844/14/LV
WP 217

Atzinums 06/2014 par personas datu apstrādātāja likumīgo interešu jēdzienu saskaņā ar Direktīvas 95/46/EK 7. pantu

Pieņemts 2014. gada 9. aprīlī

Šī darba grupa tika izveidota saskaņā ar Direktīvas 95/46/EK 29. pantu. Tā ir neatkarīga Eiropas padomdevēja struktūra jautājumos, kas saistīti ar datu aizsardzību un privātumu. Darba grupas uzdevumi ir aprakstīti Direktīvas 95/46/EK 30. pantā un Direktīvas 2002/58/EK 15. pantā.

Sekretariāta pakalpojumus nodrošina Eiropas Komisijas Tieslietu ģenerāldirektorāta C direktorāts (Pamattiesības un Savienības pilsonība), B-1049 Brisele, Beļģija, birojs Nr. MO-59 02/013.

Tīmekļa vietne: http://ec.europa.eu/justice/data-protection/index_lv.htm

Satura rādītājs

Kopsavilkums

Šajā atzinumā ir analizēti Direktīvas 95/46/EK 7. pantā izklāstītie datu apstrādes likumības kritēriji. Pievēršot uzmanību personas datu apstrādātāja likumīgajām interesēm, tajā sniegti norādījumi, kā piemērot 7. panta f) punktu saskaņā ar pašreizējo tiesisko regulējumu, un pausti ieteikumi turpmākiem uzlabojumiem.

Direktīvas 7. panta f) punktā minēts pēdējais no sešiem personas datu likumīgas apstrādes pamatojumiem. Faktiski tas paredz, ka ir jālīdzsvaro personas datu apstrādātāja vai jebkādu trešo personu, kurām atklāti dati, likumīgās intereses attiecībā pret datu subjekta interesēm vai pamattiesībām. Šīs līdzsvarošanas pārbaudes rezultāti noteiks, vai uz 7. panta f) punktu var paļauties kā uz datu apstrādes likumīgu iemeslu jeb juridisku pamatojumu.

Direktīvas 29. panta darba grupa atzīst 7. panta f) punkta kritērija nozīmi un derīgumu, jo pareizos apstākļos un pienācīgu aizsardzības jeb drošības pasākumu gadījumā tas var palīdzēt novērst pārmērīgu paļaušanos uz citiem juridiskajiem pamatojumiem. 7. panta f) punktu nedrīkst izmantot kā "pēdējo līdzekli" retām vai neparedzētām situācijām, kad uzskatāms, ka citi likumīgas apstrādes pamatojumi nav izmantojami. Tomēr to arī nedrīkst izvēlēties automātiski vai tā lietojumu nepamatoti paplašināt, uzskatot, ka tas ir mazāk ierobežojošs nekā citi pamatojumi.

Pienācīgs 7. panta f) punkta novērtējums nav vienkārša līdzsvarošanas pārbaude, kas tiek veikta, savstarpēji salīdzinot tikai divus skaitliski viegli izsakāmus un salīdzināmus "lielumus". Tā vietā šādā pārbaudē ir pilnvērtīgi jāapskata vairāki faktori, lai nodrošinātu, ka tiek pienācīgi ņemtas vērā datu subjektu intereses un pamattiesības. Vienlaikus pārbaudei jābūt izmantojamai dažādos mērogos — no vienkāršas līdz sarežģītai —, un tā nedrīkst radīt pārmērīgi lielu slogu. Faktori, kas jāņem vērā, veicot līdzsvarošanas pārbaudi, ir šādi:

- likumīgo interešu veids un avots, kā arī tas, vai datu apstrāde jāveic, lai īstenotu pamattiesības, vai tā kā citādi ir sabiedrības interesēs un vai atzīšana attiecīgajā kopienā dod labumu;

- ietekme uz datu subjektu un tā pamatotas gaidas attiecībā uz datu turpmāko lietojumu, kā arī datu un to apstrādes veids;

- papildu drošības pasākumi, kas varētu ierobežot nepamatotu ietekmi uz datu subjektu, piemēram, izmantoto datu apjoma samazināšana, privātuma uzlabošanas tehnoloģijas, labāka pārredzamība, vispārējas un beznosacījuma atteikuma tiesības, kā arī datu pārnesamība.

29. panta darba grupa iesaka ierosinātajā regulā turpmāk iekļaut apsvērumu par galvenajiem faktoriem, kas jāņem vērā, veicot līdzsvarošanas pārbaudi. 29. panta darba grupa arī iesaka pievienot apsvērumu, kurā personas datu apstrādātājam attiecīgā gadījumā noteikts dokumentēt savu novērtējumu, lai nodrošinātu labāku pārskatatbildību. Visbeidzot, 29. panta darba grupa arī atbalsta pamatnoteikuma iekļaušanu, personas datu apstrādātājiem nosakot par pienākumu paskaidrot datu subjektiem, kāpēc, viņuprāt, datu subjektu intereses, pamattiesības un brīvības nav pārākas par apstrādātāju tiesībām.

DARBA GRUPA PERSONU AIZSARDZĪBAI ATTIECĪBĀ UZ PERSONAS DATU APSTRĀDI,

kas izveidota ar Eiropas Parlamenta un Padomes 1995. gada 24. oktobra Direktīvu 95/46/EK,

ņemot vērā minētās direktīvas 29. pantu, 30. panta 1. punkta a) apakšpunktu un 30. panta 3. punktu,

ņemot vērā tās Reglamentu,

IR PIEŅĒMUSI ŠO ATZINUMU.

I. Ievads

Šajā atzinumā ir analizēti Direktīvas 95/46/EK[1] (turpmāk — "direktīva") 7. pantā izklāstītie datu apstrādes likumības kritēriji. Tajā īpaša uzmanība pievērsta personas datu apstrādātāju likumīgajām interesēm saskaņā ar 7. panta f) punktu.

Direktīvas 7. pantā uzskaitītie kritēriji ir saistīti ar plašāko "likumības" principu, kas ir izklāstīts 6. panta 1. punkta a) apakšpunktā, kurā noteikts, ka personas dati jāapstrādā "godīgi un likumīgi".

Direktīvas 7. pantā noteikts, ka personas datus apstrādā tikai tādā gadījumā, ja ir piemērojams vismaz viens no sešiem juridiskajiem pamatojumiem. Konkrēti, personas datus atļauts apstrādāt, a) tikai pamatojoties uz datu subjekta nepārprotamu piekrišanu[2] vai ja — īsi sakot[3] — apstrāde jāveic šādām vajadzībām:

b) lai izpildītu ar datu subjektu noslēgtā līgumā paredzētus nosacījumus;
c) lai ievērotu personas datu apstrādātājam noteiktas juridiskas saistības;
d) lai aizsargātu būtiskas datu subjekta intereses;
e) lai veiktu uzdevumu sabiedrības interesēs vai
f) lai ievērotu personas datu apstrādātāja īstenotas likumīgas intereses, kurām jāveic papildu līdzsvarošanas pārbaude attiecībā pret datu subjekta tiesībām un interesēm.

Šis pēdējais pamatojums ļauj veikt apstrādi, kas "vajadzīga personas datu apstrādātāja vai trešo personu, kurām dati tiek atklāti, likumīgo interešu ievērošanai, izņemot, ja šīs intereses ignorē, ņemot vērā datu subjekta intereses vai[4] pamattiesības un brīvības, kurām nepieciešama aizsardzība saskaņā ar 1. panta 1. punktu". Citiem vārdiem sakot, 7. panta f) punktā ir atļauts apstrādāt datus, ja tiek veikta līdzsvarošanas pārbaude, kurā salīdzinātas personas datu

[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. 29. panta datu aizsardzības darba grupas Atzinumu 15/2011 par jēdziena "piekrišana" definīciju, kas pieņemts 13.07.2011. (WP187).

[3] Šie noteikumi turpmāk atzinumā ir apspriesti sīkāk.

[4] Kā paskaidrots III.3.2. sadaļā, šķiet, ka direktīvas angļu valodas versijā ir kļūda — "interests for fundamental rights" vietā jābūt "interests or fundamental rights".

apstrādātāja vai jebkādu trešo personu, kurām atklāti dati, likumīgās intereses attiecībā pret datu subjekta interesēm vai pamattiesībām.[5]

Konsekventākas un saskaņotākas pieejas nepieciešamība visā Eiropā

Pētījumos, ko Komisija veikusi, pārskatot direktīvu[6], kā arī sadarbojoties un apmainoties ar viedokļiem ar valsts datu aizsardzības iestādēm ("DAI"), konstatēts, ka direktīvas 7. panta f) punkts netiek interpretēts saskaņoti, un tas ir radījis tā dažādu izmantojumu dalībvalstīs. Proti, lai gan vairākās dalībvalstīs noteikts, ka jāveic reāla līdzsvarošanas pārbaude, dažkārt 7. panta f) punkts tiek uztverts kā iespēja padarīt par likumīgu jebkāda veida datu apstrādi, kam neatbilst neviens cits juridiskais pamatojums.

Konsekventas pieejas trūkums var radīt juridiskās noteiktības un paredzamības trūkumu, vājināt datu subjektu stāvokli un arī radīt nevajadzīgu regulatīvo slogu uzņēmumiem vai citām organizācijām, kas darbojas pāri robežām. Šādas neatbilstības dēļ jau ir sākta tiesvedība Eiropas Savienības Tiesā ("EST")[7].

Tāpēc, turpinot darbu pie jaunas vispārīgās Datu aizsardzības regulas, šis ir īpaši piemērots brīdis, lai precīzāk definētu datu apstrādes sesto pamatojumu (ko apzīmē ar "likumīgām interesēm") un tā saistību ar citiem datu apstrādes pamatojumiem. Jo īpaši — tā kā runa ir par datu subjektu pamattiesībām, piemērojot visus sešus pamatojumus, ir pienācīgi un līdzvērtīgi jāņem vērā šīs tiesības. 7. panta f) punkts nedrīkst kļūt par vieglu iespēju, kā neievērot datu aizsardzības tiesību aktus.

Tāpēc 29. panta datu aizsardzības darba grupa ("darba grupa"), īstenojot savu darba programmu 2012.–2013. gadam, izlēma rūpīgi izskatīt šo tematu un — lai izpildītu savu darba programmu[8] — apņēmās sagatavot šo atzinumu.

Pašreizējā tiesiskā regulējuma piemērošana un sagatavošanās nākotnei

Pašā darba programmā ir skaidri norādīti divi mērķi: "pašreizējā tiesiskā regulējuma saskaņota un pareiza piemērošana" un arī "sagatavošanās nākotnei".

Attiecīgi šā atzinuma pirmais mērķis ir izveidot kopīgu izpratni par pašreizējo tiesisko regulējumu. Šis mērķis izriet no iepriekšējiem atzinumiem par citiem svarīgiem direktīvas

[5] Atsauci uz 1. panta 1. punktu nedrīkst interpretēt, lai ierobežotu datu subjektu interešu, pamattiesību un brīvību apmēru. Šī atsauce drīzāk paredzēta, lai uzsvērtu datu aizsardzības tiesību aktu un pašas direktīvas kopējo mērķi. Faktiski 1. panta 1. punkts attiecas ne vien uz privātuma aizsardzību, bet arī uz visām pārējām "fizisku personu pamattiesībām un brīvībām", un privātumsir tikai viena no tām.

[6] Eiropas Komisija 2012. gada 25. janvārī pieņēma dokumentu kopumu Eiropas datu aizsardzības regulējuma reformēšanai. Šajā dokumentu kopumā ir iekļauts i) paziņojums (COM(2012) 9 *final*), ii) priekšlikums vispārīgajai Datu aizsardzības regulai ("ierosinātā regula)" (COM(2012) 11 *final*) un iii) priekšlikums Direktīvai par datu aizsardzību krimināltiesību piemērošanas jomā (COM(2012) 10 *final*). Pievienotais ietekmes novērtējums, kurā ietverti 10 pielikumi, ir izklāstīts Komisijas darba dokumentā (SEC(2012) 72 *final*). Jo īpaši — sk. pētījumu "Evaluation of the implementation of the Data Protection Directive" (Datu aizsardzības direktīvas īstenošanas novērtējums), kas ir iekļauts Eiropas Komisijas datu aizsardzības reformu dokumentu kopumam pievienotā ietekmes novērtējuma 2. pielikumā.

[7] Sk. 7. lpp., "II.1. Īsa vēsture", "*Direktīvas īstenošana; spriedums ASNEF un FECEMD lietās*".

[8] Sk. 29. panta datu aizsardzības darba grupas darba programmu 2012.–2013. gadam, kas pieņemta 2012. gada 1. februārī (WP190).

noteikumiem[9]. Otrkārt, pamatojoties uz analīzi, šajā atzinumā arī formulēti politikas ieteikumi, kuri jāizskata datu aizsardzības tiesiskā regulējuma pārskatīšanas procesā.

Atzinuma struktūra

Pēc likumīgo interešu un citu datu apstrādes pamatojumu vēstures un nozīmes īsa pārskata II un III nodaļā apskatīti un interpretēti attiecīgie direktīvas noteikumi, ņemot vērā kopīgas īstenošanas iezīmes valstu mērogā. Šī analīze ir ilustrēta ar praktiskiem piemēriem no valstu pieredzes. Analīze apstiprina IV nodaļā paustos ieteikumus gan par pašreizējā tiesiskā regulējuma piemērošanu, gan saistībā ar direktīvas pārskatīšanu.

II. Vispārīgi apsvērumi un politikas jautājumi

II.1. Īsa vēsture

Šajā pārskatā uzmanība pievērsta likumības un datu apstrādes juridiskā pamatojuma (tai skaitā likumīgo interešu) jēdzienu attīstībai. Tajā īpaši skaidrots, kā sākotnēji juridiskā pamata nepieciešamība tikusi izmantota kā prasība saistībā ar atkāpēm no privātās dzīves neaizskaramības tiesībām un vēlāk attīstījusies par atsevišķu prasību datu aizsardzības kontekstā.

Eiropas Cilvēktiesību konvencija ("*ECTK*"*)*

1950. gadā pieņemtās Eiropas Cilvēktiesību konvencijas 8. pantā ir noteiktas privātās dzīves neaizskaramības tiesības, t. i., tiesības uz ikvienas personas privātās un ģimenes dzīves, mājokļa un sarakstes neaizskaramību. Tajā aizliegts traucēt baudīt tiesības uz privātās dzīves neaizskaramību, izņemot gadījumus, kas ir "paredzēti likumā" un "nepieciešami demokrātiskā sabiedrībā", lai nodrošinātu noteiktu veidu īpaši uzskaitītas nenoraidāmas sabiedrības intereses.

ECTK 8. pantā uzmanība ir pievērsta privātajai dzīvei, un tajā noteikts, ka, jebkādā veidā pārkāpjot privātās dzīves neaizskaramību, nepieciešams attaisnojums. Šīs pieejas pamatā ir vispārējs aizliegums pārkāpt privātās dzīves neaizskaramības tiesības, un izņēmumi ir pieļaujami tikai stingri definētos apstākļos. "Privātās dzīves neaizskaramības traucēšanas" gadījumos ir nepieciešams juridiskais pamats, kā arī likumīgs nolūks, kas ir priekšnosacījums šādas traucēšanas nepieciešamības novērtēšanai. Saskaņā ar šo pieeju ECTK nav sniegts iespējamo juridisko pamatojumu saraksts, taču ir pievērsta uzmanība juridiskā pamata nepieciešamībai un nosacījumiem, kam jāatbilst šādam juridiskajam pamatam.

Konvencija Nr. 108

Eiropas Padomes Konvencijā Nr. 108[10], kas tika atvērta parakstīšanai 1981. gadā, personas datu aizsardzība ieviesta kā atsevišķs jēdziens. Tobrīd idejas pamatā nebija uzskats, ka

[9] Piemēram, 3.4.2013. pieņemtais Atzinums 3/2013 par nolūka ierobežojumu (WP203), Atzinums 15/2011 par jēdziena "piekrišana" definīciju (minēts 2. zemsvītras piezīmē), 16.12.2010. pieņemtais Atzinums 8/2010 par piemērojamiem tiesību aktiem (WP179), kā arī 16.2.2010. pieņemtais Atzinums 1/2010 par "personas datu apstrādātāja" un "apstrādātāja" jēdzienu (WP169).

personas datu apstrāde vienmēr ir uzskatāma par "privātās dzīves neaizskaramības *traucēšanu*" — tā bija paredzēta, lai *aizsargātu* personu pamattiesības un brīvības, jo īpaši tiesības uz privātās dzīves neaizskaramību, tāpēc personas datu apstrādei vienmēr jāatbilst noteiktiem nosacījumiem. Tādējādi 5. pantā ir noteikti datu aizsardzības tiesību aktu pamatprincipi, tostarp prasība, ka "automātiski apstrādātajiem personas datiem ir jābūt: a) iegūtiem un apstrādātiem godīgi un saskaņā ar likumu." Tomēr konvencijā nav sniegti detalizēti datu apstrādes pamatojumi[11].

ESAO pamatnostādnes[12]

ESAO pamatnostādnēs, kas tika sagatavotas līdztekus Konvencijai Nr. 108 un pieņemtas 1980. gadā, bija līdzīga "likumības" izpratne, lai gan šis jēdziens bija izklāstīts citādi. Pamatnostādnes tika atjauninātas 2013. gadā, būtiski nemainot likumības principu. ESAO pamatnostādņu 7. pantā īpaši noteikts, ka "jābūt noteiktiem personas datu vākšanas ierobežojumiem, šādi dati jāiegūst likumīgā un godīgā ceļā un vajadzības gadījumā — informējot datu subjektu vai saņemot tā piekrišanu". Šajā gadījumā piekrišanas juridiskais pamatojums ir nepārprotami minēts kā neobligāts — izmantojams "vajadzības gadījumā". Šādā gadījumā ir jāveic attiecīgo interešu un tiesību novērtēšana, kā arī jānosaka, cik traucējoša ir datu apstrāde. Šajā ziņā ESAO pieeja zināmā mērā līdzinās daudz izvērstākajiem Direktīvas 95/46/EK kritērijiem.

Direktīva 95/46/EK

Kad 1995. gadā tika pieņemta direktīva, tās pamatā bija iepriekšēji datu aizsardzības instrumenti, tostarp Konvencija Nr. 108 un ESAO pamatnostādnes. Tika ņemta vērā arī dažu dalībvalstu sākotnējā pieredze datu aizsardzības jomā.

Papildus 6. panta 1. punkta a) apakšpunkta plašākai prasībai, ka personas dati jāapstrādā "godīgi un likumīgi", direktīva ir papildināta ar konkrētu papildu prasību kopumu, kas vēl nebija iekļauts ne Konvencijā Nr. 108, ne ESAO pamatnostādnēs — personas datu apstrādes pamatā jābūt kādam no sešiem juridiskajiem pamatojumiem, kas norādīti 7. pantā.

Direktīvas īstenošana; spriedums ASNEF un FECEMD lietās[13]

Komisijas ziņojumā "Datu aizsardzības direktīvas īstenošanas novērtējums"[14] ir uzsvērts, ka direktīvas noteikumu īstenošana valsts tiesību aktos dažkārt bijusi neapmierinoša. Tehniskajā analīzē par direktīvas transponēšanu dalībvalstīs[15] Komisija sniedz papildu informāciju par 7. panta īstenošanu. Analīzē paskaidrots, ka, lai arī lielākajā daļā dalībvalstu tiesību aktu seši

---

[10] Konvencija Nr. 108 par personu aizsardzību attiecībā uz personas datu automātisko apstrādi.

[11] Modernizētās konvencijas projekta tekstā, kas tika pieņemts *T-PD* 2012. gada novembra plenārsēdē, norādīts, ka datu apstrādi var veikt, ja saņemta datu subjekta piekrišana vai saskaņā ar "dažiem likumā noteiktiem leģitīmiem pamatiem", līdzīgi kā noteikts Eiropas Savienības Pamattiesību hartā, kas minēta 8. lappusē.

[12] ESAO pamatnostādnes par privātās dzīves aizsardzību un personas datu pārrobežu plūsmu, 2013. gada 11. jūlijs.

[13] Tiesas spriedums (24.11.2011.) lietās C-468/10 un C-469/10 (*ASNEF un FECEMD*).

[14] Skatiet 6. zemsvītras piezīmē minēto Komisijas datu aizsardzības reformu dokumentu kopumam pievienotā ietekmes novērtējuma 2. pielikumu.

[15] Analīze un ietekmes pētījums par Direktīvas 95/46/EK īstenošanu dalībvalstīs. Sk. http://ec.europa.eu/justice/policies/privacy/docs/lawreport/consultation/technical-annex_en.pdf.

juridiskie pamatojumi ir izklāstīti relatīvi līdzīgi kā direktīvā, faktiski šo principu elastība ir izraisījusi to atšķirīgu piemērošanu.

Ņemot vērā šo kontekstu, ir īpaši svarīgi, ka Eiropas Savienības Tiesa savā 2011. gada 24. novembra spriedumā *ASNEF un FECEMD* lietās uzskatīja, ka Spānija nav pareizi transponējusi direktīvas 7. panta f) punktu, nosakot, ka gadījumā, ja nav saņemta datu subjekta piekrišana, visi attiecīgie izmantotie dati ir jādara pieejami publiskos avotos. Spriedumā tika arī atzīts, ka 7. panta f) punktam ir tieša ietekme. Ar šo spriedumu tiek ierobežota dalībvalstu rīcības brīvība, īstenojot 7. panta f) punktu. Jo īpaši — tās nedrīkst pārkāpt smalko robežu starp precizēšanu, no vienas puses, un papildu prasību noteikšanu, kas mainītu 7. panta f) punkta piemērošanas jomu, — no otras puses.

Spriedumam, kurā skaidri noteikts, ka dalībvalstīm nav atļauts savos valsts tiesību aktos noteikt vienpusējus papildu ierobežojumus un prasības attiecībā uz likumīgas datu apstrādes juridiskajiem pamatojumiem, ir būtiskas sekas. Valstu tiesām un citām attiecīgajām struktūrām ir jāinterpretē valstu tiesību akti, ņemot vērā šo spriedumu, un vajadzības gadījumā jāaptur konfliktējoši valsts noteikumi un prakse.

Ņemot vērā šo spriedumu, ir vēl jo svarīgāk, lai valstu datu aizsardzības iestādes (DAI) un/vai Eiropas likumdevēji nonāktu pie skaidras un kopīgas izpratnes par 7. panta f) punkta piemērojamību. Tas ir jādara līdzsvaroti, nedz nepamatoti neierobežojot, nedz paplašinot šā noteikuma piemērošanas jomu.

Pamattiesību harta

Kopš Lisabonas līguma stāšanās spēkā 2009. gada 1. decembrī Eiropas Savienības Pamattiesību hartai (turpmāk — "harta") ir "tāds pats juridiskais spēks kā Līgumiem".[16] Hartas 8. pantā personas datu aizsardzība ir paredzēta kā pamattiesības, kas atšķiras no 7. pantā minētās privātās un ģimenes dzīves neaizskaramības. 8. pantā ir noteikta prasība nodrošināt datu apstrādes likumīgu pamatojumu. Jo īpaši tajā noteikts, ka personas dati ir jāapstrādā "ar attiecīgās personas piekrišanu vai ar citu likumīgu pamatojumu, kas paredzēts tiesību aktos".[17] Šie noteikumi stiprina gan likumības principa nozīmi, gan pienācīga personas datu apstrādes juridiskā pamata nepieciešamību.

Ierosinātā Datu aizsardzības regula

Saistībā ar Datu aizsardzības regulas pārskatīšanas procesu pašlaik tiek apspriesta 7. pantā minēto likumīguma pamatojumu un jo īpaši 7. panta f) punkta piemērošanas joma.

Ierosinātās regulas 6. pantā ir uzskaitīti personas datu likumīgas apstrādes pamatojumi. Ar dažiem izņēmumiem (kas aprakstīti turpmāk) kopumā seši pieejamie pamatojumi nav mainīti, ja tos salīdzinām ar pašlaik direktīvas 7. pantā noteiktajiem pamatojumiem. Tomēr Komisija ir ierosinājusi sniegt turpmākus norādījumus deleģētu aktu veidā.

[16] Sk. LES 6. panta 1. punktu.
[17] Sk. hartas 8. panta 2. punktu.

Interesanti, ka attiecīgā Eiropas Parlamenta komiteja savā darbā[18] bija mēģinājusi precizēt likumīgu interešu jēdzienu pašā ierosinātajā regulā. Tika sagatavots saraksts ar gadījumiem, kādos personas datu apstrādātāja likumīgās intereses pēc būtības būtu pārākas par datu subjekta likumīgajām interesēm, pamattiesībām un brīvībām, kā arī otrs saraksts, kurā šī attiecība ir apvērsta. Šie saraksti, kas bija iekļauti vai nu noteikumos, vai arī apsvērumos, sniedz būtisku ieguldījumu personas datu apstrādātāja un datu subjekta tiesību un interešu līdzsvara novērtējumā un ir ņemti vērā šajā atzinumā[19].

II.2. Jēdziena nozīme

Personas datu apstrādātāja likumīgās intereses — līdzsvarošanas pārbaude kā galīgais līdzeklis?

Direktīvas 7. panta f) punkts ir norādīts kā pēdējais no sešiem pamatojumiem, kas ļauj veikt personas datu likumīgu apstrādi. Tajā izteikts aicinājums veikt līdzsvarošanas pārbaudi — tas, kas ir vajadzīgs personas datu apstrādātāja (vai trešo personu) likumīgajām interesēm, ir jālīdzsvaro ar datu subjekta interesēm vai pamattiesībām un brīvībām. Šīs līdzsvarošanas pārbaudes rezultāti nosaka, vai uz 7. panta f) punktu var paļauties kā uz datu apstrādes juridisko pamatojumu.

Šā noteikuma atvērtā forma rada daudzus svarīgus jautājumus attiecībā uz tā konkrēto darbības jomu un piemērošanu, un tie analizēti šajā atzinumā. Tomēr, kā turpmāk paskaidrots, tas nebūt nenozīmē, ka šo iespēju vajadzētu uztvert kā tādu, ko izmantot tikai retos gadījumos, lai rastu risinājumu retās vai neparedzētās situācijās, izmantot "kā pēdējo līdzekli" vai pēdējo iespēju, ja citus pamatojumus izmantot nevar. Tomēr to arī nevajadzētu uztvert kā vēlamo variantu un tā lietojumu nevajadzētu nepamatoti paplašināt, uzskatot, ka tas ir mazāk ierobežojošs nekā citi pamatojumi.

Direktīvas 7. panta f) punktam ir sava dabiska nozīme, un tas var būt ļoti noderīgs kā likumīgas datu apstrādes pamatojums, ja vien ir ievēroti vairāki būtiski nosacījumi.

Izmantojot 7. panta f) punktu piemēroti, pareizos apstākļos un ievērojot pienācīgus drošības pasākumus, var arī novērst citu juridisko pamatojumu ļaunprātīgu izmantošanu vai pārmērīgu paļaušanos uz tiem.

Direktīvas 7. panta pirmo piecu pamatojumu balsts ir datu subjekta piekrišana, līgumsaistības, juridiskas saistības vai citi īpaši noteikti likumīguma pamatojumi. Ja apstrāde balstās uz kādu no šiem pieciem pamatojumiem, tā *a priori* tiek uzskatīta par likumīgu, tāpēc ir tikai jānodrošina tās atbilstība citiem piemērojamiem tiesību aktu noteikumiem. Citiem vārdiem sakot, pastāv pieņēmums, ka tiek nodrošināts līdzsvars starp dažādām attiecīgajām tiesībām un interesēm — tai skaitā personas datu apstrādātāja un datu subjekta tiesībām un interesēm —, protams, pieņemot, ka ir ievēroti visi pārējie datu aizsardzības tiesību aktu

[18] Pilsoņu brīvību, tieslietu un iekšlietu komitejas (*LIBE*) ziņojuma projekts par priekšlikumu Eiropas Parlamenta un Padomes regulai par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula), (COM(2012) 11 – C7-0025/2012 – 2012/0011(COD)), 16.1.2013. ("*LIBE* komitejas ziņojuma projekts"). Jo īpaši skatiet 101. un 102. grozījumu. Skatiet arī komitejas 21.10.2013. galīgajā ziņojumā ("*LIBE* komitejas galīgais ziņojums") pieņemtos grozījumus.

[19] Jo īpaši skatiet III.3.1. sadaļas aizzīmes 24. un 25. lpp., kurās iekļauts papildināms saraksts ar dažiem biežāk sastopamajiem gadījumiem, kādos var rasties likumīgu interešu problēma saistībā ar 7. panta f) punktu.

noteikumi. Turpretim 7. panta f) punktā ir prasīta *konkrēta* pārbaude gadījumos, kas neatbilst iepriekš a)–e) punkta pamatojumā definētajiem scenārijiem. Tas nodrošina, ka gadījumos, kas neatbilst šiem scenārijiem, attiecībā uz jebkādu personas datu apstrādi ir jāveic līdzsvarošanas pārbaude, pienācīgi ņemot vērā datu subjekta intereses un pamattiesības.

Noteiktos gadījumos pēc šādas pārbaudes pārsvars var būt datu subjektu interešu un pamattiesību pusē, tādēļ datu apstrāde nevar tikt veikta. Savukārt pienācīga līdzsvara samēra novērtēšana saskaņā ar 7. panta f) punktu (bieži vien ar izvēles iespēju atteikties no datu apstrādes) citos gadījumos var būt derīga alternatīva, lai, piemēram, neatbilstīgi neizmantotu "piekrišanas" vai "līguma [..] izpildes" pamatojumu. Raugoties no šāda skatpunkta, 7. panta f) punkts rada papildu drošību, un, salīdzinot ar citiem iepriekš noteiktiem pamatojumiem, tajā prasīts veikt atbilstīgus pasākumus. Tādēļ to nevajadzētu uztvert kā "vājāko posmu" vai iespēju padarīt par likumīgu jebkāda veida datu apstrādi, kam neatbilst neviens cits juridiskais pamatojums.

Darba grupa atgādina, ka, interpretējot 7. panta f) punkta piemērošanas jomu, tās mērķis ir izveidot līdzsvarotu pieeju, kas personas datu apstrādātājiem nodrošina vajadzīgo elastību gadījumos, kad netiek radīta nepamatota ietekme uz datu subjektiem, vienlaikus nodrošinot pietiekamu juridisko noteiktību un garantijas datu subjektiem, ka šādas atvērtas formas noteikums netiks izmantots ļaunprātīgi.

II.3. Saistītie jēdzieni

Direktīvas 7. panta f) punkta saistība ar citiem likumīguma pamatojumiem

Direktīvas 7. pantā kā pirmā tiek minēta piekrišana, un turpmāk uzskaitīti citi likumīguma pamatojumi, tostarp līgumi un juridiskās saistības, pakāpeniski pārejot pie likumīgu interešu pārbaudes, kas ir uzskaitīta kā pēdējā no sešiem pieejamajiem pamatojumiem. 7. pantā uzskaitīto juridisko pamatojumu secība dažkārt ir interpretēta kā norāde uz attiecīgo pamatojumu svarīgumu. Tomēr, kā jau uzsvērts darba grupas atzinumā par piekrišanas jēdzienu[20], direktīvas tekstā šie seši pamatojumi nav juridiski nošķirti un starp tiem nav paredzēta nekāda veida hierarhija. Nav nekādu norāžu, ka 7. panta f) punkts būtu jāizmanto tikai ārkārtas gadījumos, un arī pašā tekstā nav nekā citādi norādīts, ka šo sešu juridisko pamatojumu konkrētajai secībai būtu kāda juridiska nozīme. Tajā pašā laikā 7. panta f) punkta konkrētā nozīme un tā saistība ar citiem likumīguma pamatojumiem jau ilgi bijusi samērā neskaidra.

Šādos apstākļos un ņemot vērā atšķirīgās vēsturiskās un kultūras iezīmes, kā arī direktīvas atvērto formulējumu, ir izstrādātas dažādas pieejas — dažas dalībvalstis ir uztvērušas 7. panta f) punktu kā vismazāk vēlamo pamatojumu, ko paredzēts izmantot vienīgi dažos izņēmuma gadījumos, kad nevar piemērot nevienu no pārējiem pieciem pamatojumiem[21]. Turpretim citas dalībvalstis to uztver tikai kā vienu no sešām iespējām, kas nav svarīgāka vai mazāk svarīga par citiem pamatojumiem un ko var piemērot ļoti daudzās un dažādās situācijās, ja tiek ievēroti attiecīgie priekšnosacījumi.

[20] Sk. iepriekš 2. zemsvītras piezīmi.

[21] Ir arī jānorāda, ka *LIBE* komitejas ziņojuma projekta 100. grozījumā ir ierosināts nošķirt 7. panta f) punktu no pārējiem juridiskajiem pamatojumiem, kā arī — kā aprakstīts turpmāk — ierosinātas papildu prasības gadījumā, ja tiek izmantots šis juridiskais pamatojums, tostarp labāka pārredzamība un stingrāka pārskatatbildība.

Ņemot vērā šīs atšķirības, kā arī spriedumu *ASNEF* un *FECEMD* lietās, ir svarīgi precizēt "likumīgo interešu" pamatojuma saistību ar citiem likumīguma pamatojumiem (piemēram, attiecībā uz piekrišanu, līgumiem, uzdevumiem sabiedrības interesēs), kā arī sasaisti ar datu subjekta un objekta tiesībām. Šādi varētu labāk definēt likumīgo interešu pamatojuma nozīmi un funkciju, tādējādi veicinot juridisko noteiktību.

Turklāt jānorāda, ka attiecībā uz likumīgo interešu pamatojumu līdzās citiem pamatojumiem (izņemot piekrišanu) ir nepieciešama "vajadzības" pārbaude. Tas stingri ierobežo katra pamatojuma piemērošanas apstākļus. Eiropas Savienības Tiesa uzskatīja, ka "vajadzība" ir autonoms Kopienu tiesību jēdziens[22]. Noderīgas norādes sniedza arī Eiropas Cilvēktiesību tiesa[23].

Turklāt piemērots juridiskais pamatojums neatbrīvo personas datu apstrādātāju no 6. pantā noteiktajām saistībām attiecībā uz godīgumu, likumību, vajadzīgumu un samērīgumu, kā arī datu kvalitāti. Piemēram, pat ja personas datu apstrādes pamatā ir likumīgu interešu pamatojums vai līguma izpilde, tas neļauj vākt tādu datu apjomu, kas ir pārmērīgs attiecībā uz norādīto nolūku.

Likumīgas intereses un citi 7. pantā minētie pamatojumi ir alternatīvi pamatojumi, tāpēc ir pietiekami, ja piemērojams ir tikai viens no tiem. Tomēr tiem ir kumulatīva ietekme ne vien ar 6. panta prasībām, bet arī citiem datu aizsardzības principiem un prasībām, kas, iespējams, jāpiemēro.

Citas līdzsvarošanas pārbaudes

Direktīvas 7. panta f) punkts nav vienīgā direktīvā paredzētā līdzsvarošanas pārbaude. Piemēram, 9. pantā ir izteikts aicinājums līdzsvarot tiesības uz personas datu aizsardzību ar vārda brīvību. Ar šo pantu dalībvalstīm tiek ļauts noteikt izņēmumus un atkāpes no personas datu apstrādes, "kas veikta tikai un vienīgi žurnālistikas nolūkiem vai mākslinieciskās vai literārās izteiksmes nolūkiem [..], ja tie vajadzīgi, lai saskaņotu tiesības uz privātās dzīves neaizskaramību ar normām, kas reglamentē vārda brīvību".

Turklāt arī daudzos citos direktīvas noteikumos ir paredzēta katra atsevišķa gadījuma analīze, līdzsvarojot attiecīgās intereses un tiesības, kā arī elastīgs vairāku faktoru novērtējums. Cita starpā tie ietver noteikumus par vajadzīgumu, samērīgumu un nolūka ierobežojumu, 13. pantā minētos izņēmumus, zinātnisko pētniecību un citus.

Patiešām šķiet, ka direktīva ir izstrādāta tā, lai būtu atstāta iespēja interpretācijai un interešu līdzsvarošanai. Protams, daļēji tas bija paredzēts, lai dalībvalstīm būtu lielāka rīcības brīvība, īstenojot direktīvu valstu tiesību aktos. Tomēr papildus tam zināmas elastības nepieciešamību

[22] Eiropas Savienības Tiesas 2008. gada 16. decembra spriedums lietā C-524/06 (*Heinz Huber* pret Vācijas Federatīvo Republiku), 52. punkts: "Tāpēc, ņemot vērā mērķi visās dalībvalstīs nodrošināt vienādu aizsardzības līmeni, vajadzības jēdzienam, kas izriet no Direktīvas 95/46 7. panta e) punkta, kurā ir paredzēts precīzi noteikt vienu no gadījumiem, kad personas datu apstrāde ir likumīga, nevar būt atšķirīgs saturs atkarībā no dalībvalsts. Tādējādi tas ir autonoms Kopienu tiesību jēdziens, kas ir jāinterpretē tā, lai tas pilnībā atbilstu šīs direktīvas mērķim, kas ir noteikts tās 1. panta 1. punktā."

[23] Eiropas Cilvēktiesību tiesas 1983. gada 25. marta spriedums lietā *Silver* un citi pret Apvienoto Karalisti, 97. pants, kurā apspriests termins "vajadzīgs demokrātiskā sabiedrībā": "īpašības vārds "vajadzīgs" nav sinonīms terminam "obligāti nepieciešams", un tā nozīme nav arī tik elastīga kā tādiem apzīmējumiem kā "pieņemams", "ierasts", "noderīgs", "pamatots" vai "vēlams"[..]".

nosaka pašas tiesības uz personas datu aizsardzību un privātās dzīves neaizskaramību. Patiesi, tiek uzskatīts, ka šīs divas tiesības kopā ar lielāko daļu citu pamattiesību (taču ne visām), ir relatīvas jeb kvalificētas cilvēktiesības[24]. Šāda veida tiesības vienmēr ir jāinterpretē, ņemot vērā to kontekstu. Kad ir ieviesti atbilstīgi drošības pasākumi, tās var līdzsvarot ar citu personu tiesībām. Dažās situācijās un arī saskaņā ar atbilstīgiem drošības pasākumiem tās var ierobežot sabiedrības interešu dēļ.

II.4. Konteksts un stratēģiskās sekas

Gan likumības, gan elastības nodrošināšana — 7. panta f) punkta precizēšanas līdzekļi

Direktīvas 7. panta f) punkta pašreizējam tekstam ir atvērts formulējums. Tas nozīmē, ka to var izmantot ļoti dažādās situācijās, ja vien tiek ievērotas tā prasības, tai skaitā līdzsvarošanas pārbaude. Tomēr šādai elastībai ir arī negatīvas sekas. Lai tā neradītu nekonsekventu piemērošanu valstīs vai juridiskās noteiktības trūkumu, svarīga nozīme ir turpmākām norādēm.

Komisija ierosinātajā regulā ir paredzējusi šādus norādījumus deleģēto aktu veidā. Ir arī citas iespējas — sniegt paskaidrojumus un detalizētus noteikumus pašas ierosinātās regulas tekstā[25] un/vai uzticēt uzdevumu sniegt papildu norādījumus šajā jomā Eiropas Datu aizsardzības kolēģijai ("EDAK").

Katrai no šīm iespējām ir savas priekšrocības un trūkumi. Ja novērtējums jāgatavo katrā atsevišķā gadījumā bez papildu norādījumiem, var rasties nekonsekventas piemērošanas un prognozējamības trūkuma risks, kā tas bijis iepriekš.

Savukārt, ja pašas ierosinātās regulas tekstā tiek iekļauti detalizēti un izsmeļoši tādu situāciju saraksti, kurās personas datu apstrādātāja likumīgās intereses vienmēr ir pārākas par datu subjekta pamattiesībām vai otrādi, tie var būt maldinoši, nevajadzīgi preskriptīvi vai gan vieni, gan otri reizē.

Tomēr šādas pieejas var būt par iedvesmas avotu līdzsvarotam risinājumam, pašā ierosinātajā regulā iekļaujot detalizētāku informāciju un deleģētos aktos vai EDAK dokumentos sniedzot papildu norādījumus[26].

Atzinuma III nodaļā izvērstās analīzes mērķis ir radīt pamatu šādas pieejas atrašanai, kas nebūtu nedz pārāk vispārīga, tādējādi kļūstot bezjēdzīga, nedz arī pārāk specifiska, kļūstot pārmēru neelastīga.

---

[24] Pastāv tikai dažas cilvēktiesības, ko nevar līdzsvarot ar citu personu tiesībām vai plašākas sabiedrības interesēm. Tās zināmas kā absolūtās tiesības. Šīs tiesības nevar ierobežot nekādos apstākļos — pat kara gadījumā vai ārkārtas situācijās. Viens šāds piemērs ir tiesības netikt pakļautam spīdzināšanai un necilvēcīgai vai pazemojošai izturēšanās. Nekādā gadījumā nav pieļaujams spīdzināt kādu vai pret viņu izturēties necilvēcīgi vai pazemojoši neatkarīgi no apstākļiem. Neabsolūtu cilvēktiesību piemēri ir tiesības uz privātās un ģimenes dzīves neaizskaramību, tiesības uz vārda brīvību un domu, pārliecības un ticības brīvību.

[25] Sk. II.1. sadaļas "Īsa vēsture"' rindkopu "Ierosinātā Datu aizsardzības regula" 8.–9. lappusē.

[26] Attiecībā uz deleģētiem aktiem un EDAK norādījumiem darba grupa savā Atzinumā 08/2012 — papildu ieguldījums diskusijās par datu aizsardzības tiesiskā regulējuma reformu, kas tika pieņemts 5.10.2012. (WP199), pauda stingru atbalstu otrajai iespējai (sk. 13.–14. lpp.).

III. Noteikumu analīze

III.1. Direktīvas 7. panta pārskats

Direktīvas 7. pantā noteikts, ka personas datus apstrādā tikai tādā gadījumā, ja ir piemērojams vismaz viens no sešiem juridiskajiem pamatojumiem. Pirms katra pamatojuma analīzes šajā III.1. sadaļā ir sniegts pārskats par 7. pantu un tā saistību ar 8. pantu par datu īpašajām kategorijām.

III.1.1. Piekrišana vai "vajadzīga .."

Gadījumu, kad personas dati tiek apstrādāti saskaņā ar datu subjekta nepārprotamu piekrišanu (7. panta a) punkts), var nošķirt no pārējiem pieciem gadījumiem (7. panta b)–f) punkts). Īsi sakot, šie pieci gadījumi ietver scenārijus, kādos apstrāde var būt vajadzīga noteiktā kontekstā, piemēram, lai izpildītu līgumu ar datu subjektu, izpildītu uz personas datu apstrādātāju attiecināmas juridiskas saistības u. c.

Pirmajā gadījumā, kas minēts 7. panta a) punktā, personas datu apstrādi atļauj paši datu subjekti. Par personas datu apstrādi lemj viņi paši. Tajā pašā laikā šāda piekrišana neatceļ nepieciešamību ievērot 6. pantā izklāstītos principus[27]. Turklāt, lai piekrišana būtu likumīga, tai jāatbilst noteiktiem būtiskiem nosacījumiem, kas ir paskaidroti darba grupas Atzinumā 15/2011[28]. Tā kā galu galā lietotāja datu apstrādes veikšana ir atkarīga no viņa paša, šajā gadījumā tiek uzsvērts datu subjekta piekrišanas derīgums un darbības joma.

Citiem vārdiem sakot, pirmajā pamatojumā (7. panta a) punktā) uzmanība ir pievērsta datu subjekta pašnoteikšanās principam kā likumīguma pamatojumam. Turpretim visi pārējie pamatojumi pieļauj apstrādi (ja ir veikti drošības un citi pasākumi) gadījumos, kad neatkarīgi no piekrišanas datus var apstrādāt un tie ir jāapstrādā noteiktā kontekstā, lai īstenotu konkrētas likumīgas intereses.

Panta b), c), d) un e) punktā ir norādīti kritēriji, kas ļauj datu apstrādi padarīt likumīgu:

b) lai izpildītu ar datu subjektu noslēgtā līgumā paredzētus nosacījumus;
c) lai ievērotu personas datu apstrādātājam noteiktas juridiskas saistības;
d) lai aizsargātu būtiskas datu subjekta intereses;
e) lai veiktu uzdevumu sabiedrības interesēs.

Direktīvas 7. panta f) punkts nav tik specifisks un vispārīgākā formā norāda uz (jebkāda veida) personas datu apstrādātāja likumīgajām interesēm (jebkādā kontekstā). Attiecībā uz šo vispārīgo noteikumu ir īpaši noteikta papildu līdzsvarošanas pārbaude, kuras mērķis ir aizsargāt datu subjektu intereses un tiesības, kā turpmāk aprakstīts III.2. sadaļā.

[27] Nīderlandes Augstākās tiesas 2011. gada 9. septembra spriedums lietā ECLI:NL:HR:2011:BQ8097, 3. punkta 3. apakšpunkta e) punkts par proporcionalitātes principu. Sk. arī iepriekš 2. zemsvītras piezīmē minētā darba grupas Atzinuma 15/2011 7. lpp.: ".. piekrišanas iegūšana neatbrīvo personas datu apstrādātāju no 6. pantā minētajiem pienākumiem attiecībā uz godīgumu, nepieciešamību, samērīgumu un datu kvalitāti. Piemēram, tas, ka personas datu apstrāde notiek, pamatojoties uz lietotāja piekrišanu, nenozīmē, ka datu vākšana pārmērīgā apjomā konkrētam nolūkam būtu likumīga."

[28] Sk. arī iepriekš 2. zemsvītras piezīmē minētā Atzinuma 15/2011 11.–25. lpp.

Novērtējums par to, vai ir ievēroti 7. panta a)–f) punktā izklāstītie kritēriji, ir jāveic visos gadījumos — to sākotnēji veic personas datu apstrādātājs saskaņā ar piemērojamajiem tiesību aktiem un norādījumiem par tiesību aktu piemērošanu. Otrajā gadījumā attiecībā uz apstrādes likumību var veikt papildu novērtējumu, un to var apstrīdēt datu subjekti, citas ieinteresētās personas, datu aizsardzības iestādes un, visbeidzot — lēmumu var pieņemt tiesa.

Noslēdzot šo īso pārskatu, jāpiemin, ka (kā izklāstīts III.3.6. sadaļā) vismaz e) un f) punktā minētajos gadījumos datu subjekts var īstenot 14. pantā noteiktās iebildumu paušanas tiesības[29]. To darot, būs jāsagatavo jauns iesaistīto interešu novērtējums vai tiešās tirdzniecības jeb tirgvedības gadījumā (14. panta b) punkts) — apstrādātājam būs jāpārtrauc personas datu apstrāde, neveicot turpmāku novērtējumu.

III.1.2. Saistība ar 8. pantu

Direktīvas 8. pantā ir papildus reglamentēta noteiktu īpašu personas datu kategoriju apstrāde. Tas konkrēti attiecas uz tādu datu apstrādi, "kas atklāj rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās, kā arī uz veselību vai seksuālo dzīvi attiecināmu datu apstrādi" (8. panta 1. punkts), un datiem, kas attiecas uz "noziedzīgiem nodarījumiem" vai "kriminālas vajāšanas gadījumiem" (8. panta 5. punkts).

Šādu datu apstrāde principā ir aizliegta, taču ir piemērojami daži izņēmumi. 8. panta 2. punkta a)–e) apakšpunktā ir minēti vairāki šāda aizlieguma izņēmumi. 8. panta 3. un 4. punktā ir aprakstīti citi papildu izņēmumi. Daži no šiem noteikumiem līdzinās, taču nav identiski 7. panta a)–f) punktā izklāstītajiem noteikumiem.

Direktīvas 8. panta konkrētie nosacījumi, kā arī tas, ka daži no 7. pantā uzskaitītajiem pamatojumiem atgādina 8. pantā izklāstītos nosacījumus, liek izvirzīt jautājumu par saistību starp šiem abiem noteikumiem.

Ja 8. pants ir paredzēts kā *lex specialis*, ir jānoskaidro, vai tas izslēdz 7. panta piemērojamību kopumā. Tādā gadījumā tas nozīmētu, ka personas datu īpašās kategorijas var apstrādāt, neievērojot 7. panta nosacījumus, ja ir piemērojams kāds no 8. pantā minētajiem izņēmumiem. Tomēr var būt arī tā, ka šī saistība ir sarežģītāka un ka 7. un 8. pants ir jāpiemēro kumulatīvi[30].

Jebkurā gadījumā ir skaidrs, ka politikas mērķis ir nodrošināt papildu aizsardzību īpašām datu kategorijām. Tādēļ analīzes galarezultātam jābūt vienlīdz skaidram — 8. panta piemērošanas (atsevišķi vai kumulatīvi ar 7. pantu) mērķis ir nodrošināt augstāku aizsardzības līmeni īpašām datu kategorijām.

[29] Turklāt 14. panta a) punktā noteikts, ka šīs tiesības var īstenot, "ja vien attiecīgās valsts tiesību akti neparedz citādi". Piemēram, Zviedrijā valsts tiesību aktos nav pieļauta iespēja paust iebildumus par datu apstrādi, kuras pamatā ir 7. panta e) punkts.

[30] Tā kā 8. pants ir paredzēts kā *aizliegums ar izņēmumiem*, šos izņēmumus var uztvert kā prasības, kas tikai ierobežo aizlieguma piemērošanas jomu, taču paši par sevi tie nav pietiekams juridiskais pamatojums, lai veiktu apstrādi. Šādā lasījumā 8. panta izņēmumu piemērojamība neizslēdz 7. pantā noteikto prasību piemērojamību, un abus attiecīgā gadījumā var lietot kumulatīvi.

Praksē tas gan nav attiecināms uz visiem noteikumiem (lai gan dažos gadījumos 8. pantā ir noteiktas stingrākas prasības, piemēram, "precīzi formulēta" piekrišana, kā paredzēts 8. panta 2. punkta a) apakšpunktā, salīdzinot ar "nepārprotamu piekrišanu", kā minēts 7. pantā). Daži 8. pantā paredzētie izņēmumi nešķiet līdzvērtīgi 7. pantā uzskaitītajiem pamatojumiem vai stingrāki par tiem. Piemēram, būtu neatbilstīgi secināt, ka tas, ja kāds ir publiski darījis zināmas atklātībai īpašās datu kategorijas saskaņā ar 8. panta 2. punkta e) apakšpunktu, vienmēr pats par sevi būtu pietiekams nosacījums, lai ļautu turpmāku datu apstrādi, neveicot attiecīgo interešu un tiesību līdzsvara novērtējumu, kas paredzēts 7. panta f) punktā[31].

Dažās situācijās tas, ka personas datu apstrādātājs ir politiska partija, arī atceltu aizliegumu apstrādāt īpašas datu kategorijas atbilstīgi 8. panta 2. punkta d) apakšpunktam. Tomēr tas nenozīmē, ka jebkāda veida apstrāde, kurai piemērojams šis noteikums, ir likumīga. Tas ir jānovērtē atsevišķi, un personas datu apstrādātājam, piemēram, var nākties nodemonstrēt, ka datu apstrāde ir vajadzīga līguma izpildei (7. panta b) punkts) vai ka likumīgās intereses saskaņā ar 7. panta f) punktu ir pārākas. Šajā pēdējā gadījumā pēc tam, kad ir novērtēts, ka personas datu apstrādātājs atbilst 8. panta prasībām, ir jāveic 7. panta f) punktā paredzētā līdzsvarošanas pārbaude.

Tāpat jau tas, ka "datu apstrādi pieprasa profilaktiskās medicīnas, medicīniskas diagnozes, aprūpes vai ārstēšanas vai veselības aprūpes pakalpojumu pārvaldības nodrošināšanas nolūkiem" un ka šos datus apstrādā saskaņā ar dienesta noslēpuma pienākumu (kā norādīts 8. panta 3. punktā), paredz šādas sensitīvu datu apstrādes *atbrīvojumu no* 8. panta 1. punktā *norādītā aizlieguma.* Tomēr ar to nebūt nepietiek, lai arī nodrošinātu likumīgumu saskaņā ar 7. pantu, un ir vajadzīgs juridisks pamatojums, piemēram, līgums ar pacientu atbilstīgi 7. panta b) punktam, juridiskas saistības saskaņā ar 7. panta c) punktu, sabiedrības interesēs realizējama uzdevuma izpilde saskaņā ar 7. panta e) punktu vai novērtējums atbilstīgi 7. panta f) punktam.

Kopumā darba grupa uzskata, ka katrā konkrētā gadījumā jāveic analīze par to, vai 8. pants pats par sevi nodrošina stingrākus un pietiekamus nosacījumus[32], vai arī gan 8., gan 7. pants ir jāpiemēro kumulatīvi, lai nodrošinātu datu subjektu pilnīgu aizsardzību. Pārbaudes rezultāti nekādā gadījumā nedrīkst paredzēt zemāku aizsardzības līmeni īpašajām datu kategorijām[33].

Tas arī nozīmē, ka personas datu apstrādātājs, kas apstrādā īpašās datu kategorijas, nekādā gadījumā nedrīkst atsaukties *vienīgi* uz 7. pantā minētu juridisku pamatojumu, lai leģitimizētu datu apstrādes darbību. Attiecīgā gadījumā 7. pants nebūs *pārāks*, taču tas vienmēr būs jāpiemēro *kumulatīvi* kopā ar 8. pantu, lai nodrošinātu visu attiecīgo drošības un citu pasākumu ievērošanu. Tas būs vēl jo būtiskāk gadījumā, ja dalībvalstis nolems saskaņā ar 8. panta 4. punkta nosacījumiem 8. pantam pievienot papildu izņēmumus.

---

[31] Turklāt 8. panta 2. punkta e) apakšpunktu nevajadzētu interpretēt *a contrario*, pieņemot, ka gadījumā, ja dati, kurus datu subjekts ir darījis zināmus atklātībai, nav sensitīvi, tos var apstrādāt bez papildu nosacījumiem. Publiski pieejami dati joprojām ir personas dati, kuriem piemērojamas datu aizsardzības prasības, tostarp 7. panta ievērošana, neatkarīgi no tā, vai tie ir vai nav sensitīvi dati.

[32] Sk. analīzi, kas veikta darba grupas *WADA* atzinuma 3. punkta 3. apakšpunktā, kurā ņemts vērā gan direktīvas 7., gan 8. pants: Otrais atzinums 4/2009 par Pasaules Antidopinga aģentūras (*WADA*) Starptautisko Privātuma un personas datu aizsardzības standartu, ar to saistītajiem *WADA* kodeksa noteikumiem un citiem privātuma jautājumiem kontekstā ar *WADA* un (valsts) antidopinga organizāciju cīņu pret dopingu sportā, pieņemts 6.4.2009. (WP162).

[33] Pats par sevi saprotams, ka arī attiecībā uz 8. panta piemērošanu jānodrošina citu direktīvas noteikumu (tai skaitā 6. panta) ievērošana.

III.2. Direktīvas 7. panta a)–e) punkts

Pirms III.3. sadaļā pievērsīsimies 7. panta f) punktam, šajā III.2. sadaļā ir sniegts īss pārskats par juridiskajiem pamatojumiem, kas uzskaitīti direktīvas 7. panta a)–e) punktā. Šajā analīzē būs arī uzsvērti daži šo juridisko pamatojumu biežāk izplatītie apvienošanas veidi, piemēram, atkarībā no konkrētā konteksta un attiecīgās lietas faktiem ietverot "līgumus", "juridiskās saistības" un "likumīgās intereses".

III.2.1. Piekrišana

Piekrišana kā juridisks pamatojums ir analizēta darba grupas Atzinumā 15/2011 par jēdziena "piekrišana" definīciju. Šā atzinuma galvenais secinājums ir tāds, ka piekrišana ir viens no vairākiem personas datu apstrādes juridiskajiem pamatojumiem, nevis galvenais pamatojums. Tam ir liela nozīme, taču tas neizslēdz iespēju, ka atkarībā no konteksta citi juridiskie pamatojumi var būt piemērotāki vai nu no personas datu apstrādātāja, vai arī datu subjekta perspektīvas. Ja piekrišana tiek izmantota pareizi, tas ir instruments, kas ļauj datu subjektam kontrolēt viņa datu apstrādi. Ja to izmanto nepareizi, datu subjekta kontrole kļūst iluzora, un piekrišana ir nepiemērots apstrādes pamatojums.

Viens no darba grupas ieteikumiem bija precizēt jēdziena "nepārprotama piekrišana" nozīmi: "Skaidrojumā būtu jācenšas uzsvērt, ka nepārprotamu piekrišanu var iegūt, izmantojot metodes, kas neļauj šaubīties par datu subjekta nodomu dot piekrišanu. Vienlaikus būtu jāpaskaidro, ka piekrišana, kas iegūta, izmantojot noklusējuma opcijas, kuras datu subjektam jāmaina, ja viņš vēlas liegt datu apstrādi (piekrišana, pamatojoties uz klusēšanu), nav nepārprotama piekrišana. Jo īpaši tas attiecas uz tiešsaistes vidi."[34] Tajā arī personas datu apstrādātājiem tika noteikts ieviest metodes, lai parādītu, ka ir iegūta piekrišana (saskaņā ar vispārējo pārskatatbildības principu), un tika prasīts likumdevējiem iekļaut skaidri formulētu prasību attiecībā uz piekrišanas pamatā esošās informācijas kvalitāti un pieejamību.

III.2.2. Līgums

Direktīvas 7. panta b) punktā ir norādīts juridiskais pamatojums gadījumos, kad "apstrāde vajadzīga līguma, kurā datu subjekts ir līgumslēdzēja puse, izpildei vai pasākumu veikšanai pēc datu subjekta pieprasījuma pirms līguma noslēgšanas." Tas aptver divus dažādus scenārijus.

i) Pirmkārt, šis noteikums aptver situācijas, kad apstrāde jāveic līguma, kurā datu subjekts ir līgumslēdzēja puse, izpildei. Tas var ietvert, piemēram, datu subjekta adreses apstrādi, lai varētu piegādāt tiešsaistē nopirktas preces, vai kredītkartes informācijas apstrādi, lai varētu veikt maksājumu. Nodarbinātības kontekstā saskaņā ar šo pamatojumu var veikt, piemēram, algu informācijas un banku kontu datu apstrādi, lai varētu izmaksāt algas.

   Šis noteikums ir jāinterpretē stingri, un tas neattiecas uz gadījumiem, kad apstrāde nav patiešām *vajadzīga*, lai izpildītu līgumu, bet gan to datu subjektam vienpusēji noteicis

[34] Sk. darba grupas Atzinuma 15/2011 par jēdziena "piekrišana" definīciju 37. lpp.

personas datu apstrādātājs. Turklāt arī tas, ka uz daļu datu apstrādes attiecas līgums, vēl nenozīmē, ka šāda apstrāde ir vajadzīga tā izpildei. Piemēram, 7. panta b) punkts nav piemērots juridiskais pamatojums, lai veidotu lietotāja gaumju un dzīvesstila izvēles profilu, izmantojot tīmekļa vietnes apmeklējumu vēsturi un informāciju par nopirktajām precēm. Tas ir tādēļ, ka ar personas datu apstrādātāju ir noslēgts līgums nevis par profilēšanu, bet gan, piemēram, par konkrētu preču piegādi vai pakalpojumu sniegšanu. Pat ja šādas apstrādes darbības ir konkrēti norādītas līguma mazās drukas tekstā, tas vēl nenozīmē, ka datu apstrāde ir "vajadzīga" līguma izpildei.

Šajā gadījumā ir nepārprotama saikne starp vajadzības novērtējumu un nolūka ierobežojuma principa ievērošanu. Ir svarīgi noteikt līguma konkrēto *pamatojumu*, t. i., tā būtību un pamatmērķi, jo tieši attiecībā pret šiem aspektiem tiks pārbaudīts, vai tā izpildei ir nepieciešama datu apstrāde.

Iespējams, dažās robežsituācijās to var apstrīdēt vai var būt vajadzīgi konkrētāki faktu vākšanas pasākumi, lai noteiktu, vai līguma izpildei ir nepieciešama datu apstrāde. Piemēram, tādas visa uzņēmuma mēroga iekšējo darbinieku kontaktinformācijas datubāzes izveidošana, kurā ir iekļauti visu darbinieku vārdi un uzvārdi, faktiskās adreses, tālruņa numuri un e-pasta adreses, lai darbinieki varētu sazināties ar saviem kolēģiem, var būt uzskatāma par nepieciešamu līguma izpildei saskaņā ar 7. panta b) punktu, taču tas var arī būt likumīgi saskaņā ar 7. panta f) punktu, ja tiek parādītas pārākas personas datu apstrādātāja intereses un tiek veikti visi atbilstīgie pasākumi, tai skaitā, piemēram, veikta pienācīga apspriešanās ar darba ņēmēju pārstāvjiem.

Citi gadījumi, piemēram, darba ņēmēju interneta, e-pasta vai tālruņa lietojuma elektroniska uzraudzība vai arī darbinieku videonovērošana, viennozīmīgāk ir tāda datu apstrāde, kas pārsniedz darba līguma izpildei nepieciešamos pasākumus, lai gan arī šajā gadījumā tas var būt atkarīgs no nodarbinātības veida. Krāpšanas novēršana (kas cita starpā var ietvert klientu uzraudzību un profilēšanu) ir vēl viena tipiska joma, attiecībā uz kuru var uzskatīt, ka tā pārsniedz pasākumus, kas nepieciešami līguma izpildei. Tādā gadījumā šāda apstrāde tomēr varētu būt likumīga atbilstīgi citam 7. pantā minētajam pamatojumam, piemēram, attiecīgā gadījumā — piekrišanai, juridiskām saistībām vai personas datu apstrādātāja likumīgām interesēm (7. panta a), c) vai f) punkts)[35]. Pēdējā gadījumā apstrādei būtu jāpiemēro papildu drošības un citi pasākumi, lai pienācīgi aizsargātu datu subjektu intereses vai tiesības un brīvības.

Direktīvas 7. panta b) punkts ir piemērojams vienīgi darbībām, kas nepieciešamas līguma *izpildei*. Tas neattiecas uz visiem citiem pasākumiem, kas radušies līguma neievērošanas vai cita veida līguma neatbilstīgas izpildes rezultātā. Ja apstrāde attiecas uz līguma parastu izpildi, tai varētu būt piemērojams 7. panta b) punkts. Ja līgumsaistības netiek pildītas un radies konflikts, iespējams, datu apstrāde jāveic

[35] Cits vairāku juridisko pamatojumu piemērs ir atrodams darba grupas Atzinumā 15/2011 par jēdziena "piekrišana" definīciju (minēts 2. zemsvītras piezīmē). Lai iegādātos automobili, personas datu apstrādātājs var būt tiesīgs apstrādāt personas datus saskaņā ar dažādiem nolūkiem un dažādiem pamatojumiem:
- Dati, kas vajadzīgi automobiļa iegādei: 7. panta b) punkts.
- Lai apstrādātu automobiļa dokumentus: 7. panta c) punkts.
- Klientu pārvaldības pakalpojumiem (piemēram, lai automobiļa apkopi varētu veikt dažādos saistītos uzņēmumos Eiropas Savienībā): 7. panta f) punkts.
- Lai nosūtītu datus trešām personām komerciālai izmantošanai: 7. panta a) punkts.

citādi. Datu subjekta pamatinformācijas (piemēram, vārda un uzvārda, adreses, atsauces uz nenokārtotām līgumsaistībām, lai nosūtītu oficiālus atgādinājumus) apstrāde joprojām ir iekļaujama tādas datu apstrādes kategorijā, kas nepieciešama līguma izpildei. Saistībā ar izvērstāku datu apstrādi, kas var arī ietvert trešās personas (piemēram, parāda piedziņu vai tiesvedības sākšanu pret klientu, kurš nav samaksājis par pakalpojumu), var argumentēt, ka šāda apstrāde vairs netiek veikta saskaņā ar "parastu" līguma izpildi un tāpēc neatbilst 7. panta b) punktam. Tomēr tas apstrādi nepadara pašu par sevi nelikumīgu — personas datu apstrādātājam ir likumīgas intereses meklēt veidus, kā nodrošināt savu līgumtiesību ievērošanu. Par pamatu var izmantot citus juridiskos pamatojumus (piemēram, 7. panta f) punktu), ievērojot pienācīgus drošības un citus pasākumus, kā arī nodrošinot līdzsvarošanas pārbaudi[36].

ii) Otrkārt, 7. panta b) punkts arī attiecas uz tādu datu apstrādi, kas notiek *pirms* līguma noslēgšanas. Tas ietver pirmslīgumiskās attiecības ar nosacījumu, kas pasākumi ir veikti pēc datu subjekta pieprasījuma, nevis personas datu apstrādātāja vai trešo personu iniciatīvas. Piemēram, ja persona mazumtirgotājam pieprasa nosūtīt produkta piedāvājumu, datu apstrāde šādā nolūkā, piemēram, adreses un pieprasījuma informācijas saglabāšana noteiktu laika posmu, ir uzskatāma par atbilstīgu šim juridiskajam pamatojumam. Tāpat, ja persona no apdrošinātāja pieprasa cenu piedāvājumu savam automobilim, apdrošinātājs var apstrādāt attiecīgos datus, piemēram, automobiļa modeli un ražošanas gadu, kā arī citu attiecīgu un samērīgu informāciju, lai sagatavotu cenu piedāvājumu.

Tomēr detalizētas iepriekšēju datu pārbaudes (piemēram, medicīnisko pārbaužu datu apstrāde, pirms apdrošināšanas sabiedrība izsniedz veselības vai dzīvības apdrošināšanas polisi pieteikuma iesniedzējam) nav uzskatāmas par nepieciešamiem pasākumiem, kas veikti pēc datu subjekta pieprasījuma. Arī kredītvēstures pārbaudes pirms aizdevuma piešķiršanas netiek veiktas pēc datu subjekta *pieprasījuma* saskaņā ar 7. panta b) punktu, tas drīzāk notiek saskaņā ar 7. panta f) punktu vai 7. panta c) punktu, ievērojot banku juridiskās saistības skatīt reģistrēto parādnieku oficiālo sarakstu.

Arī tiešā tirgvedība pēc mazumtirgotāja / personas datu apstrādātāja iniciatīvas nav pieļaujama saskaņā ar šo pamatojumu. Dažos gadījumos kā piemērotu juridisko pamatojumu var izmantot 7. panta f) punktu, nevis 7. panta b) punktu, ievērojot pienācīgus drošības un citus pasākumus, kā arī nodrošinot līdzsvarošanas pārbaudi. Citos gadījumos, tostarp tādos, kas ietver plašus profilēšanas, datu koplietošanas, tiešsaistes tiešās tirgvedības vai uz uzvedību balstītas reklāmas pasākumus, jāievēro piekrišana atbilstīgi 7. panta a) punktam, kā izklāstīts turpmākajā analīzē[37].

[36] Attiecībā uz datu īpašajām kategorijām, iespējams, jāņem vērā arī 8. panta 2. punkta e) apakšpunkts — "vajadzīga juridisku prasību celšanai, realizācijai vai aizstāvībai".

[37] Sk. III.3.6. sadaļas b) punkta iedaļu "Ilustrācija: pieejas attīstība attiecībā uz tiešo tirgvedību", 45.–46. lpp.

III.2.3. Juridiskas saistības

Direktīvas 7. panta c) punkts nodrošina juridisku pamatojumu apstākļos, kad "apstrāde vajadzīga, lai izpildītu uz personas datu apstrādātāju attiecināmas juridiskas saistības". Piemēram, tas var būt gadījumā, kad darba devējiem ir jāziņo savu darbinieku algas dati sociālā nodrošinājuma vai nodokļu iestādēm, vai gadījumā, kad finanšu iestāžu pienākums ir ziņot par noteiktām aizdomīgām transakcijām kompetentajām iestādēm saskaņā ar noteikumiem par nelikumīgi iegūtu līdzekļu legalizēšanas novēršanu. Tās var būt arī saistības, kas jāievēro valsts iestādei, jo nekas neierobežo 7. panta c) punkta piemērošanu privātajam vai publiskajam sektoram. Piemēram, tas varētu attiekties uz pašvaldības veiktu datu vākšanu, lai apstrādātu informāciju par naudas sodiem par automobiļu novietošanu neatļautās vietās.

Direktīvas 7. panta c) punktā atrodamas līdzības ar 7. panta e) punktu, jo uzdevums sabiedrības interesēs bieži balstās uz tiesību aktu noteikumiem vai no tiem izriet. Tomēr 7. panta c) punkta piemērošanas joma ir stingri ierobežota.

Lai varētu piemērot 7. panta c) punktu, šīm saistībām ir jābūt noteiktām ar tiesību aktu (nevis, piemēram, ar līgumsaistībām). Lai saistības būtu spēkā un tās būtu saistošas, tiesību aktam ir jāatbilst visiem attiecīgajiem nosacījumiem, un tam arī jāatbilst datu aizsardzības tiesību aktam, tostarp vajadzīguma, samērīguma[38] un nolūka ierobežojuma prasībām.

Svarīgi arī uzsvērt, ka 7. panta c) punkts attiecas uz Eiropas Savienības vai dalībvalsts tiesību aktiem. Šis pamatojums neietver saistības, kas noteiktas trešo valstu tiesību aktos (piemēram, saistības izveidot sistēmas ziņošanai par pārkāpumiem saskaņā ar *Sarbanes-Oxley* 2002. gada likumu ASV). Lai trešo valstu juridiskās saistības būtu spēkā, tām jābūt oficiāli atzītām un integrētām attiecīgās dalībvalsts tiesību sistēmā, piemēram, starptautiska nolīguma veidā[39]. Tomēr vajadzība ievērot ārvalstu saistības var būt personas datu apstrādātāja likumīgas intereses, taču tikai tad, ja tiek veikta līdzsvarošanas pārbaude atbilstīgi 7. panta f) punktam un ja ir ieviesti pienācīgi drošības pasākumi, piemēram, kompetentās datu aizsardzības iestādes apstiprinātie pasākumi.

Personas datu apstrādātājam nedrīkst būt izvēles brīvība attiecībā uz saistību ievērošanu. Tādējādi 7. panta c) punkts neattiecas uz brīvprātīgām vienpusējām attiecībām un publiskām un privātām partnerībām, kurās datus apstrādā vairāk, nekā noteikts tiesību aktā. Piemēram, ja bez nepārprotamām un konkrētām juridiskām saistībām interneta pakalpojumu sniedzējs nolemj pārraudzīt lietotājus, lai apkarotu nelikumīgas lejupielādes, 7. panta c) punkts nav piemērots juridiskais pamatojums šādam nolūkam.

Turklāt pašām juridiskajām saistībām jābūt pietiekami skaidrām attiecībā uz personas datu apstrādi, ko tās paredz. Tādējādi 7. panta c) punkts ir piemērojams, pamatojoties uz tiesību normām, kurās skaidri norādīts apstrādes veids un objekts. Personas datu apstrādātājam nedrīkst būt nesamērīga rīcības brīvība attiecībā uz tā juridisko saistību ievērošanu.

---

[38] Sk. arī darba grupas Atzinumu 01/2014 par vajadzīguma un samērīguma jēdziena un datu aizsardzības piemērošanu tiesībaizsardzības nozarē, kas pieņemts 27.2.2014. (WP 211).

[39] Šajā jautājumā skatiet 4.2.2. apakšpunktu darba grupas Atzinumā 10/2006 par personas datu apstrādi, ko veic Vispasaules Starpbanku finanšu telekomunikāciju sabiedrība (*SWIFT*), kas pieņemts 20.11.2006. (WP128), un darba grupas Atzinumu 1/2006 par ES datu aizsardzības noteikumu piemērošanu iekšējām sistēmām ziņošanai par pārkāpumiem grāmatvedības, iekšējās grāmatvedības kontroles, revīzijas, cīņas pret uzpirkšanu, banku un finanšu noziegumu jomās, kas pieņemts 1.2.2006. (WP 117).

Tiesību aktos dažkārt var būt noteikts tikai vispārējs mērķis, bet konkrētākas saistības ir noteiktas citā līmenī, piemēram, vai nu sekundāros tiesību aktos, vai ar valsts iestādes saistošu lēmumu konkrētā gadījumā. Tas var arī radīt juridiskas saistības saskaņā ar 7. panta c) punktu, ja apstrādes veids un objekts ir pienācīgi definēti un tiem piemērojams pienācīgs juridiskais pamats.

Tomēr atšķirīgs ir gadījums, kad regulējošā iestāde sniedz vienīgi vispārīgas politikas pamatnostādnes un nosacījumus, saskaņā ar kuriem tā varētu izmantot savas ieviešanas pilnvaras (piemēram, regulējoši norādījumi finanšu iestādēm par noteiktiem uzticamības pārbaužu standartiem). Šādos gadījumos apstrādes pasākumi jānovērtē saskaņā ar 7. panta f) punktu, un tos var uzskatīt par likumīgiem vienīgi pēc tam, kad veikta papildu līdzsvarošanas pārbaude[40].

Vispārīgi jāatzīmē, ka daži apstrādes pasākumi var šķist tuvi 7. panta c) punktam vai 7. panta b) punktam, lai gan tie pilnībā neatbilst šo pamatojumu piemērošanas kritērijiem. Tas gan nenozīmē, ka šāda apstrāde ir nelikumīga — dažkārt tā var būt likumīga, taču drīzāk saskaņā ar 7. panta f) punktu un ar nosacījumu, ka tiek veikta papildu līdzsvarošanas pārbaude.

III.2.4. Būtiskas intereses

Direktīvas 7. panta d) punktā ir noteikts juridiskais pamatojums situācijās, kad "apstrāde vajadzīga, lai aizsargātu datu subjekta būtiskas intereses". Šis formulējums atšķiras no 8. panta 2. punkta c) apakšpunkta formulējuma, kas ir konkrētāks un attiecas uz situācijām, kad "apstrāde vajadzīga, lai aizsargātu datu subjekta vai citas personas būtiskas intereses, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu".

Tomēr šķiet, ka abos noteikumos paredzēts, ka šim juridiskajam pamatojumam ir ierobežota piemērošanas joma. Pirmkārt, šķiet, ka pati vārdkopa "būtiskas intereses" ierobežo šī pamatojuma piemērošanu, to attiecinot vienīgi uz jautājumiem par dzīvību un nāvi, vai vismaz draudiem, kas rada traumu vai cita kaitējuma risku datu subjekta veselībai (vai 8. panta 2. punkta c) apakšpunkta gadījumā — arī citas personas veselībai).

Direktīvas 31. apsvērumā ir apstiprināts, ka šī juridiskā pamatojuma mērķis ir "aizsargāt kādu datu subjekta dzīves sfēru, kas tam ir būtiski svarīga". Tomēr direktīvā precīzi netiek norādīts, vai draudiem jābūt tūlītējiem. Tas rada problēmas attiecībā uz datu vākšanas apjomu, piemēram, kā preventīvu pasākumu vai plašāka mēroga pasākumu, piemēram, avioreisu pasažieru datu vākšana, ja konstatēts epidēmiskas slimības risks vai drošības pārkāpumi.

Darba grupa uzskata, ka šis noteikums ir jāinterpretē ierobežojoši un atbilstīgi 8. panta būtībai. Kaut arī 7. panta d) punktā šā pamatojuma izmantošana nav konkrēti ierobežota attiecībā uz situācijām, kad kā juridisko pamatojumu nevar izmantot piekrišanu 8. panta 2. punkta c) apakšpunktā minēto iemeslu dēļ, pamatoti jāpieņem, ka gadījumos, kad pastāv iespēja un vajadzība pieprasīt derīgu piekrišanu, šādu piekrišanu būtu tiešām jāmēģina iegūt, kad vien tas ir iespējams. Tas arī ierobežotu šā noteikuma piemērošanu, veicot konkrētā

[40] Tomēr regulējošās iestādes norādījumiem var būt nozīme, novērtējot personas datu apstrādātāja likumīgās intereses (sk. III.3.4. sadaļas a) punktu, jo īpaši 36. lpp.).

gadījuma analīzi, un to nevar parasti izmantot, lai leģitimizētu jebkādu personas datu masveida vākšanu vai apstrādi. Gadījumos, kad tas būtu vajadzīgs, 7. panta c) vai e) punkts būtu piemērotāks apstrādes pamatojums.

III.2.5. Uzdevums sabiedrības interesēs

Direktīvas 7. panta e) punktu var izmantot kā juridisku pamatojumu gadījumos, kad "apstrāde vajadzīga sabiedrības interesēs realizējama uzdevuma izpildei vai personas datu apstrādātājam vai trešajai personai, kurai dati tiek atklāti, piešķirto oficiālo pilnvaru realizācijai".

Svarīgi arī atzīmēt, ka tāpat kā 7. panta c) punkts arī 7. panta e) punkts attiecas uz Eiropas Savienības vai dalībvalsts sabiedrības interesēm. Tāpat ar terminu "oficiālās pilnvaras" apzīmē Eiropas Savienības vai dalībvalsts piešķirtas pilnvaras. Citiem vārdiem sakot, uzdevumi, kas tiek veikti trešās valsts sabiedrības interesēs vai īstenojot piešķirtas oficiālās pilnvaras, kas piešķirtas saskaņā ar ārvalstu tiesību aktiem, neietilpst šā noteikuma piemērošanas jomā[41].

Direktīvas 7. panta e) punkts attiecas uz divām situācijām un ir piemērojams gan publiskajā, gan privātajā sektorā. Pirmkārt, tas attiecas uz gadījumiem, kad pašam personas datu apstrādātājam ir oficiālas pilnvaras vai tas veic sabiedrības interesēs realizējamu uzdevumu (taču tam nav jābūt arī juridiskām saistībām apstrādāt datus) un kad apstrāde jāveic, lai īstenotu šīs pilnvaras vai veiktu minēto uzdevumu. Piemēram, nodokļu iestāde var vākt un apstrādāt personas nodokļu deklarāciju, lai noteiktu un pārbaudītu maksājamo nodokļu apjomu. Tā var būt arī profesionālā apvienība, piemēram, advokātu asociācija vai medicīnas darbinieku kamera, kurai ir piešķirtas attiecīgas oficiālas pilnvaras un kura var veikt disciplinārās procedūras pret apvienības locekļiem. Cits piemērs ir vietējās pārvaldes iestādes, piemēram, pašvaldība, kurai ir uzticēts uzdevums nodrošināt bibliotēkas, skolas vai vietējā peldbaseina pakalpojumus.

Otrkārt, 7. panta e) punkts arī attiecas uz situācijām, kad personas datu apstrādātājam nav oficiālu pilnvaru, taču tam pieprasa atklāt datus trešā persona, kurai ir šādas pilnvaras. Piemēram, noziegumu izmeklēšanas jomā kompetentas publiskas iestādes darbinieks var lūgt personas datu apstrādātājam sadarboties notiekošā izmeklēšanā, nevis izdot personas datu apstrādātājam rīkojumu ar konkrētu prasību sadarboties. Turklāt 7. panta e) punkts var attiekties uz situācijām, kad personas datu apstrādātājs pēc paša iniciatīvas atklāj datus trešai personai, kurai ir šādas oficiālas pilnvaras. Piemēram, tā var notikt, kad personas datu apstrādātājs konstatē, ka ir noticis noziedzīgs nodarījums, un sniedz šo informāciju kompetentajām tiesībaizsardzības iestādēm pēc paša iniciatīvas.

Atšķirībā no 7. panta c) punkta gadījumiem personas datu apstrādātājam nav noteikta prasība rīkoties saskaņā ar juridiskajām saistībām. Turpinot iepriekšējo piemēru — personas datu apstrādātājam, kas nejauši konstatē, ka veikta zādzība vai krāpšana, var nebūt juridisku saistību par to ziņot policijai, taču attiecīgos gadījumos tas to var darīt brīvprātīgi saskaņā ar 7. panta e) punktu.

[41] Līdzīga interpretācija 26. panta 1. punkta d) apakšpunktā minētajam jēdzienam "svarīgas sabiedrības intereses" ir atrodama 2.4. sadaļā darba grupas darba dokumentā par 1995. gada 24. oktobra Direktīvas 95/46/EK 26. panta 1. punkta vienotu interpretāciju, kas pieņemts 2005. gada 25. novembrī (WP114).

Tomēr apstrādei jābūt "vajadzīgai sabiedrības interesēs realizējama uzdevuma izpildei". Personas datu apstrādātājam vai trešai personai, kurai apstrādātājs atklāj datus, ir arī jābūt piešķirtām oficiālām pilnvarām, un datu apstrādei jābūt vajadzīgai, lai īstenotu pilnvaras.[42] Turklāt ir būtiski uzsvērt, ka šīs oficiālās pilnvaras vai uzdevums sabiedrības interesēs parasti būs noteikts likumdošanas aktos vai citos normatīvajos noteikumos. Ja šis process paredz privātuma pārkāpšanu vai ja tas ir kā citādi nepieciešams atbilstīgi valsts tiesību aktiem, lai nodrošinātu attiecīgu fizisku personu aizsardzību, juridiskajam pamatam jābūt pietiekami konkrētam un precīzam, lai definētu pieļaujamos datu apstrādes veidus.

Šādi gadījumi kļūst arvien izplatītāki arī ārpus publiskā sektora, ņemot vērā tendenci valsts uzdevumu veikšanu ārpakalpojumu veidā nodot privātā sektora organizācijām. Piemēram, šāds modelis var būt saistībā ar datu apstrādes pasākumiem transporta un veselības nozarēs (piemēram, epidemioloģiskie pētījumi, pētniecība). Uz šo pamatojumu var arī atsaukties tiesībaizsardzības kontekstā, kā jau norādīts iepriekšējā piemērā. Tomēr, lai noteiktu apmēru, kādā privātam uzņēmuma var būt atļauts sadarboties ar tiesībaizsardzības iestādēm, piemēram, cīņā pret krāpšanu vai nelikumīgu saturu internetā, ir jāveic analīze ne vien saskaņā ar 7. pantu, bet arī 6. pantu, ņemot vērā nolūka ierobežojuma, likumīguma un godīguma prasības[43].

Direktīvas 7. panta e) punktam ir plašas piemērošanas potenciāls, tādēļ katrā konkrētajā gadījumā ir stingri jāinterpretē un skaidri jāidentificē attiecīgās sabiedrības intereses un oficiālās pilnvaras, kas attaisno datu apstrādi. Šīs plašās piemērošanas jomas dēļ arī saprotams, kāpēc tāpat kā attiecībā uz 7. panta f) punktu 14. pantā ir paredzētas iebildumu tiesības, ja datu apstrādes pamatā ir 7. panta e) punkts[44]. Tādējādi līdzīgi papildu drošības un citi pasākumi var tikt izmantoti abos gadījumos[45].

Šajā ziņā 7. panta e) punktā atrodamas līdzības ar 7. panta f) punktu, un dažos apstākļos (īpaši attiecībā uz valsts iestādēm) 7. panta e) punkts var aizstāt 7. panta f) punktu.

Novērtējot šo noteikumu piemērošanas jomu attiecībā uz publiskā sektora struktūrām (jo īpaši, ņemot vērā ierosinātās datu aizsardzības tiesiskā regulējuma izmaiņas), vērts atzīmēt, ka Regulas 45/2001[46] pašreizējā tekstā, kurā ir iekļauti noteikumi par datu aizsardzību, kas piemērojami Eiropas Savienības iestādēm un struktūrām, nav tādu noteikumu, kas būtu pielīdzināmi 7. panta f) punktam.

Tomēr šīs regulas 27. apsvērumā ir norādīts, ka "personas datu apstrāde, pildot uzdevumus, ko Kopienas iestādes un struktūras veic *sabiedrības interesēs*, ietver to personas datu apstrādi,

---

[42] Citiem vārdiem sakot, šajos gadījumos uzdevumu sabiedriskais nozīmīgums un attiecīgā atbildība paliks spēkā, pat ja uzdevumu veiks citas organizācijas, tostarp privātas.

[43] Šajā saistībā sk. darba grupas atzinumu par *SWIFT* (iepriekš minēts 39. zemsvītras piezīmē), darba grupas Atzinumu 4/2003 par ASV nodrošināto aizsardzības līmeni pasažieru datu pārsūtīšanai, kas pieņemts 13.6.2003. (WP 78), kā arī Darba dokumentu par datu aizsardzības jautājumiem saistībā ar intelektuālā īpašuma tiesībām, kas pieņemts 18.1.2005. (WP 104).

[44] Kā norādīts iepriekš, attiecībā uz datu apstrādi saskaņā ar 7. panta e) punktu šī iebildumu paušanas iespēja dažās dalībvalstīs nepastāv (piemēram, Zviedrijā).

[45] Kā izklāstīts turpmāk, *LIBE* komitejas ziņojuma projektā gadījumos, kad piemērojams 7. panta f) punkts, tika ierosināti papildu drošības pasākumi (jo īpaši — uzlabota pārredzamība).

[46] Eiropas Parlamenta un Padomes 2000. gada 18. decembra Regula (EK) Nr. 45/2001 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Kopienas iestādēs un struktūrās un par šādu datu brīvu apriti. (OV L 8, 12.1.2001., 1. lpp.).

kas vajadzīgi šo iestāžu un struktūru pārvaldībai un funkcionēšanai". Tādējādi šis noteikums pieļauj datu apstrādi saskaņā ar plaši interpretēto pamatojumu "uzdevums sabiedrības interesēs" ļoti dažādos gadījumos, kuriem citādi varētu piemērot 7. panta f) punktam līdzīgu noteikumu. Telpu videonovērošana drošības nolūkā, e-pasta datplūsmas elektroniska uzraudzība vai darbinieku novērtēšana ir tikai daži piemēri, kuriem var piemērot šo plaši interpretējamo noteikumu "sabiedrības interesēs realizējami uzdevumi".

Raugoties nākotnē, svarīgi arī ņemt vērā, ka ierosinātās regulas 6. panta 1. punkta f) apakšpunktā konkrēti noteikts, ka likumīgo interešu pamatojumu "nepiemēro apstrādei, ko veic valsts iestāde, pildot savus uzdevumus". Ja šis noteikums tiks ieviests un tā interpretācija būs plaša, lai valsts iestādes kā juridisku pamatojumu vispār nevarētu izmantot likumīgas intereses, tad 7. panta e) punktā minētie pamatojumi "sabiedrības intereses" un "oficiālas pilnvaras" būs jāinterpretē tā, lai valsts iestādēm būtu vismaz daļēja rīcības brīvība, lai vismaz nodrošinātu to pareizu pārvaldību un funkcionēšanu saskaņā ar Regulas 45/2001 pašreizējo interpretāciju.

Minētā ierosinātās regulas 6. panta 1. punkta f) apakšpunkta pēdējo teikumu var arī interpretēt tā, lai valsts iestādēm netiktu pilnībā liegts kā juridisko pamatojumu izmantot likumīgas intereses. Šajā gadījumā ierosinātā 6. panta 1. punkta f) apakšpunkta teksts "apstrādei, ko veic valsts iestāde, pildot savus uzdevumus" jāinterpretē šauri. Šāda šaura interpretācija nozīmētu to, ka apstrāde šo publisko iestāžu pareizai pārvaldībai un funkcionēšanai neatbilst definīcijas "apstrādei, ko veic valsts iestāde, pildot savus uzdevumus" piemērošanas jomai. Rezultātā apstrāde šo valsts iestāžu pareizas pārvaldības un funkcionēšanas vajadzībām joprojām būtu iespējama saskaņā ar likumīgo interešu pamatojumu.

III.3. Direktīvas 7. panta f) punkts — likumīgas intereses

Direktīvas 7. panta f) punktā[47] aicināts veikt līdzsvarošanas pārbaudi — personas datu apstrādātāja (vai trešo personu) likumīgās intereses ir jāsamēro ar datu subjekta interesēm vai pamattiesībām un brīvībām. Šīs līdzsvarošanas pārbaudes rezultāti lielā mērā nosaka, vai uz 7. panta f) punktu var paļauties kā uz datu apstrādes juridisko pamatojumu.

Jau šajā brīdī ir vērts pieminēt, ka tā nav vienkārša līdzsvarošanas pārbaude, ko veidotu tikai divu skaitliski viegli izsakāmu un salīdzināmu lielumu savstarpēja salīdzināšana. Kā aprakstīts turpmāk, lai veiktu līdzsvarošanas pārbaudi, drīzāk būs jāsagatavo sarežģīts novērtējums, ņemot vērā vairākus faktorus. Lai novērtējumu varētu vieglāk strukturēt un vienkāršot, šajā atzinumā šis process ir iedalīts vairākos posmos, lai nodrošinātu, ka līdzsvarošanas pārbaudi var veikt efektīvi.

Atzinuma III.3.1. sadaļā vispirms ir skatīta viena līdzsvara puse — tas, kas veido "personas datu apstrādātāja vai trešo personu, kurām dati tiek atklāti, likumīgas intereses". III.3.2. sadaļā ir analizēta līdzsvara otra puse — tas, kas veido "datu subjekta intereses vai pamattiesības un brīvības, kurām nepieciešama aizsardzība saskaņā ar 1. panta 1. punktu".

Atzinuma III.3.3. un III.3.4. sadaļā ir sniegti norādījumi par to, kā veikt līdzsvarošanas pārbaudi. III.3.3. sadaļā ir sniegts vispārējs ievads, aprakstot trīs dažādus scenārijus. Pēc šī

[47] 7. panta f) punkta pilns teksts norādīts iepriekš 4. lappusē.

ievada III.3.4. sadaļā ir izklāstīti svarīgākie apsvērumi, kas jāņem vērā, veicot līdzsvarošanas pārbaudi, tostarp personas datu apstrādātāja veiktie drošības un citi pasākumi.

Visbeidzot, III.3.5. un III.3.6. sadaļā arī apskatīti daži konkrēti mehānismi, piemēram, pārskatatbildība, pārredzamība un tiesības iebilst, ar kuru palīdzību var labāk nodrošināt un uzlabot atbilstīgu dažādu iesaistīto interešu līdzsvaru.

III.3.1. Personas datu apstrādātāja (vai trešo personu) likumīgās intereses

Jēdziens "*intereses*"

Jēdziens "intereses" ir cieši saistīts ar direktīvas 6. pantā minēto jēdzienu "nolūks", taču vienlaikus atšķiras no tā. Datu aizsardzības jomā "nolūks" ir konkrēts datu apstrādes iemesls — datu apstrādes mērķis vai nodoms. Savukārt "intereses" ir personas datu apstrādātāja plašāka ieinteresētība apstrādē vai labums, ko personas datu apstrādātājs (vai, iespējams, sabiedrība) gūst no datu apstrādes.

Piemēram, uzņēmums var būt *ieinteresēts* savu atomelektrostacijas darbinieku veselības aizsardzībā un drošībā. Šajā saistībā uzņēmumam var būt *nolūks* īstenot noteiktas piekļuves kontroles procedūras, kas attaisno noteiktu personas datu apstrādi, lai nodrošinātu darbinieku veselības aizsardzību un drošību.

Lai varētu veikt līdzsvarošanas pārbaudi attiecībā pret datu subjekta interesēm un pamattiesībām, interesēm ir jābūt pietiekami skaidri definētām. Turklāt attiecīgajām interesēm jāattiecas uz pašu personas datu apstrādātāju. Tām jābūt reālām un pašreizējām interesēm, kas atbilst pašreizējai darbībai vai labumam, kas gaidāms drīzā nākotnē. Citiem vārdiem sakot, pārāk neskaidras vai spekulatīvas intereses nederēs.

Intereses var būt dažāda veida. Dažas intereses var būt nenoraidāmas un labvēlīgas sabiedrībai kopumā, piemēram, preses intereses publicēt informāciju par korupciju valdībā vai intereses veikt zinātniskus pētījumus (ievērojot atbilstīgus drošības pasākumus). Citas intereses var būt mazāk būtiskas sabiedrībai kopumā vai jebkurā gadījumā — to īstenošanas ietekme sabiedrībā var būt neviennozīmīga vai pretrunīga. Piemēram, tas var attiekties uz uzņēmuma ekonomiskām interesēm uzzināt pēc iespējas vairāk par tā potenciālajiem klientiem, lai tas varētu veidot mērķtiecīgāku reklāmu par saviem produktiem vai pakalpojumiem.

Kas intereses padara par "*likumīgām*" *vai* "*nelikumīgām*"*?*

Šā jautājuma mērķis ir noteikt likumīgu interešu jēdziena robežas. Ja personas datu apstrādātāja intereses ir nelikumīgas, līdzsvarošanas pārbaude nebūs piemērojama, jo nebūs sasniegta 7. panta f) punkta piemērošanas sākotnējā robeža.

Darba grupa uzskata, ka likumīgas intereses var būt ļoti dažādas — gan triviālas, gan ļoti pārliecinošas, gan nepārprotamas, gan pretrunīgākas. Tikai otrajā posmā, kad šīs intereses tiek samērotas ar datu subjektu interesēm un pamattiesībām, ir jāizmanto ierobežojošāka pieeja un jāveic pamatīgāka analīze.

Turpmāk sniegts papildināms saraksts, kurā uzskaitīti biežāk izplatītie konteksti, kādos var rasties jautājums par likumīgām interesēm 7. panta f) punkta izpratnē. Tas šeit ir izklāstīts

neatkarīgi no tā, vai pēc līdzsvara samēra noteikšanas personas datu apstrādātāja intereses galu galā būs pārākas nekā datu subjektu intereses un tiesības.

- Vārda vai informācijas brīvības tiesības, tostarp plašsaziņas līdzekļos un mākslā;
- tradicionālā tiešā tirgvedība un citi tirdzniecības vai reklāmas veidi;
- nevēlami nekomerciāli paziņojumi, tai skaitā saistībā ar politiskajām kampaņām vai līdzekļu vākšanu labdarībai;
- juridisku prasību piemērošana, tostarp parādu piedziņa, izmantojot ārpustiesas procedūras;
- krāpšanas, pakalpojumu ļaunprātīgas izmantošanas vai nelikumīgi iegūtu līdzekļu legalizēšanas novēršana;
- darbinieku uzraudzība drošības vai pārvaldības nolūkos;
- sistēmas ziņošanai par pārkāpumiem;
- fiziskā drošība, IT un tīkla drošība;
- apstrāde vēsturiskos, zinātniskos vai statistiskos nolūkos;
- apstrāde pētniecības nolūkos (tai skaitā tirgvedības pētniecība).

Attiecīgi intereses var uzskatīt par likumīgām, kamēr personas datu apstrādātājs var īstenot savas intereses tādā veidā, kas atbilst datu aizsardzības un citiem tiesību aktiem. Citiem vārdiem sakot, likumīgām interesēm jābūt "pieņemamām saskaņā ar tiesību aktiem"[48].

Lai "likumīgas intereses" varētu ņemt vērā saskaņā ar 7. panta f) punktu, tām jābūt: - likumīgām (t. i., saskaņā ar piemērojamajiem ES un valstu tiesību aktiem); - pietiekami skaidri definētām, lai varētu veikt līdzsvarošanas pārbaudi attiecībā pret datu subjekta interesēm un pamattiesībām (t. i., pietiekami konkrētām); - reālām un pašreizējām interesēm (t. i., tās nedrīkst būt spekulatīvas).

Tas, ka personas datu apstrādātājam ir šādas likumīgas intereses, apstrādājot noteiktus datus, nenozīmē, ka tas var viennozīmīgi atsaukties uz 7. panta f) punktu kā apstrādes juridisko pamatojumu. Personas datu apstrādātāja interešu likumīgums ir tikai sākumpunkts, viens no aspektiem, kas jāanalizē saskaņā ar 7. panta f) punktu. Tas, vai var izmantot 7. panta f) punktu, būs atkarīgs no turpmākās līdzsvarošanas pārbaudes rezultātiem.

Ilustrācijai — personas datu apstrādātājiem var būt likumīgas intereses noskaidrot savu klientu izdarītās izvēles, lai varētu sniegt individualizētākus piedāvājumus un galu galā — piedāvāt produktus un pakalpojumus, kas labāk atbilst klientu vajadzībām un vēlmēm. Ņemot

[48] Darba grupas Atzinuma 3/2013 par nolūka ierobežojumu (minēts 9. zemsvītras piezīmē iepriekš) III.1.3. sadaļā izklāstītie apsvērumi par "likumīguma" būtību *mutatis mutandis* attiecināmi arī šajā gadījumā. Kā minētā atzinuma 19.–20. lappusē, jēdziens "tiesību akts" šeit tiek izmantots tā visplašākajā nozīmē. Tas ietver citus piemērojamos tiesību aktus, piemēram, tiesību aktus nodarbinātības, līgumsaistību vai patērētāju aizsardzības jomā. Turklāt tiesību akta jēdziens "ietver visu veidu rakstveida un vienotās tiesības, primāros un sekundāros tiesību aktus, pašvaldību dekrētus, tiesu precedentus, konstitucionālos principus, pamattiesības, citus juridiskos principus, kā arī jurisprudenci, kad šādus "tiesību aktus" interpretē un ņem vērā kompetentās tiesas. Nosakot konkrēta nolūka likumīgumu, tiesību akta robežās var ņemt vērā arī citus aspektus, piemēram, paražas, uzvedības kodeksus, ētikas kodeksus, līgumsaistības un lietas vispārējo kontekstu un faktus. Tas ietver pamatā esošo attiecību veidu starp personas datu apstrādātāju un datu subjektiem neatkarīgi no tā, vai tās ir komerciālas vai cita veida." Turklāt tas, ko var uzskatīt par likumīgām interesēm, "laika gaitā var arī mainīties atkarībā no zinātnes un tehnoloģiju attīstības un sabiedrības un kultūras attieksmes pārmaiņām."

to vērā, 7. panta f) punkts var būt piemērots juridiskais pamatojums, ko izmantot dažu veidu tirgvedības tiešsaistes un bezsaistes aktivitātēm, ja vien tiek ieviesti atbilstīgi drošības pasākumi (kas cita starpā ietver funkcionālu sistēmu iebildumu paušanai pret šādu apstrādi saskaņā ar 14. panta b) punktu, kā tiks parādīts III.3.6. sadaļā "Tiesības iebilst un citas tiesības").

Tomēr tas nenozīmē, ka personas datu apstrādātāji var atsaukties uz 7. panta f) punktu, lai nepamatoti pārraudzītu savu klientu tiešsaistes un bezsaistes aktivitātes, kombinētu lielu datu apjomu par klientiem no dažādiem avotiem, kas sākotnēji ir vākti citos kontekstos un atšķirīgos nolūkos, un izveidot (un, piemēram, ar datu aģentu starpniecību arī tirgot) klientu personību un izdarīto izvēļu kompleksus profilus, neinformējot pašus klientus, bez funkcionālas sistēmas iebildumu paušanai, nemaz nerunājot par apzinātu piekrišanu. Šāda profilēšana var būt uzskatāma par būtisku klienta privātuma aizskārumu, un šādā gadījumā datu subjekta intereses un tiesības ir pārākas par personas datu apstrādātāja interesēm[49].

Cits piemērs — lai gan darba grupa savā atzinumā par *SWIFT*[50] atzina uzņēmuma likumīgās intereses ievērot ASV tiesību aktos noteiktos pieprasījumus, lai izvairītos no ASV iestāžu noteiktām sankcijām, tā secināja, ka šajā gadījumā 7. panta f) punktu izmantot nevar. Jo īpaši, darba grupa uzskatīja, ka, ņemot vērā tālejošo ietekmi uz fiziskām personām, ko rada datu apstrāde "slepeni, sistemātiski, masveidā un ilgtermiņā", "daudzo datu subjektu intereses vai pamattiesības un brīvības ir pārākas par *SWIFT* interesēm nesaņemt sankcijas no ASV par pieprasījumu iespējamu neizpildīšanu".

Kā paskaidrots turpmāk, gadījumā, ja personas datu apstrādātāja intereses nav pārliecinošas, ticamāk, ka datu subjekta intereses un tiesības būs pārākas par likumīgajām, taču mazāk nozīmīgajām, personas datu apstrādātāja interesēm. Vienlaikus tas nenozīmē, ka dažkārt personas datu apstrādātāja mazāk pārliecinošas intereses nevar būt pārākas par datu subjektu interesēm un tiesībām — parasti tā notiek gadījumos, kad apstrādes ietekme uz datu subjektiem arī ir mazāk nozīmīga.

Likumīgas intereses publiskajā sektorā

Direktīvas pašreizējā tekstā tādi personas datu apstrādātāji, kas ir valsts iestādes, nav konkrēti izslēgti no datu apstrādes, izmantojot 7. panta f) punktu kā apstrādes juridisko pamatojumu[51].

Tomēr ierosinātajā regulā[52] ir izslēgta iespēja "apstrādei, ko veic valsts iestāde, pildot savus uzdevumus".

Ierosinātās likumdošanas izmaiņas uzsver vispārējā principa lielo nozīmi — ka valsts iestādēm ir atļauts apstrādāt datus, pildot savus uzdevumus, tikai gadījumā, ja tām tiesību aktā

[49] Jautājums par izsekošanas tehnoloģijām un piekrišanas nozīmi saskaņā ar E-privātuma direktīvas 5. panta 3. punktu skatīts atsevišķi. Sk. III.3.6. sadaļas b) punkta iedaļu "Ilustrācija: pieejas attīstība attiecībā uz tiešo tirgvedību".

[50] Sk. arī iepriekš 39. zemsvītras piezīmē minētā atzinuma 4.2.3. sadaļu. Šajā gadījumā personas datu apstrādātāja likumīgās intereses bija arī saistītas ar trešās valsts publiskajām interesēm, uz kurām nevarēja attiecināt Direktīvu 95/46/EK.

[51] Sākotnēji Komisijas pirmajā priekšlikumā direktīvai tika nošķirta datu apstrāde privātajā sektorā un apstrāde publiskajā sektorā. Šis formālais noteikumu nošķīrums starp publisko un privāto sektoru grozītajā priekšlikumā tika atmests. Iespējams, tas arī ir radījis atšķirīgās interpretācijas un īstenošanu dažādās dalībvalstīs.

[52] Sk. ierosinātās regulas 6. panta 1. punkta f) apakšpunktu.

ir noteiktas attiecīgas pilnvaras. Šā principa ievērošana ir īpaši svarīga (un to skaidri paredz Eiropas Cilvēktiesību tiesas judikatūra) gadījumos, kad ir apdraudēts datu subjektu privātums un ar valsts iestādes darbību pārkāptu šādu privātumu.

Tāpēc tiesību aktos jābūt noteiktām pietiekami *detalizētām un konkrētām* pilnvarām (arī saskaņā ar pašreizējo direktīvu) gadījumos, kad ar valsts iestāžu veiktu apstrādi pārkāpj datu subjektu privātumu. Tās var būt vai nu konkrētas juridiskas saistības apstrādāt datus, kas var atbilst 7. panta c) punktam, vai īpašas pilnvaras (taču ne obligāti saistības) apstrādāt datus, kas var atbilst 7. panta e) vai f) punkta prasībām[53].

Trešo personu likumīgās intereses

Direktīvas pašreizējā tekstā ir ne vien atsauce uz "personas datu apstrādātāja likumīgajām interesēm", bet tajā arī atļauts izmantot 7. panta f) punktu, ja likumīgās intereses īsteno trešās personas vai "personas, kurām dati tiek atklāti"[54]. Nākamajā piemērā ir aprakstīti daži konteksti, kādos varētu piemērot šo noteikumu.

Datu publicēšana pārredzamības un pārskatatbildības nolūkā. Svarīgs konteksts, kurā 7. panta f) punkts varētu būt nozīmīgs, ir datu publicēšana pārredzamības un pārskatatbildības nodrošināšanai (piemēram, publiskojot informāciju par uzņēmuma augstākās vadības darbinieku algām). Šajā gadījumā var uzskatīt, ka publiskošana galvenokārt ir veikta nevis tā personas datu apstrādātāja interesēs, kurš publicē datus, bet gan to ieinteresēto personu (piemēram, darba ņēmēju, žurnālistu vai sabiedrības kopumā) interesēs, kurām dati tiek atklāti.

No datu aizsardzības un privātuma perspektīvas, kā arī lai nodrošinātu juridisko noteiktību, kopumā personas datus ieteicams publiskot, pamatojoties uz tiesību aktu, ar kuru tas atļauts, un attiecīgā gadījumā — skaidri norādot publicējamos datus, publicēšanas nolūkus un nepieciešamos drošības pasākumus[55]. Tas arī nozīmē, ka gadījumos, kad personas dati tiek atklāti pārredzamības un pārskatatbildības nolūkos, iespējams, vēlamāk ir izmantot 7. panta c) punktu, nevis 7. panta f) punktu[56].

[53] Šajā saistībā skatiet arī III.2.5. sadaļu par uzdevumiem sabiedrības interesēs (21.–23. lpp.), kā arī turpmāk izklāstītās nostājas sadaļā "Trešo personu likumīgās intereses" (27.–28. lpp.). Skatiet arī apsvērumus par tiesību "privātās izpildes" ierobežojumiem 35. lappusē sadaļā "Sabiedrības intereses/ plašākas kopienas intereses". Visos šajos gadījumos ir īpaši svarīgi nodrošināt, lai tiktu pilnībā ievēroti 7. panta f) punkta un arī 7. panta e) punkta ierobežojumi.

[54] Ierosinātās regulas mērķis ir ierobežot šā pamatojuma lietojumu "pārziņa [personas datu apstrādātāja] likumīgo interešu ievērošanai". No teksta vien nav skaidrs, vai ierosinātais formulējums ir tikai teksta vienkāršojums vai arī tā nolūks ir izslēgt gadījumus, kad personas datu apstrādātājs var atklāt datus citu personu likumīgās interesēs. Tomēr šis teksts nav galīgs. Trešo personu intereses, piemēram, tika atkārtoti ieviestas *LIBE* komitejas galīgajā ziņojumā, 2013. gada 21. oktobrī balsojot par Eiropas Parlamenta *LIBE* komitejas kompromisa grozījumiem. Sk. 6. panta 100. grozījumu. Darba grupa atbalsta trešo personu atkārtotu iekļaušanu priekšlikumā, jo dažās situācijās šāda iespēja var būt piemērota — arī turpmāk aprakstītajos piemēros.

[55] Šis ieteikums par labāko praksi nedrīkst ierobežot valsts tiesību normas par pārredzamību un dokumentu publisku pieejamību.

[56] Dažās dalībvalstīs attiecībā uz publisku un privātu personu veiktu apstrādi patiešām ir jāievēro atšķirīgi noteikumi. Piemēram, saskaņā ar Itālijas Datu aizsardzības kodeksu valsts iestādei atļauts izplatīt personas datus tikai tādā gadījumā, ja tas paredzēts likumos vai noteikumos (19. punkta 3. apakšpunkts).

Tomēr, ja nav konkrētu juridisko saistību vai atļaujas publicēt datus, joprojām ir iespējams atklāt personas datus attiecīgajām ieinteresētajām personām. Attiecīgos gadījumos ir arī iespējams publicēt personas datus pārredzamības un pārskatatbildības nolūkos.

Abos gadījumos (t. i., neatkarīgi no tā, vai personas datus atklāj saskaņā ar tiesību aktiem, kas to atļauj darīt) datu atklāšana ir tieši atkarīga no 7. panta f) punktā paredzētās līdzsvarošanas pārbaudes un atbilstīgu drošības un citu pasākumu īstenošanas[57].

Turklāt var būt arī vēlama jau publiskotu personas datu papildu izmantošana turpmākai pārredzamībai (piemēram, datu pārpublicēšana presē vai NVO veikta sākotnējas datu kopas turpmāka izplatīšana inovatīvākā vai lietotājam draudzīgākā veidā). Tas, vai šāda pārpublicēšana un atkārtota izmantošana būs iespējama, būs arī atkarīgs no līdzsvarošanas pārbaudes rezultātiem, kur cita starpā jāņem vērā informācijas veids un pārpublicēšanas vai atkārtotas izmantošanas ietekme uz personām[58].

Vēsturiska vai cita veida zinātniskā pētniecība. Vēl viens svarīgs konteksts, kurā varētu piemērot atklāšanu trešo personu likumīgās interesēs, ir vēsturiska vai cita veida zinātniskā pētniecība, jo īpaši, ja nepieciešama piekļuve noteiktām datubāzēm. Direktīvā ir paredzēta šādu pasākumu īpaša atzīšana, piemērojot atbilstīgus drošības un cita veida pasākumus[59], taču nevajadzētu aizmirst, ka šādu pasākumu likumīgais pamatojums bieži vien būs pienācīgi pamatots 7. panta f) punkta lietojums[60].

Vispārējas sabiedrības intereses vai trešo personu intereses. Visbeidzot, trešo personu likumīgās intereses var būt arī būtiskas citādā veidā. Tas ir gadījums, kad personas datu apstrādātājs (dažkārt — valsts iestāžu mudināts) īsteno intereses, kas atbilst vispārējām sabiedrības interesēm vai trešo personu interesēm. Tas var ietvert situācijas, kad personas datu apstrādātājs rīkojas plašāk, nekā to paredz tiesību aktos un noteikumos apstrādātājam noteiktās konkrētās juridiskās saistības, lai palīdzētu tiesībaizsardzības vai privātajām ieinteresētajām personām cīnīties pret nelikumīgām darbībām, piemēram, nelikumīgi iegūtu līdzekļu legalizēšanu, uzmākšanos bērniem vai nelikumīgu failu koplietošanu tiešsaistē.

---

[57] Kā paskaidrots darba grupas Atzinumā 06/2013 par brīvi pieejamiem datiem (sk. šā atzinuma, kas minēts turpmāk 88. zemsvītras piezīmē, 9. lappusi), "valstu praksei vai valstu tiesību aktiem attiecībā uz pārredzamību jāatbilst ECTK 8. pantam un ES Hartas 7. un 8. pantam. Tas nozīmē, kā Tiesa norādīja nolēmumos *Österreichischer Rundfunk* un *Schecke* lietās, ka būtu jāpārliecinās, vai informācijas izpaušana ir nepieciešama un proporcionāla tiesību aktā paredzētajam likumīgajam mērķim." Sk. Tiesas 2003. gada 20. maija spriedumu apvienotajās lietās C-465/00, C-138/01 un C-139/01 *Rundfunk* un Tiesas 2010. gada 9. novembra spriedumu apvienotajās lietās C-92/09 un C-93/09 *Volker* un *Markus Schecke*.

[58] Šajā gadījumā būtisks apsvērums ir arī nolūka ierobežojums. Darba grupas Atzinuma 06/2013 par brīvi pieejamiem datiem (minēts turpmāk 88. zemsvītras piezīmē) 19. lappusē 29. panta darba grupa iesaka "katrā tiesību aktā, kurā prasīta publiska piekļuve datiem, skaidri norādīt personas datu izpaušanas mērķus. Ja tas nav veikts vai arī ir veikts tikai neskaidri un vispārīgi, cietīs tiesiskā noteiktība un prognozējamība. Jo īpaši attiecībā uz jebkādu atkalizmantošanas lūgumu attiecīgajai valsts sektora iestādei un potenciālajiem atkalizmantotājiem būs ļoti grūti noteikt, kādi bija publicēšanas paredzētie sākotnējie mērķi, kā arī kādi citi mērķi būtu saderīgi ar šiem sākotnējiem mērķiem. Kā jau tika norādīts, pat tad, ja personas dati ir publicēti internetā, nav jāpieņem, ka tos var papildus apstrādāt ikvienā iespējamā nolūkā."

[59] Sk. 6. panta 1. punkta b) un e) apakšpunktu.

[60] Kā paskaidrots darba grupas Atzinumā 3/2013 par nolūka ierobežojumu (iepriekš minēts 9. zemsvītras piezīmē), attiecībā uz datu turpmāku izmantošanu sekundāriem nolūkiem jāveic divkārša pārbaude. Pirmkārt, jānodrošina, lai dati tiktu izmantoti atbilstīgiem nolūkiem. Otrkārt, jānodrošina, lai apstrādes veikšanai būtu attiecīgs juridiskais pamats saskaņā ar 7. pantu.

Tomēr šajos gadījumos ir īpaši svarīgi nodrošināt, lai tiktu pilnībā ievēroti 7. panta f) punkta ierobežojumi[61].

Apstrādei jābūt vajadzīgai paredzētajiem nolūkiem

Visbeidzot, personas datu apstrādei ir arī jābūt vajadzīgai personas datu apstrādātāja vai — atklāšanas gadījumā — trešo personu "likumīgo interešu ievērošanai". Šis nosacījums papildina 6. pantā noteikto vajadzības prasību un paredz, ka jābūt saistībai starp datu apstrādi un attiecīgajām interesēm. Šī "vajadzības" prasība ir piemērojama visos 7. pantā minētajos gadījumos (panta b)– f) punkts), taču tā ir īpaši svarīga attiecībā uz f) punktu, lai nodrošinātu, ka datu apstrāde, kuras pamatā ir likumīgas intereses, neradītu nepamatoti plašu datu apstrādes vajadzības interpretāciju. Tāpat kā citos gadījumos tas nozīmē, ka ir jāapsver, vai nav pieejami citi mazāk agresīvi līdzekļi, kas ļautu sasniegt tādu pašu mērķi.

III.3.2. Datu subjekta intereses vai tiesības

Intereses vai tiesības (nevis tiesību intereses)

Direktīvas 7. panta f) punktā ir minētas "pamattiesību un brīvību intereses, kurām nepieciešama aizsardzība saskaņā ar 1. panta 1. punktu".

Tomēr darba grupa norādīja, ka, salīdzinot direktīvas dažādu valodu versijas, frāze "interests for" (.. brīvību intereses) citās galvenajās valodās, kas tika izmantotas, risinot sarunas par šo dokumentu, bija tulkota kā "interests or" (intereses vai)[62].

Veicot sīkāku analīzi, tika secināts, ka direktīvas angļu tekstā vienkārši ieviesusies pareizrakstības kļūda — "or" bija kļūdaini uzrakstīts kā "for"[63]. Tādējādi pareizais teksts ir "interests or fundamental rights and freedoms" ("intereses vai pamattiesības un brīvības").

Jēdzieni "intereses" un "tiesības" jāinterpretē plaši

Atsauce uz "interesēm vai pamattiesībām un brīvībām" tiešā veidā ietekmē šā noteikuma piemērošanas jomu. Tā nodrošina datu subjektu lielāku aizsardzību, proti, paredz, ka jāņem vērā arī datu subjektu "intereses", nevis tikai viņu pamattiesības un brīvības. Tomēr nav iemesla pieņemt, ka 7. panta f) punkta ierobežojums attiecībā uz pamattiesībām, "kurām nepieciešama aizsardzība saskaņā ar 1. panta 1. punktu" (tādējādi skaidri atsaucoties uz

[61] Šajā saistībā skatiet, piemēram, 18.1.2005. pieņemto darba dokumentu par datu aizsardzības jautājumiem saistībā ar intelektuālā īpašuma tiesībām (WP104).

[62] Piemēram, "l'intérêt ou les droits et libertés fondamentaux de la personne concernée" franču valodā, "l'interesse o i diritti e le libertà fondamentali della persona interessata" itāļu valodā un "das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person" vācu valodā.

[63] Darba grupa norāda, ka angļu valodas versijā gramatiski pareizi būtu izmantot vārdu savienojumu "interests in", nevis "interests for", ja tāda ir bijusi teksta īstā jēga. Turklāt pirmām kārtām šķiet, ka frāzes "interests for" un "interest in" ir liekvārdība, jo parasti pilnīgi pietiktu ar atsauci uz "pamattiesībām un brīvībām", ja tāda bijusi teksta jēga. Interpretāciju par pareizrakstības kļūdu apstiprina arī tas, ka Padomes 1995. gada 20. februārī pieņemtajā Kopējā nostājā (EK) Nr. 1/95 arī minēts "interests or fundamental rights and freedoms" ("intereses vai pamattiesības un brīvības"). Visbeidzot, darba grupa arī norāda, ka Komisija ir plānojusi labot šo pareizrakstības kļūdu ierosinātajā regulā — 6. panta 1. punkta f) apakšpunktā minētas "datu subjekta intereses vai pamattiesības un brīvības, kurām nepieciešama aizsardzība", nevis "pamattiesību un brīvību intereses".

direktīvas[64] mērķi), neattiektos arī uz terminu "intereses". Tomēr paustais vēstījums ir nepārprotams — jāņem vērā visas attiecīgās datu subjektu intereses.

Šādai teksta interpretācijai ir jēga ne vien gramatiski, bet arī ņemot vērā personas datu apstrādātāja "likumīgo interešu" jēdziena plašo interpretāciju. Ja personas datu apstrādātājs (vai atklāšanas gadījumā — trešā persona) var īstenot jebkādas intereses, ja vien tās nav nelikumīgas, tad arī datu subjektiem būtu jābūt tiesīgiem ņemt vērā to visu veidu intereses un tās salīdzināt ar personas datu apstrādātāja interesēm, ja vien tās ir būtiskas attiecībā uz direktīvas piemērošanas jomu.

Laikā, kad vērojama arvien izteiktāka "informatīvās varas" nelīdzsvarotība, kad gan valdības, gan uzņēmējdarbības organizācijas apkopo līdz šim nepieredzētus datu apjomus par personām un arvien biežāk veido detalizētus profilus, kas paredzēs personu uzvedību (palielinot informācijas nesamērīgumu un samazinot to autonomiju), ir vēl jo svarīgāk nodrošināt, lai tiktu aizsargātas personu intereses aizsargāt savu privātumu un autonomiju.

Visbeidzot, ir svarīgi atzīmēt, ka atšķirībā no personas datu apstrādātāja interešu jēdziena šajā gadījumā pirms datu subjektu "interesēm" nav īpašības vārda "likumīgas". Tas paredz personu interešu un tiesību plašāku aizsardzību. Nedrīkst nesamērīgā veidā pārkāpt pat tādu personu tiesības un intereses, kas iesaistītas nelikumīgās darbībās[65]. Piemēram, tādas personas intereses, kura, iespējams, izdarījusi zādzību lielveikalā, joprojām var būt pārākas nekā veikala īpašnieka intereses publicēt šīs personas attēlu un privāto adresi uz lielveikala sienām un/vai internetā.

III.3.3. Par līdzsvarošanas pārbaudi

Gan personas datu apstrādātāja likumīgās intereses, gan ietekmi uz datu subjekta interesēm un tiesībām ir lietderīgi skatīt vienotā spektrā. Likumīgas intereses var būt gan nenozīmīgas, gan svarīgas un pat nenoraidāmas. Tāpat arī ietekme uz datu subjektu interesēm un tiesībām var būt vairāk vai mazāk nozīmīga un var būt robežās no triviālas līdz pat ļoti nopietnai.

Ja personas datu apstrādātāja likumīgās intereses ir nebūtiskas un nav pārāk pārliecinošas, tās parasti var būt pārākas par datu subjektu interesēm un tiesībām vienīgi gadījumos, kad ietekme uz šīm tiesībām un interesēm ir vēl niecīgāka. Savukārt dažos gadījumos un ievērojot attiecīgos drošības un cita veida pasākumus, svarīgas un nenoraidāmas likumīgas intereses var attaisnot pat būtiskus privātuma aizskārumus vai citu ievērojamu ietekmi uz datu subjektu interesēm un tiesībām[66].

---

[64] Sk. 1. panta 1. punktu: "Saskaņā ar šo direktīvu dalībvalstis aizsargā fizisku personu pamattiesības un brīvības un jo īpaši viņu tiesības uz privātās dzīves neaizskaramību attiecībā uz personas datu apstrādi".

[65] Protams, viena no noziedzības sekām var būt personas datu vākšana un potenciāla publicēšana saistībā ar noziedzniekiem un aizdomās turamajiem. Tomēr tas jādara saskaņā ar stingriem nosacījumiem un drošības pasākumiem.

[66] Ilustrācijai skatiet darba grupas argumentus vairākos atzinumos un darba dokumentos:
- Atzinums 4/2006 par ASV Veselības un sociālas nodrošināšanas ministrijas 2005. gada 20. novembrī izvirzīto likumprojektu par infekcijas slimību kontroli un pasažieru informācijas apkopošanu (Infekciju slimību kontrole, Ieteikts 42 CFR 70. un 71. daļa), kas pieņemts 14.6.2006. (WP 121), kad runa ir par nopietniem un konkrētiem draudiem sabiedrības veselībai.
- Atzinums 1/2006 par sistēmām ziņošanai par pārkāpumiem (minēts iepriekš 39. zemsvītras piezīmē), ja viens no līdzsvarošanas pārbaudes elementiem ir iespējama pārkāpuma nopietnība.

Šajā saistībā ir būtiski uzsvērt drošības pasākumu īpašo nozīmi[67], lai mazinātu nepamatotu ietekmi uz datu subjektiem, tādējādi mainot tiesību un interešu līdzsvaru tādā apmērā, ka personas datu apstrādātāja likumīgās intereses netiks ignorētas. Protams, ar drošības pasākumu izmantošanu vien nepietiek, lai attaisnotu jebkāda veida apstrādi jebkādos apstākļos. Turklāt attiecīgajiem drošības pasākumiem jābūt pienācīgiem un pietiekamiem, un ar tiem neapšaubāmi un būtiski jāsamazina ietekme uz datu subjektiem.

Ievadscenāriji

Pirms norādījumu izklāsta par to, kā veikt līdzsvarošanas pārbaudi, turpmāk norādītie trīs ievadscenāriji var sniegt pirmo ieskatu tajā, kā interešu un tiesību līdzsvarošana varētu izskatīties reālos apstākļos. Visu trīs piemēru pamatā ir vienkāršs un "nevainīgs" scenārijs par līdzņemšanai paredzētu itāliešu ēdienu īpašo piedāvājumu. Piemēros pakāpeniski tiek ieviesti jauni elementi, kas parāda, kā mainās līdzsvars, palielinoties ietekmei uz datu subjektiem.

1. scenārijs — picu tirgotāju tīkla īpašais piedāvājums

Klaudija pasūta picu, izmantojot sava viedtālruņa mobilo lietojumprogrammu, taču neatsakās no tīmekļa tirgvedības opcijas. Piegādes vajadzībām tiek saglabāta viņas adrese un informācija par kredītkarti. Pēc dažām dienām Klaudija mājas pastkastītē no picu tirgotāju tīkla saņem atlaižu kuponus līdzīgiem produktiem.

Īsa analīze: picu tirgotāju tīklam ir likumīgas, taču ne sevišķi pārliecinošas intereses mēģināt klientiem pārdot vairāk savu produktu. Tomēr nešķiet, ka tiek būtiski aizskarts Klaudijas privātums vai kā citādi nepamatoti ietekmētas viņas intereses un tiesības. Dati un konteksts ir relatīvi "nevainīgi" (picas lietošana uzturā). Picu tirgotāju tīkls ir ieviesis dažus drošības pasākumus — tiek izmantota tikai relatīvi ierobežota informācija (kontaktinformācija), un kuponi tiek nosūtīti, izmantojot tradicionālo pastu. Turklāt tīmekļa vietnē ir pieejama viegli lietojama iespēja atteikties no tirgvedības pasākumiem.

Rezultātā un ņemot vērā arī ieviestos drošības un citus pasākumus (tai skaitā viegli lietojamo atteikšanās rīku), nešķiet, ka datu subjekta intereses un tiesības ir pārākas par picu tirgotāju tīkla likumīgajām interesēm veikt šādu minimālu datu apstrādi.

- Darba dokuments par elektronisko sakaru kontroli darbavietā, pieņemts 29.5.2002. (WP 55), kurā darba devēja tiesības nodrošināt uzņēmējdarbības efektivitāti līdzsvarotas ar darba ņēmēja cilvēka cieņu, kā arī sarakstes slepenību.

[67] Drošības pasākumi cita starpā var būt datu vākšanas veidu stingri ierobežojumi, datu tūlītēja izdzēšana pēc lietošanas, tehniski un organizatoriski pasākumi, lai nodrošinātu funkcionālu nošķirumu, atbilstīgas anonimizācijas metodes, datu summēšana un privātuma uzlabošanas tehnoloģijas, taču arī pārredzamība, pārskatatbildība un apstrādes atteikuma iespēja. Plašāk skatiet III.3.4. sadaļas d) punktā un turpmāk.

2. scenārijs — mērķtiecīga reklāma par tādu pašu īpašo piedāvājumu

Konteksts ir tāds pats, taču šoreiz picu tirgotāju tīkls ir saglabājis ne vien Klaudijas adresi un kredītkartes datus, bet arī neseno pasūtījumu vēsturi (par trīs pēdējiem gadiem). Turklāt pirkumu vēsture ir apvienota ar datiem no lielveikala, kur Klaudija veic iepirkšanos tiešsaistē un kuru vada tas pats uzņēmums, kuram pieder picu tirgotāju tīkls. Picu tirgotāju tīkls sniedz Klaudijai īpašus piedāvājumus un mērķtiecīgu reklāmu, pamatojoties uz viņas pasūtījumu vēsturi šajos divos dažādajos pakalpojumos. Viņa saņem reklāmas un īpašus piedāvājumus gan tiešsaistē, gan bezsaistē, pa parasto pastu, e-pastu, kā arī uzņēmuma tīmekļa vietnē un vairāku citu izvēlētu partneru tīmekļa vietnēs (kad viņa piekļūst šīm vietnēm, izmantojot datoru vai mobilo tālruni). Tiek sekots arī Klaudijas pārlūkošanas vēsturei (apmeklējumu vēsturei). Tiek izsekoti arī viņas atrašanās vietas dati, izmantojot viņas mobilo tālruni. Dati tiek apstrādāti ar analīzes programmatūru, kas prognozē viņas izvēles, kā arī laiku un vietas, kad viņa varētu veikt lielākus pirkumus, būtu gatava maksāt lielāku cenu, viņu ietekmētu īpaša atlaide vai kad viņa visvairāk vēlētos nobaudīt savus iecienītos desertus vai gatavos ēdienus[68]. Klaudiju ļoti kaitina uzmācīgās reklāmas, kuras uznirstošos logos parādās viņas mobilajā tālrunī, kad viņa mājupceļā pārbauda autobusu maršrutu grafiku, un kurās reklamēti jaunākie līdzņemšanai paredzēto ēdienu piedāvājumi, kuriem viņa mēģina pretoties. Viņa nespēja atrast lietotājam draudzīgu informāciju par to, kā vienkārši izslēgt šīs reklāmas, lai gan uzņēmums apgalvo, ka ir ieviesta nozarē plaši izmantota atteikšanās sistēma. Turklāt Klaudija ar pārsteigumu atklāja, ka brīžos, kad viņa atradās rajonos ar zemāku labklājības līmeni, īpašie piedāvājumi vairs netika sūtīti. Rezultātā viņas ikmēneša izdevumi par pārtiku palielinājās par 10 %. Kāds tehniski zinošāks draugs viņai kādā tiešsaistes blogā atklāja pieņēmumus par to, ka lielveikals par pasūtījumiem iekasē vairāk no "sliktiem rajoniem", to pamatojot ar faktu, ka statistiski šādos gadījumos pastāv lielāks kredītkaršu krāpniecības risks. Uzņēmums komentārus nesniedza un norādīja, ka tā atlaižu politika un cenu noteikšanas algoritms ir konfidenciāls un to nevar atklāt.

Īsa analīze: dati un konteksts joprojām ir relatīvi "nevainīgi". Tomēr datu vākšanas apjoms un Klaudijas ietekmēšanas paņēmieni (tai skaitā dažādas izsekošanas metodes, prognozējot laiku un vietu, kad Klaudijai radīsies vēlme ieturēties, un tas, ka šajos brīžos viņa var visvieglāk ļauties kārdinājumam) ir faktori, kas jāņem vērā, novērtējot apstrādes radīto ietekmi. Pārredzamības trūkums attiecībā uz uzņēmuma datu apstrādes loģiku, kas, iespējams, izraisījusi faktisku cenu diskrimināciju, pamatojoties uz pasūtījuma vietu, kā arī ievērojamā potenciālā finansiālā ietekme uz klientiem galu galā izjauc līdzsvaru pat relatīvi "nevainīgā" līdznešanai paredzētu ēdienu un pārtikas produktu pirkšanas kontekstā. Tā vietā, lai tikai sniegtu iespēju atteikties no šāda veida profilēšanas un mērķtiecīgas reklamēšanas, būtu vajadzīga apzināta piekrišana ne vien saskaņā ar 7. panta a) punktu, bet arī E-privātuma direktīvas 5. panta 3. punktu. Tādēļ 7. panta f) punktu nevar izmantot kā datu apstrādes juridisko pamatojumu.

[68] Sk., piemēram, http://www.stanfordlawreview.org/online/privacy-and-big-data/consumer-subject-review-boards*:* "Neseni pētījumi liecina, ka gribasspēks ir galīgs resurss, ko laika gaitā var iztērēt vai atjaunot.[10] Bažas par lieko svaru liek patērētājam censties nelietot uzturā iecienītāko pusfabrikātu pārtiku. Izrādās, ka ir brīži un vietas, kad patērētājs kārdinājumam nevar pretoties. Liels datu apjoms ļauj tirgotājiem saprast, tieši kā un kad vērsties pie attiecīgā patērētāja, kad viņš ir vismazāk aizsargāts — jo īpaši pasaulē, kur lietotāji pastāvīgi raugās dažādos ekrānos un kur pat mūsu lietotās ierīces spēj būt par vietu, kur reklamēt savu produktu."

3. scenārijs — pārtikas produktu pasūtījumu izmantošana, lai pielāgotu veselības apdrošināšanas prēmijas

Informāciju par Klaudijas picu ēšanas ieradumiem, tostarp ēdienu pasūtījumu laiku un veidu, ēdināšanas tīkls ir pārdevis apdrošināšanas sabiedrībai, kas to izmanto, lai pielāgotu savas veselības apdrošināšanas prēmijas.

Īsa analīze: veselības apdrošināšanas sabiedrībai var būt likumīgas intereses (ciktāl tas atļauts piemērojamajos noteikumos) novērtēt savu klientu veselības riskus un iekasēt diferencētas prēmijas, ņemot vērā atšķirīgos riskus. Tomēr pats datu vākšanas veids un apjoms ir pārmērīgs. Jebkurš ar veselu saprātu apveltīts cilvēks Klaudijas vietā diezin vai domātu, ka informācija par viņas picu patēriņa ieradumiem tiek izmantota, lai aprēķinātu viņas veselības apdrošināšanas prēmijas.

Papildus profilēšanas pārmērīgumam un potenciāli neprecīziem secinājumiem (iespējams, pica pasūtīta kādam citam), sensitīvu datu (ar veselību saistīti dati) izsecināšana no šķietami nekaitīgiem datiem (līdzņemšanai paredzētu ēdienu pasūtījumi) rada pārsvaru datu subjekta interešu un tiesību pusē. Visbeidzot, apstrāde viņu būtiski ietekmē arī finansiāli.

Kopumā šajā konkrētajā gadījumā datu subjekta intereses un tiesības ir pārākas par veselības apdrošināšanas sabiedrības likumīgajām interesēm. Tādēļ 7. panta f) punktu nevar izmantot kā datu apstrādes juridisko pamatojumu. Ņemot vērā datu vākšanas pārmērīgo apjomu un, iespējams, arī valsts tiesību aktos noteiktus konkrētus papildu ierobežojumus, ir arī apšaubāms, vai par juridisko pamatojumu varētu izmantot 7. panta a) punktu.

Iepriekš aprakstītie scenāriji un potenciālā dažādu citu elementu variāciju ieviešana liecina, ka ir nepieciešams ierobežots galveno faktoru skaits, kas varētu palīdzēt fokusēt novērtējumu, kā arī pragmatiska pieeja, kas ļautu izmantot praktiskus pieņēmumus ("empīriskās metodes"), galvenokārt pamatojoties uz to, ko saprātīgi domājošs cilvēks attiecīgos apstākļos uzskatītu par pieņemamu ("pamatotas gaidas"), un arī pamatojoties uz datu apstrādes sekām attiecībā uz datu subjektiem ("ietekme").

III.3.4. Galvenie faktori, kas jāņem vērā, piemērojot līdzsvarošanas pārbaudi

Dalībvalstis ir noteikušas vairākus noderīgus aspektus, kas jāņem vērā, veicot līdzsvarošanas pārbaudi. Šie faktori ir apspriesti šajā sadaļā četros galvenajos punktos: a) personas datu apstrādātāja likumīgo interešu novērtēšana, b) ietekme uz datu subjektiem, c) pagaidu līdzsvars un d) personas datu apstrādātāja īstenoti papildu drošības pasākumi, lai novērstu nepamatotu ietekmi uz datu subjektiem[69].

Lai veiktu līdzsvarošanas pārbaudi, no vienas puses, vispirms ir svarīgi apsvērt likumīgo interešu veidu un avotu, bet, no otras puses — to ietekmi uz datu subjektiem. Šajā novērtējumā jau ir jāņem vērā pasākumi, ko personas datu apstrādātājs plāno pieņemt, lai ievērotu direktīvas noteikumus (piemēram, lai nodrošinātu nolūka ierobežojumu un

[69] Drošības pasākumu svarīguma dēļ daži konkrēti ar tiem saistīti jautājumi plašāk apspriesti atsevišķos III.3.5. un III.3.6. sadaļas punktos.

proporcionalitāti saskaņā ar 6. pantu vai sniegtu informāciju datu subjektiem saskaņā ar 10. un 11. pantu).

Pēc abu pušu analizēšanas un salīdzināšanas var panākt pagaidu "līdzsvaru". Ja novērtējuma rezultāti joprojām rada šaubas, nākamais solis ir novērtēt, vai papildu drošības pasākumi, kas papildus aizsargā datu subjektu, var radīt tādu pārsvaru, ka tas datu apstrādi padarītu likumīgu.

(a) Personas datu apstrādātāja likumīgo interešu novērtēšana

Tā kā likumīgo interešu jēdziens ir samērā plašs, kā iepriekš paskaidrots III.3.1. sadaļā, attiecībā uz interešu līdzsvarošanu ar datu subjektu tiesībām un interesēm liela nozīme ir šo interešu veidam. Lai gan nav iespējams izteikt vērtējošus spriedumus attiecībā uz visām iespējamajām likumīgajām interesēm, var sniegt zināmus norādījumus. Kā minēts iepriekš, šādas intereses var būt gan triviālas, gan pārliecinošas, gan nepārprotamas, gan pretrunīgākas.

i) Pamattiesību īstenošana

Vairākas no Eiropas Pamattiesību hartā ("harta")[70] un Eiropas Cilvēktiesību konvencijā ("ECTK") iekļautajām pamattiesībām un brīvībām var būt pretrunā tiesībām uz privātumu un tiesībām uz personas datu aizsardzību, piemēram, vārda un informācijas brīvība[71], humanitāro un eksakto zinātņu brīvība[72], tiesības piekļūt dokumentiem[73], kā arī, piemēram, tiesības uz brīvību un drošību[74], domu, pārliecības un ticības brīvība[75], darījumdarbības brīvība[76], tiesības uz īpašumu[77], tiesības uz efektīvu tiesību aizsardzību un taisnīgu tiesu[78] vai nevainīguma prezumpcija un tiesības uz aizstāvību[79].

Lai personas datu apstrādātāju likumīgās intereses būtu pārākas un lai varētu īstenot attiecīgās pamattiesības, datu apstrādei jābūt "vajadzīgai" un "proporcionālai".

Ilustrācijai — atkarībā no lietas faktiem laikraksts var nodrošināt atbilstību vajadzības un proporcionalitātes principam, ja tas publicē noteiktu apsūdzošu informāciju par iespējamā korupcijas skandālā iesaistītu augsta līmeņa valdības ierēdņa tēriņu ieradumiem. Tomēr plašsaziņas līdzekļiem nedrīkst būt beznosacījuma atļauja publicēt jebkāda veida nebūtisku informāciju par publisku personu privāto dzīvi. Šādi un līdzīgi gadījumi parasti rada sarežģītas novērtēšanas problēmas, un novērtējuma veikšanā liela nozīme var būt gan

[70] Hartas noteikumi attiecas uz ES iestādēm un struktūrām, pienācīgi ņemot vērā subsidiaritātes principu, kā arī valstu iestādēm tikai tādā gadījumā, ja tās īsteno ES tiesību aktus.
[71] Hartas 11. pants un ECTK 10. pants.
[72] Hartas 13. pants un ECTK 9. un 10. pants.
[73] Hartas 42. pants. "Ikvienam Savienības pilsonim un jebkurai fiziskai personai, kas dzīvo kādā dalībvalstī, vai juridiskai personai, kuras juridiskā adrese ir kādā dalībvalstī, ir tiesības piekļūt Savienības iestāžu un struktūru dokumentiem neatkarīgi no to veida". Līdzīgas piekļuves tiesības ir noteiktas vairākās dalībvalstīs attiecībā uz valsts iestāžu dokumentiem šajās dalībvalstīs.
[74] Hartas 6. pants un ECTK 5. pants.
[75] Hartas 10. pants un ECTK 9. pants.
[76] Hartas 16. pants.
[77] Hartas 17. pants un ECTK 1. protokola 1. pants.
[78] Hartas 47. pants un ECTK 6. pants.
[79] Hartas 48. pants un ECTK 6. un 13. pants.

konkrētiem tiesību aktiem, gan judikatūrai, gan jurisprudencei, gan pamatnostādnēm, gan arī uzvedības kodeksiem un citiem oficiāliem un mazāk oficiāliem standartiem[80].

Attiecīgā gadījumā (arī šajā kontekstā) liela nozīme var būt papildu drošības pasākumiem, kas var palīdzēt noteikt, kā panākt šo dažkārt trauslo līdzsvaru.

ii) Sabiedrības intereses / plašākas kopienas intereses

Iespējams, dažos gadījumos personas datu apstrādātājs vēlēsies atsaukties uz sabiedrības vai plašākas kopienas interesēm (neatkarīgi no tā, vai tas ir paredzēts valsts tiesību aktos vai noteikumos). Piemēram, labdarības organizācija var apstrādāt personas datus medicīniskās pētniecības nolūkos vai bezpeļņas organizācija — lai aktualizētu jautājumu par korupciju valdībā.

Var būt arī tā, ka uzņēmuma privātās biznesa intereses zināmā mērā sakrīt ar sabiedrības interesēm. Piemēram, tas var notikt attiecībā uz finanšu krāpniecības apkarošana vai citiem krāpnieciskiem pakalpojumu izmantošanas veidiem[81]. Pakalpojumu sniedzējam var būt likumīgas uzņēmējdarbības intereses nodrošināt, lai tā klienti neizmantotu pakalpojumu ļaunprātīgi (vai nevarētu iegūt pakalpojumus, par tiem nesamaksājot), vienlaikus arī uzņēmuma klientiem, nodokļu maksātājiem un sabiedrībai kopumā ir likumīgas intereses, ka tiek nodrošināta krāpniecisku darbību apkarošana un to konstatēšana, ja tās notikušas.

Kopumā tas, ka personas datu apstrādātājs darbojas ne vien savās likumīgās (t. i., uzņēmējdarbības) interesēs, bet arī plašākas kopienas interesēs, šīs intereses var padarīt "svarīgākas". Jo pārliecinošākas ir sabiedrības intereses vai plašākas kopienas intereses un jo kopiena un datu subjekti ir skaidrāk apstiprinājuši un uzskata, ka personas datu apstrādātājs var rīkoties un apstrādāt datus, īstenojot šīs intereses, jo lielāka ir šo likumīgo interešu nozīme līdzsvara noteikšanā.

Savukārt tiesību aktu "izpildi privātām vajadzībām" nedrīkst izmantot, lai leģitimizētu plašākas iejaukšanās praksi, kas (ja to veiktu valsts organizācija) būtu aizliegta saskaņā ar Eiropas Cilvēktiesību tiesas judikatūru, pamatojoties uz to, ka ar valsts iestādes darbību pārkāptu datu subjektu privātumu, neatbilstot stingrajai pārbaudei saskaņā ar ECTK 8. panta 2. punktu.

iii) Citas likumīgas intereses

Kā jau apspriests III.2. sadaļā, dažos gadījumos konteksts, kādā rodas likumīgas intereses, var tuvināties kādam no kontekstiem, kuros var piemērot citus juridiskos pamatojumus, jo īpaši 7. panta b) punkta (līgums), 7. panta c) punkta (juridiskās saistības) vai 7. panta e) punkta

[80] Attiecībā uz kritērijiem, kas jāpiemēro lietās, kas ietver vārda brīvību, noderīgi norādījumi atrodami arī Eiropas Cilvēktiesību tiesas judikatūrā. Sk., piemēram, ECT 2012. gada 7. februāra spriedumu lietā *von Hannover* pret Vāciju (Nr. 2), jo īpaši 95.–126. punktu. Jāņem vērā arī tas, ka direktīvas 9. pantā ("Personas datu apstrāde un vārda brīvība") dalībvalstīm ir atļauts noteikt "izņēmumus vai atkāpes no [vairākiem šās direktīvas noteikumiem] personas datu apstrādei, kas veikta tikai un vienīgi žurnālistikas nolūkiem vai mākslinieciskās vai literārās izteiksmes nolūkiem", ja "tie vajadzīgi, lai saskaņotu tiesības uz privātās dzīves neaizskaramību ar normām, kas reglamentē vārda brīvību".

[81] Sk., piemēram, Darba grupas Atzinuma 3/2013 par nolūka ierobežojumu (minēts iepriekš 9. zemteksa piezīmē) 67. lpp. — "21. piemērs: viedās mērīšanas dati, kas iegūti, lai noteiktu krāpniecisku enerģijas lietojumu".

(uzdevums sabiedrības interesēs) juridiskos pamatojumus. Piemēram, datu apstrāde var nebūt noteikti nepieciešama, taču tā var būt svarīga līguma izpildei, vai arī likumā var būt tikai atļauta, taču ne noteikta konkrētu datu apstrāde. Kā redzams, ne vienmēr ir viegli skaidri nošķirt dažādus pamatojumus, taču tieši tādēļ ir vēl jo svarīgāk analīzē iekļaut 7. panta f) punkta līdzsvarošanas pārbaudi.

Arī šajā gadījumā, tāpat kā visos citos līdz šim neminētos, bet iespējamos gadījumos —, jo pārliecinošākas personas datu apstrādātāja intereses un jo plašākā kopienā ir skaidrāk apstiprināts un tiek uzskatīts, ka personas datu apstrādātājs var rīkoties un apstrādāt datus, īstenojot šīs intereses, jo lielāka ir šo likumīgo interešu nozīme līdzsvara noteikšanā[82]. Tas noved pie nākamā jautājuma, kas ir daudz vispārīgāks.

iv) Interešu likumīguma juridiskā un kultūras / sociālā atzīšana

Attiecībā uz visiem izklāstītajiem kontekstiem noteikti ir arī būtiski, vai ES tiesību aktos vai dalībvalsts tiesību aktos ir konkrēti atļauts (ja pat netiek prasīts) personas datu apstrādātājiem veikt pasākumus, lai īstenotu attiecīgās publiskās vai privātās intereses. Būtiski ir arī jebkādi pienācīgi pieņemti un nesaistoši norādījumi, kurus izdevušas pārvaldes iestādes, piemēram, regulatīvās aģentūras, un kuros personas datu apstrādātāji mudināti apstrādāt datus, lai īstenotu attiecīgās intereses.

Ticams, ka arī datu aizsardzības iestāžu vai citu attiecīgo iestāžu izdotu nesaistošu norādījumu ievērošana par datu apstrādes veidiem varētu veicināt līdzsvara pozitīva novērtējuma iegūšanu. Nozīme var būt arī kultūras vidē un sabiedrībā valdošajām gaidām, pat ja tās nav tieši atspoguļotas likumdošanas vai reglamentējošajos instrumentos, un tās var radīt pārsvaru vienā vai otrā virzienā.

Jo skaidrāk tiesību aktos, citos reglamentējošos instrumentos (neatkarīgi no tā, vai tie ir saistoši attiecībā uz personas datu apstrādātāju) vai pat noteiktas kopienas kultūrvidē kopumā bez konkrēta juridiskā pamata ir atzīts, ka personas datu apstrādātāji var rīkoties un apstrādāt datus, lai īstenotu konkrētas intereses, jo lielāka ir šo likumīgo interešu nozīme līdzsvara noteikšanā[83].

(b) Ietekme uz datu subjektiem

Raugoties uz līdzsvara otru pusi, būtisks kritērijs ir apstrādes ietekme uz datu subjekta interesēm vai pamattiesībām un brīvībām. Turpmāk pirmajā apakšsadaļā ir vispārīgi apspriests, kā novērtēt ietekmi uz datu subjektu.

Šajā saistībā var būt noderīgi vairāki aspekti, un tie analizēti turpmākajās apakšsadaļās, tostarp personas datu veids, informācijas apstrādes veids, datu subjektu pamatotas gaidas, kā arī personas datu apstrādātāja un datu subjekta statuss. Īsi apspriesti arī jautājumi, kas saistīti ar potenciāliem riska avotiem, kuri var radīt ietekmi uz attiecīgajām personām, uz attiecīgajām personām vērstās ietekmes nopietnību un šādas ietekmes īstenošanās ticamību.

[82] Protams, novērtējumā ir arī jāiekļauj apsvērumi par potenciālo kaitējumu, kas var rasties personas datu apstrādātājam, trešām personām vai plašākai kopienai, ja datu apstrāde netiek veikta.

[83] Tomēr šīs intereses nevar izmantot, lai leģitimizētu plašu iejaukšanos, kas citādi neatbilstu pārbaudei saskaņā ar ECTK 8. panta 2. punktu.

i) Ietekmes novērtējums

Novērtējot apstrādes ietekmi[84], jāņem vērā gan pozitīvās, gan negatīvās sekas. Tās var ietvert potenciālus trešo personu turpmākus lēmumus vai rīcību, ja datu apstrāde var izraisīt personu atstumšanu vai diskrimināciju, neslavas celšanu vai, raugoties plašāk — radīt situācijas, kas var kaitēt datu subjekta reputācijai, pozīcijām sarunu risināšanā vai autonomijai.

Papildus negatīvajām sekām, ko var konkrēti paredzēt, ir arī jāņem vērā plašāka emocionālā ietekme, piemēram, aizkaitinājums, bailes un raizes, ko var sagādāt tas, ka datu subjekts zaudē kontroli pār personisko informāciju vai saprot, ka tā ir vai var tikt izmantota ļaunprātīgi vai kompromitēta, piemēram, publicējot to internetā. Pienācīgi jāņem vērā arī nepatīkamā ietekme uz aizsargātu rīcību, piemēram, informācijas iegūšanas brīvību vai vārda brīvību, ko var radīt nepārtraukta kontrole / izsekošana.

Darba grupa uzsver, ka ir svarīgi saprast, ka attiecīgā "ietekme" ir daudz plašāks jēdziens nekā vienam vai vairākiem konkrētiem datu subjektiem nodarīts kaitējums vai bojājums. Šajā atzinumā izmantotais ietekmes jēdziens ietver jebkādas "iespējamas" (potenciālas vai faktiskas) datu apstrādes sekas. Skaidrības labad jāuzsver arī tas, ka šis jēdziens nav saistīts ar datu aizsardzības pārkāpumu jēdzienu un ir daudz plašāks par ietekmi, ko var radīt datu aizsardzības pārkāpums. Tā vietā šeit izmantotais ietekmes jēdziens ietver dažādos veidus, kādos personu var pozitīvā vai negatīvā veidā ietekmēt, apstrādājot tās personas datus[85].

Svarīgi arī saprast, ka visbiežāk virkne saistītu un nesaistītu gadījumu var kumulatīvi veidot galējo negatīvo ietekmi uz datu subjektu un var būt sarežģīti identificēt, kurai apstrādes darbībai un kuram personas datu apstrādātājam ir bijusi vislielākā nozīme negatīvās ietekmes veidošanā.

Ņemot vērā to, ka šajā kontekstā datu subjektiem bieži vien ir grūti sākt tiesvedību par kompensāciju par radīto kaitējumu vai bojājumiem, ja pat sekas pašas par sevi ir pavisam reālas, ir vēl jo svarīgāk pievērst uzmanību novēršanas pasākumiem un nodrošināt, lai datu apstrādes darbības varētu veikt tikai tad, ja tās nerada risku vai rada ļoti mazu nepamatotas negatīvas ietekmes risku uz datu subjektu interesēm vai pamattiesībām un brīvībām.

Novērtējot ietekmei, zināmā mērā var līdzēt tradicionālo riska novērtējumu terminoloģija un metodoloģija, tāpēc turpmāk īsi apskatīti daži šīs metodoloģijas aspekti. Tomēr visaptveroša ietekmes novērtēšanas metodoloģija (7. panta f) punkta vai plašākā kontekstā) pārsniegtu šā atzinuma tvērumu.

---

[84] Šis ietekmes novērtējums ir jāskata 7. panta f) punkta kontekstā. Citiem vārdiem sakot, šajā gadījumā runa nav par "riska analīzi" vai "datu aizsardzības ietekmes novērtējumu" ierosinātās regulas (33. un 34. pants) un tās dažādo *LIBE* grozījumu izpratnē. Jautājums par metodoloģiju, kas izmantojama, veicot "riska analīzi" vai "datu aizsardzības ietekmes novērtējumu", pārsniedz šī atzinuma darbības jomu. Tomēr jāpatur prātā, ka tā vai citādi ietekmes analīze saskaņā ar 7. panta f) punktu var būt svarīga jebkādas "riska analīzes" vai "datu aizsardzības ietekmes novērtējuma" daļa un var arī palīdzēt identificēt situācijas, kad nepieciešama apspriešanās ar datu aizsardzības iestādi.

[85] Vienmēr pienācīgi jāņem vērā, piemēram, finansiāla kaitējuma risks, ja datu aizsardzības pārkāpuma rezultātā tiek izpausta finansiāla informācija, kuru bija paredzēts glabāt drošā vidē, un ja šāds pārkāpums galu galā ir par pamatu identitātes zādzībai vai cita veida krāpniecībai, rada traumu, sāpju, ciešanu un ērtību zuduma risku, ko galu galā ir varējusi izraisīt neatļauta medicīniskās dokumentācijas sagrozīšana un pacienta nepareiza turpmākā ārstēšana, lai gan to nekādā gadījumā nevar attiecināt vienīgi uz 7. panta f) punktā noteiktajām situācijām. Tajā pašā laikā šādi riski nav vienīgie, kas jāapskata, veicot ietekmes novērtējumu saskaņā ar 7. panta f) punktu.

Šajā saistībā tāpat kā citos kontekstos ir svarīgi identificēt datu subjektu potenciālās ietekmes avotus.

Viens no aspektiem, kas jāņem vērā, ir riska īstenošanās ticamības risks. Piemēram, interneta lietošana, datu apmaiņa ar vietnēm ārpus ES, savstarpēju savienojumu veidošana ar citām sistēmām un augsta līmeņa sistēmu neviendabīgums un dažādība var būt neaizsargātības aspekti, ko var izmantot hakeri. Šādam riska avotam ir relatīvi augsta ticamība, ka varētu īstenoties datu kompromitēšanas risks. Turpretim viendabīgai un stabilai sistēmai, kurā netiek veidoti savstarpēji savienojumi un kas nav savienota ar internetu, ir daudz zemāka datu kompromitēšanas ticamība.

Vēl viens riska novērtējuma aspekts ir riska īstenošanās seku nopietnība. Šī nopietnība var būt no niecīgas (piemēram, kaitinošā nepieciešamība atkārtoti ievadīt personisko kontaktinformāciju, jo personas datu apstrādātājs to ir zaudējis) līdz ļoti lielai (piemēram, personas nāve, ja dati par aizsargātu personu atrašanās vietu nonāk noziedznieku rokās vai, izmantojot viedās mērīšanas ierīces, kritiskos klimata vai personas veselības apstākļos tiek attālināti pārtraukta energoapgāde).

Šie divi galvenie aspekti – riska īstenošanās ticamība, no vienas puses, un seku nopietnība, no otras puses – iespaido potenciālās ietekmes kopējo novērtējumu.

Visbeidzot, piemērojot metodoloģiju, jāatceras, ka ietekmes novērtējums saskaņā ar 7. panta f) punktu nedrīkst būt mehānisks un tikai kvantitatīvs pasākums. Nosakot "nopietnību" tradicionālos riska novērtēšanas scenārijos, var ņemt vērā potenciāli ietekmēto personu skaitu. Tomēr jāpatur prātā, ka attiecībā uz personas datu apstrādi, kas ietekmē nelielu datu subjektu skaitu vai pat tikai vienu personu, ir jāveic ļoti rūpīga analīze, īpaši gadījumā, ja šāda katras atsevišķās personas ietekme ir īpaši nozīmīga.

ii) Datu veids

Vispirms būtu svarīgi novērtēt, vai tiek apstrādāti sensitīvi dati — vai nu tāpēc, ka tie ietilpst īpašās datu kategorijās saskaņā ar direktīvas 8. pantu, vai citu iemeslu dēļ, kā tas ir saistībā ar biometriskiem datiem, ģenētisko informāciju, saziņas datiem, atrašanās vietas datiem un cita veida personisko informāciju, kurai nepieciešama īpaša aizsardzība[86].

Piemēram, darba grupa uzskata, ka kopumā biometrikas izmantošana vispārējām īpašuma vai personu drošības vajadzībām ir uzskatāma par likumīgām interesēm, kuras ir pārākas par datu subjekta interesēm vai pamattiesībām un brīvībām. Tomēr tādus biometriskos datus kā pirkstu nospiedumu un/vai varavīksnenes skenēto attēlu var izmantot drošībai augsta riska zonās, piemēram, laboratorijā, kurā veic pētījumus par bīstamiem vīrusiem, ja personas datu apstrādātājs ir sniedzis konkrētus pierādījumus par ievērojamu risku[87].

[86] Saskaņā ar Komisijas priekšlikumu datu aizsardzības regulai, lasot to kopā ar *LIBE* komitejas ierosinātajiem grozījumiem, biometriskie dati un ģenētiskā informācija ir uzskatāmi par īpašām datu kategorijām. Sk. 9. panta 103. grozījumu *LIBE* komitejas galīgajā ziņojumā. Par Direktīvas 95/46/EK 7. un 8. panta savstarpējo saistību lasiet iepriekš II.1.2. sadaļā, 14.–15. lpp.

[87] Sk. 29. panta darba grupas Atzinumu 3/2012 par biometrijas tehnoloģiju attīstību (WP193). Kā citu piemēru savā Atzinumā 4/2009 par Pasaules Antidopinga aģentūru (minēts iepriekš 32. zemsvītras piezīmē) darba grupa uzsvēra, ka 7. panta f) punkts nebūtu derīgs pamatojums, lai apstrādātu medicīniskus datus un datus, kas saistīti

Kopumā — jo sensitīvāka informācija, jo vairāk seku datu subjektam. Tomēr tas nenozīmē, ka datus, kas paši par sevi var šķist nekaitīgi, var brīvi apstrādāt, pamatojoties uz 7. panta f) punktu. Patiesi, pat šādi dati atkarībā no to apstrādes veida var būtiski ietekmēt personas, kā parādīts turpmākajā iii) apakšpunktā.

Šajā saistībā būtisks aspekts varētu būt tas, vai datu subjekts vai trešās personas datus jau ir padarījušas publiski pieejamus. Šajā ziņā pirmām kārtām ir svarīgi uzsvērt, ka personas dati (pat ja tie ir publiski pieejami) joprojām ir uzskatāmi par personas datiem, tāpēc attiecībā uz to apstrādi joprojām jāveic atbilstīgi drošības pasākumi[88]. Nepastāv beznosacījuma atļaujas atkārtoti izmantot un papildus apstrādāt publiski pieejamus personas datus saskaņā ar 7. panta f) punktu.

Ņemot to vērā, fakts, ka personas dati ir publiski pieejami, var tikt uzskatīts kā faktors novērtējumā, īpaši gadījumā, ja publicēšana veikta ar pamatotām gaidām datus turpmāk izmantot noteiktiem nolūkiem (piemēram, pētniecības nolūkā vai saistībā ar pārredzamību un pārskatatbildību).

iii) Datu apstrādes veids

Ietekmes novērtēšana plašākā izpratnē var ietvert apsvērumus par to, vai dati ir publiski izpausti vai kā citādi darīti pieejami lielam skaitam personu, vai arī liels personas datu apjoms tiek apstrādāts vai kombinēts ar citiem datiem (piemēram, profilēšanas gadījumā komerciāliem, tiesībaizsardzības vai citiem nolūkiem). Lielā apjomā apstrādājot šķietami nekaitīgus datus un tos kombinējot ar citiem datiem, var secināt par sensitīvākiem datiem, kā redzams iepriekš aprakstītajā 3. scenārijā par picu patēriņa ieradumu saistību ar veselības apdrošināšanas prēmijām.

Papildus tam, ka iespējama sensitīvāku datu apstrāde, veicot šādu analīzi, var tikt iegūtas dīvainas, negaidītas un arī neprecīzas prognozes, piemēram, saistībā ar attiecīgo personu uzvedību vai raksturu. Atkarībā no šo prognožu veida un ietekmes tas var būtiski aizskart personas privātumu[89].

Iepriekšējā atzinumā darba grupa arī uzsvēra riskus, kas saistīti ar noteiktiem drošības risinājumiem (tostarp ugunsmūriem, pretvīrusa un surogātpasta novēršanas risinājumiem), jo tie var paredzēt liela apjoma padziļināto pakešu pārbaužu ieviešanu, kas var ievērojami ietekmēt tiesību līdzsvara novērtējumu[90].

Kopumā — jo negatīvāka vai neskaidrāka ir apstrādes ietekme, jo mazāk ticams, ka galu galā apstrāde tiks uzskatīta par likumīgu. Lai sasniegtu personas datu apstrādātāja mērķus, šajā saistībā noteikti būtu pamatoti apsvērt tādu alternatīvu metožu pieejamību, kas rada mazāk

---

ar pārkāpumiem antidopinga izmeklēšanu kontekstā, ņemot vērā "nopietnu privātuma aizskārumu". Datu apstrādei ir jābūt paredzētai tiesību aktā un jāatbilst direktīvas 8. panta 4. vai 5. punkta prasībām.

[88] Sk. darba grupas Atzinumu 3/2013 par nolūka ierobežojumu (minēts 9. zemsvītras piezīmē iepriekš) un darba grupas Atzinumu 06/2013 par brīvi pieejamu datu un valsts sektora informācijas ("VSI") atkalizmantošanu, kas pieņemts 5.6.2013. (WP207).

[89] Sk. atzinuma par nolūka ierobežojumu (iepriekš minēts 9. zemsvītras piezīmē) III.2.5. sadaļu un 2. pielikumu.

[90] Sk. 3.1. sadaļu darba grupas Atzinumā 1/2009 par priekšlikumiem, ar ko groza Direktīvu 2002/58/EK par privāto dzīvi un elektronisko komunikāciju (e-privātuma direktīva) (WP159).

negatīvu ietekmi uz datu subjektu. Attiecīgā gadījumā šādas iespējas izvērtēšanai var izmantot privātuma un datu aizsardzības ietekmes novērtējumus.

iv) Datu subjekta pamatotas gaidas

Šajā ziņā ļoti būtiskas ir arī datu subjekta pamatotās gaidas attiecībā uz datu izmantošanu un atklāšanu. Kā jau uzsvērts saistībā ar nolūka ierobežojuma principa analīzi[91], ir svarīgi apsvērt, vai personas datu apstrādātāja statuss[92], attiecību vai sniegtā pakalpojuma veids[93] vai arī piemērojamās juridiskās vai līgumsaistības (vai cita veida solījumi, kas pausti datu vākšanas brīdī) var radīt pamatotas gaidas attiecībā uz stingrāku konfidencialitāti un stingrākiem ierobežojumiem turpmākai izmantošanai. Vispārīgi runājot, jo konkrētāks un ierobežojošāks datu vākšanas konteksts, jo ticamāk, ka tiks izmantots lielāks ierobežojumu skaits. Tomēr arī šajā gadījumā ir jāņem vērā faktiskais konteksts, nevis vienkārši jāpaļaujas uz tekstu mazajā drukā.

v) Personas datu apstrādātāja un datu subjekta statuss

Novērtējot apstrādes ietekmi, būtisks ir arī datu subjekta un personas datu apstrādātāja statuss. Atkarībā no tā, vai personas datu apstrādātājs ir fiziska persona vai neliela organizācija, liels starptautisks uzņēmums vai publiskā sektora struktūrvienība, kā arī konkrētajiem apstākļiem, tā pozīcija var būt vairāk vai mazāk dominējoša attiecībā pret datu subjektu. Piemēram, lielam starptautiskam uzņēmumam var būt vairāk resursu un lielāks spēku samērs, risinot sarunas, nekā atsevišķam datu subjektam, tāpēc tas var būt labākā pozīcijā, lai uzspiestu datu subjektam tādu rīcību, ko tas uzskata par "likumīgām interesēm". Vēl jo vairāk tā var notikt gadījumā, ja uzņēmumam tirgū ir dominējošs stāvoklis. Ja netiek veikti kontroles pasākumi, tas var kaitēt atsevišķiem datu subjektiem. Tāpat kā patērētāju aizsardzības un konkurences tiesību akti palīdz nodrošināt, lai šāda vara netiktu izmantota ļaunprātīgi, arī datu aizsardzības tiesību aktiem ir liela nozīme, lai nodrošinātu, ka datu subjektu tiesības un intereses netiek nepamatoti ierobežotas.

Tomēr būtisks ir arī datu subjekta statuss. Lai gan līdzsvarošanas pārbaude principā būtu jāveic attiecībā pret vidējo iedzīvotāju, konkrētās situācijās vajadzētu izmantot pieeju katram atsevišķam gadījumam — piemēram, būtu svarīgi ņemt vērā, vai datu subjekts ir bērns[94] vai pieder pie kādas citas neaizsargātākas iedzīvotāju grupas, kam vajadzīga īpaša aizsardzība, piemēram, vai tā ir persona ar garīgu slimību, patvēruma meklētājs vai gados vecāka persona. Noteikti būtisks būs arī jautājums par to, vai datu subjekts ir darba ņēmējs, students, pacients, kā arī vai pastāv cita veida nelīdzsvarotība starp datu subjekta un personas datu apstrādātāja stāvokli. Ir svarīgi novērtēt faktiskās apstrādes ietekmi uz konkrētām personām.

Visbeidzot, ir svarīgi uzsvērt, ka ne visu veidu negatīva ietekme uz datu subjektiem ir vienlīdz "svarīga", lai panāktu līdzsvaru. 7. panta f) punkta līdzsvarošanas pārbaudes mērķis nav

[91] Sk. darba grupas Atzinuma 3/2013 par nolūka ierobežojumu (minēts iepriekš 9. zemsvītras piezīmē) 24.–25. lpp.

[92] "Piemēram, advokāts vai ārsts."

[93] "Piemēram, personīgo dokumentu pārvaldības mākoņdatošanas pakalpojumi, e-pasta pakalpojumi, dienasgrāmatas, e-grāmatu lasītāji, kas aprīkoti ar piezīmju veikšanas funkcijām, kā arī dažādas dzīves dokumentēšanas lietojumprogrammas, kas var ietvert ļoti personisku informāciju."

[94] Sk. darba grupas Atzinumu 2/2009 par bērnu personas datu aizsardzību (Vispārējas pamatnostādnes un personas datu aizsardzība skolās), kas pieņemts 11.2.2009. (WP160). Šajā atzinumā uzsvērta bērnu īpašā neaizsargātība un bērna pārstāvības gadījumā — vajadzība ņemt vērā bērna, nevis viņa pārstāvja intereses.

novērst jebkāda veida negatīvu ietekmi uz datu subjektu. Tās mērķis drīzāk ir novērst neproporcionālu ietekmi. Tā ir būtiska atšķirība. Piemēram, pētījumos pamatots un precīzs laikraksta raksts par iespējamu korupciju valdībā var kaitēt attiecīgo valdības ierēdņu reputācijai un var radīt ievērojamas sekas, tai skaitā reputācijas zaudēšanu, vēlētāju balsu zaudēšanu vai pat apcietinājumu, tomēr pat šādā gadījumā kā pamatojumu var izmantot 7. panta f) punktu[95].

(c) Pagaidu līdzsvars

Līdzsvarojot iepriekš aprakstītās intereses un tiesības, personas datu apstrādātāja veiktie pasākumi, lai ievērotu tā vispārējās direktīvā noteiktās saistības (tai skaitā attiecībā uz proporcionalitāti un pārredzamību), būtiski sekmēs personas datu apstrādātāja atbilstību 7. panta f) punkta prasībām. Pilnīga atbilstība nozīmētu, ka ir mazināta ietekme uz personām, ka ir *mazāk ticams*, ka tiks pārkāptas datu subjektu intereses vai pamattiesības un brīvības, un ka tāpēc ir *ticamāks*, ka personas datu apstrādātājs var atsaukties uz 7. panta f) punktu. Tam būtu jāmudina personas datu apstrādātāji labāk ievērot visus direktīvas horizontālos noteikumus[96].

Tomēr tas nenozīmē, ka ar šo horizontālo prasību ievērošanu būs pietiekami, lai nodrošinātu juridisku pamatu saskaņā ar 7. panta f) punktu. Patiesi, šādā gadījumā 7. panta f) punkts nebūtu vajadzīgs vai arī kļūtu par iespēju apiet noteikumus, padarot bezjēdzīgu visu 7. pantu, kurā aicināts apstrādei nodrošināt pienācīgu un konkrētu juridisko pamatu.

Tādēļ gadījumos, kad saskaņā ar sākotnējo analīzi nav skaidrs, kā panākt līdzsvaru, ir svarīgi veikt turpmāku līdzsvara samēra noteikšanas novērtējumu. Personas datu apstrādātājs var apsvērt, vai ir iespējams ieviest papildu pasākumus, kas pārsniedz pasākumus, ar kuriem nodrošina atbilstību direktīvas horizontālajiem noteikumiem, lai mazinātu apstrādes nepamatotu ietekmi uz datu subjektiem.

Papildu pasākumi var ietvert, piemēram, viegli izmantojamas un pieejamas sistēmas izveidi, lai datu subjektiem nodrošinātu beznosacījuma iespēju atteikties no datu apstrādes. Šie papildu pasākumi var dažos (taču ne visos) gadījumos palīdzēt panākt līdzsvaru un nodrošināt, ka apstrādes pamatā var būt 7. panta f) punkts, vienlaikus arī aizsargājot datu subjektu tiesības un intereses.

(d) Personas datu apstrādātāja lietoti papildu drošības pasākumi

Kā paskaidrots iepriekš, veids, kādā personas datu apstrādātājs piemēro attiecīgus pasākumus, dažos gadījumos var palīdzēt mainīt līdzsvara samēru. Tas, vai rezultāts būs pieņemams, būs atkarīgs no novērtējuma kopumā. Jo būtiskāka ietekme uz datu subjektiem, jo lielāka uzmanība jāpievērš attiecīgajiem drošības pasākumiem.

Šādi attiecīgi pasākumi cita starpā var būt datu vākšanas veida stingri ierobežojumi vai arī tūlītēja datu dzēšana pēc to izmantošanas. Lai gan saskaņā ar direktīvu daži no šiem

[95] Kā paskaidrots iepriekš, jāņem vērā arī visas direktīvas 9. pantā minētās attiecīgās atkāpes personas datu apstrādei, kas veikta žurnālistikas nolūkiem.

[96] Saistībā ar "horizontālās atbilstības" lielo nozīmi skatiet arī darba grupas Atzinuma 3/2013 par nolūka ierobežojumu (iepriekš minēts 9. zemsvītras piezīmē) 54. lpp.

pasākumiem jau ir obligāti, bieži vien tos var piemērot dažādos mērogos, un personas datu apstrādātājiem ir iespēja nodrošināt datu subjektu labāku aizsardzību. Piemēram, personas datu apstrādātājs var vākt mazāk datu vai sniegt vairāk informācijas, nekā konkrēti norādīts direktīvas 10. un 11. pantā.

Dažos citos gadījumos drošības pasākumi direktīvā nav *skaidri* prasīti, taču var tikt prasīti turpmāk saskaņā ar ierosināto regulu vai arī var tikt prasīti tikai konkrētos apstākļos, piemēram:

- tehniski un organizatoriski pasākumi, lai nodrošinātu, ka datus nevar izmantot, lai pieņemtu lēmumus vai veiktu citas darbības attiecībā uz personām (‘‘funkcionālais nošķīrums’’, kas bieži tiek īstenots pētniecības kontekstā);
- anonimizācijas metožu plaša izmantošana;
- datu summēšana;
- privātuma uzlabošanas tehnoloģijas, ‘‘projektētā’’ privātuma princips, privātuma un datu aizsardzības ietekmes novērtējumi;
- labāka pārredzamība;
- vispārējas beznosacījuma atteikšanās tiesības;
- datu pārnesamība un saistīti pasākumi datu subjektu tiesību stiprināšanai.

Darba grupa atzīmē, ka attiecībā uz dažiem svarīgākajiem jautājumiem, tostarp funkcionālo nošķīrumu un anonimizācijas metodēm, darba grupa jau ir sniegusi noteiktus norādījumus savu atzinumu par nolūka ierobežojumu, par brīvi pieejamiem datiem un par anonimizācijas metodēm attiecīgajās sadaļās.[97]

Attiecībā uz pseidonimizāciju un šifrēšanu darba grupa vēlas uzsvērt, ka gadījumā, ja dati nav tiešā veidā identificējami, tas pēc būtības neietekmē datu apstrādes likumības novērtēšanu — to nedrīkst uztvert kā iespēju nelikumīgu apstrādi pārvērst par likumīgu[98].

Tajā pašā laikā pseidonimizācija un šifrēšana gluži tāpat kā jebkādi citi tehniski un organizatoriski pasākumi, kas ir ieviesti personiskās informācijas aizsargāšanai, būs svarīgi, novērtējot apstrādes potenciālo ietekmi uz datu subjektu, tādēļ tiem dažkārt var būt nozīme, lai radītu pārsvaru personas datu apstrādātāja pusē. Izmantojot mazāk riskantus personas datu apstrādes veidus (piemēram, personas datu šifrēšana uzglabāšanas vai pārsūtīšanas laikā vai tādi personas dati, kas ir netiešāki un ne tik viegli identificējami), kopumā datu subjektu interešu vai pamattiesību un brīvību pārkāpšanas ticamība tiks mazināta.

Attiecībā uz šiem drošības pasākumiem un līdzsvara kopējo novērtējumu darba grupa vēlas uzsvērt trīs konkrētus aspektus, kuriem 7. panta f) punkta kontekstā bieži vien ir liela nozīme:

- attiecība starp līdzsvarošanas pārbaudi, pārredzamību un pārskatatbildības principu;

[97] Sk. darba grupas Atzinuma 3/2013 par nolūka ierobežojumu (iepriekš minēts 9. zemteksa piezīmē) III.2.3. un III.2.5. sadaļu, kā arī 2. pielikumu par turpmāku apstrādi vēsturiskos, statistiskos un zinātniskos nolūkos, kā arī par lielapjoma datiem un brīvi pieejamiem datiem. Skatiet arī darba grupas Atzinuma 6/2013 par brīvi pieejamiem datiem (iepriekš minēts 88. zemteksa piezīmē), kā arī Atzinuma 5/2014 par anonimizācijas metodēm attiecīgās daļas.

[98] Šajā saistībā skatiet grozījumus, par kuriem *LIBE* komiteja nobalsoja *LIBE* komitejas galīgajā ziņojumā, un jo īpaši 15. grozījumu par 38. apsvērumu, kurā izveidota saikne starp pseidonimizāciju un datu subjekta tiesisko paļāvību.

- datu subjekta tiesības iebilst pret apstrādi, kā arī papildus iebildumu paušanai — atteikuma iespēja bez nepieciešamības norādīt pamatojumu;
- iespējas datu subjektiem — datu pārnesamība un funkcionējoša mehānisma pieejamība, lai datu subjekti varētu mainīt, izdzēst, pārsūtīt vai kā citādi papildus apstrādāt (vai ļaut trešām personām papildus apstrādāt) savus datus vai piekļūt tiem.

Šo tematu svarīguma dēļ tie apskatīti atsevišķās sadaļās.

III.3.5. Pārskatatbildība un pārredzamība

Pirms apstrādes pasākumu veikšanas saskaņā ar 7. panta f) punktu personas datu apstrādātāja pienākums ir vispirms novērtēt, vai tam ir likumīgas intereses, vai apstrāde ir vajadzīga šādu likumīgu un interešu īstenošanai un vai konkrētā gadījumā datu subjektu intereses un tiesības nav pārākas par apstrādātāja interesēm.

Šajā ziņā 7. panta f) punkta pamatā ir pārskatatbildības princips. Personas datu apstrādātājam ir sākotnēji jāveic rūpīga un efektīva pārbaude, pamatojoties uz lietas konkrētajiem faktiem, nevis abstraktiem pieņēmumiem, ņemot vērā arī datu subjektu pamatotās gaidas. Lai nodrošinātu labu praksi, attiecīgā gadījumā ir pietiekami detalizēti un pārredzami jādokumentē šīs pārbaudes process, lai attiecīgās ieinteresētās personas (tostarp datu subjekti un datu aizsardzības iestādes, kā arī galu galā — tiesas) vajadzības gadījumā varētu pārliecināties par pārbaudes pilnīgu un pareizu piemērošanu.

Personas datu apstrādātājam vispirms jādefinē likumīgās intereses un jāveic līdzsvarošanas pārbaude, taču tas nebūt nav pilnīgs un galīgs novērtējums — ja faktiski īstenotās intereses atšķiras no personas datu apstrādātāja norādītajām interesēm vai ja personas datu apstrādātājs intereses nav definējis pietiekami detalizēti, līdzsvars ir jānovērtē atkārtoti, pamatojoties uz faktiskajām interesēm, kuras nosaka vai nu datu aizsardzības iestāde, vai tiesa.[99] Tāpat kā attiecībā uz citiem datu aizsardzības pamataspektiem, piemēram, personas datu apstrādātāja identificēšanu vai nolūka noteikšanu[100], būtiska ir personas datu apstrādātāja apgalvojumu patiesā realitāte.

Pārskatatbildības jēdziens ir cieši saistīts ar pārredzamības jēdzienu. Lai datu subjekti varētu īstenot savas tiesības un lai ieinteresētās personas varētu daudz plašāk veikt publiskas pārbaudes, darba grupa iesaka personas datu apstrādātājiem saprotami un lietotājam draudzīgā veidā izskaidrot datu subjektiem iemeslus, kāpēc tie uzskata, ka datu subjektu intereses vai pamattiesības un brīvības nav pārākas par apstrādātāju interesēm, un arī izskaidrot drošības pasākumus, kas veikti, lai aizsargātu personas datus, tostarp attiecīgā gadījumā — tiesības atteikties no apstrādes.[101]

---

[99] Piemēram, pēc sūdzības iesniegšanas vai iebildumu celšanas saskaņā ar 14. pantu.

[100] Sk. 9. zemsvītras piezīmē minētos atzinumus.

[101] Kā paskaidrots darba grupas Atzinuma 3/2013 par nolūka ierobežojumu (iepriekš minēts 9. zemsvītras piezīmē) 46. lpp. attiecībā uz profilēšanu un automātisko lēmumu pieņemšanu — "lai nodrošinātu pārredzamību, datu subjektiem/ patērētājiem jāļauj piekļūt saviem "profiliem", kā arī lēmumu pieņemšanas loģikai (algoritmam), ar kuru izveidots profils. Citiem vārdiem sakot — organizācijām ir jāatklāj savi lēmumu pieņemšanas kritēriji. Tas ir būtisks drošības pasākums un ir vēl jo svarīgāks attiecībā uz lielapjoma datiem." Neatkarīgi no tā, vai organizācija nodrošina šādu pārredzamību, tas ir ļoti būtisks aspekts, kas jāņem vērā arī līdzsvara samēra noteikšanā.

Šajā saistībā darba grupa uzsver, ka šajā gadījumā ļoti svarīgi ir arī patērētāju aizsardzības tiesību akti un jo īpaši likumi, kas patērētājus aizsargā pret negodīgu komercpraksi.

Ja personas datu apstrādātājs līguma mazajā drukā rakstītajos juridiskajos noteikumos slēpj svarīgu informāciju par datu neparedzētu turpmāku izmantošanu, šādi var tikt pārkāpti patērētāju aizsardzības noteikumi par negodīgiem līgumu noteikumiem (tostarp "pārsteidzošu noteikumu" aizliegumu), un tas arī neatbilst 7. panta a) punkta prasībām par derīgu un informētu jeb apzinātu piekrišanu vai 7. panta f) punkta prasībām attiecībā uz datu subjekta pamatotām gaidām un vispārēju pieņemamu interešu līdzsvaru. Protams, rastos arī jautājumi par 6. panta ievērošanu attiecībā uz personas datu godīgas un likumīgas apstrādes nepieciešamību.

Piemēram, vairākos gadījumos "bezmaksas" tiešsaistes pakalpojumu (piemēram, meklēšanas, e-pasta, sociālo tīklu, failu krātuvju vai citu tiešsaistes vai mobilo lietojumprogrammu) lietotāji pilnībā neapzinās to, cik lielā mērā viņu darbības tiek reģistrētas un analizētas, lai radītu vērtību pakalpojuma sniedzējam, un tāpēc viņi neapzinās iespējamos riskus.

Lai šādos gadījumos stiprinātu datu subjektu tiesības, pirmais nepieciešamais (taču nekādā gadījumā pats par sevi pietiekams) priekšnoteikums[102] ir skaidra norāde, ka pakalpojums nav bezmaksas pakalpojums un ka drīzāk patērētāji maksā ar savu personas datu izmantošanu. Lai nodrošinātu 7. panta a) punktā minētās piekrišanas derīgumu vai 7. panta f) punktā noteikto labvēlīgo līdzsvaru, katrā gadījumā ir arī skaidri jānorāda nosacījumi un drošības pasākumi, saskaņā ar kuriem datus atļauts izmantot.

III.3.6. Tiesības iebilst un citas tiesības

a) Tiesības iebilst saskaņā ar Direktīvas 14. pantu

Direktīvas 7. panta e) punkta un f) punkts ir īpaši tādā ziņā, ka, lai gan galvenokārt to pamatā ir iesaistīto interešu un tiesību objektīvs novērtējums, tie arī ļauj iesaistīt datu subjekta pašnoteikšanos (tiesības iebilst)[103] — vismaz šo divu pēdējo pamatojumu gadījumā direktīvas 14. panta a) punktā ir noteikts, ka ("ja vien attiecīgās valsts tiesību akti neparedz citādi") datu subjekts "var jebkurā laikā uz viņa konkrēto situāciju attiecināmu nenoraidāmu likumīgu iemeslu dēļ iebilst pret datu apstrādi, kas attiecas uz viņu". Tajā arī norādīts, ka gadījumā, ja iebildums ir pamatots, personas datu apstrāde jāpārtrauc.

Principā saskaņā ar pašreizējiem tiesību aktiem datu subjektam šādā gadījumā būs jādemonstrē "nenoraidāmas likumīgas intereses" apturēt viņa personas datu apstrādi (14. panta a) punkts), izņemot attiecībā uz tiešās tirgvedības pasākumiem, kad iebildumi nav jāpamato (14. panta b) punkts).

---

[102] Par potenciāliem papildu drošības pasākumiem attiecībā uz arvien biežāk izplatītākām situācijām, kad patērētāji maksā ar saviem personas datiem, skatiet III.3.6. sadaļu, jo īpaši 47.–48. lpp.: "Datu aizsardzībai draudzīgas alternatīvas "bezmaksas" tiešsaistes pakalpojumiem" un "Datu pārnesamība, "midata" un saistītie jautājumi."

[103] Tiesības iebilst nedrīkst jaukt ar piekrišanu saskaņā ar 7. panta a) punktu, kad personas datu apstrādātājs nedrīkst apstrādāt datus, kamēr nav iegūta šāda piekrišana. 7. panta f) punkta kontekstā personas datu apstrādātājs var apstrādāt datus, ja ir ievēroti nosacījumi un veikti drošības pasākumi un kamēr nav iebildis datu subjekts. Šajā ziņā tiesības iebilst drīzāk uzskatāmas par īpašu atteikšanās veidu. Detalizētāku informāciju sk. darba grupas Atzinumā 15/2011 par jēdziena "piekrišana" definīciju (minēts 2. zemsvītras piezīmē).

Tā nav jāuztver kā pretruna 7. panta f) punktā minētajai līdzsvarošanas pārbaudei, kas tiek veikta *a priori* — tas drīzāk papildina šo līdzsvara noteikšanu tādā ziņā, ka gadījumā, kad turpmāka apstrāde ir atļauta pēc tam, kad pamatotā un objektīvā veidā ir novērtētas dažādās iesaistītās tiesības un intereses, datu subjektam joprojām būs *papildu* iespēja iebilst, pamatojoties uz faktiem, kas saistīti ar viņa konkrēto situāciju. Pēc tam būs jāveic jauns novērtējums, ņemot vērā datu subjekta iesniegtos konkrētos argumentus. Principā šis jaunais novērtējums ir atkal jāpārbauda datu aizsardzības iestādei vai tiesām.

b) Papildus iebilšanas iespējai — atteikšanās kā papildu drošības pasākuma nozīme

Darba grupa uzsver, ka, pat ja attiecībā uz 14. panta a) punktā norādītajām tiesībām iebilst datu subjektam ir jānorāda pamatojums, personas datu apstrādātājam nekas neaizliedz piedāvāt atteikšanās iespēju, kura būtu plašāka un attiecībā uz kuru datu subjektam nebūtu papildus jādemonstrē likumīgas intereses (nenoraidāmas vai citādas). Šādu beznosacījuma tiesību pamatā nedrīkstētu būt datu subjektu konkrētie apstākļi.

Īpaši robežgadījumos, kad līdzsvara samēru ir grūti noteikt, labi izstrādātam un funkcionālam atteikšanās mehānismam varētu būt svarīga nozīme, lai aizsargātu datu subjektu tiesības un intereses, pat ja tas datu subjektiem nenodrošinātu visus elementus, kas atbilstu 7. panta a) punktā minētajai derīgai piekrišanai.

Šādos apstākļos ir nepieciešama niansēta pieeja, kurā tiek nošķirti gadījumi, kad vajadzīga 7. panta a) punktā noteiktā piekrišana par piedalīšanos, un gadījumi, kad funkcionējoša iespēja atteikties no apstrādes (kopā ar citiem papildu pasākumiem) var nodrošināt datu subjektu aizsardzību saskaņā ar 7. panta f) punktu.

Jo plašāk piemērojams atteikšanās mehānisms un vieglāk to izmantot, jo vairāk tas palīdzēs nodrošināt pārsvaru apstrādes pusē, lai kā juridisko pamatojumu izmantotu 7. panta f) punktu.

Ilustrācija: pieejas attīstība attiecībā uz tiešo tirgvedību

Lai ilustrētu, kā gadījumus, kad nepieciešama 7. panta a) punktā minētā piekrišana, atšķirt no gadījumiem, kad kā drošības līdzekli saskaņā ar 7. panta f) punktu varētu izmantot atteikšanās iespēju, ir noderīgi izmantot tiešās tirgvedības piemēru, attiecībā uz kuru direktīvas 14. panta b) punktā tradicionāli ir iekļauts īpašs noteikums par atteikšanos. Lai risinātu jautājumus saistībā ar tehnoloģiskās attīstības jaunumiem, šo noteikumu vēlāk papildināja ar īpašiem noteikumiem E-privātuma direktīvā[104].

Saskaņā ar E-privātuma direktīvas 13. pantu attiecībā uz noteiktiem (aizskarošākiem) tiešās tirgvedības pasākumiem (piemēram, tirgvedība ar e-pasta starpniecību un automatizētās zvanīšanas mašīnas) piekrišana ir obligāta. Izņēmuma gadījumā, kad jau izveidotās attiecībās ar klientu personas datu apstrādātājs reklamē savus "līdzīgos" produktus vai pakalpojumus, pietiek norādīt (beznosacījuma) atteikuma iespēju bez pamatojuma.

[104] Saistībā ar E-privātuma direktīvas 13. pantu skatiet arī darba grupas Atzinuma 3/2013 par nolūka ierobežojumu (iepriekš minēts 9. zemsvītras piezīmē) III.2.4. sadaļu.

Tomēr tehnoloģijas ir attīstījušās, tāpēc saistībā uz jauniem tirgvedības veidiem ir vajadzīgi līdzīgi un relatīvi vienkārši risinājumi, kuros ievērota tāda pati loģika.

Pirmkārt, ir attīstījies tirgvedības materiālu piegādes veids — vienkāršu e-pasta ziņojumu vietā, kas tika saņemti elektroniskajās pastkastītēs, tagad mērķtiecīgas, uz uzvedību balstītas reklāmas uznirstošos logos tiek parādītas arī viedtālruņu un datoru ekrānos. Iespējams, drīzumā reklāmas tiks arī iekļautas viedos priekšmetos, kas būs savstarpēji saistīti ar "lietu internetu".

Otrkārt, reklāmas kļūst arvien mērķtiecīgākas — to pamatā vairs nav tikai vienkārši klientu profili, un klientu aktivitātes tiek arvien vairāk izsekotas un informācija par tām saglabāta tiešsaistē un bezsaistē, kā arī analizēta ar aizvien sarežģītākām automatizētām metodēm[105].

Šo jauninājumu rezultātā ir mainījies līdzsvarošanas pārbaudes saturs — runa vairs nav par tiesībām uz nekomerciālu vārda brīvību, bet gan galvenokārt par uzņēmējdarbības organizāciju ekonomiskajām interesēm iegūt informāciju par saviem klientiem, izsekojot un pārraugot to aktivitātes tiešsaistē un bezsaistē, kas ir jālīdzsvaro ar šo personu (pamat)tiesībām uz privātumu un personas datu aizsardzību, kā arī to interesēm netikt nepamatoti uzraudzītiem.

Šīs valdošo uzņēmējdarbības modeļu pārmaiņas un personas datu kā uzņēmējdarbības organizāciju aktīvu vērtības palielināšanās izskaidro neseno prasību šajā kontekstā nodrošināt piekrišanu saskaņā ar E-privātuma direktīvas 5. panta 3. punktu un 13. pantu.

Tādēļ atkarībā no tirgvedības veida pastāv dažādi īpaši noteikumi, tostarp:

- beznosacījuma tiesības iebilst pret tiešo tirgvedību (attiecībā uz tradicionālo pastu, kā arī līdzīgu produktu tirgvedību) atbilstīgi direktīvas 14. panta b) punktam; šādā gadījumā kā juridisko pamatojumu var izmantot 7. panta f) punktu;
- prasība iegūt piekrišanu saskaņā ar E-privātuma direktīvas 13. pantu attiecībā uz automātiskām zvanīšanas sistēmām, faksu, īsziņām un tirgvedību ar e-pasta starpniecību (ar izņēmumiem) [106], kā arī faktiska Datu aizsardzības direktīvas 7. panta a) punkta piemērošana;
- prasība iegūt piekrišanu saskaņā ar E-privātuma direktīvas 5. panta 3. punktu (un Datu aizsardzības direktīvas 7. panta a) punktu) attiecībā uz reklāmu, kas balstīta uz uzvedību, izmantojot tādas izsekošanas metodes kā sīkfailu saglabāšanas informāciju lietotāja galaiekārtā[107].

Lai gan attiecībā uz E-privātuma direktīvu saskaņā ar 5. panta 3. punktu un 13. pantu piemērojamie juridiskie pamatojumi ir nepārprotami, visi tirgvedības veidi nav iekļauti, tāpēc būtu vēlams izveidot norādījumus par to, kādos apstākļos nepieciešama 7. panta a) punktā noteiktā piekrišana un kuros gadījumos jāpanāk līdzsvars saskaņā ar 7. panta f) punktu, tai skaitā nodrošinot atteikšanās iespēju.

[105] Sk. darba grupas Atzinuma 3/2013 par nolūka ierobežojumu (iepriekš minēts 9. zemsvītras piezīmē) III.2.5. sadaļu un 2. pielikumu.

[106] Skatiet arī E-privātuma direktīvas 13. panta 3. punktu, kurā dalībvalstīm ļauts izvēlēties starp piekrišanu un atteikšanos no tiešās tirgvedības pasākumiem, izmantojot citas metodes.

[107] Informācijai par šī noteikuma piemērošanu skatiet darba grupas Atzinumu 2/2010 par biheiviorālo reklāmu tiešsaistē (WP171).

Šajā saistībā ir noderīgi atcerēties darba grupas atzinumu par nolūka ierobežojumu, kur ir konkrēti norādīts, ka "gadījumā, ja organizācija īpaši vēlas analizēt vai prognozēt atsevišķu klientu personīgās izvēles, uzvedību un attieksmi, kas turpmāk ietekmēs pasākumus vai lēmumus, kuri tiks pieņemti attiecībā uz šiem klientiem [..], gandrīz vienmēr būs vajadzīga bezmaksas, konkrēta, apzināta un nepārprotama piekrišana dalībai. Pretējā gadījumā turpmāku izmantošanu nevar uzskatīt par atbilstošu. Svarīgi, ka šāda piekrišana ir vajadzīga, piemēram, lai veiktu izsekošanu un profilēšanu tiešās tirgvedības, uz uzvedību balstītas reklāmas, datu tirdzniecības, ar atrašanās vietu saistītas reklāmas vai ar izsekošanu saistītas digitālā tirgus izpētes nolūkos."[108].

Datu aizsardzībai draudzīgas alternatīvas "*bezmaksas*" *tiešsaistes pakalpojumiem*

Gadījumos kad, klienti reģistrējas "bezmaksas" tiešsaistes pakalpojumu izmantošanai, bet faktiski "maksā" par šiem pakalpojumiem, atļaujot izmantot savus personas datus, līdzsvars tiktu novērtēts pozitīvi vai tiktu konstatēts, ka patērētājam ir reāla izvēles brīvības un tādēļ saskaņā ar 7. panta a) punktu ir sniegta derīga piekrišana, ja personas datu apstrādātājs piedāvātu arī savu pakalpojumu alternatīvu versiju, kurā "personas dati" netiktu izmantoti tirgvedības nolūkiem.

Ja šādi alternatīvi pakalpojumi nav pieejami, kļūst grūtāk argumentēt, ka saskaņā ar 7. panta a) punktu ir sniegta derīga (brīvi pausta) piekrišana tāpēc vien, ka ir izmantoti bezmaksas pakalpojumi, vai ka pārsvars saskaņā ar 7. panta f) punktu ir jānodrošina personas datu apstrādātāja pusē.

Ar iepriekš izklāstītajiem apsvērumiem uzsvērta papildu drošības pasākumu (tai skaitā funkcionējoša mehānisma, lai atteiktos no apstrādes) lielā nozīme, lai mainītu pagaidu līdzsvaru. Tajā pašā laikā tajos arī norādīts, ka, lai varētu veikt apstrādi, dažos gadījumos kā apstrādes pamatojumu nevar izmantot 7. panta f) punktu, un personas datu apstrādātājiem jānodrošina derīga piekrišana saskaņā ar 7. panta a) punktu vai jānodrošina atbilstība citiem direktīvas nosacījumiem.

Datu pārnesamība, "midata" *un saistītie jautājumi*

Attiecībā uz papildu drošības pasākumiem, kas varētu palīdzēt nodrošināt līdzsvaru, īpaša uzmanība jāpievērš datu pārnesamībai un saistītajiem pasākumiem, kas var būt vēl jo svarīgāki tiešsaistes vidē. Darba grupa atgādina par savu atzinumu par nolūka ierobežojumu, kur tā uzsvērusi, ka "daudzos gadījumos tādi drošības pasākumi kā iespēja datu subjektiem/ klientiem tiešā veidā piekļūt saviem datiem portatīvā, lietotājam draudzīgā un ar mašīnlasāmā formātā var palīdzēt stiprināt to tiesības un kompensēt ekonomisko nelīdzsvarotību starp lielajām korporācijām, no vienas puses, un datu subjektiem / patērētājiem, no otras puses. Tas arī ļautu personām dalīties ar lielapjoma datu radīto labklājību un rosinātu izstrādātājus lietotājiem piedāvāt papildu līdzekļus un lietojumprogrammas[109].

[108] Sk. atzinuma (iepriekš minēts 9. zemsvītras piezīmē) II pielikumu (par lielapjoma datiem un brīvi pieejamiem datiem), 45. lpp.

[109] Sk. tādas iniciatīvas kā "midata" Apvienotajā Karalistē, kuru galvenais pamatprincips ir tas, ka dati ir jānodod atpakaļ patērētājiem. "Midata" ir brīvprātīga programma, un paredzams, ka laika gaitā klientiem būs arvien lielākas piekļuves iespējas saviem personas datiem portatīvā/elektroniskā formātā. Galvenā ideja ir tā, ka arī patērētājiem ir jāgūst labums no lielapjoma datiem, piekļūstot savai informācijai, lai varētu izdarīt labāku izvēli. Skatiet arī "zaļās pogas" iniciatīvas, kas ļauj patērētājiem piekļūt informācijai par savu enerģijas lietojumu.

Tādu funkcionējošu mehānismu pieejamība, kas ļauj datu subjektiem mainīt, izdzēst, pārsūtīt vai kā citādi papildus apstrādāt (vai ļaut trešām personām papildus apstrādāt) savus datus, kā arī piekļūt tiem, stiprinās datu subjektu tiesības un ļaus tiem gūt lielāku labumu no digitālajiem pakalpojumiem. Turklāt tas var veicināt konkurētspējīgākas tirgus vides veidošanos, ļaujot patērētājiem vieglāk mainīt pakalpojumu sniedzējus (piemēram, attiecībā uz internetbanku pakalpojumiem vai enerģijas piegādātājiem viedtīkla vidē). Visbeidzot, tas var arī sekmēt papildu pakalpojumu ar pievienoto vērtību attīstību, ko piedāvā trešās personas, kuras var piekļūt klientu datiem pēc klientu pieprasījuma un saskaņā ar to piekrišanu. Tāpēc, raugoties no šāda skatpunkta, datu pārnesamība sniedz labumu ne vien datu aizsardzībai, bet arī konkurētspējai un patērētāju aizsardzībai[110].

IV. Nobeiguma apsvērumi

Šajā atzinumā darba grupa analizēja direktīvas 7. pantā izklāstītos kritērijus par to, kā datu apstrādi padarīt likumīgu. Papildus norādījumiem par 7. panta f) punkta praktisko interpretāciju un piemērošanu saskaņā ar pašreizējo tiesisko regulējumu tās mērķis ir formulēt politikas ieteikumus, lai sniegtu atbalstu politikas veidotājiem, kad tie apsvērs izmaiņas, kas veicamas pašreizējā datu aizsardzības tiesiskajā regulējumā. Pirms šo ieteikumu izklāsta turpmāk ir apkopoti galvenie secinājumi attiecībā uz 7. panta interpretāciju.

IV.1. Secinājumi

Direktīvas *7. panta pārskats*

Direktīvas 7. pantā noteikts, ka personas datus apstrādā tikai tādā gadījumā, ja ir piemērojams vismaz viens no sešiem šajā pantā minētajiem juridiskajiem pamatojumiem.

Pirmajā pamatojumā (7. panta a) punktā) uzmanība ir pievērsta datu subjekta piekrišanas principam kā likumīguma pamatojumam. Pārējie pamatojumi pieļauj apstrādi (ja ir veikti drošības pasākumi) gadījumos, kad neatkarīgi no piekrišanas datus var apstrādāt un tie ir jāapstrādā noteiktā kontekstā, lai īstenotu konkrētas likumīgas intereses.

Panta b), c), d) un e) punktā ir norādīti konkrēti konteksti, kādos personas datu apstrādi var uzskatīt par likumīgu. Īpaša uzmanība jāpievērš nosacījumiem, kas ir spēkā šajos atšķirīgajos kontekstos, jo tie nosaka dažādo likumīguma pamatojumu piemērošanas jomu. Konkrēti — kritēriji "vajadzīga līguma [..] izpildei", "vajadzīga, lai izpildītu [..] juridiskas saistības", "vajadzīga, lai aizsargātu datu subjekta būtiskas intereses" un "vajadzīga sabiedrības interesēs realizējama uzdevuma izpildei vai [..] oficiālo pilnvaru realizācijai" paredz dažādas prasības, kas ir apspriestas III.2. sadaļā.

Ar f) punktu vispārīgākā formā apzīmē personas datu apstrādātāja (jebkāda veida) likumīgās intereses (jebkādā kontekstā). Tomēr attiecībā uz šo vispārīgo noteikumu ir īpaši norādīts, ka jāveic līdzsvarošanas pārbaude, kurā jāsalīdzina personas datu apstrādātāja vai jebkādu trešo

---

Plašāka informācija par iniciatīvām Apvienotajā Karalistē un Francijā ir atrodama tīmekļa vietnēs http://www.midatalab.org.uk/ un http://mesinfos.fing.org/.

[110] Par tiesībām uz datu pārnesamību skatiet ierosinātās regulas 18. pantu.

personu, kurām atklāti dati, likumīgās intereses attiecībā pret datu subjekta interesēm vai pamattiesībām.

Direktīvas *7. panta f) punkta nozīme*

Direktīvas 7. panta f) punktu nedrīkst uztvert kā juridisku pamatojumu, ko var izmantot vienīgi retos gadījumos, lai rastu risinājumu retās vai neparedzētās situācijās "kā pēdējo līdzekli" vai pēdējo iespēju, ja citus pamatojumus izmantot nevar. Tomēr to arī nevajadzētu uztvert kā vēlamo variantu un tā lietojumu nevajadzētu nepamatoti paplašināt, uzskatot, ka tas ir mazāk ierobežojošs nekā citi pamatojumi. Drīzāk tas ir tikpat derīgs līdzeklis kā jebkurš cits personas datu apstrādes likumīguma pamatojums.

Izmantojot 7. panta f) punktu piemēroti, pareizos apstākļos un ievērojot pienācīgus drošības pasākumus, var arī novērst citu juridisko pamatojumu ļaunprātīgu izmantošanu vai pārmērīgu paļaušanos uz tiem. Pienācīga līdzsvara samēra novērtēšana saskaņā ar 7. panta f) punktu (bieži vien ar izvēles iespēju atteikties no datu apstrādes) dažos gadījumos var būt derīga alternatīva, lai, piemēram, neatbilstīgi neizmantotu "piekrišanas" vai "līguma [..] izpildes" pamatojumu. Raugoties no šāda skatpunkta, 7. panta f) punkts rada papildu drošību, salīdzinot ar citiem iepriekš noteiktiem pamatojumiem. Tādēļ to nevajadzētu uztvert kā "vājāko posmu" vai iespēju padarīt par likumīgu jebkāda veida datu apstrādi, kam neatbilst neviens cits juridiskais pamatojums.

Personas datu apstrādātāja likumīgas intereses / datu subjekta intereses vai pamattiesības

Jēdziens "intereses" ir personas datu apstrādātāja plašāka ieinteresētība apstrādē vai labums, ko personas datu apstrādātājs (vai, iespējams, sabiedrība) gūst no datu apstrādes. Intereses var būt nenoraidāmas, nepārprotamas vai pretrunīgākas. Tādējādi situācijas, uz kurām sniegtas atsauces 7. panta f) punktā, var paredzēt gan pamattiesību īstenošanu vai svarīgu personīgo vai sabiedrības interešu aizsardzību, gan arī mazāk acīm redzamus vai pat problemātiskus kontekstus.

Lai intereses būtu uzskatāmas par "likumīgām" un būtiskām saskaņā ar 7. panta f) punktu, tām jābūt likumīgām, t. i., jāatbilst ES un valsts tiesību aktiem. Lai varētu veikt līdzsvarošanas pārbaudi attiecībā pret datu subjekta interesēm un pamattiesībām, tām arī jābūt pietiekami skaidri un konkrēti definētām. Turklāt tām jābūt reālām un pašreizējām interesēm, proti, tās nedrīkst būt spekulatīvas.

Ja personas datu apstrādātājam vai trešai personai, kurai dati ir atklāti, ir šādas likumīgas intereses, tas nebūt nenozīmē, ka tas var atsaukties uz 7. panta f) punktu kā apstrādes juridisko pamatojumu. Tas, vai var izmantot 7. panta f) punktu, būs atkarīgs no turpmākās līdzsvarošanas pārbaudes. Apstrādei ir arī jābūt vajadzīgai personas datu apstrādātāja vai — atklāšanas gadījumā — trešo personu "likumīgo interešu ievērošanai". Tāpēc vienmēr labāk jāizvēlas mazāk agresīvi līdzekļi, kas ļautu sasniegt tādu pašu mērķi.

Datu subjektu "interešu" jēdziens ir definēts vēl plašāk, jo tas neparedz "likumīguma" aspektu. Ja personas datu apstrādātājs vai trešā persona var īstenot jebkādas intereses, ja vien tās nav nelikumīgas, tad savukārt datu subjektiem jābūt tiesīgiem ņemt vērā to visu veidu intereses un tās salīdzināt ar personas datu apstrādātāja vai trešās personas interesēm, ja vien tās ir būtiskas attiecībā uz direktīvas piemērošanas jomu.

Līdzsvarošanas pārbaudes piemērošana

Interpretējot 7. panta f) punkta piemērošanas jomu, darba grupas mērķis ir izveidot līdzsvarotu pieeju, kas personas datu apstrādātājiem nodrošina vajadzīgo elastību gadījumos, kad netiek radīta nepamatota ietekme uz datu subjektiem, vienlaikus nodrošinot pietiekamu juridisko noteiktību un garantijas datu subjektiem, ka šādas atvērtas formas noteikums netiks izmantots ļaunprātīgi.

Lai veiktu šo līdzsvarošanas pārbaudi, no vienas puses, vispirms ir svarīgi apsvērt likumīgo interešu veidu un avotu, kā arī to, vai šādu interešu īstenošanai ir vajadzīga datu apstrāde, bet, no otras puses — to ietekmi uz datu subjektiem. Veicot šo sākotnējo novērtējumu, ir jāņem vērā tādi pasākumi kā pārredzamība vai datu ierobežota vākšana, ko personas datu apstrādātājs plāno pieņemt, lai ievērotu direktīvu.

Pēc abu pušu analizēšanas un salīdzināšanas var noteikt pagaidu "līdzsvaru" — var izdarīt sākotnējos secinājumus par to, vai personas datu apstrādātāja likumīgās intereses ir pārākas par datu subjektu tiesībām un interesēm. Tomēr var būt gadījumi, kad līdzsvarošanas pārbaudes rezultāti ir neskaidri un pastāv šaubas par to, vai personas datu apstrādātāja (vai trešās personas) likumīgās intereses ir pārākas un vai apstrādes pamatā var būt 7. panta f) punkts.

Tādēļ, veicot līdzsvarošanu, ir svarīgi sagatavot turpmāku novērtējumu. Šajā posmā personas datu apstrādātājs var apsvērt, vai tas var ieviest papildu pasākumus, kas pārsniedz pasākumus, ar kuriem nodrošina atbilstību direktīvas horizontālajiem noteikumiem, lai labāk aizsargātu datu subjektus. Papildu pasākumi var ietvert, piemēram, tādas viegli izmantojamas un pieejamas sistēmas izveidi, lai datu subjektiem nodrošinātu beznosacījuma iespēju atteikties no datu apstrādes.

Galvenie faktori, kas jāņem vērā, piemērojot līdzsvarošanas pārbaudi

Pamatojoties uz iepriekš minēto, līdzsvarošanas pārbaudes īstenošanas laikā jāņem vērā šādi noderīgi faktori:

- <u>likumīgo interešu veids un avots</u>, tai skaitā:

  - tas, vai datu apstrāde jāveic, lai īstenotu pamattiesības, vai
  - tā kā citādi ir sabiedrības interesēs un vai sociāla, kultūras vai juridiska/regulatīva atzīšana attiecīgajā kopienā dod labumu;

- <u>ietekme uz datu subjektiem</u>, tai skaitā:

  - datu veids, piemēram, tas, vai tiek apstrādāti dati, kas uzskatāmi par sensitīviem, vai arī iegūti no publiski pieejamiem avotiem;
  - datu apstrādes veids, tostarp tas, vai dati ir publiski izpausti vai kā citādi darīti pieejami lielam skaitam personu vai arī liels personas datu apjoms tiek apstrādāts vai kombinēts ar citiem datiem (piemēram, profilēšanas gadījumā komerciāliem, tiesībaizsardzības vai citiem nolūkiem);
  - datu subjekta pamatotās gaidas, īpaši attiecībā uz datu izmantošanu un atklāšanu attiecīgajā kontekstā;

- personas datu apstrādātāja un datu subjekta statuss, tai skaitā datu subjekta un personas datu apstrādātāja varas līdzsvars vai tas, ka datu subjekts ir bērns vai pieder pie citas neaizsargātākas iedzīvotāju grupas;

- papildu drošības pasākumi, lai novērstu neatbilstīgu ietekmi uz datu subjektiem, tai skaitā:

  - datu minimizācija (piemēram, datu vākšanas stingri ierobežojumi vai datu tūlītēja izdzēšana pēc to izmantošanas);
  - tehniski un organizatoriski pasākumi, lai nodrošinātu, ka datus nevar izmantot, lai pieņemtu lēmumus vai veiktu citas darbības attiecībā uz personām (“funkcionālais nošķīrums”);
  - anonimizācijas metožu plaša izmantošana, datu summēšana, privātuma uzlabošanas tehnoloģijas, “projektētais” privātums, privātuma un datu aizsardzības ietekmes novērtējumi;
  - labāka pārredzamība, vispārējas beznosacījuma tiesības atteikties, datu pārnesamība un saistītie pasākumi datu subjektu tiesību stiprināšanai.

Pārskatatbildība, pārredzamība, tiesības iebilst un citas tiesības

Saistībā ar šiem drošības pasākumiem un vispārējo līdzsvara novērtējumu attiecībā uz 7. panta f) punktu būtiska nozīme bieži vien ir trīs aspektiem, kuriem jāpievērš īpaša uzmanība:

- noteikta un potenciāla papildu pasākumu nepieciešamība pārredzamības un pārskatatbildības palielināšanai;
- datu subjekta tiesības iebilst pret apstrādi, kā arī papildus iebildumu paušanai — atteikuma iespēja bez nepieciešamības norādīt pamatojumu;
- iespēju nodrošinājums datu subjektiem — datu pārnesamība un funkcionējoša mehānisma pieejamība, lai datu subjekti varētu mainīt, izdzēst, pārsūtīt vai kā citādi papildus apstrādāt (vai ļaut trešām personām papildus apstrādāt) savus datus, kā arī piekļūt tiem.

IV. 2. Ieteikumi

Direktīvas 7. panta f) punkta pašreizējam tekstam ir atvērts formulējums. Šāds elastīgs formulējums ir atstājis iespēju plašai interpretācijai un, kā rāda pieredze, dažkārt izraisījis paredzamības un juridiskās noteiktības trūkumu. Tomēr, ja to izmanto pareizā kontekstā un piemērojot atbilstīgus kritērijus, kā izklāstīts šajā atzinumā, 7. panta f) punktam ir būtiska nozīme kā likumīgas datu apstrādes juridiskajam pamatojumam.

Tāpēc darba grupa atbalsta pašreizējo pieeju, kas pausta ierosinātās regulas 6. pantā, kurā interešu līdzsvars ir saglabāts kā atsevišķs juridiskais pamatojums. Tomēr, lai nodrošinātu līdzsvarošanas pārbaudes atbilstīgu piemērošanu, būtu vēlami papildu norādījumi.

Papildu norādījumu piemērošanas joma un līdzekļi

Būtiska prasība būtu nodrošināt, lai noteikums saglabātu pietiekamu elastību un lai tajā būtu atspoguļota gan personas datu apstrādātāja, gan datu subjekta perspektīva, kā arī attiecīgo kontekstu dinamika. Tādēļ darba grupa uzskata, ka ierosinātajā regulā vai deleģētajos tiesību

aktos nebūtu ieteicams norādīt detalizētu un izsmeļošu tādu situāciju sarakstu, kurās intereses *de facto* tiktu kvalificētas kā likumīgas. Tāpat darba grupa neatbalsta tādu gadījumu definēšanu, kuros vienas puses intereses vai tiesības *principā* vai *saskaņā ar pieņēmumu* ir pārākas par otras puses interesēm vai tiesībām tikai šādu interešu vai tiesību veida dēļ vai tāpēc, ka ir veikti noteikti aizsargpasākumi, piemēram, dati ir tikai pseidonimizēti. Šādi tie varētu būt maldinoši un nevajadzīgi preskriptīvi.

Tā vietā, lai pieņemtu galīgus lēmumus par dažādo tiesību un interešu raksturlielumiem, darba grupa uzstāj uz *līdzsvarošanas pārbaudes būtisko nozīmi,* veicot 7. panta f) punktā paredzēto novērtējumu. Ir jānodrošina pārbaudes elastīgums, taču praksē jāpadara efektīvāka tās īstenošana, kā arī jāparedz efektīvāka atbilstības ievērošana. Tam jākļūst par personas datu apstrādātāju *plašākām pārskatatbildības* saistībām, kad apstrādātājs uzņemas atbildību *demonstrēt*, ka datu subjekta intereses un tiesības nav pārākas par apstrādātāja tiesībām.

Norādījumi un pārskatatbildība

Lai to panāktu, darba grupa iesaka ierosinātajā regulā sniegt norādījumus turpmāk izklāstītajā veidā.

1) Kādā apsvērumā būtu noderīgi identificēt un iekļaut papildināmu sarakstu ar galvenajiem faktoriem, kas jāņem vērā, piemērojot līdzsvarošanas pārbaudi, piemēram, likumīgo interešu veidu un avotu, ietekmi uz datu subjektiem, kā arī papildu drošības pasākumus, ko personas datu apstrādātājs var izmantot, lai novērstu apstrādes nepamatotu ietekmi uz datu subjektiem. Šie drošības pasākumi cita starpā var ietvert:
   - datu funkcionālu nošķīrumu, anonimizācijas metožu atbilstību izmantošanu, šifrēšanu un citus tehniskos un organizatoriskos pasākumus, lai ierobežotu datu subjektu potenciālos riskus;
   - kā arī pasākumus, lai nodrošinātu labāku pārredzamību un izvēli datu subjektiem, piemēram, attiecīgā gadījumā — beznosacījuma un bezmaksas iespēju atteikties no datu apstrādes tādā veidā, ko var viegli un efektīvi izmantot.

2) Darba grupa arī atbalsta papildu precizējumu iekļaušanu ierosinātajā regulā par to, kā personas datu apstrādātājs varētu *demonstrēt*[111] uzlabotu pārredzamību.

   Svarīgs pārskatatbildības aspekts jau ir mainītie nosacījumi, kas ļauj datu subjektiem īstenot savas iebildumu paušanas tiesības, kā paredzēts ierosinātās regulas 19. pantā. Ja datu subjekts iebildīs pret viņa datu apstrādi saskaņā ar 7. panta f) punktu, personas datu apstrādātājam būs jādemonstrē, ka tā intereses ir pārākas. Darba grupa noteikti atbalsta šāda demonstrēšanas pienākuma apvēršanu, jo tas veicina labākas pārskatatbildības saistības.

   Ja personas datu apstrādātājam konkrētā gadījumā neizdodas nodemonstrēt datu subjektam, ka tā intereses ir pārākas, tam var arī būt plašākas sekas attiecībā uz visu apstrādi, nevis tikai attiecībā uz datu subjektu, kurš cēlis iebildumus. Rezultātā personas datu apstrādātājs var apšaubīt vai nolemt reorganizēt visu datu apstrādi, ja tas dod labumu

[111] Šādai demonstrēšanai jābūt pamatotai un vērstai uz rezultātu, nevis administratīvo procesu.

ne vien konkrētajam datu subjektam, bet arī visiem pārējiem datu subjektiem, kuri varētu būt līdzīgā situācijā[112].

Šī prasība ir nepieciešama, taču nav pietiekama. Lai nodrošinātu aizsardzību jau no paša sākuma un novērstu to, ka tiek apieta pierādīšanas pienākuma pārnešana[113], svarīgi veikt pasākumus *pirms* apstrādes sākšanas, nevis retrospektīvu "iebildumu" procesu gaitā.

Tāpēc tiek ierosināts, ka jebkāda veida apstrādes pirmajā posmā personas datu apstrādātājam ir jāveic vairāki pasākumi. Pirmie divi pasākumi varētu būt uzskaitīti ierosinātās regulas apsvērumā, bet trešais — konkrētā noteikumā:

- Veikt novērtējumu[114], kurā jābūt iekļautiem šajā atzinumā izstrādātās un 1. pielikumā apkopotās analīzes dažādajiem posmiem. Personas datu apstrādātājam ir skaidri jāidentificē attiecīgās pārākās intereses, kā arī tas, kādēļ tās ir pārākas par datu subjektu interesēm. Šāds sākotnējs novērtējums nedrīkst radīt pārmērīgu slogu, un tam jābūt *mērogojamam* — to var ierobežot attiecībā uz pamatkritērijiem, ja apstrādes ietekme uz datu subjektiem ir *prima facie* nenozīmīga, savukārt daudz plašāk tas jāveic, ja līdzsvaru ir grūti panākt un, piemēram, vajadzīga vairāku papildu drošības pasākumu pieņemšana. Attiecīgā gadījumā (t. i., kad apstrāde rada konkrētus riskus attiecībā pret datu subjektu tiesībām un brīvībām) jāveic visaptverošāks privātuma un datu aizsardzības ietekmes novērtējums (saskaņā ar ierosinātās regulas 33. pantu), par kura svarīgu daļu var kļūt novērtējums atbilstīgi 7. panta f) punktam.

- Dokumentēt šo novērtējumu. Tāpat kā attiecībā uz veicamā novērtējuma detalizācijas *mērogojamību* arī dokumentācijas apjomam jābūt mērogojamam. Ņemot to vērā,

[112] Papildus pierādīšanas pienākuma apvēršanai darba grupa arī atbalsta to, ka ierosinātajā regulā vairs netiks prasīts, lai iebildumi tiktu pausti "uz [datu subjekta] konkrēto situāciju attiecināmu *nenoraidāmu* likumīgu iemeslu dēļ". Tā vietā saskaņā ar ierosināto regulu pietiktu sniegt atsauci uz jebkādiem (ne vienmēr "nenoraidāmiem") likumīgiem iemesliem attiecībā uz datu subjekta konkrēto situāciju. *LIBE* komitejas galīgajā ziņojumā tika ierosināta papildu iespēja — atmest prasību, ka iebildumam jābūt saistītam ar datu subjekta konkrēto situāciju. Darba grupa atbalsta šādu pieeju tādā ziņā, ka tā iesaka, ka datu subjektiem jābūt iespējai pēc vajadzības izmantot vienu vai abas šīs iespējas, t. i., iebilst, vai nu pamatojoties uz konkrēto situāciju, vai arī vispārīgāk, un šajā pēdējā gadījumā tam nav jāsniedz konkrēts pamatojums. Šajā saistībā skatiet *LIBE* komitejas galīgajā ziņojumā iekļauto grozījumu Nr. 114 attiecībā uz ierosinātās regulas 19. panta 1. punktu.

[113] Piemēram, personas datu apstrādātājiem var būt vilinājums katrā konkrētā gadījumā, izmantojot standarta pamatojumu veidlapas, demonstrēt, ka to intereses ir pārākas, vai tas var kā citādi apgrūtināt iebilšanas tiesību īstenošanu.

[114] Kā iepriekš norādīts 84. zemsvītras piezīmē, šo novērtējumu nevajadzētu jaukt ar visaptverošu privātuma un datu aizsardzības ietekmes novērtējumu. Pašlaik Eiropas mērogā nav visaptverošu norādījumu par ietekmes novērtējumiem, lai gan dažās jomās (attiecībā uz *RFID* un viedo mērīšanu) ir veikti vairāki atzinīgi vērtējami centieni, lai definētu konkrētās nozares metodoloģiju/sistēmu (un/vai modeļus), ko varētu piemērot visās Eiropas Savienībā. Sk. Komisijas viedtīklu darba grupas 2. ekspertu grupas sagatavotos dokumentus "Nozares priekšlikums par *RFID* programmnodrošinājumam paredzēto ietekmes novērtējuma uz privātumu un datu aizsardzību sistēmu" un "Datu aizsardzības ietekmes novērtējuma veidlapa viedtīkliem un viedajām mērīšanas sistēmām". Darba grupa ir sagatavojusi atkārtotus atzinumu saistībā ar abām šīm metodoloģijām.
Turklāt ir arī bijušas vairākas iniciatīvas, lai definētu vispārēju datu aizsardzības ietekmes novērtējuma metodoloģiju, kas var dot labumu centieniem konkrētās nozarēs. Sk., piemēram, projektu *PIAF* (privātuma ietekmes novērtējuma sistēma datu aizsardzībai un tiesībām uz privātumu): http://www.piafproject.eu/.
Turklāt norādījumi valsts mērogā ir atrodami, piemēram, *CNIL* metodoloģijā:
http://www.cnil.fr/fileadmin/documents/en/CNIL-ManagingPrivacyRisks-Methodology.pdf
kā arī *ICO* privātuma ietekmes novērtējuma rokasgrāmatā vietnē
http://ico.org.uk/pia_handbook_html_v2/files/PIAhandbookV2.pdf.

noteiktai pamatdokumentācijai jābūt pieejamai visos gadījumos (izņemot pašus triviālākos) neatkarīgi no tā, vai ir novērtēta apstrādes ietekme uz attiecīgo personu. Tieši pamatojoties uz šādu dokumentāciju, personas datu apstrādātāja novērtējumu var novērtēt papildus un, iespējams, arī apstrīdēt;

- Nodrošināt šādas informācijas pārredzamību un uzskatāmību datu subjektiem un citām ieinteresētajām personām. Pārredzamība jānodrošina gan attiecībā uz datu subjektiem un datu aizsardzības iestādēm, gan attiecīgā gadījumā — sabiedrību kopumā. Attiecībā uz datu subjektiem darba grupa atsaucas uz *LIBE* komitejas ziņojuma projektu[115], kurā norādīts, ka personas datu apstrādātājam ir jāinformē datu subjekts par iemesliem, kāpēc tas uzskata, ka datu subjektu intereses vai pamattiesības un brīvības nav pārākas par apstrādātāja interesēm. Pēc darba grupas domām, šādu informāciju vajadzētu sniegt datu subjektiem kopā ar informāciju, kas personas datu apstrādātajam ir jāsniedz saskaņā ar pašreizējās direktīvas 10. un 11. pantu (ierosinātās regulas 11. pantu). Tas datu subjektiem sniegs iespēju paust iebildumus otrajā posmā, un personas datu apstrādātājam katrā konkrētajā gadījumā būs jāsniedz papildu pamatojums par pārākajām interesēm. Turklāt datu aizsardzības iestādēm pēc pieprasījuma ir jānodrošina dokumentācija, kas ir personas datu apstrādātāja novērtējuma pamatā, lai attiecīgā gadījumā varētu veikt potenciālus pārbaudes un ieviešanas pasākumus.

Darba grupa atbalsta šo trīs pasākumu skaidru iekļaušanu ierosinātajā regulā iepriekš izklāstītajos veidos. Šādi varētu atzīt juridisko pamatojumu īpašo nozīmi, novērtējot likumību, un arī precizēt līdzsvarošanas pārbaudes nozīmi pārskatatbildības pasākumu un ietekmes novērtējumu plašākā kontekstā jaunierosinātajā tiesiskajā regulējumā.

Darba grupa uzskata, ka ir arī ieteicams uzticēt EDAK vajadzības gadījumā sniegt papildu norādījumus, pamatojoties uz šo regulējumu. Izmantojot šādu pieeju, varētu nodrošināt gan pietiekamu teksta skaidrību, gan tā īstenošanas pietiekamu elastīgumu.

[115] Ziņojuma projekts par priekšlikumu Eiropas Parlamenta un Padomes regulai par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Vispārīgā datu aizsardzības regula), (COM(2012) 0011 – C7-0025/2012 – 2012/0011(COD)).

1. pielikums. Īsi norādījumi par 7. panta f) punkta līdzsvarošanas pārbaudes veikšanu

1. posms. Saskaņā ar 7. panta a)–f) punktu potenciāli piemērojamo juridisko pamatojumu novērtējums

Datu apstrādi var veikt vienīgi tad, ja ir piemērojams viens vai vairāki no sešiem 7. panta a)–f) punktā minētajiem pamatojumiem (vienas apstrādes dažādiem posmiem var izmantot dažādus pamatojumus). Ja *prima facie* šķiet, ka kā juridisko pamatojumu var izmantot 7. panta f) punktu, pārejiet pie 2. posma.

Padomi

- Direktīvas 7. panta a) punkts ir piemērojams vienīgi tad, ja tiek piešķirta brīva, apzināta, konkrēta un nepārprotama piekrišana; to, ka persona nav iebildusi apstrādei saskaņā ar 14. pantu, nedrīkst jaukt ar piekrišanu, kura pausta saskaņā ar 7. panta a) punktu — tomēr atbilstīgi 7. panta f) punktam par svarīgu drošības pasākumu var uzskatīt viegli lietojamu mehānismu iebildumu paušanai pret apstrādi.
- Direktīvas 7. panta b) punkts attiecas uz tādu apstrādi, kas ir nepieciešama līguma izpildei; tas vien, ka datu apstrāde ir saistīta ar līgumu vai paredzēta līguma noteikumos, nebūt nenozīmē, ka var piemērot šo pamatojumu; attiecīgā gadījumā kā alternatīvu var apsvērt 7. panta f) punkta izmantošanu.
- Direktīvas 7. panta c) punkts attiecas tikai uz skaidrām un konkrētām juridiskajām saistībām saskaņā ar ES vai dalībvalsts tiesību aktiem; nesaistošu pamatnostādņu (piemēram, tādu, ko sagatavojušas regulatīvās aģentūras) vai ārvalstu juridisko saistību gadījumā kā alternatīvu var apsvērt 7. panta f) punkta izmantošanu.

2. posms. "Likumīgu" vai "nelikumīgu" interešu kvalificēšana

Lai intereses uzskatītu par likumīgām, tām kumulatīvi jāatbilst šādiem nosacījumiem:

- tām jābūt likumīgām (t. i., saskaņā ar piemērojamajiem ES un valstu tiesību aktiem);
- tām jābūt pietiekami skaidri definētām, lai varētu veikt līdzsvarošanas pārbaudi attiecībā pret datu subjekta interesēm un pamattiesībām (t. i., pietiekami konkrētām);
- tām jābūt reālām un pašreizējām interesēm (t. i., tās nedrīkst būt spekulatīvas).

3. posms. Pasākumi, lai noteiktu, vai attiecīgo interešu īstenošanai ir vajadzīga datu apstrāde

Lai nodrošinātu atbilstību šai prasībai, apsveriet, vai nav iespējami citi mazāk agresīvi līdzekļi, lai sasniegtu datu apstrādes noteikto mērķi un ļautu izpildīt personas datu apstrādātāja likumīgās intereses.

4. posms. Pagaidu līdzsvara panākšana, novērtējot, vai datu subjektu pamattiesības un intereses nav pārākas par personas datu apstrādātāja interesēm

- Apsveriet personas datu apstrādātāja interešu veidu (pamattiesības, cita veida intereses, sabiedrības intereses).
- Novērtējiet potenciālo kaitējumu, kas var rasties personas datu apstrādātājam, trešām personām vai plašākai kopienai, ja datu apstrāde netiek veikta.
- Ņemiet vērā datu veidu (vai tie ir sensitīvi šaurākā vai plašākā nozīmē).

- Apsveriet datu subjektu (nepilngadīgais, darba ņēmējs u. c.) un personas datu apstrādātāja (piemēram, vai uzņēmējdarbības organizācija ir dominējošā stāvoklī tirgū) statusu.
- Ņemiet vērā datu apstrādes veidu (lielapjoma apstrāde, datizrace, profilēšana, datu atklāšana lielam skaitam personu vai publicēšana).
- Identificējiet datu subjekta pamattiesības un/vai intereses, kas var tikt ietekmētas.
- Apsveriet datu subjektu pamatotās gaidas.
- Novērtējiet ietekmi uz datu subjektu un salīdziniet to ar labumu, kas gaidāms no personas datu apstrādātāja veiktās apstrādes.

Padoms. Apsveriet faktiskās apstrādes ietekmi uz konkrētām personām — neuztveriet to kā abstraktu vai hipotētisku uzdevumu.

5. posms. Galīgā līdzsvara noteikšana, ņemot vērā papildu drošības pasākumus

Nosakiet un īstenojiet atbilstīgus papildu drošības pasākumus, ko paredz rūpēšanās un rūpības pienākumus, piemēram:
- datu minimizācija (piemēram, datu vākšanas stingri ierobežojumi vai datu tūlītēja izdzēšana pēc to izmantošanas);
- tehniski un organizatoriski pasākumi, lai nodrošinātu, ka datus nevar izmantot, lai pieņemtu lēmumus vai veiktu citas darbības attiecībā uz personām (“funkcionālais nošķīrums”);
- anonimizācijas metožu plaša izmantošana, datu summēšana, privātuma uzlabošanas tehnoloģijas, “projektētais” privātums, privātuma un datu aizsardzības ietekmes novērtējumi;
- labāka pārredzamība, vispārējas beznosacījuma tiesības iebilst (atteikties), datu pārnesamība un saistītie pasākumi datu subjektu tiesību stiprināšanai.

Padoms. Izmantojot privātuma uzlabošanas tehnoloģijas un metodes, pārsvaru var radīt personas datu apstrādātāja pusē, kā arī aizsargāt pašas personas.

6. posms. Atbilstības demonstrēšana un pārredzamības nodrošināšana

- Lai pirms apstrādes sākšanas to pamatotu, sagatavojiet 1.–5. posma uzmetumu.
- Informējiet datu subjektus par iemesliem, kas ļauj uzskatīt, ka pārsvars ir personas datu apstrādātāja pusē.
- Nodrošiniet dokumentācijas pieejamību datu aizsardzības iestādēm.

Padoms. Šis posms ir *mērogojams* — detalizēta informācija par novērtējumu un dokumentācija ir jāpielāgo apstrādes veidam un kontekstam. Pasākumi būs plašāki, ja tiks apstrādāts liels informācijas apjoms par daudzām personām tādā veidā, kas tos var būtiski ietekmēt. Visaptverošs privātuma un datu aizsardzības ietekmes novērtējums (saskaņā ar ierosinātās regulas 33. pantu) būs vajadzīgs tikai tad, ja apstrāde radīs konkrētus riskus attiecībā uz datu subjektu tiesībām un brīvībām. Šajos gadījumos novērtējums saskaņā ar 7. panta f) punktu var kļūt par šāda plašāka ietekmes novērtējuma būtisku daļu.

7. posms. Kā rīkoties, ja datu subjekts īsteno savas iebildumu paušanas tiesības?

- Gadījumos, kad kā drošības pasākums ir pieejamas tikai kvalificētas atteikuma tiesības (tas ir skaidri noteikts 14. panta a) punktā kā minimālais drošības pasākums) — ja datu subjekts iebilst pret apstrādi, jānodrošina, ka tiek ieviests atbilstīgs un lietotājam draudzīgs mehānisms,

lai veiktu līdzsvara atkārtotu novērtēšanu saistībā ar attiecīgo personu un pārtrauktu šīs personas datu apstrādi, ja atkārtotajā novērtējumā tiek pierādīts, ka viņas intereses ir pārākas.
- Ja kā papildu drošības pasākums ir noteiktas beznosacījuma atteikšanās tiesības (vai nu tāpēc, ka tas ir nepārprotami pieprasīts saskaņā ar 14. panta b) punktu, vai arī tāpēc, ka tas ir uzskatāms par nepieciešamu vai noderīgu papildu drošības pasākumu citu iemeslu dēļ) — ja datu subjekts iebilst pret apstrādi, jānodrošina šādas izvēles ievērošana, un nav vajadzīgs veikt papildu pasākumus vai novērtēšanu.

2. pielikums. Praktiski piemēri, kuros ilustrēta 7. panta f) punkta līdzsvarošanas pārbaudes piemērošana

Šajā pielikumā ir sniegti piemēri par dažiem biežāk izplatītajiem kontekstiem, kādos var rasties jautājums par likumīgām interesēm 7. panta f) punkta izpratnē. Lielākajā daļā gadījumu ir grupēti divi vai vairāki saistīti piemēri, kurus ir vērts salīdzināt vienā sadaļā. Daudzu piemēru pamatā ir reāli gadījumi vai to elementi, ko risinājušas datu aizsardzības iestādes dažādās dalībvalstīs. Tomēr dažkārt līdz zināmai pakāpei ir mainīti fakti, lai labāk ilustrētu, kā veikt līdzsvarošanas pārbaudi.

Šie piemēri ir iekļauti, lai atspoguļotu *domāšanas procesu* — metodi, kuru izmantot, lai veiktu vairāku faktoru līdzsvarošanas pārbaudi. Citiem vārdiem sakot, šie piemēri *nav* paredzēti, lai sniegtu *galīgo* novērtējumu par aprakstītajiem gadījumiem. Jāatzīst, ka daudzos gadījumos, mainot lietas faktus (piemēram, ja personas datu apstrādātājs pieņem papildu drošības pasākumus — pilnīgāku anonimizāciju, labākus aizsargpasākumus, nodrošina labāku pārredzamību un reālākas izvēles iespējas datu subjektiem), var mainīties arī līdzsvarošanas pārbaudes rezultāts[116].

Tam būtu jāmudina personas datu apstrādātāji labāk ievērot visus direktīvas horizontālos noteikumus un attiecīgā gadījumā nodrošināt papildu aizsardzību saskaņā ar "projektētu" privātuma un datu aizsardzību. Jo lielāku uzmanību personas datu apstrādātāji pievērš personas datu aizsardzībai kopumā, jo ticamāk, ka tie atbildīs līdzsvarošanas pārbaudei.

Vārda vai informācijas brīvības tiesību īstenošana[117], tostarp plašsaziņas līdzekļos un mākslā

1. piemērs: NVO pārpublicē informāciju par parlamenta deputātu izdevumiem

Valsts iestāde saskaņā ar juridiskām saistībām (7. panta c) punkts) publicē informāciju par parlamenta deputātu izdevumiem; savukārt NVO, kas darbojas pārredzamības jomā, izanalizē un pārpublicē datus precīzā, samērīgā, taču informatīvākā un anotētā versijā, veicinot labāku pārredzamību un pārskatatbildību.

Pieņemot, ka NVO pārpublicēšanu un anotēšanu veikusi precīzi un samērīgi, pieņēmusi atbilstīgus drošības pasākumus, kopumā ievērojusi attiecīgo personu tiesības, tai vajadzētu spēt izmantot 7. panta f) punktu kā apstrādes juridisko pamatojumu. Tādi aspekti kā likumīgo interešu veids (vārda vai informācijas brīvības pamattiesības), sabiedrības intereses nodrošināt pārredzamību un pārskatatbildību, kā arī tas, ka dati jau ir publicēti un attiecas uz (relatīvi

[116] Pareizi piemērojot 7. panta f) punktu, var rasties sarežģītas novērtēšanas problēmas, un novērtējuma veikšanā liela nozīme var būt gan konkrētiem tiesību aktiem, gan judikatūrai, gan pamatnostādnēm, gan jurisprudencei, gan arī uzvedības kodeksiem un citiem oficiāliem un mazāk oficiāliem standartiem.

[117] Vārda vai informācijas brīvība ir apskatīta šī atzinuma 34. lappusē. Novērtējot šos piemērus, ir jāņem vērā arī visas direktīvas 9. pantā minētās attiecīgās valstu tiesību aktu atkāpes personas datu apstrādei, kas veikta žurnālistikas nolūkiem.

mazāk sensitīviem) personas datiem, kuri ir saistīti ar personu aktivitātēm attiecībā uz savu publisko amata pienākumu izpildi[118], apliecina apstrādes likumību. Pozitīvu novērtējumu veicina arī tas, ka sākotnējā publicēšana ir paredzēta tiesību aktā un ka tādējādi attiecīgās personas rēķinās ar to, ka viņu dati tiks publicēti. Raugoties no līdzsvara otras puses, ietekme uz personām var būt ievērojama, piemēram, publiskas pārbaudes rezultātā var tikt apšaubīts dažu personu godīgums, un tas var būt par iemeslu vēlētāju balsu zaudēšanai vai dažos gadījumos pat kriminālizmeklēšanai par krāpnieciskām darbībām. Tomēr iepriekš minētie faktori, kopā ņemot, parāda, ka galu galā personas datu apstrādātāja intereses (kā arī sabiedrības, kurai dati tiek atklāti, intereses) ir pārākas par datu subjektu interesēm.

2. piemērs: pašvaldības domes deputāts savu meitu ieceļ par palīdzi īpašos jautājumos

Žurnālists vietējā tiešsaistes laikrakstā publicē faktu ziņā precīzu un pienācīgi izpētītu rakstu par vietējo domes deputātu, atklājot, ka viņš ir apmeklējis tikai vienu no pēdējām vienpadsmit domes sēdēm un maz ticams, ka viņu pārvēlēs atkārtoti nesenā skandāla dēļ saistībā ar faktu, ka viņš savu septiņpadsmit gadus veco meitu iecēlis par palīdzi īpašos jautājumos.

Arī šeit ir izmantojama līdzīga analīze kā *1. piemērā*. Ņemot vērā faktus, attiecīgajam laikrakstam ir likumīgas intereses publicēt šo informāciju. Lai gan par domes deputātu ir atklāti personas dati, domes deputāta privātās dzīves neaizskaramības tiesības nav pārākas par vārda brīvības pamattiesībām un tiesībām publicēt šo rakstu laikrakstā. Tas ir tāpēc, ka publisku amatpersonu privātās dzīves neaizskaramības tiesības ir relatīvi ierobežotas attiecībā uz viņu publiskajām aktivitātēm, kā arī vārda brīvības īpašās nozīmes dēļ — sevišķi gadījumos, kad raksta publicēšana ir sabiedrības interesēs.

3. piemērs: populārākajos meklēšanas rezultātos joprojām tiek rādīts sīks noziedzīgs nodarījums

Laikraksta tiešsaistes arhīvā ir vecs raksts par kādu personu, kas kādreiz bijusi vietējā slavenība — kādas mazpilsētas amatieru futbola komandas kapteinis. Rakstā ir norādīts šīs personas pilns vārds, un tajā aprakstīta personas saistība ar relatīvi maznozīmīgu krimināprocesu (dzeršana un sīkais huligānisms). Šīs personas dati vairs nav sodāmības reģistrā, un tajā vairs nav minēts agrākais pārkāpums, par kuru sodu tā izcietusi pirms vairākiem gadiem. Šai personai vislielāko satraukumu rada tas, ka, meklējot tās vārdu bieži lietotā tiešsaistes meklētājprogrammā, kā viens no pirmajiem rezultātiem tiek parādīta saite uz šo veco rakstu. Neraugoties uz iesniegto pieprasījumu, laikraksts atsakās veikt tehniskus pasākumus, kas ierobežotu ar datu subjektu saistītā raksta plašāku pieejamību. Piemēram, laikraksts atsakās pieņemt tehniskus vai organizatoriskus pasākumus, kuru mērķis (ciktāl to atļauj tehnoloģijas) būtu ierobežot piekļuvi šai informācijai no ārējām meklētājprogrammām, kā meklēšanas kategoriju izmantojot attiecīgās personas vārdu.

Tas ir vēl viens gadījums, kas ilustrē potenciālo konfliktu starp vārda brīvību un privātās dzīves neaizskaramību. Tas arī parāda, ka dažos gadījumos papildu drošības pasākumiem (piemēram, nodrošinot, lai vismaz pamatota iebilduma gadījumā saskaņā ar direktīvas

[118] Nevar izslēgt, ka informācija par noteiktiem izdevumiem var atklāt sensitīvākus datus, piemēram, par veselību. Šādā gadījumā pirms publicēšanas šāda informācija vispār ir jāizrediģē no datu kopas. Ir ieteicams rīkoties saskaņā ar "aktīvu pieeju" un dot personām iespēju pārskatīt savus datus pirms to publicēšanas, un tās skaidri informēt par publicēšanas iespējām un veidiem.

14. panta a) punktu laikraksta arhīva attiecīgajai daļai vairs nevarētu piekļūt, izmantojot ārējas meklētājprogrammas, vai arī informācijas parādīšanas formāts vairs neļautu meklēt pēc vārda) var būt svarīga nozīme, lai panāktu pienācīgu līdzsvaru starp abām attiecīgajām pamattiesībām. Tas gan nekādā gadījumā neierobežo jebkādus citus pasākumus, ko varētu veikt meklētājprogrammu izstrādātāji vai citas trešās personas[119].

Tradicionālā tiešā tirgvedība un citi tirgvedības vai reklāmas veidi

4. piemērs: datorveikals klientiem reklamē līdzīgus produktus

Datorveikals saistībā ar kāda produkta tirdzniecību iegūst savu klientu kontaktinformāciju un to izmanto tirgvedībai, pa parasto pastu reklamējot savus līdzīgos produktus. Veikals arī pārdod produktus tiešsaistē un nosūta reklāmas e-pasta ziņojumus, kad sortimentā parādās jauna produktu līnija. Kontaktinformācijas vākšanas brīdī klienti tiek skaidri informēti par iespēju bez maksas un ērtā veidā iebilst; tas tiek arī atgādināts, ikreiz nosūtot ziņojumu, gadījumā, ja klients sākotnēji nav paudis iebildumus.

Apstrādes pārredzamība, tas, ka persona var pamatoti cerēt saņemt piedāvājumus par līdzīgiem produktiem kā veikala klients, kā arī tas, ka klientam ir tiesības iebilst, palīdz stiprināt apstrādes likumīgumu un aizsargāt personas tiesības. Raugoties no līdzsvara otras puses, nešķiet, ka būtu nesamērīgi ietekmētas personas tiesības uz privātās dzīves neaizskaramību (šajā piemērā mēs pieņēmām, ka datorveikals par saviem klientiem neveido sarežģītus profilus, piemēram, izmantojot apmeklējumu vēstures datu detalizētu analīzi).

5. piemērs: tiešsaistes aptieka veic plašu profilēšanu

Tiešsaistes aptieka veic tirgvedības pasākumus, izmantojot datus par klientu nopirktām zālēm un citiem produktiem, tostarp recepšu zālēm. Tā analizē šo informāciju kopā ar demogrāfisko informāciju par klientiem (piemēram, to dzimumu un vecumu), lai veidotu atsevišķu klientu "veselības un labklājības" profilu. Tiek arī izmantoti apmeklējumu vēstures dati, kas tiek vākti ne vien par klientu iegādātiem produktiem, bet arī par citiem produktiem un informāciju, kuru tie pārlūkojuši tīmekļa vietnē. Klientu profilos ir iekļauta informācija vai prognozes par to, ka noteikts klients ir grūtniece, cieš no konkrētas hroniskas slimības vai arī noteiktos gada periodos vēlētos iegādāties pārtikas piedevas, sauļošanās losjonu vai citus ādas kopšanas līdzekļus. Tiešsaistes aptiekas analītiķi izmanto šo informāciju, lai konkrētām personām piedāvātu bezrecepšu zāles, pārtikas piedevas un citus produktus, tos reklamējot pa e-pastu. Šajā gadījumā, veidojot un izmantojot savu klientu profilus tirgvedības vajadzībām, aptieka nevar paļauties uz savām likumīgajām interesēm. Šeit aprakstītā profilēšana rada vairākas problēmas. Šāda informācija ir īpaši sensitīva un var daudz ko atklāt par jautājumiem, kurus daudzas personas nevēlētos atklāt citiem[120]. Arī profilēšanas apmērs un veids (apmeklējumu vēstures datu un prognozējošu algoritmu izmantošana) liecina par ievērojamu privātuma aizskārumu. Tomēr attiecīgos gadījumos kā alternatīvu varētu izskatīt piekrišanu saskaņā ar 7. panta a) punktu un 8. panta 2. punkta a) apakšpunktu (ja nav iesaistīti sensitīvi dati).

[119] Sk. arī lietu C-131/12 *Google Spain* pret *Agencia Española de Proteccion de Datos*, kas pašlaik tiek izskatīta Eiropas Savienības Tiesā.

[120] Papildus datu aizsardzības tiesību aktos noteiktiem ierobežojumiem ES tiek stingri reglamentētas arī recepšu zāles, kā arī pastāv zināmi ierobežojumi attiecībā uz bezrecepšu zāļu reklamēšanu. Turklāt jāņem vērā arī prasības, kas izklāstītas 8. pantā par īpašām datu kategorijām (piemēram, datiem par veselību).

Nevēlami nekomerciāli paziņojumi, tai skaitā saistībā ar politiskajām kampaņām vai līdzekļu vākšanu labdarībai

6. piemērs: pašvaldību vēlēšanu kandidāte mērķtiecīgi izmanto vēlētāju reģistru

Kandidāte pašvaldību vēlēšanās izmanto vēlētāju reģistru[121], lai nosūtītu iepazīstināšanas vēstuli, kurā tā popularizē savu kampaņu pirms gaidāmajām vēlēšanām katram potenciālajam vēlētājam savā vēlēšanu apgabalā. Kandidāte izmanto datus, kas iegūti no vēlētāju reģistra, tikai lai nosūtītu vēstuli, un pēc kampaņas beigām nesaglabā šos datus.

Šāds vēlētāju reģistra lietojums, ja tas tiek izmantots pirmsvēlēšanu periodā, atbilst personu pamatotām gaidām — personas datu apstrādātāja intereses ir skaidras un likumīgas. Arī informācijas ierobežotā un mērķtiecīgā izmantošana ļauj radīt pārsvaru personas datu apstrādātāja likumīgo interešu pusē. Šādu vēlētāju reģistru lietojumu no sabiedrības interešu perspektīvas var arī reglamentēt ar valsts mēroga tiesību aktiem, paredzot īpašus noteikumus, ierobežojumus un drošības pasākumus attiecībā uz vēlētāju reģistra lietojumu. Lai šādā gadījumā nodrošinātu apstrādes likumību, ir arī jāievēro šie īpašie noteikumi.

7. piemērs: bezpeļņas organizācija vāc informāciju, lai vērstos pie mērķauditorijas

Filozofiskas ievirzes organizācija, kuras mērķi ir cilvēka un sociālā attīstība, nolemj organizēt līdzekļu vākšanas pasākumus, izmantojot savu dalībnieku profilus. Šajā nolūkā tā sociālo tīklu vietnēs vāc datus, izmantojot speciālu programmatūru, kas vērsta uz personām, kuras organizācijas lapu novērtējušas, atzīmējot "patīk", vai kuras organizācijas lapā publicētos ziņojumus novērtējušas, atzīmējot "patīk", vai kuras dalījušās ar šādiem ziņojumiem, regulāri skatījušas noteiktas sadaļas vai atbildējušas uz organizācijas *Twitter* ziņojumiem. Pēc tam organizācija nosūta ziņojumus un biļetenus saviem dalībniekiem, ņemot vērā to profilus. Piemēram, vecāka gadagājuma suņu īpašnieki, kuri ar "patīk" atzīmēja rakstus par dzīvnieku patversmēm, saņēma atšķirīgus ziedošanas aicinājumus nekā ģimenes ar maziem bērniem; atšķirīgus ziņojumus saņēma arī personas no atšķirīgām etniskajām grupām.

Apstrādājot īpašas datu kategorijas (filozofiskā pārliecība), ir jānodrošina atbilstība 8. pantam — šķiet, ka šis nosacījums ir ievērots, jo datu apstrāde notiek, veicot organizācijas likumīgās aktivitātes. Tomēr šajā gadījumā tas nav pietiekams nosacījums — datu izmantošanas veids pārsniedz personu pamatotas gaidas. Savākto datu apjoms, pārredzamības trūkums attiecībā uz tādu datu vākšanu un atkārtotu izmantošanu, kas sākotnēji publicēti vienā nolūkā, bet izmantoti pavisam citā, liek secināt, ka šajā gadījumā nevar atsaukties uz 7. panta f) punktu. Tāpēc apstrāde nav pieļaujama, izņemot gadījumus, kad var izmantot citu pamatojumu, piemēram, personu piekrišanu saskaņā ar 7. panta a) punktu.

[121] Tiek pieņemts, ka piemērā aprakstītajā dalībvalstī vēlētāju reģistrs ir izveidots saskaņā ar likumu.

Juridisku prasību piemērošana, tostarp parādu piedziņa, izmantojot ārpustiesas procedūras

8. piemērs: strīds par atjaunošanas darbu kvalitāti

Klients ir uzsācis strīdu par virtuves atjaunošanas darbu kvalitāti un atsakās maksāt pilnu summu. Būvuzņēmums savam juristam pārsūta attiecīgus samērīga apjoma datus, lai tas varētu atgādināt klientam par veicamo maksājumu un meklēt risinājumu ar klientu sarunu ceļā, ja klients joprojām atsakās veikt apmaksu.

Šajā gadījumā būvuzņēmuma veiktie sākotnējie pasākumi, izmantojot pamatinformāciju par datu subjektu (piemēram, vārdu un uzvārdu, adresi un līguma atsauci), lai datu subjektam nosūtītu atgādinājumu (tiešā veidā vai izmantojot jurista pakalpojumus, kā šajā gadījumā), joprojām var atbilst apstrādes nepieciešamībai līguma izpildes vajadzībām (7. panta b) punkts). Tomēr, ja tiek veikti turpmāki pasākumi[122], tai skaitā parādu piedziņas aģentūras iesaistīšana, tie ir jānovērtē saskaņā ar 7. panta f) punktu, cita starpā izvērtējot šādu pasākumu uzmācīguma pakāpi un ietekmi uz datu subjektu, kā parādīts turpmākajā piemērā.

9. piemērs: klients, kas kredītā iegādājies automobili, nav atrodams

Klients neveic maksājumus par dārgu sporta automobili, kas iegādāts kredītā, bet pēc tam "pazūd". Automobiļu izplatītājs noslēdz līgumu ar trešo personu — "parādu piedziņas aģentu". Parādu piedziņas aģents veic uzmācīgu "tiesībaizsardzības iestāžu stila" izmeklēšanu, cita starpā izmantojot tādus paņēmienus kā slēpta videonovērošana un telefonsarunu noklausīšanās.

Lai gan automobiļu izplatītāja un parādu piedziņas aģenta intereses ir likumīgas, pārsvars nav viņu pusē informācijas vākšanai izmantoto uzmācīgo metožu dēļ, no kurām dažas ir nepārprotami aizliegtas ar likumu (telefonsarunu noklausīšanās). Secinājums būtu citāds, ja, piemēram, automobiļu izplatītājs vai parādu piedziņas aģents veiktu tikai ierobežotas pārbaudes, lai noskaidrotu datu subjekta kontaktinformāciju nolūkā sākt tiesvedību.

Krāpšanas, pakalpojumu ļaunprātīgas izmantošanas vai nelikumīgi iegūtu līdzekļu legalizēšanas novēršana

10. piemērs: klientu datu pārbaude pirms bankas konta atvēršanas

Finanšu iestāde veic pamatotas un samērīgas procedūras (saskaņā ar kompetentas valdības finanšu uzraudzības iestādes nesaistošām pamatnostādnēm), lai pārbaudītu to personu identitāti, kuras vēlas bankā atvērt kontu. Tā glabā šādas informācijas reģistru, lai pārbaudītu personas identitāti.

Personas datu apstrādātāja intereses ir likumīgas, datu apstrāde ietver vienīgi ierobežotas un vajadzīgas informācijas apstrādi (standarta prakse šajā nozarē, ko pamatoti gaida datu subjekti un ko iesaka veikt kompetentās iestādes). Ir ieviesti atbilstīgi drošības pasākumi, lai ierobežotu nesamērīgu un neatbilstīgu ietekmi uz datu subjektiem. Tāpēc personas datu

[122] Pašlaik dažādās dalībvalstīs pastāv zināmas atšķirības attiecībā uz to, kādus pasākumus var uzskatīt par nepieciešamiem līguma izpildei.

apstrādātājs var atsaukties uz 7. panta f) punktu. Ciktāl veicamie pasākumi ir īpaši noteikti piemērojamajos tiesību aktos, var arī piemērot 7. panta c) punktu.

11. piemērs: informācijas apmaiņa, lai cīnītos pret nelikumīgi iegūtu līdzekļu legalizēšanu

Finanšu iestāde pēc konsultācijām ar kompetento datu aizsardzības iestādi īsteno procedūras, ievērojot konkrētus un ierobežotus kritērijus, lai apmainītos ar datiem par nelikumīgi iegūtu līdzekļu legalizēšanas apkarošanas noteikumu potenciālu ļaunprātīgu izmantošanu starp vienas uzņēmumu grupas vairākiem uzņēmumiem, stingri ierobežojot piekļuvi, garantējot drošību un aizliedzot datu turpmāku izmantošanu citiem nolūkiem.

Iemesli ir līdzīgi ar iepriekš izklāstītajiem, un atkarībā no lietas faktiem datu apstrādes pamatā varētu būt 7. panta f) punkts. Ciktāl veicamie pasākumi ir īpaši noteikti piemērojamajos tiesību aktos, var arī piemērot 7. panta c) punktu.

12. piemērs: agresīvu narkomānu "**melnais saraksts**"

Vairākas slimnīcas izveido kopīgu melno sarakstu, kurā iekļautas "agresīvas" personas, kuras meklē narkotikas, lai liegtu tām piekļuvi visu šo slimnīcu ārstniecības telpām.

Pat ja personas datu apstrādātāju intereses uzturēt savās iestādēs drošību ir likumīgas, tās ir jālīdzsvaro ar privātās dzīves neaizskaramības pamattiesībām un citiem nenoraidāmiem jautājumiem, piemēram, nepieciešamību neliegt attiecīgajām personām pieeju veselības aprūpei. Tas, ka tiek apstrādāti sensitīvi dati (piemēram, dati par veselību saistībā ar narkomāniju), arī liek secināt, ka šajā gadījumā apstrāde diezin vai būs pieņemama saskaņā ar 7. panta f) punktu[123]. Iespējams, apstrāde būtu pieņemama, ja tā, piemēram, būtu reglamentēta tiesību aktā, kurā paredzēti konkrēti drošība pasākumi (pārbaudes un kontroles pasākumi, pārredzamība, automatizētu lēmumu novēršana), nodrošinot, ka personas netiktu diskriminētas vai pārkāptas to pamattiesības[124]. Šajā pēdējā gadījumā atkarībā no tā, vai šajā konkrētajā tiesību aktā datu apstrāde ir noteikta obligāti vai tikai atļauta, kā juridisko pamatojumu var izmantot 7. panta c) punktu vai 7. panta f) punktu.

Darbinieku uzraudzība drošības vai pārvaldības nolūkos

13. piemērs: juristu darba stundu skaits tiek izmantots gan algu izmaksai, gan prēmiju noteikšanai

Advokātu biroja juristu apmaksājamo darba stundu skaits tiek apstrādāts gan algu, gan ikgadējo prēmiju noteikšanai. Šī sistēma ir pārredzamā veidā izskaidrota darbiniekiem, kuriem ir skaidri noteiktas tiesības nepiekrist secinājumiem gan attiecībā uz algu aprēķinu, gan prēmiju izmaksāšanu, ko pēc tam var apspriest ar uzņēmuma vadību.

Apstrāde šķiet vajadzīga personas datu apstrādātāja likumīgo interešu īstenošanai, un nešķiet, ka būtu kāds mazāk traucējošs veids, kā to sasniegt. Ietekmi uz darbiniekiem ierobežo arī

[123] Jāņem vērā arī prasības, kas izklāstītas 8. pantā par īpašām datu kategorijām (piemēram, datiem par veselību).

[124] Sk. darba dokumentu par melnajiem sarakstiem (WP 65), kas pieņemts 2002. gada 3. oktobrī.

ieviestie drošības pasākumi un procesi. Tāpēc šajā gadījumā kā piemērotu juridisko pamatojumu var izmantot 7. panta f) punktu. Atbalstam var arī argumentēt, ka apstrāde vienam vai abiem nolūkiem ir vajadzīga, lai pildītu līgumu.

14. piemērs: interneta lietošanas elektroniskā uzraudzība[125]

Darba devējs darba laikā uzrauga darbinieku interneta lietojumu, lai pārbaudītu, vai tie uzņēmuma IT resursus pārmērīgi neizmanto personiskajām vajadzībām. Tiek vākti tādi dati kā darbinieku datoros saglabātie pagaidu faili un ģenerētie sīkfaili, kas parāda darba laikā apmeklētās tīmekļa vietnes un veiktās lejupielādes. Dati tiek apstrādāti, iepriekš neapspriežoties ar datu subjektiem un arodbiedrības pārstāvjiem / uzņēmuma padomi. Attiecīgajām personām arī netiek sniegta pietiekama informācija par šādām darbībām.

Savākto datu apjoms un veids liecina par būtisku darbinieku privātās dzīves aizskārumu. Papildus jautājumiem par samērīgumu, svarīgi arī apsvērt šādu darbību pārredzamību, kas ir cieši saistītas ar datu subjektu pamatotajām gaidām. Pat ja darba devējam ir likumīgas intereses ierobežot laiku, ko darbinieki pavada, apmeklējot tīmekļa vietnes, kas nav tieši saistītas ar viņu darba pienākumiem, izmantotās metodes neatbilst 7. panta f) punktā noteiktajai līdzsvarošanas pārbaudei. Darba devējam ir jāizmanto mazāk traucējošas metodes (piemēram, noteiktu vietņu pieejamības ierobežošana), kuras vēlamā gadījumā ir apspriestas un par kurām panākta vienošanās ar darba ņēmēju pārstāvjiem, kā arī par kurām darbinieki informēti pārredzamā veidā.

Sistēmas ziņošanai par pārkāpumiem

15. piemērs: sistēma ziņošanai par pārkāpumiem, lai ievērotu ārvalstu juridiskās saistības

ASV uzņēmumu grupas ES filiāle izveido ierobežotas darbības sistēmu ziņošanai par pārkāpumiem, lai varētu ziņot par nopietniem pārkāpumiem grāmatvedības un finanšu jomā. Grupas uzņēmumiem ir noteikts labas pārvaldības kodekss, kurā izteikts aicinājums stiprināt iekšējās kontroles un riska vadības procedūras. Tā kā grupa darbojas starptautiskā mērogā, ES filiālei ir jāsniedz uzticami finanšu dati citiem grupas dalībniekiem ASV. Sistēma ir izstrādātā tā, lai tā atbilstu gan ES tiesību aktiem, gan ES valsts datu aizsardzības iestāžu sniegtajām pamatnostādnēm.

Ir ieviesti arī drošības pasākumi — apmācības nodarbībās un izmantojot citus līdzekļus, darbiniekiem ir sniegti skaidri norādījumi par apstākļiem, kādos sistēma jāizmanto. Darbinieki ir brīdināti neizmantot šo sistēmu ļaunprātīgi, piemēram, lai sniegtu nepatiesas vai nepamatotas apsūdzības pret citiem kolēģiem. Turklāt viņiem paskaidrots, ka sistēmu iespējams izmantot arī anonīmi, bet, ja vēlas — var norādīt savu identitāti. Otrajā gadījumā darbinieki tiek informēti par to, kādos apstākļos viņus identificējoša informācija tiks nodota atpakaļ darba devējam vai citām aģentūrām.

[125] Dažas dalībvalstis uzskata, ka zināma ierobežota elektroniskā uzraudzība varētu būt "vajadzīga līguma izpildei", tāpēc tās pamatā var būt 7. panta b) punkta juridiskais pamatojums, nevis 7. panta f) punkts.

Ja saskaņā ar ES tiesību aktiem vai ES dalībvalsts tiesību aktiem šāda sistēma būtu izveidojama obligāti, apstrādes pamatā varētu būt 7. panta c) punkts. Tomēr ārvalstu juridiskās saistības nav uzskatāmas par juridiskām saistībām atbilstīgi 7. panta c) punktam, un šādas saistības nevar leģitimizēt apstrādi saskaņā ar 7. panta c) punktu. Taču apstrādes pamatā varētu būt 7. panta f) punkts, piemēram, gadījumā, ja pastāv likumīgas intereses garantēt finanšu tirgu stabilitāti vai cīnīties pret korupciju un ja sistēmā ir paredzēti pietiekami drošības pasākumi saskaņā ar attiecīgo ES regulatīvo iestāžu norādījumiem.

16. piemērs: iekšējā sistēma ziņošanai par pārkāpumiem bez konsekventām procedūrām

Uzņēmums, kas sniedz finanšu pakalpojumus, nolemj izveidot sistēmu ziņošanai par pārkāpumiem, jo pastāv aizdomas, ka darbinieku vidū ir plaši izplatīta zagšana un korupcija, un uzņēmums vēlas mudināt darbiniekus ziņot par kolēģu pārkāpumiem. Lai ietaupītu naudu, uzņēmums nolemj izveidot iekšēju sistēmu, ko vada tā cilvēkresursu nodaļas darbinieki. Lai pamudinātu darbiniekus izmantot šo sistēmu, uzņēmums piedāvā beznosacījuma finansiālu atlīdzību tiem darbiniekiem, kuru veiktās ziņošanas rezultātā tiks atklāta nepareiza rīcība un atgūta nauda.

Uzņēmumam ir likumīgas intereses noteikt un novērst zādzības un korupciju. Tomēr, tā kā sistēma ziņošanai par pārkāpumiem ir tik slikti veidota un tai trūkst drošības pasākumu, par uzņēmuma interesēm pārākas ir gan darbinieku intereses, gan privātās dzīves neaizskaramības tiesības — īpaši to darbinieku tiesības, kuri kļuvuši par upuriem nepatiesai ziņošanai, kas veikta vienīgi, lai gūtu finansiālu labumu. Vēl viena problēma ir tā, ka sistēma darbojas iekšēji, nevis neatkarīgi, kā arī tas, ka trūkst apmācības un norādījumu par sistēmas izmantošanu.

Fiziskā drošība, IT un tīkla drošība

17. piemērs: biometriskā kontrole pētniecības laboratorijā

Zinātniski pētnieciskā laboratorijā, kur norit darbs ar letāliem vīrusiem, tiek izmantota biometriska piekļuves sistēma, ņemot vērā lielo risku sabiedrības veselībai gadījumā, ja vīrusi izkļūtu no telpām. Ir veikti atbilstoši drošības pasākumi, tostarp biometriskie dati tiek glabāti darbinieku personiskajās kartēs, nevis centralizētā sistēmā.

Ja pat kopumā dati ir sensitīvi, to apstrādes iemesls ir sabiedrības interesēs. Šis aspekts, kā arī tas, ka ļaunprātīgas izmantošanas riskus mazina atbilstīgs drošības pasākumu lietojums, kā piemērotu apstrādes pamatojumu ļauj izmantot 7. panta f) punktu.

18. piemērs: slēptās kameras, lai identificētu smēķējošus apmeklētājus un darbiniekus

Uzņēmums izmanto slēptās kameras, lai identificētu darbiniekus un apmeklētājus, kuri smēķē telpās, kur tas nav atļauts.

Lai gan personas datu apstrādātājam ir likumīgas intereses nodrošināt atbilstību pretsmēķēšanas noteikumiem, līdzekļi šī mērķa sasniegšanai kopumā ir nesamērīgi un nevajadzīgi traucējoši. Ir pieejamas ne tik traucējošas un pārredzamākas metodes (piemēram, dūmu detektori un norādes). Tādēļ apstrāde neatbilst 6. pantam, kurā noteikts, ka dati nedrīkst

būt "pārmērīgi" attiecībā uz to vākšanas vai turpmākas apstrādes nolūkiem. Tajā pašā laikā ļoti ticams, ka šāda datu apstrāde arī neizturētu 7. pantā noteikto līdzsvarošanas pārbaudi.

Zinātniskā pētniecība

19. piemērs: pētījumi par laulības šķiršanas un vecāku bezdarba ietekmi uz bērnu sasniegumiem izglītībā

Saskaņā ar valdības pieņemtu pētniecības programmu un kompetentas ētikas komitejas atļauju tiek veikta pētījums par laulības šķiršanas, vecāku bezdarba un bērnu izglītības sasniegumu savstarpējo saistību. Lai gan šīs ziņas nav klasificētas kā "īpašas datu kategorijas", pētījumā uzmanība tiek pievērsta tādiem jautājumiem, ko daudzas ģimenes uzskatītu par ļoti intīmu personisko informāciju. Ņemot vērā pētījumā gūtos datus, īpaša izglītības programma tiks vērsta uz bērniem, kuri citādi varētu neapmeklēt skolu, gūt sliktas sekmes mācībās, pieaugot kļūt par bezdarbniekiem vai pārkāpt likumu. Attiecīgajā dalībvalsts tiesību aktā ir skaidri atļauta personas datu apstrāde (kas nav īpašas datu kategorijas) pētniecības nolūkos, ja vien pētniecība ir vajadzīga svarīgās sabiedrības interesēs un tiek veikta, ievērojot pienācīgus drošības pasākumus, kas ir plašāk izklāstīti īstenošanas tiesību aktos. Šajā tiesiskajā regulējumā ir ne vien iekļautas konkrētas prasības, bet arī noteikta pārskatatbildības sistēma, kas ļauj katrā konkrētajā gadījumā novērtēt pētījumu pieļaujamību (ja tā tiek veikta bez attiecīgo personu piekrišanas), kā arī konkrēti pasākumi, kas jāievieš, lai aizsargātu datu subjektus.

Pētījuma veicējam ir drošas telpas pētījumiem, un drošos apstākļos attiecīgo informāciju tam sniedz iedzīvotāju reģistrs, tiesas, nodarbinātības aģentūras un skolas. Pētniecības centrs pēc tam "sajauc" personu identitātes, lai varētu saistīt datus par laulības šķiršanu, bezdarbu un izglītību, taču neatklājot personu pilsoņu "civilās" identitātes, piemēram, to vārdus un adreses. Pēc tam visi sākotnējie dati tiek neatgriezeniski dzēsti. Ir arī veikti papildu pasākumi, lai nodrošinātu funkcionālo nošķīrumu (t. i., dati tiks izmantoti tikai pētniecības vajadzībām) un mazinātu turpmākas atkārtotas identificēšanas risku.

Pētniecības centra darbinieki ir saņēmuši stingru apmācību drošības jautājumos un ir personiski (iespējams, pat krimināli) atbildīgi par jebkādiem viņu veiktiem drošības pārkāpumiem. Piemēram, ir veikti tehniski un organizatoriski pasākumi, lai nodrošinātu, ka darbinieki, kas izmanto USB zibatmiņas, nevarētu no centra „iznest" personas datus.

Pētījuma veikšana ir pētniecības centra likumīgās intereses, kā arī izteiktas sabiedrības intereses. Tās ir arī programmā iesaistīto nodarbinātības, izglītības un citu iestāžu likumīgās intereses, jo šis pētījums palīdzēs plānot un sniegt pakalpojumus tām personām, kurām tas visvairāk vajadzīgs. Sistēmas privātuma aspekts ir labi izstrādāts, un ieviestie drošības pasākumi nodrošina, ka pētniecībā iesaistīto organizāciju likumīgajām interesēm nav mazāks spēks nekā to vecāku vai bērnu interesēm vai privātās dzīves neaizskaramības tiesībām, kuru dati ir šī pētījuma pamatā.

20. piemērs: pētījums par lieko svaru

Kāda augstskola vēlas veikt pētījumu par bērnu lieko svaru vairākās pilsētās un lauku rajonos. Neraugoties uz to, ka tai ir grūtības piekļūt attiecīgajiem datiem skolās un citās iestādēs, tai izdodas pārliecināt vairākus desmitus skolotāju noteiktu laika posmu reģistrēt, kuri bērni klasēs ir ar lieko svaru, un uzdot viņiem jautājumus par diētu, fizisko aktivitāšu daudzumu,

datorspēlēm u. c. Šie skolotāji arī pieraksta intervēto bērnu vārdus un adreses, lai viņiem kā atlīdzību par piedalīšanos pētījumā varētu nosūtīt tiešsaistes mūzikas kuponu. Pēc tam pētnieki izveido datubāzi ar bērnu datiem, lieko svaru saistot ar fiziskajām aktivitātēm un citiem faktoriem. Augstskolas arhīvos uz nenoteiktu un laiku bez pienācīgiem drošības pasākumiem tiek glabātas aizpildīto aptaujas anketu papīra kopijas — joprojām tādā veidā, ka var identificēt konkrētos bērnus. Visu aptaujas anketu fotokopijas pēc pieprasījuma var iegūt jebkurš minētās augstskolas vai tās partneraugstskolu maģistrantūras vai doktorantūras students, kurš izrāda interesi par pētījuma datu turpmāku izmantošanu.

Lai gan augstskolas likumīgajās interesēs ir veikt pētniecību, šajā pētījumā ir vairāki aspekti, kas liecina, ka bērnu intereses un privātās dzīves neaizskaramības tiesības ir pārākas par augstskolas interesēm. Nemaz nerunājot par pētījuma metodoloģiju, kurai trūkst zinātniskas precizitātes, galvenokārt problēmu rada tas, ka pētījuma formātam nav pieeju, kas stiprinātu privātās dzīves neaizskaramību, un ka savāktie personas dati ir plaši pieejami. Bērnu dati nevienā posmā netiek šifrēti vai anonimizēti, un nav veikti arī citi pasākumi, lai garantētu datu drošību vai to funkcionālo nošķīrumu. Nav iegūta derīga piekrišana saskaņā ar 7. panta a) punktu un 8. panta 2. punkta a) apakšpunktu, un nav skaidrs, vai bērniem vai viņu vecākiem ir paskaidrots, kādā nolūkā viņu personas dati tiks izmantoti un kam tie tiks nodoti.

Ārvalstu juridiskās saistības

21. piemērs: trešās valsts nodokļu tiesību aktu ievērošana

ES bankas ievāc un pārsūta zināmu daļu savu klientu datu, lai nodrošinātu, ka klienti ievēro trešās valsts nodokļu saistības. Datu vākšana un pārsūtīšana ir noteikta starp ES un ārvalsti noslēgtā starptautiskā nolīgumā un atbilst tā nosacījumiem un drošības pasākumiem.

Kaut arī ārvalstu saistības pašas par sevi nevar uzskatīt par apstrādes likumīgu pamatojumu saskaņā ar 7. panta c) punktu, tomēr šāds pamatojums tikpat labi var būt derīgs, ja minētās saistības ir noteiktas starptautiskā nolīgumā. Šajā otrajā gadījumā apstrādi var uzskatīt par vajadzīgu, lai ievērotu juridiskās saistības, kas iekšējā tiesiskajā regulējumā ir iekļautas ar starptautisku nolīgumu. Tomēr, ja šāda nolīguma nav, datu vākšana un pārsūtīšana ir jānovērtē saskaņā ar 7. panta f) punkta prasībām, un to var atļaut vienīgi tad, ja ir ieviesti pienācīgi drošības pasākumi, piemēram, tādi pasākumi, ko apstiprinājusi kompetentā datu aizsardzības iestāde (skatiet arī iepriekš aprakstīto *15. piemēru*).

22. piemērs: datu pārsūtīšana saistībā ar disidentiem

ES uzņēmums pēc pieprasījuma pārsūta datus par ārvalstu pilsoņiem totalitāram trešās valsts režīmam, kas vēlas piekļūt datiem par disidentiem (piemēram, to e-pasta datplūsmas informācijai, e-pasta saturam, pārlūkošanas vēsturei vai privātajiem ziņojumiem sociālajos tīklos).

Atšķirībā no iepriekšējā piemēra šajā gadījumā nav noslēgta starptautiska nolīguma, saskaņā ar kuru kā juridisko pamatojumu varētu izmantot 7. panta c) punktu. Turklāt vairāki elementi ir pretrunā 7. panta f) punkta izmantošanai kā atbilstīgam apstrādes pamatojumam. Lai arī personas datu apstrādātājam, iespējams, ir ekonomiskas intereses nodrošināt ārvalstu valdības pieprasījumus (iespējams, pretējā gadījumā trešās valsts valdība pret to var izturēties mazāk labvēlīgi, salīdzinot ar citiem uzņēmumiem), saskaņā ar ES pamattiesību regulējumu šādas datu pārsūtīšanas likumīgums un samērīgums ir ļoti apšaubāms. Arī pārsūtīšanas potenciāli

milzīgā ietekme uz attiecīgajām personām (piemēram, diskriminācija, ieslodzījums, nāvessods) noteikti runā par labu attiecīgo personu interesēm un tiesībām.

Publiski pieejamu datu atkārtota izmantošana

23. piemērs: politiķu novērtēšana[126]

NVO, kas darbojas pārredzamības jomā, izmanto publiski pieejamus datus par politiķiem (solījumiem priekšvēlēšanu periodā un faktiskajiem datiem par šo politiķu balsojumiem), lai novērtētu, cik labi viņu turējuši savus solījumus.

Pat ja ietekme uz attiecīgajiem politiķiem var būt ievērojama, tas, ka apstrādes pamatā ir publiska informācija un tā ir saistīta ar šo personu publiskajiem pienākumiem, kā arī nepārprotamie pārredzamības un pārskatatbildības uzlabošanas nodomi rada pārsvaru personas datu apstrādātāja interešu pusē[127].

Bērni un citas neaizsargātas personas

24. piemērs: informācijas tīmekļa vietne pusaudžiem

NVO tīmekļa vietnē, kur tiek piedāvāti padomi pusaudžiem saistībā ar tādiem jautājumiem kā narkomānija, nevēlama grūtniecība un pārmērīga alkohola lietošana, vāc datus par vietnes apmeklētājiem, izmantojot savu serveri. Dati pēc tam tiek nekavējoties anonimizēti un pārvērsti par vispārēju statistiku par to, kuras tīmekļa vietnes daļas ir vispopulārākās starp apmeklētājiem no dažādiem valsts ģeogrāfiskajiem reģioniem.

Šajā gadījumā kā juridisko pamatojumu var izmantot 7. panta f) punktu, pat ja tiek izmantoti dati par neaizsargātām personām, jo šāda apstrāde ir sabiedrības interesēs un ir ieviesti stingri drošības pasākumi (dati tiek nekavējoties padarīti anonīmi un tiek izmantoti tikai statistikas veidošanai), kas palīdz radīt pārsvaru personas datu apstrādātāja pusē.

Integrētas privātuma aizsardzības risinājumi kā papildu drošības pasākumi

25. piemērs: piekļuve lietojumprogrammas lietotāju un nelietotāju mobilo tālruņu numuriem: "**salīdzināt un aizmirst**"

Personu dati tiek apstrādāti, lai pārbaudītu, vai tie jau iepriekš ir pauduši nepārprotamu piekrišanu (t. i., kā drošības pasākums tiek izmantota sistēma "salīdzināt un aizmirst)".

Lietojumprogrammas izstrādātājam ir jāsaņem datu subjektu nepārprotama piekrišana attiecībā uz viņu personas datu apstrādi, piemēram — lietojumprogrammas izstrādātājs vēlas piekļūt visai lietojumprogrammas lietotāju elektroniskajai adrešu grāmatiņai un iegūt no tās datus, tai skaitā tādu kontaktpersonu mobilo tālruņu numurus, kuras neizmanto šo

[126] Skatiet arī iepriekš aprakstīto 7. piemēru un salīdziniet ar to.

[127] Tāpat kā *1. un 2. piemērā* (tika pieņemts, ka publikācija ir precīza un samērīga) drošības pasākumu trūkums un citi faktori var mainīt interešu līdzsvaru atkarībā no konkrētās lietas faktiem.

programmu. Lai to varētu izdarīt, iespējams, izstrādātājam sākumā ir jānosaka, vai programmas lietotāju adrešu grāmatiņās iekļautie mobilo tālruņu numuru īpašnieki ir pauduši nepārprotamu piekrišanu (saskaņā ar 7. panta a) punktu) savu datu apstrādei.

Attiecībā uz šādu ierobežotu sākotnējo apstrādi (t. i., īstermiņa lasīšanas piekļuvi visai programmas lietotāja adrešu grāmatiņai) lietojumprogrammas izstrādātājs kā juridisko pamatojumu var izmantot 7. panta f) punktu, veicot attiecīgus drošības pasākumus. Šajos drošības pasākumos jābūt iekļautiem tehniskiem un organizatoriskiem pasākumiem, lai nodrošinātu, ka uzņēmums šo piekļuvi izmanto tikai tāpēc, lai lietotājs varētu noteikt, kuras viņa kontaktpersonas jau ir attiecīgās programmas lietotāji un tāpēc jau ir iepriekš sniegušas nepārprotamu piekrišanu uzņēmumam vākt un apstrādāt tālruņa numurus šādā nolūkā. To personu mobilo tālruņu numurus, kuras nav programmas lietotāji, var vākt un izmantot tikai un vienīgi ar mērķi pārbaudīt, vai tie ir snieguši nepārprotamu piekrišanu apstrādāt savus datus, un tie pēc tam ir nekavējoties jāizdzēš.

Personīgās informācijas apvienošana dažādos tīmekļa pakalpojumos

26. piemērs: personīgās informācijas apvienošana dažādos tīmekļa pakalpojumos

Interneta uzņēmums, kas sniedz dažādus pakalpojumus, tostarp nodrošina meklēšanas programmu, video koplietošanu un sociālos tīklus, izstrādā konfidencialitātes politiku, kurā ir iekļauts punkts, kas tam ļauj "kombinēt visu personīgo informāciju", kas ir savākta par katru lietotāju attiecībā uz dažādiem izmantotajiem pakalpojumiem, nenosakot datu glabāšanas periodu. Kā norāda uzņēmums, tas tiek darīts, lai garantētu "vislabāko iespējamo pakalpojumu kvalitāti".

Uzņēmums dažādu kategoriju lietotājiem piedāvā vairākus rīkus savu tiesību īstenošanai (piemēram, deaktivizēt mērķtiecīgas reklāmas, iebilst pret noteikta veida sīkfailu iestatīšanu).

Tomēr ar pieejamajiem rīkiem lietotāji nevar efektīvi kontrolēt savu datu apstrādi — lietotāji nevar kontrolēt savu datu konkrētās kombinācijas dažādos pakalpojumos, un lietotāji nevar iebilst pret savu datu kombinēšanu. Kopumā nav līdzsvara starp uzņēmuma likumīgajām interesēm un lietotāju pamattiesību aizsardzību, tāpēc kā apstrādes juridisko pamatojumu nevar izmantot 7. panta f) punktu. Atbilstošāks pamatojums būtu 7. panta a) punkts, ja vien tiek ievēroti derīgas piekrišanas nosacījumi.