EIROPAS KOMISIJA

Briselē, 4.11.2010
COM(2010) 609 galīgā redakcija

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Vispusīga pieeja personas datu aizsardzībai Eiropas Savienībai

KOMISIJAS PAZIŅOJUMS EIROPAS PARLAMENTAM, PADOMEI, EIROPAS EKONOMIKAS UN SOCIĀLO LIETU KOMITEJAI UN REĢIONU KOMITEJAI

Vispusīga pieeja personas datu aizsardzībai Eiropas Savienībai

1. PERSONAS DATU AIZSARDZĪBA JAUNU PROBLĒMU PRIEKŠĀ

Datu aizsardzības direktīva[1], ko pieņēma 1995. gadā, iezīmēja jaunu pavērsienu personas datu aizsardzības vēsturē Eiropas Savienībā. Direktīvā ietverti divi vecākie, vienlīdz svarīgie Eiropas integrācijas procesa mērķi – indivīdu pamattiesību un brīvību aizsardzība, proti, tiek aizsargātas pamattiesības uz personas datu aizsardzību, un iekšējā tirgus izveide, šajā gadījumā – personas datu brīva plūsma.

Piecpadsmit gadus vēlāk, šis dubultais mērķis joprojām nav zaudējis aktualitāti un direktīvā ietvertie principi turpina darboties. **Tomēr spējā tehnoloģiju attīstība un globalizācija ir ievērojami mainījušas mūsu pasauli un radījušas jaunas problēmas datu aizsardzības jomā.**

Mūsdienu tehnika ļauj indivīdiem viegli dalīties ar informāciju par savu uzvedību un vēlmēm un ļauj padarīt šo informāciju publiski pieejamu visā pasaulē vēl nepieredzētā mērogā. Sociālo kontaktu vietnes ar simtiem miljonu pa visu pasauli izkaisītu lietotāju, iespējams, ir redzamākais, bet ne vienīgais, šā fenomena piemērs. "Mākoņdatošana", tas ir, skaitļošana internetā, kad programmatūra, kopīgie resursi un informācija atrodas uz attālas piekļuves serveriem (mākoņos), arī var izvērsties par problēmu datu aizsardzībai, jo tā var būt saistīta ar indivīda kontroles zudumu pār iespējami sensitīvu informāciju, kad tie saglabā savus datus ar programmām, kas izvietotas uz kādam citam piederošas aparatūras. Nesen veikts pētījums apstiprināja, ka šajā jautājumā viedokļi saskan – datu aizsardzības iestādes, uzņēmumu apvienības un patērētāju organizācijas uzskata, ka līdz ar tiešsaistes aktivitātēm palielinās arī risks privātuma un personas datu aizsardzībai[2].

Tajā pašā laikā **personas datu vākšana ir kļuvusi īpaši izsmalcināta, un to vairs nav tik viegli pamanīt.** Piemēram, uzņēmēji var labāk pieskaņoties indivīdu vēlmēm, izmantojot modernus rīkus viņu uzvedības novērošanai. Un augošais procedūru skaits, kas padara iespējamu automātisku datu vākšanu, piemēram, elektroniskās transporta biļetes, ceļa nodevas iekasēšanas automāti vai atrašanās vietas noteikšanas ierīces, atvieglo indivīdu atrašanās vietas noteikšanu tāpēc vien, ka viņš lieto kādu mobilu ierīci. Arī valsts iestādes aizvien vairāk izmanto personas datus dažādiem nolūkiem, piemēram indivīdu izsekošanai infekcijas slimības izplatīšanās gadījumā, efektīvākai terorisma un noziedzības novēršanai un apkarošanai, sociālā nodrošinājuma shēmu vai nodokļu pārvaldībai, e-pārvaldības ietvaros utml.

---

1 Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (OV L 281, 23.11.1995., 31. lpp.).

2 Sk. *Study on the economic benefits of privacy enhancing technologies, London Economics,* 2010. gada jūlijs (http://ec.europa.eu/justice/policies/privacy/docs/studies/final_report_pets_16_07_10_en.pdf), 14. lpp.

Visi šie aspekti nenovēršami noved pie jautājuma, vai ES tiesību akti datu aizsardzības jomā joprojām pilnībā un efektīvi spēj risināt šīs problēmas.

Lai izpētītu šo jautājumu, Komisija uzsāka tiesiskā regulējuma pārskatīšanas procesu, sarīkojot augsta līmeņa konferenci 2009. gada maijā, kurai sekoja sabiedriskā apspriešana, kas turpinājās līdz 2009. gada beigām[3]. Turklāt tika sākti vairāki pētījumi[4].

Rezultāti apstiprināja, ka direktīvas pamatprincipi joprojām ir derīgi un tās neitrālais ar konkrētām tehnoloģijām nesaistītais raksturs būtu jāsaglabā. Tomēr vairāki jautājumi izrādījās problemātiski un izraisīja īpašas bažas. Tie ir šādi.

- *Jauno tehnoloģiju ietekmes atspoguļojums*

Atbildes, kas tika saņemtas apspriešanās laikā gan no privātpersonām, gan organizācijām, apstiprināja, ka ir nepieciešams skaidrot un konkretizēt datu aizsardzības principu piemērošanu jaunām tehnoloģijām, lai nodrošinātu, ka indivīdu personas dati patiešām tiek aizsargāti neatkarīgi no tā, kādas tehnoloģijas tiek izmantotas datu apstrādei, un lai par datu apstrādi atbildīgās personas pilnībā apzinātos jauno tehnoloģiju ietekmi uz datu aizsardzību. Daļēji šis jautājums ir risināts Direktīvā 2002/58/EK (tā sauktajā "e-privātuma" Direktīvā)[5], ar kuru konkretizēta un papildināta vispārīgā Datu aizsardzības direktīva elektroniskās komunikācijas nozarē[6].

- *Datu aizsardzības veicināšana iekšējā tirgū*

Viena no galvenajām bažām, ko atkārtoti izteica vairākas ieinteresētās personas, jo īpaši daudznacionāli uzņēmumi, ir saskaņas trūkums dalībvalstu datu aizsardzības tiesību aktu starpā, neskatoties uz vienoto ES tiesisko regulējumu. Tās norādīja, ka ir nepieciešams vairot tiesisko noteiktību, samazināt administratīvo slogu un nodrošināt vienādus spēles noteikumus uzņēmumiem un citām par datu apstrādi atbildīgajām personām.

---

3 Atbildes uz Komisijas rīkoto sabiedrisko apspriešanu skatīt šeit: http://ec.europa.eu/justice/news/consulting_public/news_consulting_0003_en.htm. Visa 2010. gada laikā norisinājās konkrētāka apspriešanās ar ieinteresētajām personām. Priekšsēdētāja vietniece Viviāna Redinga vadīja arī augsta līmeņa sanāksmi ar ieinteresētajām personām 2010. gada 5. oktobrī Briselē. Komisija apspriedās arī ar 29. panta darba grupu, kura sniedza vispusīgu pienesumu 2009. gada apspriešanai (WP 168) un 2010. gada jūlijā pieņēma īpašu atzinumu par pārskatatbildības principu (WP 173).

4 Papildus Pētījumam par privātuma aizsardzību uzlabojošo tehnoloģiju ekonomiskajām priekšrocībām (sk. 2. zemsvītras piezīmi) skatīt arī Salīdzinošo pētījumu par dažādām pieejām aktuālajām privātuma problēmām, jo īpaši ņemto vērā tehnoloģiju attīstību, 2010. gada janvāris (http://ec.europa.eu/justice/policies/privacy/docs/studies/new_privacy_challenges/final_report_en.pdf). Pašlaik tiek pētīts turpmākā ES personas datu aizsardzības tiesiskā regulējuma ietekmes novērtējums.

5 Eiropas Parlamenta un Padomes 2002. gada 12. jūlija Direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektroniskajām komunikācijām) (OV L 201, 31.7.2002., 37. lpp.).

6 Datu aizsardzības direktīva 95/46/EK nosaka datu aizsardzības standartus visiem ES tiesību aktiem, tostarp arī e-privātuma Direktīvai 2002/58/EK (grozīta ar Direktīvu 2009/136/EK – OV L 335, 18.12.2009., 11. lpp.). E-privātuma direktīva attiecas uz personas datu apstrādi saistībā ar publiski pieejamu elektronisko komunikāciju pakalpojumu sniegšanu publiskos komunikāciju tīklos. Ar to datu aizsardzības direktīvas principi tika pārveidoti īpašos elektroniskās komunikācijas nozarei piemērojamos noteikumos. Direktīva 95/46/EK *inter alia* attiecas uz komunikācijas pakalpojumiem, kas nav publiski.

- *Ar globalizāciju saistītie jautājumi un datu starptautiskās pārsūtīšanas uzlabošana*

Vairākas ieinteresētas personas norādīja, ka datu apstrādei aizvien vairāk izmanto ārpakalpojumus un ļoti bieži šie pakalpojumi tiek sniegti ārpus ES, tas savukārt izraisa vairākas problēmas attiecībā uz apstrādei piemērojamo tiesību un ar to saistītās atbildības noteikšanu. Saistībā ar datu starptautisku pārsūtīšanu daudzas organizācijas uzskatīja, ka spēkā esošās sistēmas nav pilnībā atbilstošas un tās ir jāpārskata un jāsaskaņo, lai pārsūtīšana kļūtu vienkāršāka un ne tik apgrūtinoša.

- *Spēcīgāka institucionālā kārtība datu aizsardzības noteikumu efektīvākai izpildei*

Ieinteresēto personu vidū valda vienprātība, ka datu aizsardzības iestāžu loma ir jānostiprina, lai nodrošinātu labāku datu aizsardzības noteikumu izpildi. Dažas organizācijas pieprasīja uzlabot 29. panta darba grupas darba caurskatāmību (*sk. turpmāk 2.5. punktu*) un precizēt tās uzdevumus un pilnvaras.

- *Datu aizsardzības tiesiskā regulējuma saskaņotības uzlabošana*

Sabiedriskās apspriešanās laikā visas ieinteresētās personas norādīja, ka ir nepieciešams "jumta" tiesību akts, kas būtu piemērojams datu apstrādes darbībām visās nozarēs un Savienības politikas jomās, nodrošinot saskaņotu pieeju un viengabalainu, konsekventu un efektīvu aizsardzību[7].

Visu minēto problēmjautājumu risināšanai **ES ir jāizstrādā vispusīga un saskaņota pieeja**, kas garantē **indivīdu pamattiesību uz personas datu aizsardzību pilnīgu ievērošanu visā ES un ārpus tās**. Ar Lisabonas līgumu ES ir ieguvusi papildu rīkus minētā uzdevuma sasniegšanai – juridiski saistoša ir kļuvusi ES Pamattiesību harta, kuras 8. pantā ir atzītas patstāvīgas tiesības uz personas datu aizsardzību, un ir ieviests jauns juridiskais pamats[8], kas ļauj izstrādāt vispusīgus un saskaņotus Savienības tiesību aktus par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti. Jo īpaši jaunais juridiskais pamats ļauj ES izstrādāt vienotu tiesību aktu datu aizsardzības regulēšanai, aptverot arī policijas un tiesu iestāžu sadarbību krimināllietās. LESD 16. pants tikai daļēji attiecas uz Kopējās ārpolitikas un drošības politikas jomu, jo īpašie noteikumi par dalībvalstu veikto datu apstrādi ir jānosaka ar Padomes lēmumu, kam ir cits juridiskais pamats[9].

Izmantojot šīs jaunās juridiskās iespējas, Komisija datu aizsardzības pamattiesības ievērošanas nodrošināšanai visā ES un visās tās politikas jomās piešķirs visaugstākās prioritātes statusu, tajā pašā laikā stiprinot iekšējā tirgus lomu un atvieglojot personas datu brīvu plūsmu. Šajā saistībā jānorāda, ka, nodrošinot pamattiesības uz personas datu aizsardzību, pilnībā jāievēro arī citas Hartā ietvertās pamattiesības un pārējie Līgumu mērķi.

Šā paziņojuma mērķis ir noteikt Komisijas pieeju personas datu aizsardzības ES tiesiskās sistēmas modernizācijai visās Savienības rīcības jomās, jo īpaši ņemot vērā problēmas saistībā ar globalizāciju un jaunām tehnoloģijām, lai arī turpmāk varētu garantēt indivīdu augsta

---

7 Atsevišķos dokumentos, kas sagatavoti pēc publiskās apspriešanās pabeigšanas, Eiropols un *Eurojust* uzstāja, ka ir jāņem vērā viņu darba specifika attiecībā uz tiesībaizsardzības koordināciju un noziedzības novēršanu.

8 Sk. Līguma par Eiropas Savienības darbību (LESD) 16. pantu.

9 Sk. LESD 16. panta 2. punkta pēdējo rindkopu un Līguma par Eiropas Savienību (LES) 39. pantu.

līmeņa aizsardzību attiecībā uz personas datu apstrādi visās Savienības rīcības jomās. Tādējādi ES varēs arī turpmāk būt par augstu datu aizsardzības standartu ieviešanas dzinējspēku pasaulē.

2. VISPUSĪGĀS PIEEJAS DATU AIZSARDZĪBAI GALVENIE MĒRĶI

2.1. Indivīdu tiesību spēcināšana

2.1.1. Indivīdu pienācīga aizsardzība visos apstākļos

Spēkā esošo ES datu aizsardzības tiesību aktu noteikumu mērķis **ir aizsargāt fizisku personu pamattiesības un jo īpaši tiesības uz personas datu aizsardzību**, saskaņā ar ES Pamattiesību hartu [10].

"Personas datu" jēdziens ir viens no svarīgākajiem jēdzieniem, lai ar ES datu aizsardzības tiesību aktiem varētu īstenot indivīdu aizsardzību, un tas ir noteicošais saistošu pienākumu piemērošanai personas datu apstrādātājiem un apstrādātājiem[11]. "Personas datu" definīcijas mērķis ir aptvert visu informāciju, kas ir tieši vai netieši saistīta ar identificētu vai identificējamu personu. Lai noteiktu, vai persona ir identificējama, būtu jāņem vērā "visi līdzekļi, ko personas datu apstrādātājs vai kāda cita persona pamatoti varētu izmantot, lai identificētu attiecīgo personu"[12]. Šīs likumdevēja apzināti izvēlētās pieejas priekšrocības ir elastīgums, kas ļauj to piemērot visdažādākajām situācijām un norisēm, kas ietekmē pamattiesības, tostarp arī tām, kas nebija paredzamas, pieņemot direktīvu. Tomēr šādas plašas un elastīgas pieejas sekas ir arī tas, ka daudzos gadījumos, īstenojot direktīvu, nav skaidrs, kuru pieeju izvēlēties, vai indivīdiem šajā gadījumā ir tiesības uz datu aizsardzību un vai personas datu apstrādātājiem ir jāievēro direktīvā paredzētie pienākumi[13].

Ir arī situācijas, kad tiek apstrādāta īpaša informācija, kuras apstrādei būtu vajadzīgi papildu pasākumi saskaņā ar ES tiesībām. Dažos gadījumos šādi pasākumi jau pastāv. Piemēram, informācijas glabāšana termināliekārtās (piemēram, mobilajos telefonos) ir atļauta tikai ar nosacījumu, ka indivīds ir devis savu piekrišanu. Šo jautājumu iespējams vajadzētu risināt arī ES līmenī, piemēram, attiecībā uz kodētiem datiem, atrašanās vietas datiem, "datizraces" tehnoloģijām, kas ļauj kombinēt datus no dažādiem avotiem, vai attiecībā uz gadījumiem, kad jānodrošina informācijas tehnoloģiju sistēmu konfidencialitāte un integritāte[14].

Visi iepriekšminētie jautājumi ir rūpīgi jāizpēta.

---

10 Sk. Eiropas Savienības Tiesas spriedumus lietās C-101/01, '*Bodil Lindqvist*', ECR [2003], I-1297, 96, 97, un C-275/06, *Productores de Música de España (Promusicae) v Telefónica de España SAU*, ECR [2008] I-271. Sk. arī Eiropas Cilvēktiesību tiesas judikatūru, piemēram, lietas *S. and Marper v. the United Kingdom*, 4.12.2008. (Pieteikums Nr. 30562/04 un 30566/04), kā arī *Rotaru v. Romania*, 4.5.2000.; Nr. 28341/95, § 55, *ECHR* 2000-V.

11 Sk. "personas datu apstrādātāja" un "apstrādātāja" definīcijas Direktīvas 95/46/EK 2. panta d) un e) punktā.

12 Sk. Direktīvas 95/46/EK 26. apsvērums.

13 Sk., piemēram, jautājumu par IP adresēm, ko Atzinumā 4/2007 par personas datu jēdzienu pētījusi 29. panta darba grupa (WP 136).

14 Sk., piemēram, Vācijas Konstitucionālās tiesas (*Bundesverfassungsgericht*) 2008. gada 27. februāra spriedumu 1 BvR 370/07.

Komisija apsvērs, **kā nodrošināt saskaņotu datu aizsardzības noteikumu piemērošanu, ņemot vērā jauno tehnoloģiju ietekmi uz indivīdu tiesībām un brīvībām, un kā sasniegt mērķi nodrošināt personas datu brīvu apriti iekšējā tirgū.**

2.1.2. Caurskatāmības uzlabošana datu subjektu labā

Caurskatāmība ir pamatnosacījums, lai indivīdi varētu kontrolēt savus datus un lai varētu nodrošināt efektīvu personas datu aizsardzību. Tāpēc ir īpaši būtiski nodrošināt, ka personas datu apstrādātāji **caurskatāmā veidā labi un skaidri informē** indivīdus par to, kādā veidā, kas, kāpēc un cik ilgi vāc un apstrādā viņu datus, un kādas ir viņu tiesības, ja viņi vēlas piekļūt datiem, tos labot un dzēst. Attiecīgie noteikumi par datu subjektiem sniedzamo informāciju[15] nav pietiekami.

Caurskatāmības pamatelements ir prasība, ka **informācijai jābūt viegli pieejamai un viegli saprotamai un ir jāizmanto skaidra un vienkārša valoda**. Tas ir īpaši svarīgi tiešsaistes vidē, kur paziņojumi par privātumu bieži ir neskaidri, grūti pieejami, necaurskatāmi[16] un ne vienmēr pilnībā atbilst noteikumiem. Viena no jomām, kur tas varētu būt aktuāls jautājums, ir tiešsaistes paradumorientētā reklāma, jo paradumorientētās reklāmas pakalpojumos iesaistīto pušu daudzums un praktiskās īstenošanas mehānismu sarežģītība apgrūtina indivīda iespējas zināt un saprast, vai tiek vākti personas dati, kas to dara un kādiem mērķiem.

Šajā saistībā īpašu aizsardzību ir pelnījuši **bērni**, jo viņi var neapzināties ar personas datu apstrādi saistītos riskus, sekas, aizsardzības pasākumus un tiesības[17].

Komisija apsvērs:

- **vispārīga** personas datu **caurskatāmas apstrādes principa** ieviešanu tiesiskajā regulējumā;

- **īpašu pienākumu** ieviešanu personas datu apstrādātājiem attiecībā uz to, kāda veida informācija ir sniedzama un kāda ir sniegšanas **kārtība**, tostarp attiecībā uz **bērniem**;

- vienas vai vairāku **ES standarta formu (privātuma informācijas paziņojumi)** izstrādi, kas jāizmanto personas datu apstrādātājiem.

Turklāt ir svarīgi, lai indivīdus informētu, ja viņu datus nejauši vai nelikumīgi iznīcina, pazaudē vai groza, tiem nelikumīgi ir piekļuvušas citas personas vai tie ir neatļauti atklāti citām personām. Nesenās e-privātuma direktīvas pārskatīšanas laikā tika ieviests **obligāts paziņojums par personas datu aizsardzības pārkāpumu**, taču tas attiecas tikai uz telekomunikācijas nozari. Ņemot vērā, ka datu aizsardzības pārkāpumi notiek arī citās nozarēs (piemēram, finanšu nozarē), Komisija izpētīs kārtību, kā varētu paplašināt šo pienākumu paziņot par personas datu aizsardzības pārkāpumu, ietverot citas nozares, saskaņā ar Komisijas 2009. gada paziņojumu Eiropas Parlamentam par personas datu aizsardzības pārkāpumu saistībā ar elektronisko komunikāciju nozares tiesiskā regulējuma reformu[18]. Šī

---

15 Sk. Direktīvas 95/46/EK 10. un 11. pantu.

16 *Eurobarometer* aptauja 2009. gadā parādīja, ka aptuveni puse respondentu uzskatīja paziņojumus par privātumu tīmekļa vietnēs par "ļoti" vai "diezgan neskaidriem". (Sk. *Eurobarometer* zibensaptauja Nr. 282. http://ec.europa.eu/public_opinion/flash/fl_282_en.pdf).

17 Sk. Drošāks internets bērniem, kvalitātes pētījums attiecībā uz 9-10 un 12-14 gadu veciem bērniem, kas parādīja, ka bērni sliecas nepietiekami novērtēt riskus, kas saistīti ar interneta lietošanu, un noniecināt savas riskantās uzvedības sekas (pieejams http://ec.europa.eu/information_society/activities/sip/surveys/qualitative/index_en.htm).

18 Komisija īpašu uzmanību velta tam, ko vēlētos Eiropas Parlaments, proti, lai šis pienākums — ziņot par personas datu aizsardzības pārkāpumiem — attiektos ne tikai uz elektronisko sakaru nozari, bet arī uz

izpēte neietekmēs e-privātuma direktīvas noteikumus, kas jātransponē valstu tiesībās līdz 2011. gada 25. maijam[19]. Jānodrošina konsekventa un saskaņota pieeja šim jautājumam.

Komisija apņemas

- izpētīt kārtību, kā vispārīgajā tiesiskajā regulējumā ieviest **vispārīgu paziņojumu par personas datu aizsardzības pārkāpumu**, tostarp norādot šā paziņojuma adresātus un kritērijus, saskaņā ar kuriem rodas pienākums sniegt šādu paziņojumu.

2.1.3. Kontroles pār saviem datiem uzlabošana

Divi svarīgi priekšnoteikumi, lai nodrošinātu indivīdiem datu augsta līmeņa aizsardzību, ir **mērķa ierobežojums personas datu apstrādātāja apstrādes darbībām** (datu minimizācijas princips) un datu subjekta **efektīvas kontroles saglabāšana pār saviem datiem**. Hartas 8. panta 2. punktā teikts, ka "ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos". Indivīdiem vienmēr jāspēj piekļūt saviem datiem, dzēst vai bloķēt tos, ja vien nav likumā noteiktu leģitīmu iemeslu, kas to liedz. Šīs tiesības jau ir paredzētas pašreizējā tiesiskajā regulējumā. Tomēr veids, kā šīs tiesības var izmantot, nav saskaņots, un tāpēc to izmantošana dažās dalībvalstīs ir vieglāka nekā citās. Šis jautājums turklāt ir kļuvis īpaši problemātisks tiešsaistē, kur datus bieži saglabā, attiecīgo personu par to vispār neinformējot, un/vai bez tās piekrišanas.

Šeit īpaši iederas piemērs par tiešsaistes sociālo kontaktu vietnēm, kas ir īpaši problemātiskas, skatoties no indivīda efektīvas kontroles pār saviem personas datiem viedokļa. Komisija ir saņēmusi daudzus pieprasījumus no indivīdiem, kuri ne vienmēr var atgūt datus no tiešsaistes pakalpojumu sniedzējiem, piemēram, fotogrāfijas, un kuru piekļuves, labošanas un dzēšanas tiesību izmantošana tādējādi ir apgrūtināta.

Šādas tiesības tāpēc ir jāpadara nepārprotamākas, skaidrākas un iespējami stiprākas.

Komisija tāpēc izpētīs iespējas

- stiprināt **datu minimizācijas principu;**

- **uzlabot kārtību**, kā praktiski **izmantojamas piekļuves, labošanas, dzēšanas vai datu bloķēšanas tiesības** (piemēram, nosakot termiņus atbildēm uz indivīdu pieprasījumiem, ļaujot izmantot šīs tiesības elektroniski vai paredzot, ka piekļuves tiesības principā jānodrošina bez maksas);

- precizēt tā sauktās "**tiesības tikt aizmirstam**", tas ir, indivīdu tiesības prasīt, lai viņu datus vairs neapstrādā un dzēš, ja tie vairs nav vajadzīgi likumīgo mērķu sasniegšanai. Piemēram, gadījumā, kad apstrāde pamatojas uz personas piekrišanu un persona atsauc savu piekrišanu vai beidzas glabāšanas termiņš;

---

tādiem subjektiem kā informācijas sabiedrības pakalpojumu sniedzēji (..). Tāpēc Komisija nekavējoties uzsāks nepieciešamo sagatavošanās darbu, cita starpā apspriežoties ar ieinteresētajām personām, lai šajā jomā līdz 2011. gada beigām iesniegtu atbilstošus priekšlikumus (..)", pieejams: http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//LV . Sk. arī Direktīvas 2009/136/EK, ar ko groza e-privātuma Direktīvu 2002/58/EK, 59. apsvērumu: "Šī lietotāju vispārējā interese saņemt paziņojumu neattiecas vienīgi uz elektronisko sakaru nozari, tāpēc skaidras, obligātas paziņošanas prasības, kas piemērojamas visām nozarēm jāievieš Kopienas līmenī prioritārā kārtā."

[19] Direktīvas 2009/136/EK 4. pants.

- papildināt datu subjektu tiesības, nodrošinot "**datu pārnesamību**", tas ir, sniedzot indivīdam nepārprotamas tiesības atsaukt savus datus (piemēram, fotogrāfijas vai draugu sarakstu) no lietojumprogrammas vai pakalpojuma, lai atsauktos datus varētu pārnest uz citu lietojumprogrammu vai pakalpojumu, ciktāl tas tehniski ir iespējams, bez kavēkļiem no personas datu apstrādātāja puses.

2.1.4. Izpratnes veicināšana

Kaut arī caurskatāmība ir īpaši svarīga, tāpat ir nepieciešams, lai sabiedrība, un jo īpaši jaunieši, labāk apzinātos riskus, kas saistīti ar personas datu apstrādi, un savas tiesības. *Eurobarometer* aptauja 2008. gadā parādīja, ka liels vairums cilvēku ES dalībvalstīs uzskata, ka izpratne par personas datu aizsardzību viņu valstī ir zema[20]. Tāpēc visām iesaistītajām pusēm, piemēram, dalībvalstu iestādēm, jo īpaši datu aizsardzības un izglītības iestādēm, kā arī personas datu apstrādātājiem un pilsoniskās sabiedrības apvienībām, ir jāveicina un jārosina izpratnes veicināšanas pasākumi. Šiem pasākumiem jāietver neleģislatīvi pasākumi, kā izpratnes veicināšanas kampaņas rakstītajos un elektroniskajos plašsaziņas līdzekļos, saprotama informācija tīmekļa vietnēs, kas skaidri norāda datu subjekta tiesības un personas datu apstrādātāja pienākumus.

Komisija apņemas izpētīt

- iespēju **izpratnes veicināšanas pasākumus par datu aizsardzību līdzfinansēt** no Savienības budžeta;

- nepieciešamību un iespējas iekļaut tiesiskajā regulējumā **pienākumu veikt izpratnes veicināšanas pasākumus** šajā jomā.

2.1.5. Apzinātas un brīvprātīgas piekrišanas nodrošināšana

Ja ir nepieciešama apzināta piekrišana, noteikumi paredz, ka indivīda piekrišanai savu personas datu apstrādei ir jābūt "labprātīgi sniegtam šīs personas vēlmju konkrētam un paziņotam norādījumam", ar kuru indivīds izsaka savu piekrišanu uz viņu attiecināmu personas datu apstrādei[21]. Tomēr šos nosacījumus dalībvalstis interpretē ļoti dažādi, sākot ar vispārīgu prasību pēc rakstiskas piekrišanas un beidzot ar netiešas piekrišanas pieļaujamību.

Turklāt tiešsaistē, ņemot vērā datu aizsardzības nostājas necaurredzamību, indivīdiem bieži ir ļoti grūti apzināties savas tiesības un sniegt apzinātu piekrišanu. To vēl vairāk sarežģī fakts, ka dažos gadījumos, nav pat skaidrs, kas būtu uzskatāms par labprātīgi sniegtu, konkrētu un apzinātu piekrišanu datu apstrādei, piemēram, paradumorientētās reklāmas gadījumā, kad interneta pārlūkprogrammas iestatījumus daži, bet ne visi, uzskata par lietotāja piekrišanu.

Tāpēc ir jāprecizē datu subjekta piekrišanas nosacījumi, lai vienmēr garantētu apzinātu piekrišanu un nodrošinātu, ka saskaņā ar ES Pamattiesību hartas 8. pantu indivīds pilnībā apzinās, ka viņš sniedz piekrišanu un kādai datu apstrādei viņš piekrīt. Skaidrība par galvenajiem jēdzieniem uzlabos arī pašregulācijas pasākumu izstrādi, lai izveidotu praktiskus risinājumus, kas ir saskaņā ar ES tiesībām.

---

20 Sk. *Eurobarometer* zibensaptauja 225 – Datu aizsardzība Eiropas Savienībā: http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

21 Sal. Direktīvas 95/46/EK 2. panta h) apakšpunkts.

Komisija izpētīs, kā būtu iespējams **precizēt un stiprināt noteikumus par piekrišanu**.

2.1.6. Sensitīvu datu aizsardzība

Sensitīvu datu apstrāde, kuri atklāj rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisku vai filozofisku pārliecību, dalību arodbiedrībās, kā arī uz veselību vai seksuālo dzīvi attiecināmu datu apstrāde jau ir aizliegta, ar atsevišķiem izņēmumiem un ievērojot konkrētus nosacījumus un drošības garantijas[22]. Tomēr ņemot vērā tehnikas attīstību un citas pārmaiņas sabiedrībā, vajag no jauna izvērtēt noteikumus par sensitīviem datiem, lai izpētītu, vai sensitīvu datu jēdzienā nebūtu jāiekļauj arī citas datu kategorijas, un precizētu nosacījumus to apstrādei. Tas attiecas, piemēram, uz ģenētiskajiem datiem, kas pagaidām nav nepārprotami minēti kā sensitīvu datu kategorija.

Komisija apsvērs:

- vai "**sensitīvu datu**" jēdzienā nebūtu jāiekļauj citas datu kategorijas, piemēram, **ģenētiskie** dati;

- sensitīvo datu kategoriju apstrādes **nosacījumu** precizēšanu un **saskaņošanu**.

2.1.7. Tiesību aizsardzības līdzekļu un sankciju optimizācija

Efektīvi noteikumi par tiesību aizsardzības līdzekļiem un sankcijām ir ļoti būtiski, lai nodrošinātu datu aizsardzības noteikumu izpildi. Daudzos gadījumos, kad datu aizsardzības noteikumu pārkāpums aizskar kāda indivīda tiesības, līdzīgi aizskartas ir arī daudzu citu indivīdu tiesības.

Tādēļ Komisija:

- apsvērs iespēju arī datu aizsardzības iestādēm un pilsoniskās sabiedrības organizācijām, kā arī **citām apvienībām, kas pārstāv datu subjektu intereses**, **piešķirt tiesības celt prasību valsts tiesā**

- novērtēs vajadzību **stiprināt pašreizējos noteikumus par sankcijām**, piemēram, paredzot kriminālas sankcijas nopietnu datu aizsardzības pārkāpumu gadījumos, lai uzlabotu sankciju efektivitāti.

2.2. Iekšējā tirgus lomas stiprināšana

2.2.1. Tiesiskās noteiktības vairošana un vienādu spēles noteikumu nodrošināšana personas datu apstrādātājiem

Iekšējam tirgum ir svarīga loma datu aizsardzībā ES, proti, ir nepieciešams nodrošināt personas datu brīvu plūsmu starp dalībvalstīm iekšējā tirgū. Tāpēc direktīvā paredzētā valstu datu aizsardzības likumu saskaņošana nav minimuma saskaņošana, tās mērķis ir vispārīgi pilnīga saskaņošana[23].

Tajā pašā laikā direktīva pieļauj zināmu dalībvalstu rīcības brīvību atsevišķās jomās un atļauj tām saglabāt vai ieviest no jauna īpašus noteikumus īpašām situācijām[24]. Iepriekšminētais

[22] Sal. Direktīvas 95/46/EK 8. pants.

[23] Eiropas Savienības Tiesa, C-101/01, '*Bodil Lindqvist*', ECR [2003], I-1297, 96. un 97. punkts.

[24] Turpat, 97. punkts. Sk. arī Direktīvas 95/46/EK 9. pantu.

kopā ar faktu, ka dalībvalstis dažkārt ir nepareizi īstenojušas direktīvu, ir radījis situāciju, ka **valstu noteikumi direktīvas īstenošanai ir dažādi, kas savukārt ir pretrunā ar vienu no tās galvenajiem mērķiem, proti, nodrošināt personas datu brīvu plūsmu iekšējā tirgū.** Šāda situācija ir izveidojusies vairākās nozarēs, piemēram, apstrādājot personas datus saistībā ar nodarbinātību vai sabiedrības veselības aizsardzības nolūkos. Saskaņotības trūkums ir viena no visbiežāk sastopamajām un galvenajām problēmām, uz ko norāda privātas ieinteresētās personas, jo īpaši uzņēmumi, jo viņiem tas nozīmē papildu izmaksas un administratīvo slogu. Jo īpaši tas attiecas uz personas datu apstrādātājiem, kas veic uzņēmējdarbību vairākās dalībvalstīs un ir spiesti ievērot visu šo valstu prasības un praksi. Turklāt atšķirības direktīvas īstenošanas noteikumos dalībvalstīs rada tiesisko nenoteiktību ne tikai personas datu apstrādātājiem, bet arī datu subjektiem, radot risku, ka būs izjaukta aizsardzības līmeņa līdzvērtība, ko direktīvai būtu jāsasniedz un jānodrošina.

Komisija izpētīs, kā būtu iespējams panākt **turpmāku datu aizsardzības noteikumu saskaņošanu ES līmenī**.

2.2.2. Administratīvā sloga mazināšana

Nodrošinot vienādus spēles noteikumus, samazināsies vajadzība pieskaņoties atšķirīgiem valstu noteikumiem, tādējādi ievērojami samazināsies administratīvais slogs personas datu apstrādātājiem. Vēl viens konkrēts personas datu apstrādātāju administratīvā sloga un izmaksu mazināšanas pasākums būtu **paziņošanas sistēmas pārskatīšana un vienkāršošana**[25]. Personas datu apstrādātāju vidū valda vienprātība, ka vispārīgā prasība ziņot par visām datu apstrādes darbībām datu aizsardzības iestādēm ir visai apgrūtinošs pienākums, kas pats par sevi nesniedz nekādu reālu pienesumu indivīdu personas datu aizsardzībā. Turklāt šis ir viens no gadījumiem, kad direktīva pieļauj zināmu dalībvalstu rīcības brīvību, jo tās ir tiesīgas lemt par iespējamiem izņēmumiem un vienkāršošanu, kā arī par piemērojamām procedūrām.

Saskaņota un vienkāršota sistēma samazinātu izmaksas un administratīvo slogu, jo īpaši daudznacionālām sabiedrībām, kas veic uzņēmējdarbību vairākās dalībvalstīs.

Komisija izpētīs dažādas iespējas **paziņošanas sistēmas vienkāršošanai un saskaņošanai**, tostarp arī iespēju izstrādāt **vienotu ES reģistrācijas formu**.

2.2.3. Jautājuma par piemērojamām tiesībām un dalībvalstu atbildību precizēšana

Komisija pirmajā ziņojumā par datu aizsardzības direktīvas īstenošanu[26] jau 2003. gadā uzsvēra, ka noteikumi par piemērojamām tiesībām[27] dažos gadījumos bija "nepilnīgi, tāpēc tiesību kolīzijas, ko ar šā panta palīdzību bija gribēts novērst, tomēr ir iespējamas." Kopš tā laika situācija nav uzlabojusies, un gadījumos, kuros ir iesaistītas vairākas dalībvalstis, personas datu apstrādātājiem un datu aizsardzības uzraudzības iestādēm ne vienmēr ir skaidrs, kura dalībvalsts ir atbildīga un kuras tiesības ir piemērojamas. Jo īpaši ar šo problēmu jāsaskaras gadījumos, kad uz personas datu apstrādātāju attiecas dažādu dalībvalstu dažādi noteikumi, kad daudznacionāls uzņēmums nodarbojas ar uzņēmējdarbību vairāk nekā vienā dalībvalstī vai kad personas datu apstrādātājs nenodarbojas ar uzņēmējdarbību ES, taču sniedz savus pakalpojumus ES iedzīvotājiem.

---

25 Sk. Direktīvas 95/46/EK 18. pantu.

26 Komisijas ziņojums – Pirmais ziņojums par datu aizsardzības direktīvas (95/46/EC) īstenošanu, COM(2003)265.

27 Sk. Direktīvas 95/46/EK 4. pantu.

Globalizācijas un tehnikas attīstības iespaidā situācija kļūst aizvien sarežģītāka – personas datu apstrādātāji aizvien vairāk strādā vairākās dalībvalstīs un jurisdikcijās, sniedzot pakalpojumus un palīdzību jebkurā laikā. Internets ievērojami atvieglo personas datu apstrādātājiem iespējas veikt uzņēmējdarbību ārpus Eiropas Ekonomikas zonas (EEZ)[28], sniedzot pakalpojumus attālināti un apstrādājot personas datus tiešsaistē; bieži vien ir grūti noteikt, kur konkrētā brīdī atrodas personas dati un izmantotās iekārtas (piemēram, "mākoņdatošanas" lietojumprogrammas un pakalpojumi).

Tomēr Komisija uzskata, ka indivīdiem nevar atņemt aizsardzību, uz ko tiem ir tiesības saskaņā ar ES Pamattiesību hartu un ES datu aizsardzības tiesību aktiem, tikai tāpēc, ka personas datus apstrādā personas datu apstrādātājs trešās valstīs.

Komisija izpētīs, kā **pārstrādāt un precizēt noteikumus par piemērojamām tiesībām**, tostarp arī kritērijus pēc kuriem nosaka piemērojamās tiesības, lai uzlabotu tiesisko noteiktību, precizētu dalībvalstu atbildību datu aizsardzības noteikumu piemērošanā un visbeidzot nodrošinātu tāda paša līmeņa aizsardzību ES datu subjektiem, neatkarīgi no personas datu apstrādātāja ģeogrāfiskās atrašanās vietas.

2.2.4. Personas datu apstrādātāju atbildības pastiprināšana

Administratīvo procedūru vienkāršošanai **nebūtu jānoved pie tā, ka samazinās personas datu apstrādātāju atbildība nodrošināt datu efektīvu aizsardzību**. Gluži otrādi, Komisija uzskata, ka viņu pienākumi tiesiskā regulējuma ietvaros ir jāformulē daudz skaidrāk, tostarp attiecībā uz iekšējiem kontroles mehānismiem un sadarbību ar datu aizsardzības uzraudzības iestādēm. Turklāt jānodrošina, ka šie pienākumi ir piemērojami arī personas datu apstrādātājiem, uz kuriem attiecas profesionālā noslēpuma neizpaušanas pienākums (piemēram, advokātiem), kā arī gadījumos, kad personas datu apstrādātāji deleģē apstrādi citiem (piemēram, apstrādātājiem), ņemot vērā, ka šādu gadījumu skaits aizvien turpina palielināties.

Komisija tāpēc izpētīs kā būtu iespējams **nodrošināt, ka personas datu apstrādātāji ievieš efektīvas vadlīnijas un mehānismus, lai panāktu atbilstību datu aizsardzības noteikumiem.** Komisija ņems vērā diskusiju par iespēju ieviest "pārskatatbildības" principu, (*'accountability' principle*)[29]. Tā mērķis nebūtu palielināt administratīvo slogu personas datu apstrādātājiem, jo šie pasākumi būtu vairāk vērsti uz tādu drošības garantiju un mehānismu izveidi, kas optimizē datu aizsardzību, tajā pašā laikā samazinot un vienkāršojot atsevišķas administratīvās formalitātes, piemēram, paziņošanu (sk. iepriekš 2.2.2. punktu).

Šajā saistībā, tostarp arī attiecībā uz datu drošības nodrošināšanu, nozīmīga loma varētu būt pasākumiem, kas uzlabotu privātuma aizsardzību uzlabojošu tehnoloģiju (PUT) izmantošanu, kā minēts Komisijas 2007. gada paziņojumā par šo jautājumu, un "integrētas privātuma aizsardzības" principa aktīvāku piemērošanu[30].

---

28 Eiropas Ekonomikas zona ietver arī Norvēģiju, Lihtenšteinu un Īslandi.

29 Sk. jo īpaši atzinumu, ko 13. jūlijā pieņēmusi 29. panta darba grupa, Nr. 3/2010.

30 Attiecībā uz PUT sk. Komisijas paziņojumu Eiropas Parlamentam un Padomei par datu aizsardzības veicināšanu, izmantojot privātuma uzlabojošas tehnoloģijas (PUT), COM/2007/228. "Integrētas privātuma aizsardzības" princips nozīmē, ka privātums un datu aizsardzība ir ietverta visā tehnoloģiju dzīves ciklā no agrīnās projektēšanas līdz ieviešanai, izmantošanai un galīgai likvidēšanai. Cita starpā šis princips minēts arī Komisijas paziņojumā par "Eiropas digitalizācijas programmu" COM(2010)245.

Komisija izpētīs šādus pasākumus personas datu apstrādātāju atbildības pastiprināšanai:

– ieviest obligātu pienākumu iecelt **datu aizsardzības inspektoru** un saskaņot noteikumus par tā uzdevumiem un kompetenci[31], paturot prātā, ka ir vajadzīgi piemēroti kritēriji, lai izvairītos no nevajadzīga administratīvā sloga, jo īpaši maziem un mikro uzņēmumiem;

– tiesiskajā regulējumā ietvert personas datu apstrādātāju pienākumu īpašos gadījumos veikt **datu aizsardzības ietekmes novērtējumu**, piemēram, ja tiek apstrādāti sensitīvi dati vai apstrādes veids kā citādi ir saistīts ar īpašiem riskiem, jo īpaši, ja tiek izmantotas īpašas tehnoloģijas, mehānismi vai procedūras, tostarp profilēšana vai video novērošana;

– turpmāk veicināt PUT izmantošanu un iespējami konkrēti īstenot "**integrētas privātuma aizsardzības**" jēdzienu.

2.2.5. Pašregulācijas iniciatīvu rosināšana un ES sertifikācijas sistēmu izpēte

Komisija joprojām uzskata, ka personas datu apstrādātāju **pašregulācijas iniciatīvas** var **uzlabot datu aizsardzības noteikumu izpildi**. Pašregulācijas noteikumi datu aizsardzības direktīvā, proti, profesionālās ētikas kodeksu izstrāde[32], līdz šim ir reti izmantoti, un privātā sektora ieinteresētās personas tos uzskata par nepietiekamiem.

Turklāt Komisija izpētīs iespēju izveidot ES **sertifikācijas sistēmas (piemēram, "privātuma zīmogi")** procesiem, tehnikai, produktiem un pakalpojumiem, kas ievēro privātumu[33]. Tie ne tikai palīdzētu orientēties indivīdam kā šādu tehnoloģiju, produktu un pakalpojumu lietotājam, bet būtu nozīmīgi arī saistībā ar personas datu apstrādātāju atbildību – izvēle par labu sertificētām tehnoloģijām, produktiem vai pakalpojumiem, varētu palīdzēt pierādīt, ka personas datu apstrādātājs ir izpildījis savus pienākumus (sk. iepriekš 2.2.4. punktu). Protams, īpaši svarīgi būtu **nodrošināt šādu privātuma zīmogu uzticamību** un redzēt tos kopsakarā ar tiesiskajiem pienākumiem un starptautiskajiem tehniskajiem standartiem.

Komisija apņemas

- izpētīt iespējas **turpmāk rosināt pašregulācijas iniciatīvas**, tostarp aktīvu profesionālās ētikas kodeksu veicināšanu;

- izpētīt **ES sertifikācijas sistēmu** izveides praktiskās iespējas privātuma un datu aizsardzības jomā.

2.3. Datu aizsardzības noteikumu pārskatīšana policijas un tiesu iestāžu sadarbības krimināllietās jomā

Datu aizsardzības direktīva ir piemērojama visām personas datu apstrādes darbībām dalībvalstīs gan valsts, gan privātajā sektorā. Tomēr, tā neattiecas uz personas datu apstrādi tādu pasākumu gaitā, uz kuriem neattiecas Kopienas tiesību akti, kā pasākumi policijas un tiesu iestāžu sadarbības krimināllietās jomā[34]. Ar Lisabonas līgumu ir likvidēta ES "pīlāru struktūra" un ieviests jauns visaptverošs juridiskais pamats personas datu aizsardzībai visās

---

31 Vairākās dalībvalstīs jau ir paredzēts, ka personas datu apstrādātājs var iecelt datu aizsardzības inspektoru, lai patstāvīgi nodrošinātu ES un valsts datu aizsardzības noteikumu ievērošanu un palīdzētu indivīdiem (piemēram, *Beauftragter für den Datenschutz* Vācijā un *correspondant informatique et libertés (CIL)* Francijā).

32 Sk. Direktīvas 95/46/EK 27. pantu.

33 Šajā jautājumā sk. arī PUT paziņojumu, kas minēts 30. zemsvītras piezīmē.

34 Sk. Direktīvas 95/46/EK 3. panta 2. punkta pirmo ievilkumu.

ES politikas jomās[35]. Ņemot vērā šīs pārmaiņas un ES Pamattiesību hartu, Komisijas paziņojumos par Stokholmas programmu un par Stokholmas programmas rīcības plānu[36] ir uzsvērta nepieciešamība izveidot "*pilnīgu aizsardzības režīmu*" un "*stiprināt ES nostāja attiecībā uz indivīda personas datu aizsardzību visu ES politikas virzienu kontekstā, tostarp tiesībaizsardzībā un noziegumu novēršanā"*.

ES tiesību akts personas datu aizsardzībai policijas un tiesu iestāžu sadarbības krimināllietās jomā ir **Pamatlēmums 2008/977/TI**[37]. Pamatlēmums ir svarīgs solis uz priekšu jomā, kur vienoti datu aizsardzības standarti ir ļoti vajadzīgi. Tomēr darbs šajā jomā ir jāturpina.

Pamatlēmums attiecas tikai uz personas datu pārrobežu apmaiņu ES, to nepiemēro vietējām apstrādes darbībām dalībvalstīs. Šo atšķirību praksē ir grūti ievērot, un tā var sarežģīt pamatlēmuma īstenošanu un piemērošanu[38].

Tātad **Pamatlēmumā ir pārāk plašs izņēmums mērķa ierobežojuma principam**. Vēl viena nepilnība ir tāda noteikuma trūkums, kas paredzētu, ka jānodala dažādas datu kategorijas atkarībā no to precizitātes un uzticamības līmeņa, lai datus, kas balstīti uz faktiem varētu atšķirt no datiem, kas balstīti uz viedokļiem vai personīgiem novērtējumiem[39], un ka jānodala arī dažādu kategoriju datu subjekti (noziedznieki, aizdomās turētie, cietušie, liecinieki utml.), paredzot īpašas drošības garantijas datiem, kas saistīti ar personām, kas netiek turētas aizdomās[40].

Turklāt **Pamatlēmums neaizstāj daudzos sektorālos tiesību aktus policijas un tiesu iestāžu sadarbībai krimināllietās, kas pieņemti ES līmenī[41]**, jo īpaši tos, kas regulē Eiropola, *Eurojust*, Šengenas informācijas sistēmas (*SIS*) un Muitas informācijas sistēmas (*CIS*)[42] darbību, kuros arī ir ietverti īpaši datu aizsardzības režīmi un/vai atsauce uz Eiropas Padomes datu aizsardzības dokumentiem. Pasākumiem policijas un tiesu iestāžu sadarbības jomā visas dalībvalstis ir parakstījušas Eiropas Padomes Ieteikumu Nr. R(87)15, kurā ietverti Konvencijas Nr.108 principi attiecībā uz policijas sektoru. Taču tas nav juridiski saistošs akts.

Šī situācija var tieši ietekmēt indivīdu iespējas izmantot viņu datu aizsardzības tiesības šajā jomā (piemēram, zināt, kādi personas dati tiek apstrādāti un ar kādiem datiem notiek apmaiņa, kas to dara un kādiem nolūkiem, un kā izmantot tādas tiesības kā tiesības uz piekļuvi datiem).

---

35 Sk. LESD 16. pantu.

36 Sk. COM(2009) 262, 10.6.2009. un COM(2010) 171, 20.4.2010.

37 Padomes 2008. gada 27. novembra Pamatlēmums 2008/977/TI par tādu personas datu aizsardzību, ko apstrādā, policijas un tiesu iestādēm sadarbojoties krimināllietās (OV L 350, 30.12.2008., 60. lpp.). Pamatlēmumā paredzēta datu aizsardzības standartu minimuma saskaņošana.

38 Eiropas Padomes tiesību aktos šāda atšķirība nepastāv, piemēram, Konvencijā par indivīda aizsardzību attiecībā uz personas datu automātisko apstrādi (CETS Nr. 108), tās Papildprotokolā par uzraudzības iestādēm un pārrobežu datu plūsmām (ETS Nr. 181) un Ministru komitejas Ieteikumā Nr. R (87) 15, kas regulē personas datu izmantošanu policijas darbā, pieņemts 1987. gada 17. septembrī.

39 Kā tas prasīts 3.2. punktā Ieteikumā Nr. R (87) 15.

40 Pretēji 2. principam Ieteikumā Nr. R (87)15 un tā novērtējuma ziņojumiem.

41 Pārskatu par šiem tiesību aktiem sk. Komisijas paziņojumā "Pārskats par informācijas pārvaldību brīvības, drošības un tiesiskuma jomā" – COM(2010)385.

42 Papildus Eiropas Datu aizsardzības uzraudzītāja (EDAU) vispārīgajām uzraudzības tiesībām pār Savienības institūcijām, iestādēm, birojiem un aģentūrām, kas pamatojas uz Regulu EK Nr. 45/2001, attiecīgajos tiesību aktos ir paredzētas apvienotās uzraudzības iestādes, lai nodrošinātu datu aizsardzības uzraudzību.

Mērķis izveidot vispusīgu un saskaņotu sistēmu ES un attiecībās ar trešām valstīm nozīmē, ka **ir nepieciešams apsvērt, vai nebūtu jāpārskata datu aizsardzības noteikumi policijas un tiesu iestāžu sadarbības kriminālllietās jomā.** Komisija norāda, ka pilnīga datu aizsardzības režīma jēdziens neizslēdz iespēju vispārējā tiesiskā regulējuma ietvaros paredzēt īpašus noteikumus datu aizsardzībai policijas un tiesu iestāžu sektorā, ņemot vērā šīs jomas īpašo dabu, kā tas norādīts Lisabonas līgumam pievienotajā 21. deklarācijā. Tas nozīmē, piemēram, nepieciešamību apsvērt, kādā apmērā atsevišķu datu aizsardzības tiesību izmantošana konkrētā lietā varētu kavēt noziedzīgu nodarījumu novēršanu, izmeklēšanu, atklāšanu vai saukšanu pie atbildības par tiem vai krimināLo sankciju izpildi.

Komisija jo īpaši

- apsvērs iespēju **paplašināt vispārīgo datu aizsardzības noteikumu piemērošanas jomu un attiecināt tos arī uz policijas un tiesu iestāžu sadarbību kriminālllietās**, tostarp arī attiecībā uz apstrādi uz vietas dalībvalstīs, nepieciešamos gadījumos nosakot saskaņotus ierobežojumus atsevišķām indivīdu datu aizsardzības tiesībām, piemēram, viņu tiesībām piekļūt datiem vai caurskatāmības principam;

- izpētīs vajadzību jaunajā vispārīgajā tiesiskajā regulējumā ieviest **īpašus un saskaņotus noteikumus**, piemēram, par datu aizsardzību, apstrādājot **ģenētiskos datus** krimināltiesību vajadzībām, vai par dažādu datu subjektu kategoriju nošķiršanu (liecinieki, aizdomās turētie utml.) policijas sadarbības un tiesu iestāžu sadarbības kriminālllietās jomā;

- 2011. gadā sāks **apspriešanos** ar visām ieinteresētajām personām par to, kā labāk **pārskatīt uzraudzības sistēmas policijas un tiesu iestāžu sadarbības kriminālllietās jomā**, lai nodrošinātu datu aizsardzības efektīvu un konsekventu uzraudzību visās Savienības institūcijās, iestādēs, birojos un aģentūrās;

– novērtēs vajadzību ilgtermiņā **saskaņot dažādos sektoru īpašos noteikumos, kas pieņemti ES līmenī speciālajos tiesību aktos par policijas un tiesu iestāžu sadarbību kriminālllietās**, ar jauno datu aizsardzības vispārīgo tiesisko regulējumu.

2.4. Datu aizsardzība pasaules mērogā

2.4.1. Datu starptautiskas nosūtīšanas noteikumu precizēšana un vienkāršošana

Viens no līdzekļiem, kas padara iespējamu personas datu nosūtīšanu ārpus ES un EEZ, ir tā sauktais **"pietiekamības novērtējums"**. Pašlaik trešās valsts datu aizsardzības līmeņa pietiekamību, tas ir, vai trešā valsts nodrošina tādu aizsardzības līmeni, ko ES uzskata par pietiekamu, var konstatēt Komisija un dalībvalstis.

Komisijas pietiekamības lēmuma sekas ir tādas, ka ir atļauta brīva personas datu plūsma no visām 27 ES dalībvalstīm un trim EEZ dalībvalstīm uz konkrēto trešo valsti bez jebkādām papildu drošības garantijām. Tomēr datu aizsardzības direktīvā nav pietiekami skaidru un detalizētu noteikumu par kritērijiem, kas piemērojami Komisijas lēmumam par pietiekamību. Savukārt iepriekš minētajā Pamatlēmumā šāda lēmuma pieņemšana Komisijai vispār nav paredzēta.

Dažās dalībvalstīs pietiekamību vispirms novērtē pats personas datu apstrādātājs, kas nosūta datus uz trešo valsti, dažkārt šo novērtējumu pēc tam pārbauda datu aizsardzības uzraudzības iestāde. Tādējādi var pastāvēt dažādas pieejas trešo valstu vai starptautisko organizāciju datu aizsardzības līmeņa pietiekamības novērtēšanai, kas **nozīmē arī risku, ka trešās valsts nodrošinātā datu subjekta aizsardzības līmeņa novērtējums dalībvalstu starpā atšķiras**.

Turklāt tiesību aktos nav precīzu, saskaņotu noteikumu, saskaņā ar kuriem nosūtīšanu var uzskatīt par likumīgu. Tādējādi arī prakse dalībvalstu starpā ir dažāda.

Turklāt attiecībā uz datu nosūtīšanu uz trešām valstīm, kas nenodrošina pietiekamu aizsardzības līmeni, Komisijas standarta klauzulas par personas datu nosūtīšanu personas datu apstrādātājiem[43] un apstrādātājiem[44] nav domātas ārpuslīgumiskām attiecībām un, piemēram, tās nevar izmantot nosūtīšanai valsts pārvaldes iestāžu starpā.

Turklāt, starptautiskos nolīgumos, ko noslēgusi ES vai tās dalībvalstis, bieži tiek prasīts ietvert datu aizsardzības principus un īpašus noteikumus. Tādējādi var rasties dažādi teksti ar nesaskaņotiem noteikumiem un tiesībām, kas līdz ar to ir arī dažādi interpretējami, kaitējot datu subjektam. Rezultātā Komisija paziņoja, ka tā gribētu izstrādāt pamatelementus personas datu aizsardzībai nolīgumos starp Savienību un trešām valstīm tiesībaizsardzības nolūkā[45].

Lai likumīgi nosūtītu personas datus starp uzņēmumiem, kas pieder pie vienas uzņēmumu grupas, noderīgi var būt arī citi līdzekļi, kas izveidoti pašregulācijas mehānismu veidā, piemēram, iekšējie uzņēmuma profesionālās ētikas kodeksi, pazīstami arī kā "Saistošie uzņēmumu noteikumi" (*Binding Corporate Rules*)[46]. Tomēr ieinteresētās personas ir ierosinājušas, ka varētu uzlabot šo mehānismu un atvieglot tā īstenošanu.

Lai risinātu šeit norādītos problēmjautājumus, **nepieciešams vispār uzlabot mehānismus personas datu starptautiskai nosūtīšanai**, vienlaicīgi nodrošinot, ka personas dati ir pietiekami aizsargāti, kad tos nosūta un apstrādā ārpus ES un EEZ.

Komisija ir apņēmusies izpētīt, kā

- **uzlabot un saskaņot** datu starptautiskas nosūtīšanas **procedūras**, tostarp juridiski saistošus aktus un uzņēmumu saistošos noteikumus, lai nodrošinātu **vienādu un saskaņotu ES pieeju** attiecībā pret trešām valstīm un starptautiskām organizācijām;

- **precizēt Komisijas veikto pietiekamības novērtēšanas procedūru** un labāk izstrādāt **kritērijus un prasības** datu aizsardzības līmeņa novērtēšanai trešā valstī un starptautiskas organizācijas ietvaros.

- definēt **ES datu aizsardzības pamatelementus**, ko varētu izmantot visa veida starptautiskos nolīgumos.

---

43 Komisijas 2001. gada 15. jūnija Lēmums 2001/497/EK par līguma standartklauzulām attiecībā uz personas datu nosūtīšanu trešām valstīm saskaņā ar Direktīvu 95/46/EK (OV L 181., 4.7.2001., 19. lpp.); Komisijas 2001. gada 27. decembra Lēmums 2002/16/EK par līguma standartklauzulām attiecībā uz personas datu nosūtīšanu apstrādātājiem trešās valstīs saskaņā ar Direktīvu 95/46/EK (OV L 6., 10.1.2002., 52. lpp.); Komisijas 2004. gada 27. decembra Lēmums 2004/915/EK, ar ko groza Lēmumu 2001/497/EK attiecībā uz alternatīvu līguma standartklauzulu ieviešanu personas datu nosūtīšanai trešām valstīm (OV L 385., 29.12.2004., 74. lpp.).

44 Komisijas 2010. gada 5. februāra Lēmums par līguma standartklauzulām attiecībā uz personas datu pārsūtīšanu trešās valstīs reģistrētiem apstrādātājiem saskaņā ar Eiropas Parlamenta un Padomes Direktīvu 95/46/EK (OV L 39, 12.2.2010., 5. lpp).

45 Stokholmas Rīcības plāns sk. 36. zemsvītras piezīmi.

46 Saistošie uzņēmuma noteikumi ir profesionālās ētikas kodeksi, kas pamatojas uz Eiropas datu aizsardzības standartiem un ko daudznacionālas organizācijas brīvprātīgi izstrādā un ievēro, lai nodrošinātu atbilstīgas drošības garantijas personas datu nosūtīšanai vai dažādiem personas datu nosūtīšanas veidiem starp uzņēmumiem, kas pieder pie vienas uzņēmumu grupas un ko saista šie uzņēmuma noteikumi. Sk.: http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

2.4.2. Vispārēju principu veicināšana

Datu apstrāde notiek pasaules mērogā un tai ir nepieciešami vispārīgi principi indivīdu aizsardzībai attiecībā uz personas datu apstrādi.

ES datu aizsardzības tiesiskais regulējums **trešām valstīm** bieži ir kalpojis **par paraugu, uz ko tiekties, regulējot datu aizsardzību**. Tā sekas un ietekme Savienībā un ārpus tās ir bijušas ļoti nozīmīgas. Tāpēc **Eiropas Savienībai**, pamatojoties uz attiecīgajiem ES un citiem Eiropas tiesību aktiem par datu aizsardzību, **ir jāturpina būt personas datu aizsardzības attīstības dzinējspēkam un starptautisko tiesisko un tehnisko standartu veicinātājai**. Tas ir jo īpaši svarīgi ES paplašināšanās politikas ietvaros.

Attiecībā uz starptautiskiem tehniskiem standartiem, ko izstrādājušas standartizācijas organizācijas, Komisija uzskata, ka nākotnē plānotā tiesiskā regulējuma saskaņa ar šiem standartiem ir ļoti būtiska, lai nodrošinātu, ka personas datu apstrādāji konsekventi un praktiski īsteno datu aizsardzības noteikumus.

Komisija apņemas

- arī turpmāk **veicināt datu aizsardzības augsta līmeņa tiesisko un tehnisko standartu izstrādi** trešās valstīs un starptautiskā līmenī;

- censties panākt **aizsardzības savstarpības principa ievērošanu ES starptautiskās rīcības kontekstā** un jo īpaši attiecībā uz datu subjektiem, kuru datus eksportē no ES uz trešām valstīm;

- **šajā saistībā uzlabot sadarbību ar trešām valstīm un starptautiskām organizācijām**, piemēram, ESAO, Eiropas Padomi, Apvienoto Nāciju Organizāciju un citām reģionālām organizācijām;

- **cieši sekot līdzi starptautisko tehnisko standartu izstrādei, ko veic tādas standartizācijas organizācijas** kā *CEN* un *ISO*, lai nodrošinātu, ka tie lietderīgi papildina tiesiskos noteikumus, un nodrošinātu operatīvu un efektīvu datu aizsardzības galveno prasību īstenošanu.

2.5. Spēcīgāka institucionālā kārtība datu aizsardzības noteikumu labākai izpildei

Datu aizsardzības principu un noteikumu īstenošana un izpilde ir īpaši svarīgs elements indivīda tiesību ievērošanas garantēšanai.

Šajā saistībā datu aizsardzības noteikumu izpildei **īpaši nozīmīga ir datu aizsardzības iestāžu loma**. Tās ir neatkarīgi pamattiesību un brīvību sargi personas datu aizsardzības jomā, un indivīdi paļaujas, ka tās nodrošinās viņu personas datu aizsardzību un apstrādes darbību likumību. Tādēļ Komisija uzskata, ka to loma ir jāstiprina, jo īpaši ņemot vērā neseno Tiesas spriedumu par šo iestāžu neatkarību[47], turklāt tām jāpiešķir attiecīgās pilnvaras un resursi, kas nepieciešami uzdevumu veikšanai gan valsts līmenī, gan sadarbojoties vienai ar otru.

Tajā pašā laikā Komisija uzskata, ka **datu aizsardzības iestādēm ir jāuzlabo sadarbība un labāk jākoordinē savas darbības**, jo īpaši saskaroties ar pēc būtības pārrobežu jautājumiem. Jo īpaši tas sakāms par tādiem gadījumiem, kad daudznacionāli uzņēmumi atrodas vairākās

[47] Tiesas spriedums Komisija pret Vāciju, Lieta C-518/07, 9.3.2010.

dalībvalstīs un veic savas darbības katrā no šīm valstīm, vai arī gadījumos, kad ir nepieciešama koordinēta Eiropas Datu Aizsardzības uzrauga (EDAU) uzraudzība[48].

Šajā saistībā **svarīga loma varētu būt 29. panta darba grupai**[49], kuras uzdevums papildus padomdevējai funkcijai[50] jau ir veicināt vienotu ES datu aizsardzības noteikumu piemērošanu valstu līmenī. Tomēr tas, ka datu aizsardzības iestādes joprojām dažādi piemēro un interpretē ES noteikumus, kaut arī datu aizsardzības problēmas visā ES ir vienas un tas pašas, parāda, ka ir nepieciešams stiprināt darba grupas lomu datu aizsardzības iestāžu pozīcijas koordinēšanā, nodrošinot vienotāku piemērošanu valstu līmenī un tādējādi līdzvērtīgu datu aizsardzības līmeni.

Komisija izpētīs

- kā **stiprināt, precizēt un saskaņot valstu datu aizsardzības iestāžu statusu un pilnvaras** jaunā tiesiskā regulējuma ietvaros, ietverot "pilnīgas neatkarības" jēdziena īstenošanu[51];

- kā **uzlabot sadarbību un koordināciju datu aizsardzības iestāžu starpā**;

- **kā** nodrošināt ES datu aizsardzības noteikumu konsekventāku piemērošanu iekšējā tirgū. Tas varētu ietvert **valstu datu aizsardzības uzraugu lomas stiprināšanu, viņu darba labāku koordināciju ar 29. panta darba grupas starpniecību (kas varētu kļūt par caurskatāmāku vienību) un/vai Eiropas Komisijas vadīta mehānisma izveidi, kas nodrošinātu konsekvenci iekšējā tirgū.**

3. SECINĀJUMS. NĀKOTNES PERSPEKTĪVAS

Līdz ar tehniku nepārtraukti mainās arī veids, kā sabiedrībā izmanto mūsu personas datus un apmainās ar tiem. Tāpēc likumdevējam ir jāsastopas ar problēmu, kā izveidot tiesisko regulējumu, kas spēj tikt līdzi laikam. Reformu procesa beigās Eiropas datu aizsardzības noteikumiem arī turpmāk ir jāgarantē augsta līmeņa aizsardzība un jāsniedz tiesiskā noteiktība indivīdiem, valsts pārvaldei un uzņēmējiem iekšējā tirgū vairākās paaudzēs. Neatkarīgi no situācijas sarežģītības vai tehnikas attīstības, jāpastāv skaidrībai par piemērojamiem noteikumiem un standartiem, kas valstu iestādēm ir jāīsteno un kas uzņēmumiem un tehnoloģiju izstrādātājiem ir jāievēro. Arī indivīdiem ir jābūt skaidrībai par savām tiesībām.

Komisijas vispusīgā pieeja, lai risinātu šos jautājumus un sasniegtu šajā paziņojumā minētos galvenos mērķus, būs par pamatu turpmākai diskusijai ar citām Eiropas iestādēm un ieinteresētajām pusēm un vēlāk pārtaps konkrētos leģislatīvos un cita veida priekšlikumos un pasākumos. Šā mērķa sasniegšanai Komisija ar prieku sagaida atsauksmes par jautājumiem, kas iztirzāti šajā paziņojumā.

---

48 Šāda uzraudzība ir nepieciešama lielapjoma IT sistēmu gadījumos, piemēram, *SIS II* (sal. 46. pants Regulā (EK) Nr. 1987/2006 - OV L 318, 28.12.2006., 4. lpp.) un VIS (sal. 43. pants Regulā (EK) Nr. 767/2008 – OV L 218, 13.8.2008., 60. lpp.).

49 29. panta darba grupa ir padomdevēja institūcija, kuras sastāvā ir viens datu uzraudzības iestāžu pārstāvis no katras dalībvalsts, viens Eiropas Datu aizsardzības uzrauga (EDAU) un viens Komisijas pārstāvis (bez tiesībām balsot), Komisija nodrošina darba grupai sekretariāta pakalpojumus. Sk.: http://ec.europa.eu/justice/policies/privacy/workinggroup/index_en.htm .

50 29. panta darba grupa sniedz Komisijai padomus par aizsardzības līmeni ES un trešās valstīs un par jebkuriem citiem pasākumiem, kas saistīti ar personas datu apstrādi.

51 Sk. Tiesas spriedumu Komisija pret Vāciju, Lieta C-518/07, 9.3.2010.

Uz šā pamata un pēc ietekmes novērtējuma sagatavošanas, ņemot vērā ES Pamattiesību hartu, **2011. gadā** Komisija **iesniegs tiesību aktu priekšlikumus**, kuru mērķis būs pārskatīt datu aizsardzības tiesisko regulējumu, lai stiprinātu ES nostāju indivīdu personas datu aizsardzības jomā saistībā ar visām ES politikas nozarēm, tostarp arī tiesībaizsardzības un noziedzības novēršanas jomās, ņemot vērā to īpašo raksturu. Paralēli tiks īstenoti cita veida pasākumi, piemēram pašregulācijas mehānismu veicināšana un ES privātuma zīmogu praktiskās īstenošanas izpēte.

Pēc tam Komisija novērtēs **nepieciešamību** jaunajam vispārīgajam tiesiskajam regulējumam **pielāgot citus tiesību aktus**. Pirmkārt, tas attiecas uz Regulu (EK) Nr. 45/2001, kuras noteikumi būs jāpielāgo jaunajam vispārīgajam tiesiskajam regulējumam. Vēlāk būs nopietni jāizvērtē arī ietekme uz tiesību aktiem citās nozarēs.

Komisija turpinās nodrošināt Savienības tiesību pareizas īstenošanas pienācīgu uzraudzību šajā jomā, piekopjot **aktīvu pārkāpuma procedūru ierosināšanas politiku** gadījumos, kad ES datu aizsardzības noteikumi nebūs pareizi īstenoti un piemēroti. Patiesi, datu aizsardzības tiesību aktu pārskatīšana neietekmē dalībvalstu pienākumu īstenot un nodrošināt pareizu spēkā esošo tiesību aktu piemērošanu personas datu aizsardzības jomā[52].

Augsts un vienāds datu aizsardzības līmenis visā ES ir labākais veids, kā stiprināt un izplatīt ES datu aizsardzības standartus pasaulē.

[52] Tas attiecas arī uz Padomes Pamatlēmumu 2008/977/TI: dalībvalstīm tiek pieprasīts veikt vajadzīgos pasākumus, lai izpildītu šā pamatlēmuma noteikumus līdz 2010. gada 27. jūlijam.