Datu valsts inspekcijas rekomendācijas novērtējumam par ietekmi uz datu aizsardzību

Eiropas Parlamenta un Padomes 2016.gada 27.aprīļa regula Nr.2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk – VDAR) paredz uzraudzības iestādei pienākumu publicēt sarakstu ar apstrādes darbības veidiem, attiecībā uz kuriem būs veicams novērtējums par ietekmi uz datu aizsardzību (VDAR 35.panta 4.punkts) (turpmāk – Saraksts).

Datu valsts inspekcija paskaidro, ka tai nav tiesiska pamata Saraksta publiskošanai pirms 2018.gada 25.maija (VDAR tiešas piemērošanas uzsākšanas). Jāņem vērā arī tas, ka institūcija, kurai Datu valsts inspekcijai jāpaziņo par Saraksta publiskošanu un saturu, lai nodrošinātu harmonizētu VDAR piemērošanu Eiropas Savienībā – Eiropas Datu aizsardzības kolēģija – vēl nav uzsākusi darbību un līdz ar to Datu valsts inspekcijai pašlaik nav iespējams pilnībā izpildīt VDAR noteikto pienākumu.

Vienlaikus Datu valsts inspekcija izprot pārziņu vēlmi rast skaidrību par apstrādes darbību veidiem, uz kuriem varētu attiekties VDAR 35.panta 1.punktā noteiktais pienākums veikt novērtējumu par ietekmi uz datu aizsardzību.

Ņemot vērā iepriekš minēto, Datu valsts inspekcija, pārziņiem vērtējot veiktās personas datu apstrādes un plānojot novērtējuma par ietekmi uz datu aizsardzību veikšanas nepieciešamību, rekomendē ņemt vērā sekojošo:

Viens no galvenajiem VDAR mērķiem ir panākt Eiropas Savienības dalībvalstu pieņemto tiesību aktu un izpratnes par personas datu aizsardzību harmonizāciju. Līdz ar to savstarpējai komunikācijai starp dažādu dalībvalstu uzraudzības iestādēm ir izšķiroša nozīme. Forums, kurā pieredzes apmaiņa notiek pašlaik ir Direktīvas 95/46/EK 29.panta darba grupa (turpmāk – Darba grupa). Datu valsts inspekcija vērš uzmanību, ka jaunā Eiropas Savienības institūcija, kurai cita starpā ir jāpaziņo Saraksts, Eiropas Datu aizsardzības kolēģija ir lielā mērā uzskatāma par 29.panta darba grupas mantinieci.

29.panta darba grupa ir izstrādājusi un 2017.gada 4.oktobrī pieņēmusi "Pamatnostādnes novērtējuma par ietekmi uz datu aizsardzību (NIDA)[1] veikšanai un noskaidrošanai, vai apstrāde "varētu radīt augstu risku" Regulas 2016/679 izpratnē (WP 248)" (turpmāk – Vadlīnijas) (http://ec.europa.eu/newsroom/document.cfm?doc_id=47711). Viens no Vadlīniju galvenajiem uzdevumiem ir definēt harmonizētas pamatnostādnes, kuras izmantotu Eiropas Savienības datu aizsardzības uzraudzības iestādes. Cita starp Vadlīnijās tiek definēti kritēriji, kurus piemērojot var identificēt, vai datu apstrāde uzskatāma par tādu, kurā veicams novērtējums par ietekmi uz datu aizsardzību, tādējādi nodrošinot to, ka pirms lēmuma pieņemšanas par Sarakstā iekļaujamajām datu apstrādēm, tiek publiskoti kritēriji, kurus uzraudzības iestādes izmantos, lai konkrētās apstrādes identificētu.

Šo Datu valsts inspekcijas rekomendāciju izstrādē lielā mērā ir izmantotas iepriekš pieminētajās 29.panta darba grupas vadlīnijās paustās atziņas.

---

[1] Citā kontekstā izmanto terminu "ietekmes uz privātumu novērtējums" (IPN), lai atsauktos uz to pašu jēdzienu

Datu valsts inspekcija paskaidro, ka, izvērtējot gadījumus, kad novērtējums par ietekmi uz datu aizsardzību veicams, ir secināms, ka tas pēc būtības ir risku analīzes rīks. Pirmkārt, tas ir jāveic gadījumos, kad ir iespējams augsts risks attiecībā uz fizisku personu tiesībām un brīvībām. Otrkārt, viens no ietekmes novērtējuma galvenajiem uzdevumiem ir identificēt galvenos riskus un iespējamos pasākumus konstatēto risku mazināšanai.

Datu valsts inspekcija vērš uzmanību, ka, lai arī novērtējuma par ietekmi uz datu aizsardzību veikšana ir jauns pienākums, vienlaikus Latvijā pašlaik tiek piemēroti 2015.gada 12.maija Ministru kabineta noteikumi Nr.216 "Kārtība, kādā sagatavo un iesniedz personas datu apstrādes atbilstības novērtējumu" (turpmāk – Noteikumi), kas nosaka idejiski radniecīga pašvērtējuma veikšanu. Privātpersonas ar šiem Noteikumiem varētu būt mazāk pazīstamas, jo personas datu apstrādes atbilstības novērtējuma veikšana ir obligāta valsts un pašvaldību iestādēm. Vienlaikus Datu valsts inspekcija informē, ka, izmantojot iepriekš pieminētos Noteikumus novērtējuma par ietekmi uz datu aizsardzību izstrādei, tas ir jādara, paturot prātā katra novērtējuma veicēja atsevišķo vajadzību, un nepieciešamības gadījumā veicot arī tādas darbības, kas Noteikumos nav paredzētas.

Vienlaikus personām, kas veiks novērtējumu par ietekmi uz datu aizsardzību, ir jāsaprot, ka minētais process ir daļa no VDAR paredzētās pārskatatbildības sistēmas. Līdz ar to lēmumu pieņemšanas process gadījumā, ja tiek nolemts neveikt ietekmes novērtējumu, būtu jādokumentē.

Papildus iepriekš minētajam pārziņiem ir jāapzinās, ka novērtējums par ietekmi uz datu aizsardzību ir pastāvīgs process. Pārziņiem ir jāseko līdzi, vai datu apstrāde, kura neradīja lielus riskus fiziskas personām tiesībām un brīvībām pagātnē, piemēram, ņemot vērā tehnoloģiju attīstību, nerada riskus pašlaik. Pārziņiem nevajadzētu paļauties, ka datu apstrāde ir statiska rakstura, ja pārzinis tajā neveic izmaiņas, jo riskus veiktajai datu apstrādei rada arī ārēji faktori.

Saskaņā ar VDAR galvenais apstāklis, kas jāņem vērā pārzinim, analizējot, vai ir veicams novērtējums par ietekmi uz datu aizsardzību, ir augsts risks fiziskas personas tiesībām un brīvībām. Papildus iepriekš minētajam likumdevējs VDAR 35.panta 3.punktā ir identificējis trīs gadījumus, kad pārzinim jo īpaši būtu jāvērtē augsta riska personu tiesībām un brīvībām iestāšanās:

a) ar fiziskām personām saistītu personisku aspektu sistemātiska un plaša novērtēšana, kuras pamatā ir automatizēta apstrāde, tostarp profilēšana, un ar kuru pamato lēmumus, kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu;

b) 9.panta 1.punktā minēto īpašo kategoriju datu vai 10.pantā minēto personas datu par sodāmību un pārkāpumiem apstrāde plašā mērogā; vai

c) publiski pieejamas zonas sistemātiska uzraudzība plašā mērogā.

Pārziņiem nav jāuzskata, ka, ja plānotā vai veiktā datu apstrāde neatbilst kādai no iepriekš pieminētajām, tad novērtējums par ietekmi uz datu aizsardzību nav veicams. Izšķirošais faktors ietekmes novērtējuma veikšanai ir augsts risks datu subjekta tiesībām un brīvībām, līdz ar to novērtējuma par ietekmi uz datu aizsardzību veikšanas nepieciešamību vērtēt nepieciešams arī datu apstrādēm, kas neatbilst VDAR 35.panta 3.punkta apakšpunktos.

Datu valsts inspekcija vērš uzmanību, ka, ņemot vērā ietekmes novērtējuma lomu pārskatatbildības nodrošināšanas mehānismā, gadījumos, kad pārzinim ir šaubas par novērtējuma par ietekmi uz datu aizsardzību nepieciešamību, ir rekomendējams novērtējumu par ietekmi uz datu aizsardzību veikt. Datu valsts inspekcija informē, ka novērtējums par ietekmi uz datu aizsardzību var atvieglot pārziņa pienākumu veikšanu gan attiecībā uz datu subjektu tiesību nodrošināšanu, gan arī uz nepieciešamo tehnisko un organizatorisko datu aizsardzības drošības pasākumu ieviešanu.

Lai atvieglotu pārziņiem veiktās personas datu apstrādes analīzes procesu attiecībā uz to gadījumu identifikāciju, kad veicams novērtējums par ietekmi uz datu aizsardzību, Vadlīnijās ir iekļauti deviņi kritēriji. Lielākajā daļā gadījumu novērtējums par ietekmi uz datu aizsardzību būs veicams, ja uz plānoto datu apstrādi būs attiecināmi vismaz divi no Vadlīnijās minētajiem kritērijiem.

Vadlīnijās norādīti šādi kritēriji:

1. Vērtēšana vai punktu piešķiršana, tostarp profilēšana un prognozes, īpaši ņemot vērā "aspektus saistībā ar datu subjekta sniegumu darbā, ekonomisko situāciju, veselību, personīgām vēlmēm vai interesēm, uzticamību vai uzvedību, atrašanās vietu vai pārvietošanos" (VDAR 71. un 91.apsvērums). *Var minēt šādus piemērus: finanšu iestāde, kas pārbauda klientus, izmantojot kredītu uzziņas datubāzi vai datubāzi saistībā ar nelikumīgi iegūtu līdzekļu legalizāciju un terorisma finansēšanas apkarošanu (AML/CTF) vai krāpšanas gadījumiem; biotehnoloģiju uzņēmums, kas piedāvā ģenētiskus izmeklējumus tieši klientiem, lai novērtētu un prognozētu slimības/veselības riskus; uzņēmums, kas izstrādā rīcības vai mārketinga profilus, balstoties uz tā tīmekļa vietnes lietošanu.*

2. Tādu lēmumu automatizēta pieņemšana, kuriem ir tiesiskas vai līdzīgi būtiskas sekas: apstrāde, kuras mērķis ir pieņemt lēmumus par datu subjektiem, "kas fiziskai personai rada tiesiskās sekas vai līdzīgi būtiski ietekmē fizisko personu" (VDAR 35.panta 3.punkta a) apakšpunkts). *Piemēram, datu apstrādes rezultātā personas var tikt izslēgtas vai diskriminētas. Apstrāde, kam ir neliela ietekme uz personām vai tādas nav, neatbilst šim īpašajam kritērijam. Sīkāki paskaidrojumi par šiem jēdzieniem būs sniegti 29.panta darba grupas pamatnostādnēs par profilēšanu, kas tiks izdotas drīzumā.*

3. Sistemātiska novērošana: apstrāde, ko izmanto, lai novērotu, uzraudzītu vai kontrolētu datu subjektus, tostarp dati, kas iegūti tīmeklī vai "publiski pieejamas zonas sistemātiskas uzraudzības" rezultātā (VDAR 35.panta 3.punkta c) apakšpunkts) Šāda veida uzraudzība ir kritērijs tāpēc, ka personas datus var ievākt apstākļos, kad datu subjekti, iespējams, nezina, kas vāc viņu datus un kā tie tiks izmantoti. Tāpat personām var nebūt iespējas izvairīties no šādas viņu datu apstrādes publiskajā(-ās) (vai publiski pieejamajā(-ās)) zonā(-ās).

4. Sensitīvi dati vai ļoti personiska rakstura dati: tie ietver personas datu īpašas kategorijas, kā definēts VDAR 9.pantā *(piemēram, informācija par personas politiskajiem uzskatiem)*, kā arī personas datus, kas attiecas uz sodāmību vai noziedzīgiem nodarījumiem, kā definēts VDAR 10.pantā. *Var minēt šādus piemērus: slimnīcas uzskaite, kurā glabā pacientu medicīniskos datus; privāta izmeklētāja uzskaite, kurā saglabātas ziņas par pārkāpējiem.* Papildus šiem

noteikumiem, kas definēti VDAR, var uzskatīt, ka dažas datu kategorijas palielina iespējamo risku personu tiesībām un brīvībām. Šie personas dati ir uzskatāmi par sensitīviem (kā šo terminu ierasti izprot) tāpēc, ka tie ir saistīti ar sadzīves un privātām darbībām *(piemēram, elektroniskā saziņa, kuras konfidencialitāte ir jāaizsargā)*, tie ietekmē pamattiesību īstenošanu *(piemēram, atrašanās vietas datu vākšana, ja tas apdraud pārvietošanās brīvību)* vai to aizsardzības pārkāpšana nepārprotami būtiski ietekmē datu subjekta ikdienas dzīvi *(piemēram, finanšu dati, ko var izmantot krāpšanai saistībā ar maksājumiem)*. Šajā sakarā var būt nozīmīgi, vai datu subjekts vai trešās personas jau ir padarījušas datus publiski pieejamus. Faktu, ka personas dati ir publiski pieejami, var uzskatīt par faktoru, novērtējot, vai datus bija paredzēts tālāk izmantot noteiktiem nolūkiem. Šis kritērijs var aptvert arī šādus datus: privāti dokumenti, e-pasta ziņojumi, dienasgrāmatas, piezīmes e-lasītāju ierīcēs, kas aprīkotas ar piezīmju funkcijām, un ļoti personiska rakstura informācija ikdienas norišu reģistrēšanas lietotnēs.

5. Plašā mērogā apstrādāti dati: VDAR nav definēts, kas ir plaša mēroga apstrāde, taču VDAR 91.apsvērumā ir dotas dažas norādes. Jebkurā gadījumā 29.panta darba grupa iesaka, nosakot, vai apstrādi veic plašā mērogā[2], jo īpaši ņemt vērā šādus faktorus:

a) attiecīgo datu subjektu skaits — vai nu kā konkrēts skaitlis, vai kā attiecīgās populācijas daļa;

b) datu apjoms un/vai dažādo apstrādāto datu vienumu klāsts;

c) datu apstrādes darbības ilgums vai pastāvīgums;

d) apstrādes darbības ģeogrāfiskais tvērums.

6. Datu kopu saskaņošana vai apkopošana — *piemēram, tādu, kuras iegūst no divām vai vairākām datu apstrādes darbībām, kas veiktas citam nolūkam un/vai ko veica citi datu pārziņi,* — tādējādi, ka tas pārsniedz saprātīgas datu subjekta gaidas.

7. Dati par neaizsargātiem datu subjektiem (VDAR 75.apsvērums): šāda veida datu apstrāde ir noteikta kā kritērijs tāpēc, ka pastāv paaugstināta nelīdzsvarotība iespēju ziņā starp datu subjektiem un datu pārzini, un tas nozīmē, ka, iespējams, personas nevar bez grūtībām piekrist savu datu apstrādei vai iebilst pret to, vai īstenot savas tiesības. Neaizsargāti datu subjekti var būt bērni (var uzskatīt, ka viņi nevar apzināti vai pārdomāti iebilst pret savu datu apstrādi vai piekrist tai), darba ņēmēji, tādu neaizsargātāku iedzīvotāju slāņi, kuriem nepieciešama īpaša aizsardzība (garīgi slimas personas, patvēruma meklētāji, vecāka gadagājuma cilvēki, pacienti utt.), un jebkurā gadījumā — datu subjekti gadījumos, kad var konstatēt nelīdzsvarotību attiecībās starp datu subjekta un pārziņa stāvokli.

8. Jaunu tehnoloģisko vai organizatorisko risinājumu izmantošana vai piemērošana, *piemēram, pirkstu nospiedumu un sejas atpazīšanas vienlaicīga izmantošana, lai uzlabotu fiziskās piekļuves kontroli, utt.* VDAR ir skaidri noteikts (35.panta 1.punkts un 89. un 91.apsvērums), ka jaunas tehnoloģijas lietošana, kā

[2] Datu valsts inspekcija 2018.gada februārī plāno publiskot izvērstāku skaidrojumu attiecībā uz termina plašs mērogs skaidrojumu. Lūdzam sekot līdzi informācijai Datu valsts inspekcijas mājas lapā.

definēts — "saskaņā ar sasniegto tehnoloģisko zināšanu līmeni" (VDAR 91.apsvērums), var noteikt nepieciešamību veikt novērtējumu par ietekmi uz datu aizsardzību. Tas tā ir tāpēc, ka šādas tehnoloģijas lietošana var ietvert jaunus datu vākšanas un lietošanas veidus, kuri, iespējams, rada augstu risku attiecībā uz personu tiesībām un brīvībām. Personiska un sociāla rakstura sekas, ko rada jaunas tehnoloģijas lietošanas uzsākšana, var nebūt zināmas. Novērtējums par ietekmi uz datu aizsardzību palīdzēs datu pārzinim izprast un novērst šādus riskus. *Piemēram, dažām "lietiskā interneta" lietotnēm varētu būt būtiska ietekme uz personu ikdienu un privātumu, tāpēc ir jāveic novērtējums par ietekmi uz datu aizsardzību*.

9. Ja apstrāde kā tāda "kavē datu subjektus īstenot savas tiesības vai izmantot pakalpojumu vai līgumu" (VDAR 22.pants un 91.apsvērums). Tas ietver apstrādes darbības, kuru mērķis ir ļaut vai liegt datu subjektiem piekļuvi pakalpojumam vai līguma noslēgšanai, vai grozīt šādas piekļuves nosacījumus. *Kā piemēru var minēt gadījumus, kad banka pārbauda savus klientus, izmantojot kredītu uzskaites datubāzi, lai izlemtu, vai piedāvāt tiem aizdevumu.*

Datu valsts inspekcija vērš uzmanību, ka, izmantojot iepriekš minētos kritērijus, tiks izstrādāts un publiskots to apstrādes darbību saraksts, attiecībā uz kurām ir jāveic novērtējums par ietekmi uz datu aizsardzību, kad šādu sarakstu būs iespējams iesniegt Eiropas datu aizsardzības kolēģijai. Vienlaikus netiek izslēgta iespēja laika gaitā papildināt sarakstu ar, piemēram, jebkāda veida biometrisko datu vai bērnu datu apstrādi.

Vadlīnijās sniegti šādi apstrādes piemēri, kurus samērojot ar kritērijiem, var identificēt apstrādes, kuras veicot nepieciešams novērtējums par ietekmi uz datu aizsardzību:

Apstrādes piemēri	**Iespējami nozīmīgie kritēriji**	**Vai varētu būt vajadzīgs novērtējums par ietekmi uz datu aizsardzību**
Slimnīca apstrādā savu pacientu ģenētiskos un veselības datus (slimnīcas informācijas sistēma).	- sensitīvi dati vai ļoti personiska rakstura dati; - dati par neaizsargātiem datu subjektiem; - plašā mērogā apstrādāti dati	Jā
Ierakstīšanas sistēmas lietošana, lai uzraudzītu braukšanas kultūru uz autoceļiem. Pārzinis plāno izmantot inteliģentas video analīzes sistēmu, lai identificētu automašīnas un automātiski atpazītu numura zīmes.	- sistemātiska novērošana; - tehnoloģisku vai organizatorisku risinājumu inovatīva lietošana vai piemērošana	Jā
Uzņēmums sistemātiski novēro savu darbinieku darbības, tostarp darbinieku darbstaciju, aktivitātes tīmeklī utt.	- sistemātiska novērošana; - dati par neaizsargātiem datu subjektiem	Jā
Publiski pieejamu sociālo	- vērtēšana vai punktu piešķiršana;	Jā

plašsaziņas līdzekļu datu vākšana profilu izstrādei.	- plašā mērogā apstrādāti dati; - datu kopu saskaņošana vai apkopošana; - sensitīvi dati vai ļoti personiska rakstura dati	
Iestāde, kas izstrādā valsts līmeņa kredīta reitingu vai krāpšanas gadījumu datubāzi.	- vērtēšana vai punktu piešķiršana; - tādu lēmumu automatizēta pieņemšana, kuriem ir tiesiskas vai līdzīgi būtiskas sekas; - kavē datu subjektus īstenot savas tiesības vai izmantot pakalpojumu vai līgumu; - sensitīvi dati vai ļoti personiska rakstura dati	Jā
Pseidonimizētu sensitīvu personas datu uzglabāšana arhivēšanas nolūkā attiecībā uz neaizsargātiem datu subjektiem, kas piedalās izpētes projektos vai klīniskajos pētījumos	- sensitīvi dati; - dati par neaizsargātiem datu subjektiem; - kavē datu subjektus īstenot savas tiesības vai izmantot pakalpojumu vai līgumu	Jā
"Pacientu vai klientu personas datu apstrāde, ko veic konkrēts ārsts, veselības aprūpes speciālists vai advokāts" (91. apsvērums).	- sensitīvi dati vai ļoti personiska rakstura dati; - dati par neaizsargātiem datu subjektiem	Nē
Tiešsaistes žurnāls, kas izmanto adresātu sarakstu, lai saviem abonentiem nosūtītu dienas notikumu vispārēju apskatu.	- plašā mērogā apstrādāti dati	Nē
E-komercijas tīmekļa vietne, kurā reklamē antīku automašīnu rezerves daļas, veicot ierobežotu profilēšanu, ņemot vērā tīmekļa vietnē aplūkotās vai nopirktās preces.	- vērtēšana vai punktu piešķiršana	Nē
Videoreģistratora izmantošana ģimenes automašīnā[3]	- Sistēmiska novērošana,	Nē
Videoreģistratoru izmantošana loģistikas uzņēmumā, vai pasažieru pārvadāšanas uzņēmumā, ja dati tiek apkopoti[4]	- Sistēmiska novērošana - Plašs mērogs	Jā

Izprast neviennozīmīgo jautājumu par gadījumiem, kad izstrādājams novērtējums par ietekmi uz datu aizsardzību, var palīdzēt arī skaidrs priekšstats par

[3] Datu valsts inspekcijas pievienots piemērs
[4] Datu valsts inspekcijas pievienots piemērs

apstrādēm, attiecībā uz kurām novērtējums par ietekmi uz datu aizsardzību nav veicams.

Līdz ar to Datu valsts inspekcija vērš uzmanību uz Vadlīnijās izteiktajiem apsvērumiem, kad novērtējums par ietekmi uz datu aizsardzību nav jāveic:

- ja apstrāde nav tāda, kas "varētu radīt augstu risku fizisku personu tiesībām un brīvībām" (VDAR 35.panta 1.punkts);

- ja apstrādes raksturs, apmērs, konteksts un nolūki ir ļoti līdzīgi apstrādei, attiecībā uz kuru jau ir veikts novērtējums par ietekmi uz datu aizsardzību. Šādos gadījumos var izmantot tā novērtējuma par ietekmi uz datu aizsardzību rezultātus, kas veikts attiecībā uz līdzīgu apstrādi (VDAR 35.panta 1.punkts);

- ja uzraudzības iestāde pirms 2018.gada maija ir pārbaudījusi apstrādes darbības noteiktos apstākļos, kas nav mainījušies (Vadlīniju III daļas C. sadaļu);

- ja saskaņā ar VDAR 6.panta 1.punkta c) vai e) apakšpunktu apstrādes darbībai ir tiesisks pamats, kas noteikts Eiropas Savienības vai dalībvalsts tiesību aktos, ar kuriem reglamentē konkrēto apstrādes darbību, un ja novērtējums par ietekmi uz datu aizsardzību jau ir veikts saistībā ar tiesiskā pamata noteikšanu (VDAR 35.panta 10.punkts), izņemot, ja dalībvalsts uzskata, ka pirms apstrādes darbībām ir jāveic novērtējums par ietekmi uz datu aizsardzību;

- ja apstrādes darbība ir iekļauta izvēles sarakstā (ko izstrādā uzraudzības iestāde), kurā uzskaitītas tās apstrādes darbības, attiecībā uz kurām nav vajadzīgs novērtējums par ietekmi uz datu aizsardzību (VDAR 35.panta 5.punkts). Šāds saraksts var ietvert apstrādes darbības, kas atbilst šīs iestādes nosacījumiem, kuri izvirzīti, pieņemot pamatnostādnes, konkrētus lēmumus vai atļaujas, atbilstības noteikumus utt. (piem., Francijā — atļaujas, izņēmumus, vienkāršotus noteikumus, noteikumu kopumus par atbilstību u.c.). Šādos gadījumos, un ja kompetentā iestāde veic pārskatīšanu, novērtējums par ietekmi uz datu aizsardzību nav vajadzīgs, taču tikai tad, ja apstrāde precīzi ietilpst attiecīgās sarakstā minētās procedūras darbības jomā un joprojām pilnībā atbilst visām VDAR definētajām attiecīgajām prasībām.

Datu valsts inspekcija vērš uzmanību, ka novērtējums par ietekmi uz datu aizsardzību nav vajadzīgs attiecībā uz apstrādes darbībām, kuras ir pārbaudījusi uzraudzības iestāde vai datu aizsardzības speciālists saskaņā ar Direktīvas 95/46/EK 20.pantu (apstrādēm, kas reģistrētas Datu valsts inspekcijā saskaņā ar Fizisko personu datu aizsardzības likuma 21.pantu) un kuru īstenošanas veids kopš iepriekšējās pārbaudes veikšanas dienas nav mainījies. Un pretēji, tas nozīmē, ka novērtējums par ietekmi uz datu aizsardzību ir jāveic attiecībā uz jebkādu datu apstrādi, kuras īstenošanas apstākļi (apmērs, nolūks, savāktie personas dati, datu pārziņu vai saņēmēju identitāte, datu uzglabāšanas periods, tehniskie un organizatoriskie pasākumi utt.) ir mainījušies kopš iepriekšējās pārbaudes, ko veica uzraudzības iestāde vai datu aizsardzības speciālists, un ja šī apstrāde varētu radīt augstu risku.

Vienlaikus Datu valsts inspekcija paskaidro, ka prasība veikt novērtējumu par ietekmi uz datu aizsardzību ir piemērojama apstrādes darbībām, kas jau tiek veiktas, ja tās varētu radīt augstu risku fizisku personu tiesībām un brīvībām un ja

ir mainījušies ar tām saistītie riski, ņemot vērā apstrādes raksturu, apmēru, kontekstu un nolūkus.

Novērtējums par ietekmi uz datu aizsardzību ir veicams pirms personas datu apstrādes uzsākšanas. Novērtējums par ietekmi uz datu aizsardzību uzskatāms par rīku, kam jāpalīdz pieņemt lēmums par datu apstrādi.

Par novērtējuma par ietekmi uz datu aizsardzību veikšanu atbildīgs ir pārzinis. Datu aizsardzības speciālista (ja tāds uzņēmumam norīkots) iesaisti novērtējuma par ietekmi uz datu aizsardzību izstrādē ir jāvērtē, analizējot iespējamos interešu konfliktus, kā arī ņemot vērā VDAR noteiktos datu aizsardzības speciālista pienākumus.

Ja pēc novērtējuma par ietekmi uz datu aizsardzību veikšanas un pasākumu ieviešanas, pārzinis joprojām saskata augstus riskus plānotajai personas datu apstrādei, tad pārziņa pienākums ir konsultēties ar uzraudzības iestādi. Nepieņemami augsta atlikušā riska piemērs ir gadījumi, kad datu subjektiem var rasties būtiskas vai pat neatgriezeniskas sekas, kuras tie, iespējams, nevar pārvarēt *(piemēram, pretlikumīga piekļuve datiem, kā rezultātā rodas apdraudējums datu subjektu dzīvei, ir iespējama atlaišana no darba, rodas finanšu apdraudējums)*, un/vai kad šķiet pašsaprotami, ka risks radīsies (*piemēram, ja nav iespējams samazināt to cilvēku skaitu, kuri piekļūst datiem to kopīgošanas, lietojuma vai izplatīšanas veida dēļ, vai ja nav novērsta labi zināma ievainojamība)*.

Turklāt pārzinim būs jāapspriežas ar uzraudzības iestādi, ja dalībvalsts tiesību aktos ir noteikts, ka pārziņiem ir jāapspriežas ar uzraudzības iestādi un jāsaņem no tās iepriekšēja atļauja saistībā ar apstrādi, ko veic pārzinis, lai izpildītu sabiedrības interesēs īstenojamu uzdevumu, tostarp, kad minēto apstrādi veic saistībā ar sociālo aizsardzību un sabiedrības veselību (VDAR 36.panta 5.punkts). Papildus iepriekš minētajam Datu valsts inspekcija paskaidro, ka arī pašlaik spēkā esošais regulējums nosaka procedūru, kas ir veicama, kad plānotā datu apstrāde var radīt paaugstinātus riskus fizisku personu tiesībām un brīvībām. Fizisko personu datu aizsardzības likuma 21.pantā ir noteikts pārziņu pienākums pirms personas datu apstrādes uzsākšanas reģistrēt personas datu apstrādi Datu valsts inspekcijā vai norīkot fizisko personu — datu aizsardzības speciālistu —, pantā norādītajos gadījumos. Pēc būtības salīdzinot datu apstrādes, kas iekļautas 21.panta punktos un VDAR 35.panta 3.punkta apakšpunktos, varam identificēt, ka VDAR 35.panta 3.punkta a) apakšpunktā iekļautā personas datu apstrāde, lielā mērā atbilst Fizisko personu datu aizsardzības likuma 21.panta 2.punktā norādītajai, VDAR 35.panta 3.punkta b) apakšpunktā norādītais, lielā mērā atbilst Fizisko personu datu aizsardzības likuma 21.panta 3., 4. un 6.punktā norādītajam, savukārt VDAR 35.panta 3.punkta c) apakšpunktā norādītais, lielā mērā pārklājas ar Fizisko personu datu aizsardzības likuma 21.panta 6.punktā norādīto. Vienlaikus Datu valsts inspekcija vērš uzmanību, ka VDAR iekļautie īpašie gadījumi, kad veicams novērtējums par ietekmi uz datu aizsardzību, ir ievērojami šaurāki, kā tās datu apstrādes, uz kurām attiecas personas datu apstrādes reģistrācijas pienākums. Datu valsts inspekcija vērš uzmanību arī uz VDAR 89.apsvērumā minēto, ka personas datu apstrādes reģistrācijas pienākums pēc VDAR tiešas piemērošanas uzsākšanas vairs nepastāvēs, līdz ar to zināmā mērā līdzšinējo personas datu apstrādes

reģistrācijas pienākumu noteiktos gadījumos, kas uzlika pārziņiem ievērojamu administratīvo slogu, aizstāj personas datu apstrādes paškontroles mehānisms, kura obligāta izmantošana ir noteikti krietni šaurākā gadījumu skaitā, kā līdzšinējais personas datu apstrādes reģistrācijas pienākums.

Datu valsts inspekcija vērš uzmanību pilnīgākas informācijas iegūšanai attiecībā uz novērtējuma par ietekmi uz datu aizsardzību izstrādi iepazīties ar pilnu Vadlīniju tekstu, savukārt jautājumu vai neskaidrību gadījumā vērsties Datu valsts inspekcijā.