzsver, ka tādēļ būtu jāņem vērā visi EDAK atzinumā sniegtie ieteikumi;

34. atzinīgi vērtē to, ka lēmumus par aizsardzības līmeņa pietiekamību piemēros tikai četrus gadus, jo Apvienotā Karaliste tagad, kad tā vairs nav ES dalībvalsts, varētu nolemt grozīt tiesību aktus, uz kuriem attiecas Komisijas veiktais novērtējums par aizsardzības līmeņa pietiekamību; aicina Komisiju turpināt pastāvīgi uzraudzīt datu aizsardzības līmeni Apvienotajā Karalistē gan tiesību aktos, gan praksē, pirms 2025. gadā tiek atjaunots lēmums par aizsardzības līmeņa pietiekamību;

35. uzskata, ka, ja Komisija pieņems abus ES tiesību aktiem neatbilstīgos īstenošanas lēmumus, kamēr nav atrisinātas visas šajā rezolūcijā paustās bažas, tā pārkāps īstenošanas pilnvaras, kas tai piešķirti ar Regulu (ES) 2016/679 un Direktīvu (ES) 2016/680; tāpēc iebilst pret abiem īstenošanas aktiem, jo īstenošanas lēmumu projektu pamatojums neatbilst ES tiesību aktiem;

36. aicina Komisiju grozīt abu īstenošanas lēmumu projektus tā, lai tie pilnībā atbilstu ES tiesību aktiem un judikatūrai;

37. prasa valsts datu aizsardzības iestādēm apturēt tādu personas datu nosūtīšanu, kuri var tikt pakļauti Apvienotās Karalistes izlūkošanas iestāžu neselektīvai piekļuvei gadījumā, ja Komisija attiecībā uz Apvienoto Karalisti pieņems lēmumus par aizsardzības līmeņa pietiekamību, pirms Apvienotā Karaliste būs atrisinājusi iepriekš minētās problēmas;

38. aicina Komisiju un Apvienotās Karalistes kompetentās iestādes izstrādāt rīcības plānu, kura nolūks būtu iespējami drīz novērst EDAK atzinumos konstatētos trūkumus un citus datu aizsardzības jomā neatrisinātos jautājumus Apvienotajā Karalistē, kam jābūt priekšnosacījumam galīgā lēmuma par datu aizsardzības līmeņa pietiekamību pieņemšanā;

39. aicina Komisiju turpināt uzraudzīt datu aizsardzības līmeni Apvienotajā Karalistē, kā arī tiesību aktus un praksi attiecībā uz masveida uzraudzību Apvienotajā Karalistē; norāda, ka VDAR V nodaļā ir paredzētas citas likumīgas iespējas personas datu nosūtīšanai uz Apvienoto Karalisti; atgādina, ka saskaņā ar EDAK pamatnostādnēm datu nosūtīšana, kas notiek saskaņā ar īpašās situācijās piemērojamām atkāpēm, pildot VDAR 49. pantu, ir pieļaujama tikai izņēmuma gadījumā;

([29]) Eiropas Parlamenta rezolūcija par Komisijas lēmuma projektu, kurā uzsvērts to pasažieru datu reģistra (PDR) personas datu atbilstīgs aizsardzības līmenis, ko pārsūta ASV Muitas un robežapsardzības birojam (OV C 103 E, 29.4.2004., 665. lpp.).

40. pauž nožēlu par to, ka Komisija ir ignorējusi Parlamenta aicinājumus apturēt privātuma vairoga darbību līdz brīdim, kamēr ASV iestādes ievēros tā noteikumus, un tā vienmēr ir devusi priekšroku "situācijas uzraudzībai" bez jebkāda konkrēta rezultāta attiecībā uz personu datu aizsardzību un juridisko noteiktību uzņēmumiem; mudina Komisiju mācīties no tā, ka tā agrāk nav ņēmusi vērā Parlamenta un ekspertu aicinājumus attiecībā uz iepriekšējo lēmumu par aizsardzības līmeņa pietiekamību pieņemšanu un uzraudzību, un neatstāt ES datu aizsardzības tiesību aktu pienācīgu uzraudzību ES Tiesas ziņā pēc personu sūdzībām;

41. aicina Komisiju rūpīgi uzraudzīt datu aizsardzības tiesību aktus un praksi Apvienotajā Karalistē, nekavējoties informēt Parlamentu un apspriesties ar to par jebkādām turpmākām izmaiņām Apvienotās Karalistes datu aizsardzības režīmā un piešķirt Parlamentam kontroles lomu jaunajā institucionālajā sistēmā, tostarp attiecībā uz tādām attiecīgām struktūrām kā Specializētā komiteja tiesībaizsardzības un tiesu iestāžu sadarbības jautājumos;

o

o o

42. uzdod priekšsēdētājam nosūtīt šo rezolūciju Komisijai, dalībvalstīm un Apvienotās Karalistes valdībai.