

# Pamatnostādnes



**Pamatnostādnes Nr. 01/2022 par datu subjektu tiesībām.  
Piekļuves tiesības**

**Versija 2.0**

**Pieņemtas 2023. gada 28. martā**

## Versiju vēsture

Versija 1.0	2022. gada 18. janvārī	Pamatnostādņu pieņemšana sabiedriskajai apspriešanai
Versija 2.0	2023. gada 28. martā	Pamatnostādņu pieņemšana pēc sabiedriskās apspriešanas

## KOPSAVILKUMS

Datu subjektu piekļuves tiesības ir nostiprinātas ES Pamattiesību hartas 8. pantā. Tā jau no paša sākuma ir bijusi daļa Eiropas datu aizsardzības tiesiskā regulējuma un tagad ir papildināta ar konkrētākiem un precīzākiem noteikumiem VDAR 15. pantā.

### **Piekļuves tiesību mērķis un vispārējā struktūra**

Piekļuves tiesību vispārējais mērķis ir sniegt personām pietiekamu, pārredzamu un viegli pieejamu informāciju par viņu persondatu apstrādi, lai tās varētu zināt par apstrādi un pārbaudīt apstrādes likumīgumu, kā arī apstrādāto datu precizitāti. Tādējādi personai būs vieglāk — tomēr tas nav nosacījums — īstenot citas tiesības, piemēram, tiesības uz datu dzēšanu vai labošanu.

Piekļuves tiesības saskaņā ar datu aizsardzības tiesību aktiem ir jānošķir no līdzīgām tiesībām ar citiem mērķiem, piemēram, tiesībām piekļūt publiskiem dokumentiem, kuru mērķis ir nodrošināt publisko iestāžu lēmumu pieņemšanas pārredzamību un labu administratīvo praksi.

Tomēr datu subjektam nav jāmin piekļuves pieprasījuma iemesli un pārzinim nav jāanalizē, vai šis pieprasījums datu subjektam faktiski palīdzēs pārliecināties par attiecīgās apstrādes likumīgumu vai īstenot citas tiesības. Pārzinim šis pieprasījums būs jāizskata, izņemot gadījumus, kad ir skaidrs, ka tas iesniegts saskaņā ar citiem noteikumiem, kas nav datu aizsardzības noteikumi.

Piekļuves tiesības ietver trīs dažādus komponentus, proti:

- apstiprinājumu tam, ka persondati tiek vai netiek apstrādāti;
- piekļuvi šiem persondatiem;
- piekļuvi informācijai par apstrādi, piemēram, par nolūku, datu kategorijām un saņēmējiem, apstrādes ilgumu, datu subjektu tiesībām un atbilstošiem aizsardzības pasākumiem gadījumos, kad dati tiek nosūtīti trešām valstīm.

### **Vispārīgi apsvērumi attiecībā uz datu subjekta pieprasījuma novērtējumu**

Analizējot pieprasījuma saturu, pārzinim ir jānovērtē, vai pieprasījums attiecas uz pieprasījuma iesniedzējas persondatiem, vai uz pieprasījumu attiecas 15. panta darbības joma un vai pastāv citi konkrētāki noteikumi, kas reglamentē piekļuvi konkrētā nozarē. Pārzinim ir arī jānovērtē, vai pieprasījums attiecas uz visiem apstrādātajiem datu subjekta datiem vai tikai to daļu.

Īpašu prasību attiecībā uz pieprasījuma formātu nav. Pārzinim būtu jānodrošina atbilstoši un lietotājiem ērti saziņas kanāli, kurus datu subjekts var viegli izmantot. Tomēr datu subjektam šie konkrētie kanāli nav obligāti jāizmanto, un pieprasījumu viņš var nosūtīt arī pārziņa oficiālajam kontaktpunktam. Pārzinim nav pienākuma reaģēt uz pieprasījumiem, kas nosūtīti uz pilnīgi nejausām vai acīmredzami nepareizām adresēm.

Ja pārzinis nespēj identificēt datus, kuri attiecas uz datu subjektu, tas par to informē datu subjektu un var atteikt piekļuvi, ja datu subjekts nesniedz papildu informāciju, kas ļauj viņu identificēt. Turklāt, ja pārzinim ir šaubas par to, vai datu subjekts ir tas, par ko uzdodas, pārzinis var pieprasīt papildu informāciju, lai apstiprinātu datu subjekta identitāti. Lai izvairītos no pārmērīgas datu vākšanas, papildu informācijas pieprasījumam jābūt samērīgam ar apstrādāto datu veidu, iespējamo kaitējumu utt.

### **Piekļuves tiesību tvērums**

Piekļuves tiesību tvērumu nosaka VDAR 4. panta 1. punktā definētā persondatu jēdziena tvērums. Papildus tādiem personas pamatdatiem kā vārds un uzvārds, adrese, tālruna numurs u. c. šī definīcija var attiekties uz visdažādākajiem datiem, piemēram, medicīniskiem konstatējumiem, pirkumu vēsturi, kredītspējas rādītājiem, darbības žurnāliem, meklēšanas darbībām u. c. Pseudonimizēti persondati joprojām ir persondati pretstatā anonimizētiem datiem. Piekļuves tiesības attiecas uz tās personas persondatiem, kura iesniedz pieprasījumu. To nevajadzētu interpretēt pārāk šauri, proti, ietverti var būt arī dati, kuri varētu attiekties uz citām personām, piemēram, saziņas vēsture ar ienākošajiem un izejošajiem ziņojumiem.

Pārzinim ir ne vien jānodrošina piekļuve persondatiem, bet arī jāsniedz papildu informācija par apstrādi un datu subjektu tiesībām. Šādas informācijas pamatā var būt informācija, kas jau ir apkopota pārziņa apstrādes darbību reģistrā (VDAR 30. pants) un paziņojumā par privātumu (VDAR 13. un 14. pants). Tomēr šo vispārīgo informāciju pieprasījuma iesniegšanas brīdī var nākties atjaunināt vai pielāgot, lai atspoguļotu apstrādes darbības, kas tiek veiktas saistībā ar konkrēto personu, kura iesniedz pieprasījumu.

### **Kā nodrošināt piekļuvi**

Piekļuves nodrošināšanas veidi var atšķirties atkarībā no datu apjoma un veiktās apstrādes sarežģītības. Ja vien nav skaidri norādīts citādi, būtu jāuzskata, ka pieprasījums attiecas uz *visiem* datu subjekta persondatiem, un, ja pārzinis apstrādā lielu datu apjomu, tas var lūgt, lai datu subjekts pieprasījumu precizētu.

Pārzinim persondati būs jāmeklē visās IT sistēmās un ar IT nesaistītās kartotēkās, pamatojoties uz meklēšanas kritērijiem, kas atspoguļo veidu, kādā informācija ir strukturēta, piemēram, pamatojoties uz vārdu un uzvārdu un klienta numuru. Dati un cita informācija par apstrādi jāpaziņo kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu. Precīzākas prasības šajā saistībā ir atkarīgas no datu apstrādes apstākļiem, kā arī no datu subjekta spējas uztvert un saprast saziņu (piemēram, ja datu subjekts ir bērns vai persona ar īpašām vajadzībām). Ja dati sastāv no kodiem vai citiem "neapstrādātiem datiem", tie var būt jāpaskaidro, lai datu subjektam tie būtu saprotami.

Galvenais piekļuves nodrošināšanas veids ir nodrošināt datu subjektam viņa datu kopiju, bet var paredzēt arī citus veidus (piemēram, mutisku informēšanu un piekļuvi uz vietas), ja datu subjekts tos pieprasa. Datus var nosūtīt pa e-pastu, ja vien tiek piemēroti visi vajadzīgie aizsardzības pasākumi, ņemot vērā, piemēram, datu veidu, vai citādi, piemēram, pašapkalpošanās rīkā.

Dažkārt, kad datu apjoms ir liels un datu subjektam būtu grūti saprast informāciju, ja tā visa tiktu sniegta vienā reizē, jo īpaši tiešsaistes kontekstā, vispiemērotākais pasākums varētu būt vairāku līmeņu pieeja. Sniedzot informāciju dažādos līmeņos, datu subjektam var būt vieglāk datus saprast. Pārzinim jāspēj uzskatāmi parādīt, ka vairāku līmeņu pieeja nodrošina datu subjektam pievienoto vērtību, un, ja datu subjekts to izvēlas, visi līmeņi būtu jānodrošina vienlaikus.

Datu kopija un papildu informācija būtu jānodrošina pastāvīgā formā, piemēram, rakstītā tekstā, kas varētu būt parasti izmantotā elektroniskā formātā, lai datu subjekts to varētu viegli lejuplādēt. Datus var nodrošināt atšifrētā vai apkopotā veidā, ja vien tiek iekļauta visa informācija un informācijas saturs netiek pārveidots vai mainīts.

Pieprasījums jāizpilda pēc iespējas ātrāk un jebkurā gadījumā viena mēneša laikā pēc tā saņemšanas. Nepieciešamības gadījumā minēto laikposmu var pagarināt par diviem mēnešiem, ņemot vērā pieprasījumu sarežģītību un skaitu. Tādā gadījumā datu subjekts ir jāinformē par kavēšanās iemeslu.

Pārzinim ir jāisteno vajadzīgie pasākumi, lai pieprasījumus izskatītu pēc iespējas ātrāk, un jāpielāgo šie pasākumi apstrādes apstākļiem. Ja datus glabā tikai ļoti īsu laikposmu, jābūt ieviestiem pasākumiem, kas garantē, ka piekļuves pieprasījumu var izpildīt, datiem netiekot dzēstiem pieprasījuma izskatīšanas laikā. Ja tiek apstrādāts liels daudzums datu, pārzinim būs jāievieš apstrādes sarežģītībai pielāgota kārtība un mehānismi.

Pieprasījuma novērtējumam būtu jāatspoguļo situācija tajā brīdī, kad pārzinis saņēmis pieprasījumu. Būs jāsniedz pat tādi dati, kas var būt nepareizi vai nelikumīgi apstrādāti. Datus, kas jau ir dzēsti, piemēram, saskaņā ar glabāšanas politiku, un tādējādi pārzinim vairs nav pieejami, nevar sniegt.

### **Ierobežojumi**

VDAR pieļauj noteiktus piekļuves tiesību ierobežojumus. Nekādu citu izņēmumu vai atkāpju nav. Uz piekļuves tiesībām neattiecas nekādas vispārējas atrunas par samērīgumu attiecībā uz pārziņa centieniem izpildīt datu subjekta pieprasījumu.

Saskaņā ar 15. panta 4. punktu tiesības saņemt kopiju nedrīkst nelabvēlīgi ietekmēt citu personu tiesības un brīvības. EDAK uzskata, ka šīs tiesības jāņem vērā ne tikai piekļuves piešķiršanas brīdī, nodrošinot kopiju, bet arī tad, ja piekļuve datiem tiek nodrošināta citā veidā (piemēram, piekļuve uz vietas). Tomēr 15. panta 4. punkts nav piemērojams papildu informācijai par apstrādi, kā noteikts 15. panta 1. punkta a)–h) apakšpunktā. Pārzinim ir jāspēj uzskatāmi parādīt, ka konkrētajā situācijā tiktu negatīvi ietekmētas citu personu tiesības vai brīvības. Piemērojot 15. panta 4. punktu, datu subjekta pieprasījumu nevajadzētu pilnībā noraidīt; varētu tikai izlaist vai padarīt nesalasāmas tās daļas, kurām var būt negatīva ietekme uz citu personu tiesībām un brīvībām.

VDAR 12. panta 5. punkts ļauj pārziņiem noraidīt pieprasījumus, kas ir acīmredzami nepamatoti vai pārmērīgi, vai par šādiem pieprasījumiem pieprasīt saprātīgu maksu. Šie jēdzieni ir jāinterpretē šauri. Tā kā piekļuves pieprasījumiem ir ļoti maz priekšnoteikumu, pieprasījuma uzskatīšana par acīmredzami nepamatotu ir diezgan ierobežota. Pārmērīgi pieprasījumi ir atkarīgi no tās nozares specifikas, kurā pārzinis darbojas. Jo biežāk notiek izmaiņas pārziņa datubāzē, jo biežāk datu subjektam var būt jālūdz pieprasīt piekļuvi, tai neesot pārmērīgai. Tā vietā, lai atteiktu piekļuvi, pārzinis var pieņemt lēmumu datu subjektam pieprasīt samaksu. Tas attiektos tikai uz pārmērīgiem pieprasījumiem, lai segtu administratīvās izmaksas, ko šādi pieprasījumi var radīt. Pārzinim jāspēj uzskatāmi parādīt, ka pieprasījums ir acīmredzami nepamatots vai pārmērīgs.

Piekļuves tiesību ierobežojumi saskaņā ar VDAR 23. pantu un tajā paredzētajām atkāpēm var pastāvēt arī dalībvalstu tiesību aktos. Pārziņiem, kas šādus ierobežojumus plāno izmantot, ir rūpīgi jāpārbauda valsts noteikumu prasības un jāņem vērā visi īpašie nosacījumi, kas var tikt piemēroti. Šādi nosacījumi var būt tādi, ka piekļuves tiesības tiek atliktas tikai uz laiku vai ka ierobežojums attiecas tikai uz konkrētām datu kategorijām.

## Satura rādītājs

1.	Ievads. Vispārīgi apsvērumi .....	8
2.	Piekļuves tiesību mērķis, VDAR 15. panta struktūra un vispārējie principi.....	10
2.1.	Piekļuves tiesību mērķis .....	10
2.2.	VDAR 15. panta struktūra.....	11
2.2.1.	Piekļuves tiesību satura noteikšana .....	12
2.2.1.1.	Apstiprinājums par to, vai persondati tiek vai netiek apstrādāti .....	12
2.2.1.2.	Piekļuve apstrādājamajiem persondatiem.....	12
2.2.1.3.	Informācija par apstrādi un datu subjekta tiesībām .....	13
2.2.2.	Noteikumi par kārtību .....	13
2.2.2.1.	Kopijas nodrošināšana.....	13
2.2.2.2.	Papildu kopiju nodrošināšana .....	14
2.2.2.3.	Informācijas pieejamības nodrošināšana plaši izmantotā elektroniskā formātā.....	15
2.2.3.	Piekļuves tiesību iespējamais ierobežojums .....	15
2.3.	Piekļuves tiesību vispārējie principi.....	15
2.3.1.	Informācijas pilnīgums .....	16
2.3.2.	Informācijas pareizība .....	17
2.3.3.	Novērtējuma laika atskaites punkts .....	18
2.3.4.	Datu drošības prasību ievērošana .....	19
3.	Vispārīgi apsvērumi attiecībā uz piekļuves pieprasījumu novērtēšanu .....	19
3.1.	Ievads.....	19
3.1.1.	Pieprasījuma satura analīze.....	20
3.1.2.	Pieprasījuma forma .....	22
3.2.	Identifikācija un autentifikācija .....	23
3.3.	Samērīguma novērtējums attiecībā uz pieprasījuma iesniedzējas personas autentificēšanu	25
3.4.	Pieprasījumi, ko iesniedz ar trešu/pilnvarotu personu starpniecību .....	28
3.4.1.	Piekļuves tiesību īstenošana bērnu vārdā .....	29
3.4.2.	Piekļuves tiesību īstenošana, izmantojot trešas personas nodrošinātus portālus/kanālus.....	29
4.	Piekļuves tiesību un persondatu tvērums un informācija, uz ko tas attiecas .....	30
4.1.	Personas datu definīcija .....	30
4.2.	Persondati, uz kuriem attiecas piekļuves tiesības.....	33
4.2.1.	Datu subjekta persondati .....	34
4.2.2.	persondati, kas tiek apstrādāti .....	35
4.2.3.	Jauna piekļuves pieprasījuma tvērums .....	36

4.3.	Informācija par apstrādi un datu subjekta tiesībām .....	36
5.	Kā pārzinis var nodrošināt piekļuvi?.....	40
5.1.	Kā pārzinis var izgūt pieprasītos datus? .....	40
5.2.	Atbilstoši pasākumi piekļuves nodrošināšanai .....	40
5.2.1.	“Atbilstošu pasākumu” veikšana .....	41
5.2.2.	Dažādi piekļuves nodrošināšanas līdzekļi .....	42
5.2.3.	Piekļuves nodrošināšana “kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu” .....	43
5.2.4.	Lielam informācijas daudzumam ir vajadzīgas īpašas prasības attiecībā uz to, kā tiek sniegta informācija .....	45
5.2.5.	Formāts.....	46
5.3.	Piekļuves nodrošināšanas termiņi.....	48
6.	Piekļuves tiesību ierobežojumi.....	50
6.1.	Vispārīgas piezīmes .....	50
6.2.	VDAR 15. panta 4. punkts.....	50
6.3.	VDAR 12. panta 5. punkts.....	53
6.3.1.	Ko nozīmē acīmredzami nepamatots? .....	53
6.3.2.	Ko nozīmē pārmērīgs? .....	54
6.3.3.	Sekas.....	57
6.4.	Iespējamie ierobežojumi Savienības vai dalībvalstu tiesību aktos, pamatojoties uz VDAR 23. pantu, un atkāpes.....	57
	Pielikums. Plūsmkarte .....	59

## Eiropas Datu aizsardzības kolēģija,

ņemot vērā 70. panta 1. punkta e) apakšpunktu Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regulā (ES) 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”),

ņemot vērā EEZ līgumu un jo īpaši tā XI pielikumu un 37. protokolu, kas grozīts ar EEZ Apvienotās komitejas 2018. gada 6. jūlija Lēmumu Nr. 154/2018<sup>1</sup>,

ņemot vērā Reglamenta 12. un 22. punktu,

tā kā šo pamatnostādņu sagatavošanas darbs ietvēra ieinteresēto personu viedokļu apkopošanu gan rakstiski, gan īpašā ieinteresēto personu pasākumā par datu subjektu tiesībām, lai apzinātu izaicinājumus un interpretācijas problēmas, kas radušās, piemērojot attiecīgos VDAR noteikumus,

### IR PIEŅĒMUSI ŠĪS PAMATNOSTĀDNES.

## 1 IEVADS. VISPĀRĪGI APSVĒRUMI

1. Mūsdienu sabiedrībā gan publiskas, gan privātas struktūras daudzu darbību laikā dažādos nolūkos un dažādos veidos apstrādā persondatus. Personas bieži vien var būt nelabvēlīgā situācijā attiecībā uz izpratni par to, kā tiek apstrādāti viņu persondati, tai skaitā par konkrētajā gadījumā izmantoto tehnoloģiju, neatkarīgi no tā, vai persondatus apstrādā privāta vai publiska struktūra. Lai šādās situācijās aizsargātu fizisku personu persondatus, ar VDAR ir izveidots saskaņots un stabils tiesiskais regulējums, kas vispārēji piemērojams dažādiem apstrādes veidiem, tai skaitā īpaši noteikumi par datu subjektu tiesībām.
2. Tiesības piekļūt persondatiem ir vienas no VDAR III nodaļā paredzētajām datu subjektu tiesībām līdzās tādām citām tiesībām kā tiesībām uz labošanu un dzēšanu, tiesībām ierobežot apstrādi, tiesībām uz datu pārnesamību, tiesībām iebilst vai tiesībām nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana<sup>2</sup>. Datu subjekta piekļuves tiesības ir nostiprinātas gan ES Pamattiesību hartā (Harta)<sup>3</sup>, gan VDAR 15. pantā, kur tās ir precīzi formulētas kā tiesības piekļūt persondatiem un citai saistītai informācijai.
3. Saskaņā ar VDAR piekļuves tiesības veido trīs komponenti, t. i., apstiprinājums par to, vai persondati tiek vai netiek apstrādāti, piekļuve tiem un informācija par pašu apstrādi. Datu subjekts var iegūt arī apstrādāto persondatu kopiju, lai gan šī iespēja nav datu subjekta papildu tiesības, bet gan veids, kādā tiek nodrošināta piekļuve datiem. Tādējādi piekļuves tiesības var saprast gan kā datu subjekta iespēju jautāt pārzinim, vai tiek apstrādāti viņa persondati, gan kā iespēju šiem datiem piekļūt un tos

---

<sup>1</sup> Atsauces uz “dalībvalstīm” šajā dokumentā būtu jāsaprot kā atsauces uz “EEZ dalībvalstīm”.

<sup>2</sup> VDAR 15.–22. pants.

<sup>3</sup> Saskaņā ar Eiropas Savienības Pamattiesību hartas 8. panta 1. punktu ikvienai personai ir tiesības uz savu persondatu aizsardzību. Saskaņā ar 8. panta 2. punkta otro teikumu ikvienam ir pieejas tiesības datiem, kas par viņu savākti, un tiesības ieviest labojumus šajos datos.



pārbaudīt. Pamatojoties uz datu subjekta pieprasījumu, pārzinis viņam sniedz informāciju, uz kuru attiecas VDAR 15. panta 1. un 2. punkts.

4. Piekļuves tiesības tiek īstenotas gan saistībā ar datu aizsardzības tiesību aktiem saskaņā ar to mērķiem, gan, konkrētāk, saistībā ar "*fizisku personu pamattiesībām un pamatbrīvībām un jo īpaši to tiesībām uz persondatu aizsardzību*", kā minēts VDAR 1. panta 2. punktā. Piekļuves tiesības ir svarīgs elements visā datu aizsardzības sistēmā.
5. Piekļuves tiesību praktiskais mērķis ir ļaut fiziskajām personām kontrolēt savus persondatus<sup>4</sup>. Lai to efektīvi īstenotu praksē, VDAR mērķis ir šo īstenošanu veicināt, izmantojot vairākas garantijas, kas datu subjektam ļauj viegli, bez nevajadzīgiem ierobežojumiem, saprātīgos intervālos un bez pārmērīgas kavēšanās vai izdevumiem šīs tiesības īstenot. Tam visam vajadzētu veicināt datu subjektu piekļuves tiesību efektīvāku īstenošanu digitālajā laikmetā, un šo tiesību daļa plašākā nozīmē ir arī datu subjekta tiesības iesniegt sūdzību uzraudzības iestādei un tiesības uz efektīvu tiesību aizsardzību tiesā<sup>5</sup>.
6. Attiecībā uz piekļuves tiesību attīstību, kas ir daļa no datu aizsardzības tiesiskā regulējuma, būtu jāuzsver, ka tās jau no paša sākuma ir bijušas Eiropas datu aizsardzības sistēmas elements. Salīdzinot ar Direktīvu 95/46/EK, VDAR izklāstītais datu subjektu tiesību standarts ir gan pilnveidots, gan nostiprināts; tas attiecas arī uz piekļuves tiesībām. Tā kā tagad VDAR ir precizēta kārtība attiecībā uz piekļuves tiesībām, šīs tiesības gan datu subjektam, gan pārzinim ir skaidrākas arī juridiskās noteiktības ziņā. Turklāt 15. panta konkrētais formulējums un precīzs datu sniegšanas termiņš saskaņā ar VDAR 12. panta 3. punktu liek pārzinim būt sagatavotam datu subjektu pieprasījumiem, izstrādājot procedūras pieprasījumu apstrādei.
7. Piekļuves tiesības nebūtu jāskata izolēti, jo tās ir cieši saistītas ar citiem VDAR noteikumiem, jo īpaši ar datu aizsardzības principiem, arī godprātību un apstrādes likumīgumu, pārziņa pārrēķināmības pienākumu un citām datu subjektu tiesībām, kas paredzētas VDAR III nodaļā.
8. Saistībā ar datu subjektu tiesībām ir svarīgi arī uzsvērt gan VDAR 12. panta nozīmi, kurā noteiktas prasības attiecībā uz atbilstošiem pasākumiem, ko pārzinis pieņēmis saistībā ar VDAR 13. un 14. pantā minētās informācijas nodrošināšanu, gan VDAR 15.–22. un 34. pantā minēto paziņojumu nozīmi; minētajās prasībās ir vispārīgi noteikta datu subjektam sniedzamo atbilžu un jo īpaši jebkādas bērnam paredzētas informācijas forma, veids un sniegšanas termiņš.
9. EDAK uzskata, ka ir jāsniedz precīzāki norādījumi par to, kā piekļuves tiesības ir jāīsteno dažādās situācijās. Šo pamatnostādņu mērķis ir analizēt dažādos piekļuves tiesību aspektus. Konkrētāk, nākamās iedaļas mērķis ir sniegt vispārēju pārskatu un skaidrojumu par 15. panta saturu, savukārt turpmākajās iedaļās ir sniegta dziļāka analīze par visbiežākajiem praktiskajiem jautājumiem un problēmām, kas saistīti ar piekļuves tiesību īstenošanu.

---

<sup>4</sup> Sk. VDAR 7., 68., 75. un 85. apsvērumu.

<sup>5</sup> Sk. VDAR VIII nodaļas 77., 78. un 79. pantu.

## 2 PIEKĻUVES TIESĪBU MĒRĶIS, VDAR 15. PANTA STRUKTŪRA UN VISPĀRĒJIE PRINCIPI

### 2.1 Piekļuves tiesību mērķis

10. Tātad piekļuves tiesības ir paredzētas, lai nodrošinātu, ka fiziskas personas var kontrolēt ar tām saistītos persondatus, jo tās ļauj tām zināt par apstrādi un pārliecināties par tās likumīgumu<sup>6</sup>. Konkrētāk, piekļuves tiesību mērķis ir ļaut datu subjektiem saprast, kā tiek apstrādāti viņu persondati, kā arī kādas ir šādas apstrādes sekas, un pārbaudīt apstrādāto datu precizitāti, nepamatojot savu nodomu. Citiem vārdiem sakot, piekļuves tiesību mērķis ir sniegt personām pietiekamu, pārredzamu un viegli pieejamu informāciju par datu apstrādi neatkarīgi no izmantotajām tehnoloģijām un ļaut viņām pārbaudīt dažādus konkrētas apstrādes darbības aspektus saskaņā ar VDAR (piemēram, likumīgumu, precizitāti).
11. Šajās pamatnostādnēs sniegtās VDAR interpretācijas pamatā ir līdz šim pieņemtā EST judikatūra. Ņemot vērā piekļuves tiesību nozīmi, sagaidāms, ka saistītā judikatūra nākotnē būtiski mainīsies.
12. Saskaņā ar EST lēmumiem<sup>7</sup> piekļuves tiesību mērķis ir garantēt datu subjektu tiesību uz privātumu aizsardzību, kā arī datu aizsardzību, apstrādājot ar viņiem saistītos datus<sup>8</sup>, un tās var veicināt to viņu tiesību īstenošanu, kuras izriet, piemēram, no VDAR 16.–19., 21.–22. un 82. panta. Tomēr piekļuves tiesību īstenošana ir personas tiesības, un tās nav atkarīgas no citu minēto tiesību īstenošanas, un citu tiesību īstenošana nav atkarīga no piekļuves tiesību īstenošanas.
13. Ņemot vērā piekļuves tiesību plašo mērķi, to nav iespējams analizēt kā priekšnoteikumu tam, lai pārzinis varētu īstenot piekļuves tiesības, novērtējot piekļuves pieprasījumus. Tādējādi pārziniem būtu jāvērtē nevis “kāpēc” datu subjekts pieprasa piekļuvi, bet gan “ko” datu subjekts pieprasa (sk. 3. iedaļu par pieprasījuma analīzi) un vai viņu rīcībā ir persondati, kas attiecas uz šo personu (sk. 4. iedaļu). Tāpēc pārzinim, piemēram, nevajadzētu liegt piekļuvi, pamatojoties uz to vai pastāvot aizdomām par to, ka datu subjekts varētu izmantot pieprasītos datus, lai aizstāvētu sevi tiesā atlaišanas gadījumā vai komercietiskā strīdā ar pārzini<sup>9</sup>. Attiecībā uz piekļuves tiesību ierobežojumiem sk. 6. iedaļu.

**1. piemērs.** Darba devējs atlaiž personu. Pēc nedēļas persona nolemj vākt pierādījumus, lai pret šo bijušo darba devēju iesniegtu lietu tiesā par nepamatotu atlaišanu. Ņemot to vērā, persona rakstiski sazinās ar bijušo darba devēju, pieprasot piekļuvi visiem persondatiem, kas attiecas uz viņu kā datu subjektu un ko bijušais darba devējs kā pārzinis apstrādā.

Pārzinis nevērtē datu subjekta nodomu, un datu subjektam nav jāsniedz pārzinim pieprasījuma iemesls. Tāpēc, ja pieprasījums atbilst visām pārējām prasībām (sk. 3. iedaļu), pārzinim tas ir jāizpilda, ja vien tas nav acīmredzami nepamatots vai pārmērīgs saskaņā ar VDAR 12. panta 5. punktu (sk. 6.3. iedaļu), kas pārzinim ir uzskatāmi jāparāda.

**Variants.** Tiesvedības laikā datu subjekts īsteno piekļuves tiesības attiecībā uz saviem persondatiem. Tomēr dalībvalsts tiesību aktos, kas reglamentē darba attiecības starp pārzini un datu subjektu, ir

<sup>6</sup> VDAR 63. apsvērums.

<sup>7</sup> EST, C-434/16, *Nowak*, un apvienotās lietas C-141/12 un C-372/12, *YS u. c.*

<sup>8</sup> EST, C-434/16, *Nowak*, 56. punkts.

<sup>9</sup> Ar šo tematu saistīti jautājumi ir ietverti pašlaik izskatāmā lietā EST (C-307/22).

ietverti daži noteikumi, kas ierobežo tās informācijas apjomu, kura pusēm sniedzama vai ar kuru pusēm jāapmainās notiekošā vai paredzamā tiesvedībā, un kas ir piemērojami netaisnīgas atlaišanas lietai, ko datu subjekts iesniedzis tiesā. Šajā kontekstā un ar noteikumu, ka minētie valsts noteikumi atbilst VDAR 23. panta prasībām<sup>10</sup>, datu subjektam nav tiesību no pārziņa saņemt vairāk informācijas, nekā paredzēts dalībvalsts tiesību aktos, kas reglamentē informācijas apmaiņu starp pusēm juridiskos strīdos.

14. Lai gan piekļuves tiesību mērķis ir plašs, EST ilustrēja arī datu aizsardzības tiesību un piekļuves tiesību jomas ierobežojumus. Piemēram, EST konstatēja, ka ES datu aizsardzības tiesību aktos garantēto piekļuves tiesību mērķis ir jānošķir no ES un valstu tiesību aktos noteiktajām tiesībām piekļūt publiskiem dokumentiem, kuru mērķis ir “nodrošināt valsts iestāžu lēmumu pieņemšanas procedūru pārskatāmību un (...) sekmēt labu administratīvu praksi”<sup>11</sup>, kas nav datu aizsardzības tiesību aktu mērķis. EST secināja, ka tiesības piekļūt persondatiem ir piemērojamas neatkarīgi no tā, vai ir piemērojamas cita veida piekļuves tiesības ar citu mērķi, piemēram, eksāmena procedūras kontekstā.

## 2.2 VDAR 15. panta struktūra

15. Lai atbildētu uz piekļuves pieprasījumu un nodrošinātu, ka nevienu no tā aspektiem nedrīkst neņemt vērā, vispirms ir jāizprot 15. panta struktūra un šajā pantā noteiktie piekļuves tiesību komponenti.
16. VDAR 15. pantu var sadalīt astoņos dažādos elementos, kas uzskaitīti tālākajā tabulā.

1.	Apstiprinājums par to, vai pārzinis apstrādā pieprasījuma iesniedzējas persondatus	15. panta 1. punkta teikuma pirmā daļa
2.	Piekļuve persondatiem, kas attiecas uz pieprasījuma iesniedzēju personu	15. panta 1. punkta teikuma otrā puse (pirmā daļa)
3.	Piekļuve šādai informācijai par apstrādi: a) apstrādes nolūki; b) persondatu kategorijas; c) saņēmēji vai saņēmēju kategorijas; d) paredzētais apstrādes ilgums vai ilguma noteikšanas kritēriji; e) tas, ka pastāv tiesības uz labošanu vai dzēšanu, apstrādes ierobežošanu vai tiesības iebilst pret šādu apstrādi; f) tiesības iesniegt sūdzību uzraudzības iestādei; g) visa pieejamā informācija par datu avotu, ja persondati netiek vākti no datu subjekta; h) tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, un cita ar to saistīta informācija.	15. panta 1. punkta teikuma otrā puse (otrā daļa)
4.	Informācija par aizsardzības pasākumiem saskaņā ar 46. pantu, ja persondatus nosūta trešai valstij vai starptautiskai organizācijai	15. panta 2. punkts
5.	Pārziņa pienākums nodrošināt apstrādē esošo persondatu kopiju	15. panta 3. punkta pirmais teikums

<sup>10</sup> EDAK Pamatnostādnes 10/2020 par ierobežojumiem saskaņā ar VDAR 23. pantu, versija sabiedriskajai apspriešanai, 2020. gada 18. decembris.

<sup>11</sup> EST, apvienotās lietas C-141/12 un C-372/12, *YS u. c.*, 47. punkts.

6.	Saprātīgas samaksas iekasēšana, ko pārzinis veic, pamatojoties uz administratīvajām izmaksām, par visām datu subjekta pieprasītajām papildu kopijām	15. panta 3. punkta otrais teikums
7.	Informācijas sniegšana elektroniskā formā	15. panta 3. punkta trešais teikums
8.	Citu personu tiesību un brīvību ņemšana vērā	15. panta 4. punkts

Lai gan piekļuves tiesību saturu nosaka visi 15. panta 1. un 2. punkta elementi kopā, 15. panta 3. punkts papildus vispārīgajām prasībām, kas izklāstītas VDAR 12. pantā, attiecas uz piekļuves kārtību. Ar 15. panta 4. punktu papildina ierobežojumus, kas paredzēti VDAR 12. panta 5. punktā attiecībā uz visām datu subjektu tiesībām, īpašu uzmanību pievēršot citu personu tiesībām un brīvībām saistībā ar piekļuvi.

### 2.2.1 Piekļuves tiesību satura noteikšana

17. VDAR 15. panta 1. un 2. punktā ir ietverti šādi trīs aspekti: pirmkārt, apstiprinājums par to, vai tiek apstrādāti pieprasījuma iesniedzējas persondati, otrkārt, ja minētie dati tiek apstrādāti, piekļuve šiem datiem, un, treškārt, informācija par apstrādi. Tos var uzskatīt par trim dažādiem komponentiem, kas kopā veido piekļuves tiesības.

#### 2.2.1.1 Apstiprinājums par to, vai persondati tiek vai netiek apstrādāti

18. Iesniedzot pieprasījumu par piekļuvi persondatiem, datu subjektiem vispirms ir jāzina, vai pārzinis apstrādā vai neapstrādā datus, kas uz viņiem attiecas. Tādējādi šī informācija ir piekļuves tiesību pirmais komponents saskaņā ar 15. panta 1. punktu. Ja pārzinis neapstrādā persondatus, kas attiecas uz datu subjektu, kurš pieprasa piekļuvi, sniedzamā informācija būtu tikai apstiprinājums, ka ar datu subjektu saistīti persondati netiek apstrādāti. Ja pārzinis apstrādā datus, kas attiecas uz pieprasītāju personu, pārzinim šis fakts attiecīgajai personai ir jāapstiprina. Šo apstiprinājumu var paziņot atsevišķi vai to kā daļu var ietvert informācijā par apstrādājamajiem persondatiem (sk. tālāk).

#### 2.2.1.2 Piekļuve apstrādājamajiem persondatiem

19. Piekļuve persondatiem ir piekļuves tiesību otrais komponents saskaņā ar 15. panta 1. punktu, un tā ir šo tiesību kodols. Tā attiecas uz persondatu jēdzienu, kas definēts VDAR 4. panta 1. punktā. Papildus tādiem personas pamatdatiem kā vārds un uzvārds un adrese šī definīcija var attiekties uz neierobežotu datu klāstu, ar nosacījumu, ka tie ietilpst VDAR materiālajā darbības jomā, jo īpaši attiecībā uz veidu, kādā tos apstrādā (VDAR 2. pants). Piekļuve persondatiem nozīmē piekļuvi pašiem faktiskajiem persondatiem, ne tikai vispārīgu datu aprakstu vai atsauci uz pārziņa apstrādāto persondatu kategorijām. Ja ierobežojumi nav piemērojami<sup>12</sup>, datu subjektiem ir tiesības piekļūt visiem apstrādātajiem datiem, kas uz viņiem attiecas, vai datu daļām atkarībā no pieprasījuma tvēruma (sk. 2.3.1. iedaļu). Pienākums nodrošināt piekļuvi datiem nav atkarīgs no šo datu veida vai avota. To pilnā mērā piemēro pat gadījumos, kad pieprasījuma iesniedzēja persona sākotnēji ir sniegusi pārzinim datus, jo tā mērķis ir informēt datu subjektu par šo datu faktisko apstrādi, ko veic pārzinis. persondatu tvērums saskaņā ar 15. pantu ir sīkāk izskaidrots tālāk 4.1. un 4.2. iedaļā.

<sup>12</sup> Sk. šo pamatnostādņu 6. iedaļu.

### 2.2.1.3 Informācija par apstrādi un datu subjekta tiesībām

20. Piekļuves tiesību trešais komponents ir informācija par apstrādi un datu subjektu tiesībām, kas pārzinim ir jāsniedz saskaņā ar 15. panta 1. punkta a) līdz h) apakšpunktu un 15. panta 2. punktu. Šādas informācijas pamatā varētu būt teksts, kas ņemts, piemēram, no pārziņa paziņojuma par privātumu<sup>13</sup> vai VDAR 30. pantā minētā pārziņa apstrādes darbību reģistra, bet tā var būt jāatjaunina un jāpielāgo datu subjekta pieprasījumam. Informācijas saturs un specifikācijas pakāpe ir sīkāk izklāstīta 4.3. iedaļā.

### 2.2.2 Noteikumi par kārtību

21. VDAR 15. panta 3. punkts papildina VDAR 12. pantā noteiktās prasības attiecībā uz kārtību, kādā sniedzama atbilde uz piekļuves pieprasījumiem, ar dažām specifikācijām saistībā ar piekļuves pieprasījumiem.

#### 2.2.2.1 Kopijas nodrošināšana

22. Saskaņā ar VDAR 15. panta 3. punkta pirmo teikumu pārzinis nodrošina to persondatu bezmaksas kopiju, uz kuriem attiecas apstrāde. Tādējādi kopija attiecas tikai uz piekļuves tiesību otro komponentu ("piekļuve apstrādājamiem persondatiem", sk. iepriekš). Pārzinim pirmā kopija jānodrošina bez maksas, pat ja tas uzskata, ka kopijas sagatavošanas izmaksas ir augstas (piemēram, telefonsarunas ieraksta kopijas nodrošināšanas izmaksas).
23. Pienākums nodrošināt kopiju nav jāsaprot kā datu subjekta papildu tiesības, bet gan kā kārtība, kādā nodrošina piekļuvi datiem. Tas stiprina tiesības piekļūt datiem<sup>14</sup> un palīdz šīs tiesības interpretēt, jo skaidri parāda, ka piekļuve datiem saskaņā ar 15. panta 1. punktu ietver pilnīgu informāciju par visiem datiem un nav saprotama tikai kā datu kopsavilkuma sniegšana. Vienlaikus pienākums nodrošināt kopiju nav paredzēts, lai paplašinātu piekļuves tiesību tvērumu: tas attiecas (tikai) uz apstrādājamo persondatu kopiju, nevis uz oriģinālo dokumentu pavairošanu (sk. 5. iedaļas 152. punktu). Vispārīgāk, nodrošinot datu subjektam kopiju, papildu informācija nav jāsniedz: kopijā iekļaujamās informācijas tvērums ir 15. panta 1. punktā minētās piekļuves datiem tvērums (iepriekš minētais piekļuves tiesību otrais komponents, sk. 19. punktu), un tas ietver visu informāciju, kura vajadzīga, lai datu subjekts varētu gūt izpratni par apstrādi un pārliecināties par tās likumīgumu<sup>15</sup>.
24. Ņemot vērā iepriekš minēto, ja piekļuve datiem 15. panta 1. punkta nozīmē tiek sniegta, nodrošinot kopiju, 15. panta 3. punktā minētais pienākums nodrošināt kopiju tiek ievērots. Kopijas nodrošināšanas pienākums atbilst piekļuves tiesību mērķiem ļaut datu subjektam zināt par apstrādi un pārliecināties par tās likumīgumu (63. apsvēruma). Lai šos mērķus sasniegtu, datu subjektam vairumā gadījumu informācija būs jāredz ne tikai īslaicīgi. Tāpēc datu subjektam būs jāiegūst piekļuve informācijai, saņemot persondatu kopiju.
25. Ņemot vērā iepriekš minēto, kopijas jēdziens ir jāinterpretē plašā nozīmē, un tas ietver dažādu veidu piekļuvi persondatiem, ja vien kopija ir pilnīga (t. i., ietver visus pieprasītos persondatus) un datu subjekts to var glabāt. Tādējādi prasība nodrošināt kopiju nozīmē to, ka informācija par persondatiem, kas attiecas uz personu, kura iesniedz pieprasījumu, datu subjektam tiek sniegta tādā veidā, ka datu subjekts visu informāciju var saglabāt un aplūkot atkārtoti.

---

<sup>13</sup> Informāciju par šo sk. 29. panta darba grupas Pārredzamības pamatnostādnes saskaņā ar Regulu 2016/679 (WP260 rev.01, 2018. gada 11. aprīlis), kuras apstiprinājusi EDAK (tālāk "29. panta darba grupas Pārredzamības pamatnostādnes, ko apstiprinājusi EDAK").

<sup>14</sup> Kopijas nodrošināšanas pienākums nebija minēts Datu aizsardzības direktīvā 95/46/EK.

<sup>15</sup> Jautājumi, kas saistīti ar šā punkta tematu, ir ietverti pašlaik izskatāmā lietā EST (C-487/21).

26. Neraugoties uz šo plašo izpratni par to, kas ir kopija, un to, ka tas ir galvenais veids, kādā būtu jānodrošina piekļuve, dažos gadījumos varētu būt piemērota cita kārtība. Papildu skaidrojumi par kopijām un citu piekļuves nodrošināšanas kārtību ir sniegti 5. iedaļā, jo īpaši 5.2.2.–5.2.5. punktā.

#### 2.2.2.2 Papildu kopiju nodrošināšana

27. VDAR 15. panta 3. punkta otrais teikums attiecas uz situācijām, kad datu subjekts pārzinim pieprasa vairāk nekā vienu kopiju, piemēram, ja pirmā kopija ir nozaudēta vai bojāta vai datu subjekts kopiju vēlas nodot citai personai vai uzraudzības iestādei. Pamatojoties uz to, ka pārzinim pēc datu subjekta pieprasījuma ir jānodrošina papildu kopijas, 15. panta 3. punkta noteikumi paredz, ka par jebkuru pieprasīto papildu kopiju pārzinis var iekasēt samērīgu maksu, kas balstīta uz administratīvām izmaksām (15. panta 3. punkta otrais teikums).
28. Ja datu subjekts lūdz papildu kopiju pēc pirmā pieprasījuma iesniegšanas, var rasties jautājumi par to, vai tas būtu jāuzskata par jaunu pieprasījumu vai arī datu subjekts vēlas saņemt datu papildu kopiju 15. panta 3. punkta otrā teikuma nozīmē un par to var iekasēt samaksu. Atbilde uz šiem jautājumiem ir atkarīga tikai no pieprasījuma satura: pieprasījums būtu jāinterpretē kā lūgums pēc papildu kopijas, ciktāl tas laika un tvēruma ziņā attiecas uz to pašu persondatu apstrādi, uz ko attiecās iepriekšējais pieprasījums. Tomēr, ja datu subjekta mērķis ir iegūt informāciju par datiem, kas apstrādāti citā laikā, vai informāciju par datu kopu, kas atšķiras no sākotnējā pieprasījumā iekļautās, atkal ir piemērojamas tiesības saņemt bezmaksas kopiju saskaņā ar 15. panta 3. punktu. Tas attiecas arī uz gadījumiem, kad datu subjekts pirmo pieprasījumu ir iesniedzis neilgi pirms tam. Datu subjekts var izmantot savas piekļuves tiesības, iesniedzot turpmāku pieprasījumu, un saņemt bezmaksas kopiju, ja vien pieprasījumu neuzskata par pārmērīgu saskaņā ar 12. panta 5. punktu, šādā gadījumā, iespējams, iekasējot samērīgu samaksu saskaņā ar 12. panta 5. punkta a) apakšpunktu (par atkārtotu pieprasījumu pārmērīgumu, sk. 6. iedaļu).

**2. piemērs.** Klients tirdzniecības uzņēmumam iesniedz piekļuves pieprasījumu. Vienu gadu pēc uzņēmuma atbildes saņemšanas tas pats klients tam pašam uzņēmumam iesniedz piekļuves pieprasījumu saskaņā ar 15. pantu. Neatkarīgi no tā, vai kopš iepriekšējā pieprasījuma pušu starpā ir notikuši jauni biznesa darījumi vai cita saziņa, šis otrais pieprasījums ir uzskatāms par jaunu pieprasījumu. Pat ja uzņēmuma veiktā datu apstrāde nav mainījusies — kas datu subjektam ne vienmēr ir zināms —, datu subjektam ir tiesības saņemt datu bezmaksas kopiju.

**1. variants.** Pat ja klients jauno pieprasījumu iepriekš minētajos gadījumos iesniedz, piemēram, tikai vienu nedēļu pēc pirmā pieprasījuma iesniegšanas, to var uzskatīt par jaunu pieprasījumu saskaņā ar 15. panta 1. punktu un 3. punkta pirmo teikumu, ja vien to nevar interpretēt tikai kā atgādinājumu par pirmo pieprasījumu. Attiecībā uz īso intervālu un atkarībā no jaunā pieprasījuma konkrētajiem apstākļiem runa ir par tā pārmērīgumu saskaņā ar 12. panta 5. punktu (skat. 6. iedaļu).

**2. variants.** Tādas informācijas “jaunas kopijas” pieprasījums, kas kopijas veidā jau bija sniegta, atbildot uz iepriekšēju pieprasījumu, piemēram, gadījumā, kad klients iepriekš saņemto kopiju ir nozaudējis, parasti būtu jāuzskata par papildu kopijas pieprasījumu, jo datu apstrādes tvēruma un laika ziņā tas attiecas uz iepriekšējo pieprasījumu.

29. Ja datu subjekts atkārtoti iesniedz pirmo piekļuves pieprasījumu, pamatojoties uz to, ka saņemtā atbilde nav pilnīga vai atteikums nav pamatots, šis pieprasījums nav uzskatāms par jaunu pieprasījumu, jo tas ir tikai atgādinājums par pirmo neizpildīto pieprasījumu.
30. Attiecībā uz izmaksu sadali gadījumos, kad tiek pieprasīta papildu kopija, 15. panta 3. punktā ir noteikts, ka pārzinis var iekasēt samērīgu samaksu, pamatojoties uz administratīvajām izmaksām, kas

radušās pieprasījuma dēļ. Tas nozīmē, ka būtisks kritērijs samaksas apmēra noteikšanai ir administratīvās izmaksas. Vienlaikus samaksai vajadzētu būt atbilstoši, ņemot vērā to, cik svarīgas ir piekļuves tiesības kā datu subjekta pamattiesības. Pārzinim nevajadzētu novirzīt pieskaitāmās izmaksas vai citus vispārīgus izdevumus uz datu subjektu, bet būtu jākoncentrējas uz konkrētajām izmaksām, kas rodas, nodrošinot papildu kopiju. Organizējot šo procesu, pārzinim būtu efektīvi jāizmanto savi cilvēkresursi un materiālie resursi, lai kopijas izmaksas saglabātu zemas, arī tad, ja pārzinis iesaista ārēju atbalstu.

31. Ja pārzinis nolemj iekasēt samaksu, tam būtu iepriekš jānorāda, ka maksa tiks iekasēta, un pēc iespējas precīzi, jānorāda to izmaksu apmērs, ko tas no datu subjekta plāno iekasēt, lai datu subjektam dotu iespēju izlemt, vai pieprasījumu saglabāt vai atsaukt.

#### 2.2.2.3 Informācijas pieejamības nodrošināšana plaši izmantotā elektroniskā formātā

32. Ja pieprasījums iesniegts elektroniskā formātā, informāciju, ja iespējams, sniedz elektroniskā formā, izņemot, ja datu subjekts pieprasa citādi (sk. VDAR 12. panta 3. punktu). Šo prasību saistībā ar piekļuves pieprasījumiem papildina 15. panta 3. punkta trešais teikums, kurā norādīts, ka pārzinim turklāt ir pienākums sniegt atbildi plaši izmantotā elektroniskā formātā, ja vien datu subjekts nepieprasa citādi. VDAR 15. panta 3. punktā ir paredzēts, ka pārziņi, kas var saņemt elektroniskus pieprasījumus, atbildi uz šādiem pieprasījumiem varēs sniegt plaši izmantotā elektroniskā formātā (sīkāku informāciju sk. 5.2.5. iedaļā). Šis noteikums attiecas uz visu informāciju, kas jāsniedz saskaņā ar 15. panta 1. un 2. punktu. Tāpēc, ja datu subjekts piekļuves pieprasījumu iesniedz elektroniski, visa informācija ir jāsniedz plaši izmantotā elektroniskā formātā. Ar formātu saistītie jautājumi ir sīkāk izklāstīti 5. iedaļā. Pārzinim, kā vienmēr, būtu jāievieš atbilstoši drošības pasākumi, jo īpaši attiecībā uz īpašas kategorijas persondatiem (sk. tālāk 2.3.4. iedaļu).

#### 2.2.3 Piekļuves tiesību iespējamais ierobežojums

33. Visbeidzot, saistībā ar piekļuves tiesībām 15. panta 4. punktā ir paredzēts īpašs ierobežojums. Tajā norādīts, ka ir jāņem vērā iespējamā negatīvā ietekme uz citu personu tiesībām un brīvībām. Jautājumi par šā ierobežojuma tvērumu un sekām, kā arī par papildu ierobežojumiem, kas noteikti VDAR 12. panta 5. punktā vai VDAR 23. pantā, tiek skaidroti 6. iedaļā.

### 2.3 Piekļuves tiesību vispārējie principi

34. Kad datu subjekti iesniedz pieprasījumu par piekļuvi saviem datiem, principā vienmēr ir jāsniedz visa VDAR 15. pantā minētā informācija. Attiecīgi, ja pārzinis apstrādā datus, kas attiecas uz datu subjektu, tas sniedz visu 15. panta 1. punktā minēto informāciju un attiecīgā gadījumā 15. panta 2. punktā minēto informāciju. Pārzinim jāveic atbilstīgi pasākumi, lai nodrošinātu, ka informācija ir pilnīga, pareiza un atjaunināta un pēc iespējas labāk atbilst datu apstrādes stāvoklim pieprasījuma saņemšanas brīdī<sup>16</sup>. Ja datus kopīgi apstrādā divi vai vairāki pārziņi, kopīgo pārziņu vienošanās par viņu attiecīgajiem pienākumiem saistībā ar datu subjekta tiesību īstenošanu, jo īpaši saistībā ar atbildēšanu uz piekļuves pieprasījumiem, neietekmē datu subjekta tiesības attiecībā pret pārzini, kuram viņi adresē savu pieprasījumu<sup>17</sup>.

---

<sup>16</sup> Norādījumus par atbilstošiem pasākumiem sk. 5. iedaļas 123.–129. punktā.

<sup>17</sup> EDAK Pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR, 162.f. punkts. Apstrādātājiem ir jāpalīdz pārzinim, sk. turpat 129. punktu.



### 2.3.1 Informācijas pilnīgums

35. Datu subjektiem ir tiesības — izņemot tālāk minētos izņēmumus — pilnā mērā saņemt visus ar viņiem saistītos datus (sīkaku informāciju par tvērumu sk. 4.2. iedaļā). Ja vien datu subjekts nav skaidri pieprasījis citādi, pieprasījumu izmantot piekļuves tiesības jāsaprot vispārīgi, aptverot visus datu subjekta persondatus<sup>18</sup>. Piekļuves ierobežošanu daļai informācijas var apsvērt šādos gadījumos:
- a) datu subjekts ir skaidri ierobežojis pieprasījumu, attiecinot to tikai uz datu apakškopu. Lai izvairītos no nepilnīgas informācijas sniegšanas, pārzinis šo datu subjekta pieprasījuma ierobežojumu var apsvērt tikai tad, ja ir skaidrs, ka šī interpretācija atbilst datu subjekta vēlmēm (sīkaku informāciju sk. 3.1.1. iedaļas 51. punktā). Principā datu subjektam nav atkārtoti jāpieprasa visu to datu nosūtīšana, kurus datu subjekts ir tiesīgs iegūt;
  - b) situācijās, kad pārzinis attiecībā uz datu subjektu apstrādā lielu datu apjomu, pārzinim var rasties šaubas, vai ļoti vispārīgi izteikta piekļuves pieprasījuma mērķis patiešām ir saņemt detalizētu informāciju par visu veidu apstrādātajiem datiem vai par visām pārziņa darbības nozarēm. Šaubas jo īpaši var rasties situācijās, kad datu subjektam nav bijis iespējams nodrošināt rīkus, ar ko jau no paša sākuma precizēt viņa pieprasījumu, vai kad datu subjekts tos nav izmantojis. Tādā gadījumā pārzinis saskaras ar problēmām saistībā ar to, kā sniegt pilnīgu atbildi, vienlaikus izvairoties no pārmērīgas tādas informācijas sniegšanas datu subjektam, kas datu subjektu neinteresē un ar ko viņš nevar efektīvi rīkoties. Atkarībā no apstākļiem un tehniskajām iespējām šo problēmu var atrisināt, piemēram, nodrošinot pašapkalpošanās rīkus tiešsaistē (sk. 5. iedaļu par vairāku līmeņu pieeju). Ja šādi risinājumi nav piemērojami, pārzinis, kas apstrādā lielu informācijas apjomu saistībā ar datu subjektu, var pieprasīt, lai datu subjekts pirms informācijas nosūtīšanas precizētu, uz kuru informāciju vai apstrādes darbībām pieprasījums attiecas (sk. VDAR 63. apsvērumu). Kā piemēru var minēt uzņēmumu, kas darbojas vairākās jomās, vai publisku iestādi ar dažādām administratīvām vienībām, ja pārzinis ir atklājis, ka šajās filiālēs tiek apstrādāts daudz datu saistībā ar datu subjektu. Lielu datu apjomu var apstrādāt arī pārziņi, kas vāc datus par datu subjekta biežām darbībām ilgākā laikposmā.

**3. piemērs.** Publiska iestāde apstrādā datus par datu subjektu vairākos dažādos departamentos un dažādos kontekstos. Datu pārvaldība un glabāšana daļēji tiek veikta, izmantojot neautomatizētus līdzekļus, un lielākā daļa datu tiek glabāta tikai papīra formātā. Pieprasījuma vispārīgā formulējuma dēļ publiskā iestāde šaubās par to, vai datu subjektam ir zināms pieprasījuma apjoms, jo īpaši daudzveidīgās apstrādes darbības, ko pieprasījums aptvertu, informācijas apjoms un to lapu skaits, ko datu subjekts saņemtu.

**4. piemērs.** Liela apdrošināšanas sabiedrība saņem vēstuli ar vispārīgu piekļuves pieprasījumu no personas, kas daudzus gadus ir bijusi tās klients. Lai gan datu dzēšanas periodi tiek pilnībā ievēroti, uzņēmums faktiski apstrādā lielu datu apjomu saistībā ar klientu, jo apstrāde joprojām ir nepieciešama, lai izpildītu līgumsaistības, kas izriet no līgumattiecībām ar klientu (ieskaitot, piemēram, turpmākas saistības, saziņu par strīdīgiem jautājumiem ar klientu un trešām personām u. c.), vai lai izpildītu juridiskas saistības (arhivēti dati, kas jāglabā nodokļu vajadzībām utt.). Apdrošināšanas sabiedrībai var rasties šaubas par to, vai ļoti vispārīgi izteiktais pieprasījums patiešām attiecas uz visiem šo datu veidiem. Īpaši problemātiski tas var būt gadījumā, kad apdrošināšanas sabiedrībai ir tikai datu subjekta pasta adrese un tāpēc tai visa informācija ir jānosūta papīra formātā. Tomēr tādas pašas šaubas var rasties arī tad, ja informāciju sniedz, izmantojot citus līdzekļus.

<sup>18</sup> Sīkaku informāciju sk. tālāk 5.2.3. iedaļā par vairāku līmeņu pieejas tematu.



Ja šādos gadījumos pārzinis nolemj lūgt datu subjektu precizēt pieprasījumu, lai izpildītu savu pienākumu veicināt piekļuves tiesību īstenošanu (VDAR 12. panta 2. punkts), pārzinis vienlaikus sniedz jēgpilnu informāciju par savām apstrādes darbībām, kas varētu attiekties uz datu subjektu, informējot par tā darbībām attiecīgās filiālēs, par tā datubāzēm utt.

**5. piemērs.** Darba ņēmējs ir iesniedzis vispārīgi formulētu piekļuves pieprasījumu, no kura nav skaidrs, vai viņš vēlas saņemt visus lietotāja pieteikšanās datus, datus par piekļuvi darbvietai, datus par norēķiniem ēdnīcā, datus par algu maksājumiem utt. No darba devēja pieprasījuma sniegt precizējumu varētu izrietēt, piemēram, tas, ka darbinieka interesēs ir saprast vai pārbaudīt, kam ir nodots viņa veikuma novērtējums. Nepieprasot precizējumu, darbinieks saņemtu daudz informācijas, kuras lielākā daļa viņu neinteresē. Vienlaikus darba devējam būtu jāsniedz informācija par dažādiem apstrādes kontekstiem, kas varētu attiekties uz darba ņēmēju, lai darba ņēmējs pieprasījumu varētu saprātīgi precizēt.

Ir svarīgi uzsvērt, ka precizēšanas pieprasījuma mērķis nav ierobežot atbildi uz piekļuves pieprasījumu, un to neizmanto, lai slēptu jebkādu informāciju par datiem vai apstrādi, kas attiecas uz datu subjektu. Ja datu subjekts, kuram lūgts precizēt pieprasījuma tvērumu, apstiprina, ka vēlas pieprasīt visus persondatus, kas uz viņu attiecas, pārzinim tie, protams, ir jāsniedz pilnā apmērā.

Katrā ziņā pārzinim vienmēr būtu jāspēj pierādīt, ka pieprasījuma apstrādes veida mērķis ir piešķirt visplašākās piekļuves tiesības un ka tas atbilst tā pienākumam veicināt datu subjektu tiesību īstenošanu (VDAR 12. panta 2. punkts). Ievērojot minētos principus, pārzinis pirms papildu datu sniegšanas saskaņā ar datu subjekta vēlmēm var sagaidīt datu subjekta atbildi, ja tas datu subjektam ir sniedzis skaidru pārskatu par visām apstrādes darbībām, kas uz viņu varētu attiekties, ieskaitot jo īpaši darbības, kuras datu subjekts varētu nebūt paredzējis, un ja pārzinis ir arī devis piekļuvi visiem datiem, kuriem datu subjekts ir skaidri vēlējis piekļūt, un ja turklāt šī informācija ir apvienota ar skaidru norādi par to, kā iegūt piekļuvi pārējām apstrādāto datu daļām;

- c) piekļuves tiesībām piemēro izņēmumus vai ierobežojumus (sk. tālāk 6. iedaļu). Šādos gadījumos pārzinim būtu rūpīgi jāpārbauda, uz kurām informācijas daļām izņēmums attiecas, un jāsniedz visa informācija, kas ar šo izņēmumu nav izslēgta. Izņēmums var neskart, piemēram, apstiprinājumu par persondatu apstrādi kā tādu (1. komponents). Rezultātā ir jāsniedz informācija par visiem persondatiem un visa 15. panta 1. un 2. punktā minētā informācija, uz ko neattiecas izņēmums vai ierobežojums.

### 2.3.2 Informācijas pareizība

36. Informācijai, kas iekļauta datu subjektam nodrošinātajā persondatu kopijā, jāietver faktiskā informācija par datu subjektu vai viņa persondati. Tas ietver pienākumu sniegt informāciju par neprecīziem datiem vai par datu apstrādi, kas nav vai vairs nav likumīga. Datu subjekts var izmantot piekļuves tiesības, piemēram, lai uzzinātu tādu neprecīzu datu avotu, ar ko apmainās dažādi pārziņi. Ja pārzinis neprecīzus datus izlabotu pirms datu subjekta informēšanas par tiem, datu subjektam šāda iespēja tiktu liegta. Tas pats attiecas uz nelikumīgu apstrādi. Iespēja zināt par nelikumīgu apstrādi, kas attiecas uz datu subjektu, ir viens no galvenajiem piekļuves tiesību mērķiem. Pienākums informēt par to, ka apstrāde nav mainījies, neskar pārziņa pienākumu izbeigt nelikumīgu apstrādi vai izlabot neprecīzus datus. Jautājumi par kārtību, kādā šie pienākumi būtu jāizpilda, tiek aplūkoti tālāk.

### 2.3.3 Novērtējuma laika atskaites punkts

37. Apstrādājamo datu novērtējums iespējami precīzi atspoguļo situāciju brīdī, kad pārzinis saņem pieprasījumu, un atbildē būtu jāietver visi šajā brīdī pieejamie dati. Tas nozīmē, ka pārzinim bez nepamatotas kavēšanās ir jāmēģina noteikt visas datu apstrādes darbības, kas saistītas ar datu subjektu. Tāpēc pārziņiem nav jāsniedz persondati, kurus tie apstrādājuši iepriekš, bet kuri vairs nav to rīcībā<sup>19</sup>. Piemēram, pārzinis var būt dzēsis persondatus saskaņā ar savu datu glabāšanas politiku un/vai tiesību aktu noteikumiem un tādējādi pieprasītos persondatus vairs nevar sniegt. Šajā kontekstā būtu jāatgādina, ka datu glabāšanas ilgums būtu jānosaka saskaņā ar VDAR 5. panta 1. punkta e) apakšpunktu, jo jebkādi datu glabāšanai jābūt objektīvi pamatojami.
38. Vienlaikus pārzinis iepriekš īsteno vajadzīgos pasākumus, lai veicinātu piekļuves tiesību īstenošanu un izskatītu šādus pieprasījumus iespējami ātri (sk. 12. panta 3. punktu) un pirms dati būs jādzēš. Tāpēc, ja glabāšanas periodi ir īsi, pasākumi, kas veikti, lai atbildētu uz pieprasījumu, būtu jāpielāgo attiecīgajam glabāšanas periodam, lai veicinātu piekļuves tiesību īstenošanu un izvairītos no tā, ka pieprasījuma iesniegšanas brīdī pastāvīgi nav iespējams nodrošināt piekļuvi apstrādātajiem datiem<sup>20</sup>. Dažos gadījumos tomēr var nebūt iespējams atbildēt uz pieprasījumu pirms plānotās datu dzēšanas. Piemēram, ja, iespējami ātri atbildot uz pieprasījumu, pārzinis izgūst persondatus, kurus bija plānots dzēst nākamajā dienā, pārzinim var būt vajadzīgs papildu laiks, lai apsvērtu, vai pirms persondatu kopijas nodošanas pieprasījuma iesniedzējam tā ir jāredīgē, lai aizsargātu citu personu brīvības. Ja dati ir izgūti plānotajā glabāšanas laikposmā, pārzinis var turpināt šo datu apstrādi, lai izpildītu savu pienākumu atbildēt uz pieprasījumu. Šādos gadījumos apstrādes pamats var būt VDAR 6. panta 1. punkta c) apakšpunkts kopā ar 15. pantu, un tās ilgumam ir jāatbilst VDAR 12. panta 3. punkta prasībām<sup>21</sup>. Šā juridiskā pamata piemērošana attiecas tikai uz to datu apstrādi, kas identificēti kā vajadzīgi, lai atbildētu uz konkrēto pieprasījumu, un to nedrīkst izmantot kā pamatojumu glabāšanas periodu vispārējai pagarināšanai.
39. Turklāt pārzinis apzināti nevairās no pienākuma sniegt pieprasītos persondatus, tos atbildē uz piekļuves pieprasījumu dzēšot vai izmainot (sk. 2.3.2. punktu). Ja piekļuves pieprasījuma apstrādes gaitā pārzinis atklāj neprecīzus datus vai nelikumīgu apstrādi, pārzinim pirms citu savu pienākumu izpildes ir jānovērtē apstrādes stāvoklis un attiecīgi jāinformē datu subjekts. Savās interesēs, lai izvairītos no turpmākas saziņas par šo jautājumu, kā arī lai nodrošinātu atbilstību pārredzamības principam, pārzinim būtu jāpievieno informācija par turpmākiem labojumiem vai dzēšanu.

**6. piemērs.** Atbildot uz piekļuves pieprasījumu, pārzinis saprot, ka datu subjekta pieteikums vakancei pārziņa uzņēmumā ir glabāts pēc glabāšanas perioda beigām. Šādā gadījumā pārzinis nevar vispirms dzēst datus un pēc tam datu subjektam atbildēt, ka nekādi dati (kas attiecas uz pieteikumu) netiek apstrādāti. Tam ir vispirms jānodrošina piekļuve datiem un pēc tam šie dati jādzēš. Lai izvairītos no

<sup>19</sup> Šajā saistībā sk. papildu skaidrojumus šo pamatnostādņu 4. iedaļā, kā arī Eiropas Savienības Tiesas 2009. gada 7. maija spriedumā lietā *C-553/07, College van burgemeester en wethouders van Rotterdam pret M. E. E. Rijkeboer*, par tiesībām piekļūt informācijai par saņēmējiem vai saņēmēju kategorijām saistībā ar pagātni.

<sup>20</sup> Piemēram, lai veicinātu ātru rīcību, varētu apsvērt tāda pašapkalpošanās rīka ieviešanu, kas datu subjektam ļauj viegli piekļūt pieprasītajiem persondatiem, un tādas paziņošanas sistēmas ieviešanu, kura pārzini brīdina par pieprasījumu, kas attiecas uz persondatiem, kurus glabā īsu laikposmu.

<sup>21</sup> Tas neskar datu turpmāku apstrādi pierādījumu nolūkos saistībā ar piekļuves pieprasījuma apstrādi par attiecīgu laikposmu.

turpmāka dzēšanas pieprasījuma, tādā gadījumā būtu ieteicams pievienot informāciju par dzēšanas faktu un laiku.

Lai ievērotu pārredzamības principu, pārziniem būtu jāinformē datu subjektus par konkrēto apstrādes brīdi, uz kuru attiecas pārziņa atbilde. Dažos gadījumos, piemēram, biežu saziņas darbību kontekstā, starp šo laika atskaites punktu, kurā apstrāde novērtēta, un brīdi, kad pārzinis sniedz atbildi, var notikt datu papildu apstrāde vai izmaiņas tajos. Ja pārzinis par šādām izmaiņām zina, ieteicams iekļaut informāciju par šīm izmaiņām, kā arī informāciju par papildu apstrādi, kas vajadzīga, lai atbildētu uz pieprasījumu.

#### 2.3.4 Datu drošības prasību ievērošana

40. Tā kā persondatu paziņošana un pieejamības nodrošināšana datu subjektam ir apstrādes darbība, pārzinim vienmēr ir pienākums īstenot atbilstošus tehniskus un organizatoriskus pasākumus, lai nodrošinātu apstrādes riskam atbilstošu drošības līmeni (sk. VDAR 5. panta 1. punkta f) apakšpunktu, 24. un 32. pantu). Tas ir spēkā neatkarīgi no kārtības, kādā tiek nodrošināta piekļuve. Ja datu subjektam datus nosūta neelektroniski, atkarībā no apstrādes radītajiem riskiem pārzinis var apsvērt iespēju izmantot ierakstītu vēstuli vai alternatīvi piedāvāt, bet neuzspiest datu subjektam attiecīgo dokumentu saņemt pret parakstu tieši kādā no pārziņa uzņēmumiem. Ja saskaņā ar 12. panta 1. un 3. punktu informāciju sniedz elektroniski, pārzinis izvēlas elektroniskus līdzekļus, kas atbilst datu drošības prasībām. Arī tad, ja datu kopiju nodrošina plaši izmantotā elektroniskā formātā (sk. 15. panta 3. punktu), pārzinis, izvēloties attiecīgos līdzekļus elektroniskās datnes nosūtīšanai datu subjektam, ņem vērā datu drošības prasības. Tās var ietvert šifrēšanu, aizsardzību ar parolēm utt. Lai atvieglotu piekļuvi šifrētiem datiem, pārzinim būtu jānodrošina arī atbilstoša informācija, lai datu subjekts varētu piekļūt atšifrētajai informācijai. Gadījumos, kad datu drošības prasību dēļ būtu vajadzīga elektroniskā pasta pilnīga (*end-to-end*) šifrēšana, bet pārzinis var nosūtīt tikai parastu e-pastu, pārzinim būs jāizmanto citi līdzekļi, piemēram, jānosūta datu subjektam USB zibatmiņa (ierakstītā) vēstulē.

## 3 VISPĀRĪGI APSVĒRUMI ATTIECĪBĀ UZ PIEKĻUVES PIEPRASĪJUMU NOVĒRTĒŠANU

### 3.1 Ievads

41. Saņemot pieprasījumus par piekļuvi persondatiem, pārzinim katrs pieprasījums ir atsevišķi jānovērtē. Pārzinis cita starpā ņem vērā tādus tālākajos punktos izklāstītus aspektus kā to, vai pieprasījums attiecas uz persondatiem, kas saistīti ar pieprasījuma iesniedzēju personu, un to, kas ir pieprasījuma iesniedzēja persona. Šis iedaļas mērķis ir precizēt, kādi piekļuves pieprasījuma elementi pārzinim būtu jāņem vērā, veicot savu novērtējumu, un aprakstīt iespējamās šāda novērtējuma scenārijus, kā arī tā sekas. Novērtējot pieprasījumu piekļūt persondatiem, pārzinis saskaņā ar VDAR 12. panta 2. punktu ņem vērā arī pienākumu veicināt datu subjekta tiesību īstenošanu, vienlaikus paturot prātā persondatu pienācīgu drošību<sup>22</sup>.

---

<sup>22</sup> Pārzinis nodrošina pienācīgu persondatu drošību saskaņā ar integritātes un konfidencialitātes principu (VDAR 5. panta 1. punkta f) apakšpunkts), īstenojot atbilstīgus tehniskus un organizatoriskus pasākumus, kā minēts VDAR 32. pantā un sīkāk izklāstīts VDAR 24. pantā. Pārzinim jāspēj uzskatāmi parādīt, ka tas nodrošina pienācīgu datu aizsardzības līmeni saskaņā ar pārskatatbildības principu (sk. arī 29. panta darba grupas Atzinumu 3/2010 par pārskatatbildības principu, kas pieņemts 2010. gada 13. jūlijā (00062/10/EN WP 173) un EDAK Pamatnostādnes 07/2020 par pārziņa un apstrādātāja jēdzieniem VDAR).

42. Tāpēc pārziņiem vajadzētu būt proaktīvi gataviem izskatīt pieprasījumus par piekļuvi persondatiem. Tas nozīmē, ka pārziņim vajadzētu būt gatavam saņemt pieprasījumu, to pienācīgi novērtēt (šis novērtējums ir šis pamatnostādņu iedaļas priekšmets) un bez nepamatotas kavēšanās sniegt atbilstošu atbildi pieprasījuma iesniedzējai personai. Veidam, kādā pārziņi sagatavosies piekļuves tiesību īstenošanas pieprasījumiem, vajadzētu būt adekvātam un samērīgam un atkarīgam no apstrādes rakstura, apjoma, konteksta un nolūkiem, kā arī riskiem attiecībā uz fizisku personu tiesībām un brīvībām saskaņā ar VDAR 24. pantu. Atkarībā no konkrētajiem apstākļiem, pārziņiem, piemēram, var tikt prasīts īstenot atbilstošu procedūru, kurai būtu jāgarantē datu drošība, nekavējot datu subjekta tiesību īstenošanu.

### 3.1.1 Pieprasījuma satura analīze

43. Šo aspektu var konkrētāk novērtēt, uzdodot tālāk minētos jautājumus.

*a) Vai pieprasījums attiecas uz persondatiem?*

44. Saskaņā ar VDAR pieprasījuma tvērums attiecas tikai uz persondatiem<sup>23</sup>. Tāpēc neviens pieprasījums sniegt informāciju par citiem aspektiem, tai skaitā vispārīgu informāciju par pārziņi, tā darījumdarbības modeļiem vai apstrādes darbībām, kura nav saistīta ar persondatiem, nav uzskatāms par pieprasījumu, kas iesniegts saskaņā ar VDAR 15. pantu. Turklāt piekļuves tiesību tvērumā neietilps pieprasījums sniegt informāciju par anonīmiem datiem vai datiem, kas neattiecas uz pieprasījuma iesniedzēju personu vai personu, kuras vārdā pieprasījumu ir iesniegusi pilnvarotā persona. Šis jautājums tiks sīkāk analizēts 4. iedaļā.

45. Atšķirībā no anonīmiem datiem (kas nav persondati) pseidonimizēti dati, kurus, izmantojot papildu informāciju, varētu attiecināt uz fizisku personu, ir persondati<sup>24</sup>. Tādējādi uzskatāms, ka pieprasījuma tvērumā ietilpst pseidonimizēti dati, kurus var sasaistīt ar datu subjektu, piemēram, ja datu subjekts sniedz attiecīgo identifikatoru, kas ļauj viņu identificēt, vai ja pārziņis spēj sasaistīt datus ar pieprasījuma iesniedzēju personu, izmantojot savus līdzekļus<sup>25</sup>.

*b) Vai pieprasījums attiecas uz pieprasījuma iesniedzēju personu (vai personu, kuras vārdā pieprasījumu iesniedz pilnvarotā persona)?*

46. Parasti pieprasījums var attiekties tikai uz pieprasījuma iesniedzējas persondatiem. Piekļuvi citu personu datiem var pieprasīt tikai ar attiecīgu pilnvaru<sup>26</sup>.

**7. piemērs.** Datu subjekts X strādā par nodaļas vadītāju uzņēmumā, kas saviem vadītājiem nodrošina stāvvietas uzņēmuma autostāvvietā. Lai gan datu subjektam X ir pastāvīga stāvvietā, kad viņš ierodas birojā uz otro maiņu, šajā vietā bieži vien jau atrodas cita automašīna. Tā kā šī situācija atkārtojas, tad, lai identificētu transportlīdzekļa vadītāju, kurš neatļauti izmanto viņa vietu, datu subjekts biroja autostāvvietas zonas videonovērošanas sistēmas pārziņim lūdz piekļuvi šā transportlīdzekļa vadītāja persondatiem. Šādā gadījumā datu subjekta X pieprasījums nebūs pieprasījums piekļūt viņa

<sup>23</sup> Ja vien pieprasījums neattiecas arī uz datiem, kas nav persondati, bet ir nesaraujami saistīti ar datu subjekta persondatiem. Sīkākus skaidrojumus sk. 100. punktā.

<sup>24</sup> Sk. VDAR 26. apsvērumu. Sīkāki skaidrojumi par anonīmu datu un pseidonimizētu datu jēdzieniem atrodami 29. panta darba grupas Atzinumā Nr. 4/2007 par "persondatu" jēdzienu, 18.–21. lpp.

<sup>25</sup> 29. panta darba grupa, WP242 rev.01, 2017. gada 5. aprīlis, Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK (tālāk "WP29 Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK"), 9. lpp.

<sup>26</sup> Sk. 3.4. iedaļu ("Pieprasījumi, ko iesniedz ar trešo/pilnvarotu personu starpniecību").

persondatiem, jo šis pieprasījums attiecas nevis uz pieprasījuma iesniedzējas persondatiem, bet gan uz citas persondatiem, un tāpēc tas nebūtu jāuzskata par pieprasījumu saskaņā ar VDAR 15. pantu.

*c) Vai ir piemērojami noteikumi, kas nav VDAR un kas reglamentē piekļuvi noteiktai datu kategorijai?*

47. Datu subjektiem savā pieprasījumā nav jānorāda juridiskais pamats. Tomēr, ja datu subjekti norāda, ka viņu pieprasījuma pamatā ir nevis VDAR, bet gan nozares tiesību akti vai valsts tiesību akti, kas reglamentē konkrētu jautājumu par piekļuvi konkrētām datu kategorijām, šāds pieprasījums pārzinim attiecīgā gadījumā jāizskata saskaņā ar minētajiem nozares vai valsts noteikumiem. Bieži vien atkarībā no attiecīgajiem valsts tiesību aktiem pārzinim var būt pienākums sniegt atsevišķas atbildes, no kurām katra attiecas uz konkrētajām prasībām, kas noteiktas dažādos tiesību aktos. Tos nedrīkst jaukt ar valsts vai ES tiesību aktiem, kuros paredzēti piekļuves tiesību ierobežojumi, kas jāievēro, sniedzot atbildi uz piekļuves pieprasījumiem.
48. Ja pārzinim ir šaubas par to, kādas tiesības datu subjekts vēlas izmantot, ieteicams lūgt datu subjektam, kas iesniedzis pieprasījumu, paskaidrot pieprasījuma priekšmetu. Šāda sarakste ar datu subjektu neietekmē pārzina pienākumu rīkoties bez nepamatotas kavēšanās<sup>27</sup>. Tomēr šaubu gadījumā, ja pārzinis lūdz datu subjektam papildu skaidrojumus, bet atbildi nesaņem, tad, ņemot vērā pienākumu veicināt personas piekļuves tiesību īstenošanu, pārzinim būtu jāinterpretē pirmajā pieprasījumā ietvertā informācija un jārikojas, pamatojoties uz to. Saskaņā ar pārskatatbildības principu pārzinis var noteikt atbilstošu termiņu, kurā datu subjekts var sniegt papildu skaidrojumus. Nosakot šādu termiņu, pārzinim būtu jāparedz pietiekami daudz laika, lai pēc šā termiņa beigām izpildītu pieprasījumu, un tāpēc tam ir jāapdomā, cik daudz laika ir objektīvi vajadzīgs, lai pēc tam, kad datu subjekts ir (vai nav) sniedzis precizējumu, apkopotu un sniegtu pieprasītos datus.
49. Ja pieprasījums ietilpst VDAR darbības jomā, šādi īpaši pastāvošie tiesību akti nav svarīgāki par VDAR paredzēto piekļuves tiesību vispārējo piemērošanu. ES vai valsts tiesību aktos var būt noteikti ierobežojumi, ja to atļauj VDAR 23. pants (sk. 6.4. iedaļu).

*d) Vai pieprasījums ietilpst 15. panta darbības jomā?*

50. Būtu jānorāda, ka VDAR neievieš nekādas formālas prasības attiecībā uz personām, kas pieprasa piekļuvi datiem. Lai iesniegtu piekļuves pieprasījumu, pietiek ar to, ka pieprasījuma iesniedzējas personas norāda, ka vēlas zināt, kādus viņu persondatus pārzinis apstrādā. Tāpēc pārzinis nevar atteikties no datu sniegšanas, atsaucoties uz to, ka nav minēts pieprasījuma juridiskais pamats, un jo īpaši uz to, ka nav dota konkrēta atsauce uz piekļuves tiesībām vai VDAR.

Piemēram, lai iesniegtu pieprasījumu, pietiktu, ja pieprasījuma iesniedzēja persona norādītu, ka:

- vēlas iegūt piekļuvi persondatiem, kas uz viņu attiecas;
- izmanto savas piekļuves tiesības vai
- vēlas zināt, kādu informāciju par viņu pārzinis apstrādā.

Būtu jāpatur prātā, ka pieteikuma iesniedzēji var nezināt visas VDAR niansas un ka pret personām, kas izmanto savas piekļuves tiesības, ieteicams būt iecietīgiem, jo īpaši, ja šīs tiesības izmanto nepilngadīgie. Kā norādīts iepriekš, šaubu gadījumā pārzinim ir ieteicams lūgt datu subjektu, kas iesniedzis pieprasījumu, precizēt pieprasījuma priekšmetu.

---

<sup>27</sup> Sīkākus norādījumus par termiņu noteikšanu sk. 5.3. iedaļā.

e) Vai datu subjekti vēlas pieklūt visai apstrādātajai informācijai, kas uz viņiem attiecas, vai tās daļai?

51. Pārzinim ir jānovērtē arī tas, vai pieprasījuma iesniedzēju personu pieprasījumi attiecas uz visu apstrādāto informāciju par viņām vai tās daļu. Jebkuram datu subjektu noteiktam pieprasījuma tvēruma ierobežojumam līdz konkrētam VDAR 15. panta noteikumam ir jābūt skaidram un nepārprotamam. Piemēram, ja datu subjekti pieprasa burtiski "informāciju par datiem, kas tiek apstrādāti saistībā ar viņiem", pārzinim būtu jāpieņem, ka datu subjekti plāno pilnā mērā izmantot savas tiesības saskaņā ar VDAR 15. panta 1. un 2. punktu. Šāds pieprasījums nebūtu jāinterpretē tādējādi, ka datu subjekti vēlas saņemt tikai apstrādājamo kategoriju persondatus un nevēlas izmantot savas tiesības saņemt 15. panta 1. punkta a) līdz h) apakšpunktā uzskaitīto informāciju. Citādi būtu, piemēram, ja datu subjekti attiecībā uz viņu norādītajiem datiem vēlētos uzzināt persondatu avotu vai izcelsmi vai konkrēto glabāšanas laika posmu. Šādā gadījumā pārzinis var sniegt atbildi tikai par konkrēto pieprasīto informāciju.

### 3.1.2 Pieprasījuma forma

52. Kā norādīts iepriekš, VDAR neparedz nekādas prasības, kas datu subjektiem jāievēro attiecībā uz formu, kādā jāsniedz pieprasījums par piekļuvi persondatiem. Tāpēc principā VDAR nav nekādu prasību, kas datu subjektiem būtu jāievēro, izvēloties kanālu saziņai ar pārzini.
53. EDAK mudina pārziņus nodrošināt visatbilstošākos un lietotājiem ērtos saziņas kanālus saskaņā ar VDAR 12. panta 2. punktu un 25. pantu, lai datu subjekts varētu iesniegt efektīvu pieprasījumu. Tomēr, ja datu subjekts pieprasījumu iesniedz, izmantojot pārziņa nodrošinātu saziņas kanālu<sup>28</sup>, kas atšķiras no kanāla, kurš norādīts kā vēlmais saziņas kanāls, šādu pieprasījumu kopumā uzskata par efektīvu, un pārzinim tas būtu attiecīgi jāizskata (sk. tālāk minētos piemērus). Pārziņiem būtu jāpieliek visas saprātīgās pūles, lai nodrošinātu, ka tiek veicināta datu subjekta tiesību īstenošana (piemēram, ja datu subjekts nosūta piekļuves pieprasījumu atvaļinājumā esošam darbiniekam, saprātīgas pūles varētu būt automātisks ziņojums, ar ko datu subjektu informē par alternatīvu saziņas kanālu attiecībā uz šo pieprasījumu).
54. Būtu jānorāda, ka pārzinim nav pienākuma reaģēt uz pieprasījumu, kas nosūtīts uz nejauši izvēlētu vai nepareizu e-pasta (vai pasta) adresi, kuru pārzinis nav tieši norādījis, vai nosūtīts, izmantojot jebkuru saziņas kanālu, kas nepārprotami nav paredzēts, lai saņemtu pieprasījumus, kuri attiecas uz datu subjekta tiesībām, ja pārzinis ir nodrošinājis piemērotu saziņas kanālu, ko datu subjekts var izmantot.
55. Pārzinim nav arī pienākuma reaģēt uz pieprasījumu, kas nosūtīts uz tāda pārziņa darbinieka e-pasta adresi, kurš var nebūt iesaistīts ar datu subjektu tiesībām saistītu pieprasījumu apstrādē (piemēram, transportlīdzekļu vadītāji, uzkopšanas darbinieki u. c.). Šādus pieprasījumus neuzskata par efektīviem, ja pārzinis datu subjektam ir skaidri nodrošinājis atbilstīgu saziņas kanālu. Tomēr, ja datu subjekts nosūta pieprasījumu pārziņa darbiniekam, kas izraudzīts par datu subjekta pastāvīgo kontaktpersonu (piemēram, bankas personīgā konta vadītājam vai mobilo sakaru operatora pastāvīgam konsultantam), šāda saziņa nebūtu jāuzskata par nejaušu un pārzinim būtu jāpieliek visas saprātīgās pūles, lai šādu pieprasījumu apstrādātu tā, ka to varētu novirzīt uz kontaktpunktu un uz to varētu atbildēt VDAR noteiktajos termiņos.

---

<sup>28</sup> Tas var ietvert, piemēram, datu pārziņa kontaktinformāciju, kas sniegta paziņojumos, kuri adresēti tieši datu subjektiem, vai pārziņa publiski sniegtā kontaktinformācijā, piemēram, pārziņa privātuma politikā vai citos pārziņa obligātajos juridiskajos paziņojumos (piemēram, īpašnieka vai uzņēmuma kontaktinformācija tīmekļa vietnē).

56. Tomēr EDAK kā labu praksi iesaka pārziņiem ieviest piemērotus mehānismus, lai veicinātu datu subjektu tiesību īstenošanu, tai skaitā autoatbildētāju sistēmas informēšanai par darbinieku prombūtni un piemērotu alternatīvu kontaktpersonu, un, ja iespējams, mehānismus, lai uzlabotu iekšējo saziņu starp darbiniekiem par pieprasījumiem, kurus saņēmuši darbinieki, kas, iespējams, nav kompetenti tos izskatīt.

**8. piemērs.** Pārzinis X gan savā tīmekļa vietnē, gan paziņojumā par privātumu norāda divas e-pasta adreses, proti, pārziņa vispārējo e-pasta adresi CONTACT@X.COM un pārziņa datu aizsardzības kontaktpunkta e-pasta adresi QUERIES@X.COM. Papildus tam pārzinis X savā tīmekļa vietnē norāda, ka, lai iesniegtu jautājumus vai pieprasījumu attiecībā uz persondatu apstrādi, personām būtu jāsazinās ar datu aizsardzības kontaktpunktu, izmantojot norādīto e-pasta adresi. Tomēr datu subjekts nosūta pieprasījumu uz pārziņa vispārējo e-pasta adresi CONTACT@X.COM.

Šādā gadījumā pārzinim būtu jāpieliek visas saprātīgās pūles, lai informētu savus dienestus par pieprasījumu, kas iesniegts, izmantojot vispārējo e-pasta adresi, un lai to varētu novirzīt uz datu aizsardzības kontaktpunktu un uz to varētu atbildēt VDAR noteiktajā termiņā. Turklāt pārzinim nav tiesību pagarināt termiņu, kurā sniedzama atbilde uz pieprasījumu, tikai tāpēc, ka datu subjekts pieprasījumu ir nosūtījis uz pārziņa vispārējo e-pasta adresi, nevis uz pārziņa datu aizsardzības kontaktpunkta e-pasta adresi.

**9. piemērs.** Pārzinis Y vada fitnesa klubu tīklu. Pārzinis Y savā tīmekļa vietnē un fitnesa kluba klientiem sniedzamajā paziņojumā par privātumu norāda, ka, lai iesniegtu jebkādus jautājumus vai pieprasījumus attiecībā uz persondatu apstrādi, fiziskām personām būtu jāsazinās ar pārzini, izmantojot e-pasta adresi QUERIES@Y.COM. Tomēr datu subjekts nosūta pieprasījumu uz e-pasta adresi, ko atradis ģērbtuvē izvietotā paziņojumā “Ja jūs neapmierina telpas tīrība, lūdzam sazināties ar mums, izmantojot e-pasta adresi CLEANERS@Y.COM”, kas ir Y uzkopšanas darbinieku e-pasta adrese. Uzkopšanas darbinieki acīmredzami nav iesaistīti tādu jautājumu risināšanā, kas saistīti ar datu subjektu — fitnesa kluba klientu — tiesību īstenošanu. Lai gan minētā e-pasta adrese bija pieejama fitnesa kluba telpās, datu subjekts nevarēja pamatoti gaidīt, ka tā ir piemērota kontaktadrese šādiem pieprasījumiem, jo tīmekļa vietnē un paziņojumā par privātumu bija skaidri norādīts saziņas kanāls, kas jāizmanto datu subjektu tiesību īstenošanai.

57. Datumā, kurā pārzinis saņēmis pieprasījumu, parasti sākas viena mēneša termiņš, kurā pārzinim jāsniedz informācija par darbību, kas veikta pēc pieprasījuma, saskaņā ar VDAR 12. panta 3. punktu (sīkāki norādījumi par termiņiem ir sniegti 5.3. iedaļā). EDAK uzskata, ka pārziņu laba prakse ir pieprasījumu saņemšanas rakstiska apstiprināšana, piemēram, pieprasījuma iesniedzējām personām nosūtot e-pasta vēstuli (vai attiecīgā gadījumā informāciju pa pastu), kurā apstiprina, ka viņu pieprasījumi ir saņemti un ka viena mēneša termiņš ilgst no X dienas līdz Y dienai.

### 3.2 Identifikācija un autentifikācija

58. Lai nodrošinātu apstrādes drošību un mazinātu persondatu neatļautas izpaušanas risku, pārzinim ir jābūt iespējai uzzināt, kuri dati attiecas uz datu subjektu (identifikācija), un apstiprināt šīs personas identitāti (autentificēšana).
59. Var atgādināt, ka situācijās, kad nolūki, kādos pārzinis apstrādā persondatus, neprasa vai vairs neprasa pārzinim identificēt datu subjektu, pārzinim nav jāsauglabā identifikācija, ja vienīgais nolūks ir ievērot datu subjektu tiesības, arī ņemot vērā datu minimizēšanas principu. Šīs situācijas ir minētas VDAR 11. panta 1. punktā.

60. VDAR 12. panta 2. punktā ir noteikts, ka pārzinis neatsakās rīkoties pēc datu subjekta pieprasījuma par savu tiesību īstenošanu, ja vien pārzinis neapstrādā persondatus nolūkā, kam nav nepieciešama datu subjekta identifikācija, un uzskatāmi neparāda, ka datu subjektu nespēj identificēt. Šādos apstākļos datu subjekts tomēr var nolemt sniegt papildu informāciju, kas ļauj veikt šo identifikāciju (VDAR 11. panta 2. punkts)<sup>29</sup>.
61. Pārzinim nav pienākuma iegūt šādu papildu informāciju, lai identificētu datu subjektu tikai nolūkā izpildīt datu subjekta pieprasījumu, arī ņemot vērā datu minimizēšanas principu. Tomēr tam nebūtu jāatsakās pieņemt papildu informāciju, ko sniedz datu subjekts, lai pamatotu savu tiesību īstenošanu (VDAR 57. apsvērums).

**10. piemērs.** X ir tādu datu pārzinis, kas tiek apstrādāti saistībā ar ēkas videonovērošanu. Saskaņā ar VDAR 11. panta 1. punktu pārzinim nav pienākuma uzraudzības ietvaros identificēt visas personas, ko reģistrējusi novērošanas kamera (nolūks, kam nav vajadzīga identifikācija). Pārzinis saņem pieprasījumu par piekļuvi persondatiem no personas, kura apgalvo, ka viņu ir reģistrējusi pārziņa videonovērošanas sistēma. Pārziņa darbības būs atkarīgas no sniegtās papildu informācijas. Ja pieprasījuma iesniedzēja persona norāda konkrētu dienu un laiku, kurā kameras varētu būt ierakstījušas attiecīgo notikumu, pārzinis šādus datus, iespējams, varēs sniegt (VDAR 11. panta 2. punkts). Tomēr, ja pārzinis datu subjektu nespēj identificēt (piemēram, ja pārzinis nevar pārliecināties par to, vai pieprasījuma iesniedzēja persona faktiski ir datu subjekts, vai arī ja pieprasījums attiecas, piemēram, uz ilgu ierakstīšanas periodu un pārzinis tik lielu datu apjomu nevar apstrādāt), pārzinis var atteikties rīkoties, ja viņš pierāda, ka nespēj identificēt datu subjektu (VDAR 12. panta 2. punkts).

**11. piemērs.** Pārzinis C apstrādā persondatus, lai saviem tīmekļa lietotājiem adresētu paradumiem pieskaņotu reklāmu. Persondatus, kas savākti paradumiem pieskaņotai reklāmai, parasti vāc, izmantojot sīkdatnes, un tie ir saistīti ar nejaušiem pseidonīmiem identifikatoriem. Datu subjekts X kungs īsteno savas piekļuves tiesības attiecībā pret C, izmantojot C tīmekļa vietni. C var precīzi identificēt X kungu, lai parādītu datu subjekta paradumiem pieskaņoto reklāmu, sasaistot X kunga galiekārtu un tā reklāmas profilu ar galiekārtā ievietotajām sīkdatnēm. C arī būtu jāspēj precīzi identificēt X kungu, lai viņam piešķirtu piekļuvi saviem persondatiem, jo var atrast saikni starp apstrādātajiem datiem un datu subjektu. Tāpēc un ņemot vērā VDAR principus, iepriekš minētais piemērs neietilpst VDAR 11. panta darbības jomā. Precīzāk, iepriekš minētajā piemērā C nolūkiem ir vajadzīga datu subjekta identifikācija, savukārt VDAR 11. pants attiecas uz apstrādes situāciju, kurā identifikācija nav vajadzīga un pārzinim nav pienākuma apstrādāt papildu datus VDAR 11. panta 1. punkta nozīmē tikai nolūkā nodrošināt atbilstību VDAR. Līdz ar to dažos gadījumos, lai īstenotu datu subjekta tiesības, nekādi papildu dati nebūtu jāpieprasa.

Tomēr, ja X kungs cenšas izmantot savas piekļuves tiesības, izmantojot e-pastu vai pastu, tad šajā kontekstā C nav citas izvēles kā vien lūgt X kungu sniegt "papildu informāciju" (VDAR 12. panta 6. punkts), lai varētu identificēt ar X kungu saistīto reklāmas profilu. Šajā gadījumā papildu informācija būs X kunga galiekārtā saglabātās sīkdatnes identifikators.

62. Gadījumā, kad ir uzskatāmi parādīts, ka identificēt datu subjektu nav iespējams (VDAR 11. pants), pārzinim, ja iespējams, ir attiecīgi jāinformē datu subjekts, jo pārzinis atbild uz datu subjekta pieprasījumiem bez nepamatotas kavēšanās un norāda iemeslus, ja šādus pieprasījumus neplāno

<sup>29</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 13. lpp.



izpildīt. Šī informācija jāsniedz tikai, "ja iespējams", jo pārzinis var nespēt informēt datu subjektus, ja nav iespējama to identifikācija.

63. Gan tad, ja apstrādei nav vajadzīga identifikācija, gan tad, ja pārzinim ir pamatotas šaubas par tās fiziskās personas identitāti, kura iesniedz pieprasījumu, pārzinis var prasīt, lai tiktu sniegta papildu informācija, kas vajadzīga datu subjekta identitātes apstiprināšanai (VDAR 12. panta 6. punkts).
64. VDAR nenosaka nekādas prasības attiecībā uz to, kā autentificēt datu subjektu. Tomēr VDAR 11. un 12. pantā ir iekļauti nosacījumi visu datu subjektu tiesību, arī tiesību piekļūt persondatiem, īstenošanai.
65. Būtu jāatceras, ka parasti pārzinis nevar pieprasīt vairāk persondatu, nekā vajadzīgs autentifikācijas nodrošināšanai, un ka šādas informācijas izmantošanai būtu jāaprobežojas tikai ar datu subjektu pieprasījuma izpildi.
66. Bieži vien datu subjektu un pārziņu starpā jau pastāv autentifikācijas procedūras. Pārziņi šīs autentifikācijas procedūras var izmantot, lai pārliecinātos par to datu subjektu identitāti, kuri pieprasa savus persondatus vai izmanto VDAR piešķirtās tiesības<sup>30</sup>. Pretējā gadījumā pārziņiem būtu jāīsteno autentifikācijas procedūra, lai to izdarītu<sup>31</sup>.
67. Gadījumos, kad pārzinis pieprasa vai datu subjekts sniedz papildu informāciju, kas vajadzīga, lai apstiprinātu datu subjekta identitāti, pārzinis katru reizi novērtē, kāda informācija viņam ļaus apstiprināt datu subjekta identitāti, un, iespējams, pieprasījuma iesniedzējai personai uzdod papildu jautājumus vai pieprasa datu subjektam sniegt papildu identifikācijas elementus, ja tas ir samērīgi (sk. 3.3. iedaļu).
68. Lai datu subjekts varētu sniegt papildu informāciju, kas vajadzīga viņa datu identificēšanai, pārzinim datu subjekts būtu jāinformē par identificēšanai vajadzīgās papildu informācijas būtību. Šādai papildu informācijai nevajadzētu būt plašākai par informāciju, kas sākotnēji vajadzīga datu subjekta autentifikācijai. Kopumā tas, ka pārzinis drīkst pieprasīt papildu informāciju, lai novērtētu datu subjekta identitāti, nevar būt iemesls pārmērīgām prasībām un tādu persondatu vākšanai, kas nav būtiski vai vajadzīgi, lai stiprinātu saikni starp personu un pieprasītajiem persondatiem<sup>32</sup>.
69. Līdz ar to, ja tiešsaistē savāktā informācija ir saistīta ar pseidonīmiem vai citiem unikāliem identifikatoriem, pārzinis var īstenot atbilstīgas procedūras, kas pieprasījuma iesniedzējai personai ļauj iesniegt pieprasījumu par piekļuvi datiem un saņemt ar to saistītos datus<sup>33</sup>.

**12. piemērs.** Datu subjekts X kundze, sarunājoties ar palīdzības dienesta konsultantu elektroenerģijas uzņēmumā, ar kuru viņa noslēgusi līgumu, lūdz piekļuvi saviem datiem. Konsultants, šauboties par pieprasījuma iesniedzējas personas identitāti, divkāršās verifikācijas sistēmas ietvaros uzņēmuma sistēmā ģenerē vienreizēju unikālu kodu, ko nosūta uz lietotāja mobilā tālruņa numuru, kas norādīts konta izveides laikā, un viņa rīcība šajā gadījumā būtu jāuzskata par samērīgu.

### 3.3 Samērīguma novērtējums attiecībā uz pieprasījuma iesniedzējas personas autentificēšanu

---

<sup>30</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 14. lpp.

<sup>31</sup> Sīkākus norādījumus par autentifikāciju sk. 3.3. iedaļā.

<sup>32</sup> Turpat, 14. lpp.

<sup>33</sup> Turpat, 13. un 14. lpp.

70. Kā norādīts iepriekš, ja pārzinim ir pamatots iemesls apšaubīt pieprasījuma iesniedzējas personas identitāti, tas drīkst pieprasīt papildu informāciju, lai apstiprinātu datu subjekta identitāti. Tomēr pārzinim vienlaikus ir jānodrošina, ka tas neievāc vairāk persondatu, nekā vajadzīgs, lai varētu autentificēt pieprasījuma iesniedzēju personu. Tāpēc pārzinis veic samērīguma novērtējumu, kurā jāņem vērā apstrādājamo persondatu veids (piemēram, īpašas datu kategorijas), pieprasījuma raksturs, konteksts, kādā pieprasījums tiek iesniegts, kā arī jebkāds kaitējums, ko varētu radīt datu nepareiza izpaušana. Novērtējot samērīgumu, būtu jāpatur prātā, ka jāizvairās no pārmērīgas datu vākšanas, vienlaikus nodrošinot pienācīgu apstrādes drošības līmeni.
71. Pārzinim būtu jāīsteno autentifikācijas procedūra, lai būtu zināma to personu identitāte, kuras lūdz piekļuvi saviem datiem<sup>34</sup>, un jānodrošina apstrādes drošība visā piekļuves pieprasījumu apstrādes procesā saskaņā ar VDAR 32. pantu, ieskaitot, piemēram, drošu kanālu papildu informācijas sniegšanai datu subjektiem. Autentifikācijas metodei vajadzētu būt atbilstīgai, piemērotai, samērīgai, un tajā būtu jāievēro datu minimizēšanas princips. Ja pārziņa noteiktie pasākumi, kuru mērķis ir autentificēt datu subjektu, ir apgrūtināši, pārzinim tie ir pienācīgi jāpamato un jānodrošina atbilstība visiem pamatprincipiem, ieskaitot datu minimizēšanu un pienākumu veicināt datu subjektu tiesību īstenošanu (VDAR 12. panta 2. punkts).
72. Tiešsaistes kontekstā autentifikācijas mehānisms var ietvert tos pašus akreditācijas datus, kurus datu subjekts izmanto, lai pieteiktos datu pārziņa piedāvātajiem tiešsaistes pakalpojumiem (VDAR 57. apsvērums)<sup>35</sup>.
73. Praksē autentifikācijas procedūras tiek izmantotas bieži, un pārziņiem nav jāievieš papildu aizsardzības pasākumi, lai novērstu neatļautu piekļuvi pakalpojumiem. Lai personas varētu piekļūt viņu kontos (piemēram, e-pasta kontā, sociālo tīklu kontā vai tiešsaistes veikalos) iekļautajiem datiem, pārziņi, visticamāk, pieprasīs pieteikšanos, izmantojot lietotāja lietotājvārdu un paroli, ar ko šādos gadījumos vajadzētu pietikt, lai autentificētu datu subjektu<sup>36</sup>. Turklāt pārzinis datu subjektus bieži vien jau ir autentificējis pirms līguma noslēgšanas vai viņu piekrišanas apstrādei saņemšanas, un līdz ar to persondatus, ko izmanto, lai reģistrētu personu, uz kuru attiecas apstrāde, var izmantot arī kā pierādījumu, lai autentificētu datu subjektu piekļuves nolūkos<sup>37</sup>. Tādējādi nav samērīgi pieprasīt personu apliecinoša dokumenta kopiju, ja pārzinis jau ir autentificējis datu subjektu, kas iesniedz pieprasījumu.
74. Būtu jāuzsver, ka personu apliecinoša dokumenta kopijas izmantošana autentifikācijas procesā rada risku persondatu drošībai un var izraisīt neatļautu vai nelikumīgu apstrādi, tādējādi tā būtu uzskatāma par nepiemērotu, ja vien tā nav vajadzīga, piemērota un neatbilst valsts tiesību aktiem. Šādos gadījumos, lai saņemtu šādus datus, pārziņiem vajadzētu būt ieviestām sistēmām, kuras nodrošina tādu drošības līmeni, kas ir piemērots, lai mazinātu lielāku risku attiecībā uz datu subjekta tiesībām un brīvībām. Svarīgi ir arī norādīt, ka autentifikācija, izmantojot personas apliecību, ne vienmēr palīdz tiešsaistes kontekstā (piemēram, izmantojot pseidonīmus), ja attiecīgā persona nevar sniegt nekādus citus pierādījumus, piemēram, papildu raksturīgas pazīmes, kas atbilst lietotāja kontam.

---

<sup>34</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 14. lpp.

<sup>35</sup> Papildu norādījumus par autentifikācijas metodēm sk. 30.–31. lpp. EDAK Pamatnostādnēs 01/2021 par persondatu aizsardzības pārkāpumu paziņošanu — piemēri, kas pieņemtas 2021. gada 14. janvārī, un 3.7. iedaļā EDAK Pamatnostādnēs 02/2021 par balsis virtuālajiem asistentiem, versija 2.0, kas pieņemtas 2021. gada 7. jūlijā.

<sup>36</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 14. lpp.

<sup>37</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 14. lpp.

75. Ņemot vērā to, ka daudzas organizācijas (piemēram, viesnīcas, bankas, automašīnu nomas uzņēmumi) pieprasa savu klientu personas apliecības kopijas, kopumā to nevajadzētu uzskatīt par piemērotu autentifikācijas veidu. Alternatīvi pārzinis var īstenot ātru un efektīvu drošības pasākumu, lai datu subjektu identificētu, pamatojoties uz viņa iepriekš veikto autentifikāciju, piemēram, izmantojot e-pastu vai īsziņu ar apstiprinājuma saitēm, drošības jautājumus vai apstiprinājuma kodus<sup>38</sup>.
76. Personas apliecībā iekļauto informāciju, kas nav vajadzīga datu subjekta identitātes apstiprināšanai, piemēram, piekļuvi tai un sērijas numuru, valstspiederību, garumu, acu krāsu, fotogrāfiju un mašīnlasāmo joslu, izvērtējot katru gadījumu atsevišķi, datu subjekts pirms iesniegšanas pārzinim var rediģēt vai paslēpt, izņemot gadījumus, kad valsts tiesību aktos ir prasīta personas apliecības pilna, nerediģēta kopija (sk. 78. punktu). Parasti pietiek ar izdošanas datumu vai derīguma termiņu, izdevējstādi un pilnu vārdu un uzvārdu, kas norādīts tiešsaistes kontā, lai pārzinis varētu pārbaudīt identitāti, ja vien vienmēr tiek nodrošināts kopijas autentiskums un saikne ar pieteikuma iesniedzēju. Papildu informāciju, piemēram, datu subjekta dzimšanas datumu, var pieprasīt tikai tad, ja pastāv kļūdainas identitātes risks un ja pārzinis to var salīdzināt ar informāciju, ko tas jau apstrādā.
77. Lai ievērotu datu minimizēšanas principu, pārzinim būtu jāinformē datu subjekts par informāciju, kas nav vajadzīga, un par iespēju rediģēt vai paslēpt attiecīgās personu apliecinošā dokumenta daļas. Šādā gadījumā, ja datu subjekts nezina, kā šādu informāciju rediģēt, vai nespēj to izdarīt, pārziņa īstenota laba prakse ir to rediģēt pēc dokumenta saņemšanas, ja viņš to var izdarīt, ņemot vērā viņam pieejamos līdzekļus konkrētajos apstākļos.

**13. piemērs.** Lietotāja Y kundze tiešsaistes veikalā ir izveidojusi ar paroli aizsargātu kontu, norādot savu e-pasta adresi un/vai lietotājvārdu. Pēc tam konta īpašniece lūdz pārzinim informāciju par to, vai tas apstrādā viņas persondatus, un, ja apstrādā, tad lai tas nodrošina tiem piekļuvi saskaņā ar 15. pantu. Lai apstiprinātu pieprasījuma iesniedzējas personas identitāti, pārzinis lūdz viņas personas apliecību. Šajā gadījumā pārziņa rīcība ir nesamērīga un izraisa nevajadzīgu datu vākšanu.

Tomēr, lai apstiprinātu pieprasījuma iesniedzējas personas identitāti, vienlaikus izvairoties no nevajadzīgas datu vākšanas, pārzinis varētu lūgt viņu autentificēties, piesakoties kontā, vai uzdot viņai (neintruzīvus) drošības jautājumus, uz kuriem atbilde būtu zināma tikai datu subjektam, vai izmantot vairākfaktoru autentifikāciju, kas konfigurēta, datu subjektam reģistrējot savu kontu, vai izmantot citus esošos saziņas līdzekļus, par kuriem zināms, ka tie pieder datu subjektam, piemēram, e-pasta adresi vai tālruņa numuru, lai nosūtītu piekļuves paroli.

**14. piemērs.** Bankas klients Y kungs plāno ņemt patēriņa kredītu. Šajā nolūkā Y kungs dodas uz bankas filiāli, lai iegūtu informāciju, arī viņa persondatus, kas vajadzīgi viņa kredītspējas novērtēšanai. Lai pārbaudītu datu subjekta identitāti, konsultants lūdz viņa identitātes notariālu apliecinājumu, lai varētu sniegt viņam vajadzīgo informāciju.

Pārzinim nebūtu jāpieprasa notariāli apliecināts identitātes apstiprinājums, ja vien tas nav nepieciešams, piemērots un neatbilst valsts tiesību aktiem (piemēram, ja personai uz laiku nav neviena personu apliecinoša dokumenta, bet valsts tiesību aktos ir prasīts datu subjekta identitātes

---

<sup>38</sup> Sk. arī Eiropas Parlamenta un Padomes Regulu (ES) Nr. 910/2014 (2014. gada 23. jūlijs) par elektronisko identifikāciju un uzticamības pakalpojumiem elektronisko darījumu veikšanai iekšējā tirgū un ar ko atceļ Direktīvu 1999/93/EK, kurā ir paredzēti dažādi pakalpojumi, kas ļauj veikt drošu attālinātu identifikāciju.

apliecinājums, lai veiktu juridisku darbību). Šāda prakse rada papildu izmaksas pieprasījuma iesniedzējām personām un pārmērīgu slogu datu subjektiem, kavējot viņu piekļuves tiesību īstenošanu.

78. Neskarot iepriekš minētos vispārīgos principus, noteiktos apstākļos autentifikācija, pamatojoties uz personas apliecību, var būt pamatots un samērīgs pasākums, jo īpaši attiecībā uz vienībām, kas apstrādā īpašu kategoriju persondatus vai veic datu apstrādi, kura var radīt risku datu subjektam (piemēram, medicīniska vai ar veselību saistīta informācija). Tomēr vienlaikus būtu jāpatur prātā, ka dažos valstu noteikumos ir paredzēti ierobežojumi attiecībā uz publiskos dokumentos, arī dokumentos, kas apliecina personas identitāti, ietverto datu apstrādi (arī pamatojoties uz VDAR 87. pantu). Ierobežojumi attiecībā uz to datu apstrādi, kas iegūti no šiem dokumentiem, jo īpaši var attiekties uz personas apliecību skenēšanu vai kopēšanu vai oficiālu personas identifikācijas numuru apstrādi<sup>39</sup>.
79. Ņemot vērā iepriekš minēto, ja tiek pieprasīta personas apliecība (un tas ir gan saskaņā ar valsts tiesību aktiem, gan pamatoti un samērīgi saskaņā ar VDAR), pārzinim ir jāīsteno aizsardzības pasākumi, lai novērstu personas apliecības nelikumīgu apstrādi. Neatkarīgi no jebkādiem piemērojamiem valsts noteikumiem par autentifikāciju, izmantojot personas apliecību, tie var ietvert atturēšanos no kopijas izgatavošanas vai kopijas dzēšanu tūlīt pēc datu subjekta identitātes sekmīgas autentifikācijas. Tas ir tāpēc, ka personas apliecības kopijas turpmāka glabāšana varētu būt nolūka ierobežojuma un glabāšanas ierobežojuma princips (VDAR 5. panta 1. punkta b) un e) apakšpunkts) pārkāpums, kā arī valsts tiesību aktu par valsts identifikācijas numura apstrādi (VDAR 87. pants) pārkāpums. Lai izvairītos no nevajadzīgas personas apliecību kopiju izgatavošanas vai glabāšanas, EDAK kā labu praksi pārzinim iesaka pēc personas apliecības pārbaudes atzīmēt, piemēram, ka "personas apliecība ir pārbaudīta".

### 3.4 Pieprasījumi, ko iesniedz ar trešu/pilnvarotu personu starpniecību

80. Lai gan piekļuves tiesības parasti īsteno datu subjekti, jo tās attiecas uz viņiem, pieprasījumu datu subjekta vārdā var iesniegt arī trešā persona. Tas cita starpā var attiekties uz pilnvarotas personas vai likumīgu aizbildņu rīkošanos nepilngadīgo vārdā, kā arī uz rīkošanos ar citu struktūru starpniecību, izmantojot tiešsaistes portālus. Dažos gadījumos var būt jāveic pārbaude attiecībā uz tās personas identitāti, kura ir pilnvarota izmantot piekļuves tiesības, kā arī attiecībā uz pilnvaru rīkoties datu subjekta vārdā, ja tā ir piemērota un samērīga (sk. 3.3. iedaļu)<sup>40</sup>. Būtu jāatgādina, ka persondatu pieejamības nodrošināšana personai, kurai nav tiesību tiem piekļūt, var būt persondatu aizsardzības pārkāpums<sup>41</sup>.
81. To darot, būtu jāņem vērā valsts tiesību akti, kuri reglamentē tiesisko pārstāvību (piemēram, pilnvaras) un kuros var būt noteiktas īpašas prasības attiecībā uz to, kā pierādīt, ka pastāv pilnvara iesniegt pieprasījumu datu subjekta vārdā, jo VDAR šo jautājumu nereglamentē. Saskaņā ar pārskatatbildības principu, kā arī citiem datu aizsardzības principiem pārzinim jāspēj pierādīt, ka pastāv attiecīgā pilnvara datu subjekta vārdā iesniegt pieprasījumu un saņemt pieprasīto informāciju, izņemot gadījumus, kad valsts tiesību akti atšķiras (piemēram, valsts tiesību aktos ir ietverti īpaši noteikumi par advokātu uzticamību), ļaujot pārzinim pārbaudīt pilnvarotās personas identitāti (piemēram, ja advokāti pārbauda reģistrāciju advokatūrā). Tāpēc šajā sakarā ieteicams savākt attiecīgus dokumentus saistībā ar iepriekš norādītajiem vispārīgajiem noteikumiem par pieprasījuma iesniedzējas fiziskas personas

<sup>39</sup> Vairākas dalībvalstis ievieša šādu ierobežojumu savos valsts noteikumos, šajā saistībā, piemēram, norādot, ka personas apliecību kopiju izgatavošana ir likumīga tikai tad, ja tā tieši paredzēta tiesību akta noteikumos.

<sup>40</sup> Attiecībā uz piekļuves tiesību īstenošanas termiņiem, kuros pārzinim ir jāiegūst papildu informācija, sk. 157. punktu.

<sup>41</sup> VDAR 4. panta 12. punkts.

identitātes apstiprināšanu, un, ja pārzinim ir pamatotas šaubas par tās personas identitāti, kura rīkojas datu subjekta vārdā, tas pieprasa papildu informāciju, lai apstiprinātu šīs personas identitāti.

82. Vēl viens piemērs attiecībā uz piekļuvi datiem, ko īsteno trešā persona, kas nav datu subjekts, ir tiesību piekļūt mirušu personu persondatiem īstenošana, tomēr 27. apsvērumā ir norādīts, ka VDAR neattiecas uz mirušu personu persondatiem. Tāpēc šis jautājums tiek risināts valstu tiesību aktos, un dalībvalstis var paredzēt noteikumus par mirušu personu persondatu apstrādi. Tomēr būtu jāpatur prātā, ka šādi dati var attiekties arī uz dzīvām trešām personām, piemēram, ja tiek pieprasīta piekļuve mirušas personas korespondencei. Šādu datu konfidencialitāte joprojām ir jāaizsargā.

#### 3.4.1 Piekļuves tiesību īstenošana bērnu vārdā

83. Bērniem pienākas īpaša persondatu aizsardzība, jo viņi var pietiekami neapzināties attiecīgos riskus, sekas un aizsardzības pasākumus attiecībā uz savām tiesībām saistībā ar persondatu apstrādi<sup>42</sup>. Ja tiek apstrādāti bērna persondati, informācija bērnam būtu jāsniedz un saziņa ar viņu jāveic tik skaidrā un vienkāršā valodā, lai bērns to varētu viegli saprast<sup>43</sup>.
84. Bērni ir datu subjekti paši par sevi, un tādējādi piekļuves tiesības pieder bērnam. Atkarībā no bērna brieduma un spējām bērnam var būt vajadzīga trešā persona, kas rīkojas viņa vārdā, piemēram, persona, kam ir vecāku atbildība.
85. Bērna interesēm vajadzētu būt galvenajam apsvērumam visos lēmumos, kas pieņemti attiecībā uz piekļuves tiesību īstenošanu saistībā ar bērniem, jo īpaši gadījumos, kad piekļuves tiesības bērna vārdā īsteno, piemēram, persona, kurai ir vecāku vara.
86. Ņemot vērā VDAR ietverto bērnu persondatu īpašo aizsardzību, pārzinis veic atbilstošus pasākumus, lai nepieļautu nepilngadīgā persondatu izpaušanu nepilnvarotai personai (šajā saistībā sk. arī 3.4. iedaļu iepriekš).
87. Visbeidzot, personas, kurai ir vecāku atbildība, tiesības rīkoties bērna vārdā nevajadzētu jaukt ar gadījumiem, uz kuriem datu aizsardzības tiesību akti neattiecas un kuros personas, kam ir vecāku atbildība, tiesības pieprasīt un saņemt informāciju par bērnu (piemēram, par bērna sniegumu skolā) var būt paredzētas valsts tiesību aktos.

#### 3.4.2 Piekļuves tiesību īstenošana, izmantojot trešas personas nodrošinātus portālus/kanālus

88. Ir uzņēmumi, kas sniedz pakalpojumus, kuri datu subjektiem ļauj iesniegt piekļuves pieprasījumus portālā. Datu subjekts piesakās portālā, iegūst piekļuvi tam un tajā var dažādiem pārzinim iesniegt, piemēram, piekļuves pieprasījumu, pieprasīt datu labošanu vai datu dzēšanu. Saistībā ar trešo personu nodrošināto portālu izmantošanu rodas dažādi jautājumi.
89. Pirmā problēma, kas pārzinim šajos apstākļos jārisina, ir nodrošināt, ka trešā persona datu subjekta vārdā rīkojas likumīgi, jo ir jāpārlicinās, ka dati netiek izpausti nepilnvarotām personām.

---

<sup>42</sup> VDAR 38. apsvēruma. Kā noteikts EDAK darba programmā, tās mērķis ir sniegt norādījumus par bērnu datiem. Paredzams, ka šādā dokumentā tiks sniegts vairāk norādījumu par nosacījumiem, saskaņā ar kuriem bērns var izmantot savas piekļuves tiesības un persona, kam ir vecāku atbildība, var izmantot piekļuves tiesības bērna vārdā.

<sup>43</sup> VDAR 58. apsvēruma. EDAK Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679, 7. iedaļa.

90. Turklāt pārzinim, kas saņem pieprasījumu, kurš iesniegts, izmantojot šādu portālu, minētais pieprasījums vienmēr ir savlaicīgi jāizskata<sup>44</sup>. Tomēr pārzinim nav pienākuma sniegt datus saskaņā ar VDAR 15. pantu tieši portālam, ja pārzinis, piemēram, konstatē, ka drošības pasākumi ir nepietiekami vai ka būtu lietderīgi izmantot citu veidu, lai datus izpaustu datu subjektam. Šādos apstākļos, ja pārzinis ir ieviesis citas procedūras, lai efektīvi un droši izskatītu piekļuves pieprasījumus, tas var sniegt pieprasīto informāciju, izmantojot šīs procedūras.

## 4 PIEKĻUVES TIESĪBU UN PERSONDATU TVĒRUMS UN INFORMĀCIJA, UZ KO TAS ATTIECAS

91. Šīs iedaļas mērķis ir izskaidrot persondatu definīciju (4.1. iedaļa) un kopumā precizēt tās informācijas tvērumu, uz kuru attiecas piekļuves tiesības (4.2. un 4.3. iedaļa). Jāņem vērā, ka persondatu jēdziena tvērums un līdz ar to persondatu nošķiršana no citiem datiem ir tāda novērtējuma neatņemama daļa, ko pārzinis veic, lai noteiktu to datu apjomu, kuriem datu subjektam ir tiesības iegūt piekļuvi<sup>45</sup>.
92. Vispirms būtu jāatgādina, ka piekļuves tiesības var īstenot tikai attiecībā uz tādu persondatu apstrādi, kuri ietilpst VDAR materiālajā un teritoriālajā darbības jomā. Tāpēc piekļuves tiesības neattiecas uz persondatiem, kurus neapstrādā ar automatizētiem līdzekļiem vai kuri neveido daļu no kartotēkas vai nav paredzēti, lai veidotu daļu no kartotēkas, saskaņā ar VDAR 2. panta 1. punktu, vai kurus apstrādā fiziska persona tikai personiska vai mājsaimnieciska pasākuma gaitā saskaņā ar VDAR 2. panta 2. punktu.

### 4.1 Personas datu definīcija

93. VDAR 15. panta 1. un 3. punktā attiecīgi ir minēti “persondati” un “apstrādē esošie persondati”. Tāpēc piekļuves tiesību tvērumu vispirms un galvenokārt nosaka VDAR 4. panta 1. punktā definētā jēdziena “persondati” tvērums<sup>46</sup>. persondatu jēdziens jau ir aplūkots vairākos 29. panta darba grupas<sup>47</sup> dokumentos<sup>48</sup>, un to ir interpretējusi EST, arī saistībā ar piekļuves tiesībām saskaņā ar Direktīvas 95/46/EK 12. pantu.

---

<sup>44</sup> Attiecībā uz piekļuves tiesību īstenošanas termiņiem, kuros pārzinim ir jāiegūst papildu informācija, sk. 157. punktu.

<sup>45</sup> Saskaņā ar integrētas privātuma aizsardzības principu šāda analīze ir daļa no tādu atbilstošu pasākumu un aizsardzības pasākumu novērtējuma, kuru mērķis ir aizsargāt datu aizsardzības principus un datu subjektu tiesības, un to veic “gan apstrādes līdzekļu noteikšanas, gan pašas apstrādes laikā”, piemēram, viens no rādītājiem var būt atbildes laika saīsināšana, kad datu subjekti īsteno savas tiesības. Sīkākus skaidrojumus sk. Pamatnostādnēs 4/2019 par 25. pantu “Integrēta datu aizsardzība un datu aizsardzība pēc noklusējuma”.

<sup>46</sup> Saskaņā ar VDAR 4. panta 1. punktu ““persondati” ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu (“datu subjekts”); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;”.

<sup>47</sup> 29. panta darba grupa ir neatkarīga Eiropas darba grupa, kas līdz 2018. gada 25. maijam (VDAR piemērošanas sākumam) risināja jautājumus, kuri saistīti ar privātuma un persondatu aizsardzību, un tā ir EDAK priekštece.

<sup>48</sup> Piemēram, dokuments WP251rev01 — Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem, t. i., 19. lpp.; 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 9.

94. 29. panta darba grupa uzskatīja, ka Direktīvā 95/46/EK ietvertā persondatu definīcija “*atspoguļo Eiropas likumdevēja vēlmi pēc plašas persondatu izpratnes*”<sup>49</sup>. Saskaņā ar VDAR definīcija joprojām attiecas uz “*jebkuru informāciju, kas attiecas uz identificētu vai identificējamu fizisku personu*”. Papildus tādiem personas pamatdatiem kā vārds un uzvārds, adrese, tālruņa numurs u. c. šajā definīcijā var ietilpt neierobežoti plašs datu klāsts, arī medicīniskie konstatējumi, pirkumu vēsture, kredītpējas rādītāji, saziņas saturs u. c. Ņemot vērā persondatu definīcijas plašo tvērumu, pārziņa veikts šīs definīcijas ierobežojošs novērtējums izraisītu persondatu kļūdainu klasificēšanu<sup>50</sup> un galu galā piekļuves tiesību pārkāpumu.
95. Apvienotajās lietās C-141/12 un C-372/12<sup>51</sup> EST nolēma, ka piekļuves tiesības attiecas uz persondatiem, kas iekļauti protokolos, proti, pieteikuma iesniedzēja uzvārdu, dzimšanas datumu, pilsonību, dzimumu, etnisko piederību, reliģiju un valodu un attiecīgā gadījumā protokolā iekļautajā juridiskajā analīzē ietvertajiem datiem, bet ne pašu juridisko analīzi<sup>52</sup>. Šajā kontekstā juridiskā analīze pati par sevi nevarēja būt nedz datu subjekta veiktas pareizības pārbaudes, nedz arī labošanas priekšmets. Turklāt piekļuves nodrošināšana juridiskajai analīzei neatbilst mērķim garantēt privātumu, bet gan piekļuvi administratīviem dokumentiem.
96. *Nowak* lietā<sup>53</sup> EST veica plašāku analīzi un konstatēja, ka rakstiskās atbildes, kuras eksaminējamā persona sniegusi profesionālās kvalifikācijas eksāmenā, un visi eksaminētāja komentāri par šīm atbildēm ir persondati, kas attiecas uz eksaminējamo personu. Precīzāk, šāda subjektīva informācija ir persondati “viedokļa vai vērtējumu formā, ja vien šī informācija ir “attiecībā uz” konkrēto personu”<sup>54</sup> pretstatā eksāmena jautājumiem, kurus par persondatiem neuzskata<sup>55</sup>. Tādējādi kontekstuālam novērtējumam būtu jāizskaidro, kāda var būt informācijas ietekme vai rezultāts attiecībā uz personu un līdz ar to piekļuves tiesību tvērumu.

**15. piemērs.** Personai ir darba intervija uzņēmumā. Šajā saistībā darba meklētājs iesniedz CV un pieteikuma vēstuli. Intervijas laikā personāldaļas darbinieks veic piezīmes datorā, lai interviju dokumentētu. Pēc tam darba meklētājs kā datu subjekts lūdz piekļuvi viņa persondatiem, ko uzņēmums kā pārzinis ir savācis, veicot darbā pieņemšanas procedūru.

Pārzinim ir pienākums sniegt datu subjektam persondatus, ko datu subjekts pats pēc savas ierosmes darījis zināmus savā CV un pieteikuma vēstulē. Turklāt pārzinim ir jāsniedz datu subjektam intervijas kopsavilkums, arī subjektīvi komentāri par datu subjekta uzvedību, kurus personāldaļas darbinieks pierakstījis darba intervijas laikā, ievērojot visus izņēmumus, kas paredzēti valsts tiesību aktos un VDAR 23. pantā.

97. Tādējādi, ņemot vērā gadījuma konkrētos faktus, konkrēta piekļuves pieprasījuma novērtēšanas laikā pārziņiem, neskarot VDAR 15. panta 4. punktu, cita starpā ir jāsniedz šādu veidu dati:
- Īpašu kategoriju persondati saskaņā ar VDAR 9. pantu,

<sup>49</sup> 29. panta darba grupas Atzinums Nr. 4/2007 par “persondatu” jēdzienu, 4. lpp.

<sup>50</sup> Kā informāciju, kas neattiecas uz identificētu vai identificējamu fizisku personu.

<sup>51</sup> EST, apvienotās lietas C-141/12 un C-372/12, *YS pret Minister voor Immigratie, Integratie en Asiel un Minister voor Immigratie, Integratie en Asiel* pret M un S, 2014. gada 17. jūlijs.

<sup>52</sup> EST, apvienotās lietas C-141/12 un C-372/12, *YS* u. c., 38. un 48. punkts.

<sup>53</sup> EST, C-434/16, *Peter Nowak* pret *Data Protection Commissioner*, 2017. gada 20. decembris.

<sup>54</sup> EST, C 434/16, *Nowak*, 34. un 35. punkts.

<sup>55</sup> EST, C-434/16, *Nowak*, 58. punkts.

- persondati par sodāmību un pārkāpumiem saskaņā ar VDAR 10. pantu,
- dati, ko aktīvi un apzināti sniedzis datu subjekts (piemēram, konta dati, kas iesniegti, izmantojot veidlapas, atbildes uz anketas jautājumiem)<sup>56</sup>,
- novēroti dati vai neapstrādāti dati, ko datu subjekts sniedzis, izmantojot pakalpojumu vai ierīci (piemēram, dati, ko apstrādā savienoti objekti, darījumu vēsture, darbību žurnāli, piemēram, piekļuves žurnāli, tīmekļa vietņu izmantošanas vēsture, meklēšanas darbības, atrašanās vietas dati, klikšķināšanas darbības, unikāli personas uzvedības aspekti, piemēram, rokraksts, taustiņsitieni, īpašs gaitas vai runas veids)<sup>57</sup>,
- dati, kas izriet no citiem datiem, kurus datu subjekts nav tieši sniedzis (piemēram, kredīta koeficients, klasifikācija, kuras pamatā ir kopīgas datu subjektu pazīmes, rezidences vietas valsts, ko atklāj pasta indekss)<sup>58</sup>,
- dati, kas iegūti no citiem datiem, kurus datu subjekts nav tieši sniedzis (piemēram, dati, kas sniegti, lai piešķirtu kredītnovērtējumu vai nodrošinātu nelikumīgi iegūtu līdzekļu legalizācijas novēršanas noteikumu ievērošanu, algoritmiskie rezultāti, veselības novērtējuma vai personalizācijas vai ieteikumu procesa rezultāti)<sup>59</sup>,
- pseidonimizēti dati pretstatā anonimizētiem datiem (sk. arī šo pamatnostādņu 3. iedaļu).

**16. piemērs.** Elementi, kuri izmantoti, lai pieņemtu lēmumu par, piemēram, darbinieka paaugstināšanu amatā, darba samaksas palielināšanu vai jaunu darba uzdevumu (piemēram, gada snieguma pārskati, apmācības pieprasījumi, disciplinārie ieraksti, novērtējums, karjeras potenciāls), ir persondati, kas attiecas uz šo darbinieku. Tādējādi šādiem elementiem datu subjekts var piekļūt, iesniedzot pieprasījumu un, ja, piemēram, persondati attiecas arī uz citu personu, ievērojot VDAR 15. panta 4. punktu (piemēram, uz tāda cita darbinieka identitāti vai identitāti atklājošiem elementiem, kura liecība par profesionālo sniegumu ir iekļauta gada snieguma pārskatā, var attiekties VDAR 15. panta 4. punktā noteiktie ierobežojumi, un tādējādi ir iespējams, ka tos datu subjektam nevar paziņot, lai aizsargātu minētā darbinieka tiesības un brīvības). Tomēr var piemērot valsts darba tiesību aktu noteikumus, piemēram, attiecībā uz darbinieku piekļuvi personāla lietām, vai citus valsts noteikumus, piemēram, noteikumus par dienesta noslēpumu. Jebkurā gadījumā šādiem datu subjekta piekļuves tiesību (vai citu tiesību) izmantošanas ierobežojumiem, kas paredzēti valsts tiesību aktos, ir jāatbilst VDAR 23. panta nosacījumiem (sk. 6.4. iedaļu).

98. No iepriekš minētā neizsmeļošā to persondatu saraksta, kurus datu subjektam var sniegt saistībā ar piekļuves pieprasījumu, var izdarīt vairākus apsvērumus. No minētā izriet, ka pārzinis, sniedzot piekļuvi persondatiem, nevar nošķirt papīra formātā glabātos datus no elektroniski glabājamiem datiem, ja vien tie ietilpst VDAR darbības jomā. Citiem vārdiem sakot, uz persondatiem, kas tiek glabāti papīra formātā kā daļa no kartotēkas vai kas ir paredzēti, lai veidotu daļu no kartotēkas, piekļuves tiesības attiecas

<sup>56</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 9. lpp.

<sup>57</sup> 29. panta darba grupas Atzinums Nr. 4/2007 par "persondatu" jēdzienu, 8. lpp.

<sup>58</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 10. un 11. lpp.

<sup>59</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 10.–11. lpp.; 29. panta darba grupa, WP251rev.01, 2018. gada 6. februāris, Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem, ko apstiprinājusi EDAK (tālāk "29. panta darba grupas Pamatnostādnes par automatizētu individuālu lēmumu pieņemšanu un profilēšanu, ko apstiprinājusi EDAK"), 9.–10. lpp.



tāpat kā uz persondatiem, kuri tiek glabāti datora atmiņā, izmantojot, piemēram, bināro kodu vai videoierakstu.

99. Turklāt, tāpat kā lielākā daļa datu subjektu tiesību, piekļuves tiesības ietver gan izrietošos, gan iegūtos datus, arī persondatus, ko izveidojis pakalpojumu sniedzējs, savukārt tiesības uz datu pārnesamību ietver tikai datu subjekta sniegtos datus<sup>60</sup>. Tāpēc piekļuves pieprasījuma gadījumā un atšķirībā no datu pārnesamības pieprasījuma datu subjektam būtu jānodrošina ne tikai persondati, kas sniegti pārzinim, lai veiktu šo datu turpmāku analīzi vai novērtējumu, bet arī šādas turpmākas analīzes vai novērtējuma rezultāts.
100. Svarīgi ir arī atgādināt, ka pastāv arī tāda informācija kā anonīmi dati<sup>61</sup>, kas nav tieši vai netieši saistīti ar identificējamu personu un tādējādi ir izslēgti no VDAR darbības jomas. Piemēram, tā servera atrašanās vieta, kurā apstrādāti datu subjekta persondati nav persondati. Nodalīšana var būt sarežģīta, un pārzini var jautāt, kā skaidri nošķirt persondatus no datiem, kas nav persondati, jo īpaši jauktu datu kopu gadījumā. Šādā gadījumā var būt lietderīgi nošķirt jauktas datu kopas, kurās persondati un dati, kas nav persondati, ir nedalāmi saistīti, no datu kopām, kurās tas tā nav. Persondati un dati, kas nav persondati, jauktās datu kopās var būt nedalāmi saistīti un uz tiem kopumā var attiekties tā datu subjekta piekļuves tiesības, uz kuru attiecas persondati<sup>62</sup>. Citos gadījumos persondati un dati, kas nav persondati, jauktās datu kopās nedrīkst būt nedalāmi saistīti, nodrošinot, ka datu subjektam datu kopā ir pieejami tikai persondati. Piemēram, uzņēmumam varētu būt jāsniedz datu subjektam individuālie ziņojumi par IT incidentiem, ko viņš izraisījis, bet ne uzņēmuma zināšanu datubāze par IT problēmām. Tomēr tas, kādus drošības pasākumus pārzinis ieviesis, parasti nav jāsaprot kā persondati, ja vien tie nav nedalāmi saistīti ar persondatiem, un tāpēc uz tiem neattiecas piekļuves tiesības.
101. Pirms iedaļas noslēgšanas EDAK šajā kontekstā atgādina, ka fizisku personu aizsardzība attiecībā uz persondatu apstrādi ietver visu iepriekš uzskaitīto veidu persondatus un ka definīcijas šaura interpretācija ir pretrunā VDAR noteikumiem un galu galā pārkāpj Pamattiesību hartas 8. pantu. Atšķirīga režīma piemērošanu tiesību īstenošanai saistībā ar dažu veidu persondatiem, kas nav paredzēta VDAR, var ieviest tikai ar tiesību aktiem saskaņā ar VDAR 23. pantu (kā sīkāk paskaidrots 6.4. iedaļā). Tādējādi pārzini nevar ierobežot piekļuves tiesību īstenošanu, nepamatoti ierobežojot persondatu apjomu.

## 4.2 Persondati, uz kuriem attiecas piekļuves tiesības

102. Saskaņā ar VDAR 15. panta 1. punktu *“datu subjektam ir tiesības saņemt no pārzina apstiprinājumu par to, vai attiecībā uz datu subjektu tiek vai netiek apstrādāti personas dati, un, ja tiek, datu subjektam ir tiesības piekļūt attiecīgajiem datiem un saņemt šādu informāciju”* (izcēlums pievienots).

---

<sup>60</sup> Kā iepriekš norādīts 29. panta darba grupas Pamatnostādnēs par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 10. lpp., un atkārtoti norādīts 29. panta darba grupas Pamatnostādnēs par automatizētu individuālu lēmumu pieņemšanu un profilēšanu, ko apstiprinājusi EDAK, 17. lpp.

<sup>61</sup> Papildu skaidrojumi par anonimizācijas jēdzienu ir atrodami 29. panta darba grupas Atzinumā 05/2014 par anonimizācijas metodēm, WP216, 2014. gada 10. aprīlis, 5.–19. lpp.

<sup>62</sup> Komisijas paziņojums Eiropas Parlamentam un Padomei “Vadlīnijas par Regulu par satvaru nepersondatu brīvai plūsmai Eiropas Savienībā”, 29.05.2019., COM/2019/250 final.

103. No VDAR 15. panta 1. punkta izriet vairāki elementi. Punktā ir *expressis verbis* minēti datu subjekta persondati (4.2.1. iedaļa), ko pārzinis apstrādā (4.2.2. iedaļa).

#### 4.2.1 Datu subjekta persondati

104. Piekļuves tiesības var īstenot tikai attiecībā uz persondatiem, kas attiecas uz datu subjektu, kurš pieprasa piekļuvi, vai attiecīgā gadījumā tās var īstenot pilnvarota persona (sk. 3.4. iedaļu). Ir arī situācijas, kurās dati ir saistīti nevis ar personu, kas īsteno piekļuves tiesības, bet gan ar citu personu. Tomēr datu subjektam ir tiesības tikai uz saviem persondatiem, izņemot datus, kas attiecas tikai uz kādu citu personu<sup>63</sup>.
105. Tomēr datu klasificēšana par persondatiem, kas attiecas uz datu subjektu, nav atkarīga no tā, vai šie persondati attiecas arī uz kādu citu personu<sup>64</sup>. Tādējādi ir iespējams, ka persondati vienlaikus attiecas uz vairāk nekā vienu personu. Tas automātiski nenozīmē, ka būtu jāpiešķir piekļuve persondatiem, kas attiecas arī uz kādu citu personu, jo pārzinim ir jāievēro VDAR 15. panta 4. punkts.
106. Pārziņiem nevajadzētu "pārāk ierobežoti" interpretēt frāzi "datu subjekta persondati", kā 29. panta darba grupa jau ir norādījusi attiecībā uz tiesībām uz datu pārnesamību<sup>65</sup>. Attiecībā uz piekļuves tiesībām — EDAK uzskata, ka tās var attiekties, piemēram, uz tādu telefonsarunu ierakstiem (un to pierakstiem), kas notikušas starp datu subjektu, kurš pieprasa piekļuvi, un pārzini, ja tie ir persondati<sup>66</sup>. Ja tiek piemērota VDAR un uz apstrādi neattiecas mājsaimnieciska rakstura atbrīvojums saskaņā ar VDAR 2. panta 2. punkta c) apakšpunktu un ja datu subjekts iegūto ierakstu, kas satur sarunu partnera persondatus, izmanto citiem nolūkiem, piemēram, šo ierakstu publicē, datu subjekts kļūst par pārzini, kurš apstrādā šos persondatus, kas attiecas uz citu personu, kuras balss ir ierakstīta. Lai gan tas pārzini neatbrīvo no datu aizsardzības pienākumiem, kuri tam jāveic, pienācīgi analizējot, vai var tikt nodrošināta piekļuve pilnam ierakstam, pārzinis tiek mudināts informēt datu subjektu par to, ka šādā gadījumā viņš var kļūt par pārzini. Tas neskar turpmākus novērtējumus saskaņā ar VDAR 15. panta 4. punktu, kas sīkāk aprakstīti 6. iedaļā. Tāpat piekļuves tiesības var attiekties uz ziņojumiem, ko datu subjekti citiem nosūtījuši starppersonu ziņojumu veidā un no savas ierīces izdzēsuši, bet kas joprojām ir pieejami pakalpojumu sniedzējam.
107. Turklāt ir situācijas, kad saikne starp datiem un atsevišķām personām pārzinim var šķist neskaidra, piemēram, identitātes zādzības gadījumā. Identitātes zādzības gadījumā persona krāpnieciski rīkojas citas personas vārdā. Šajā kontekstā ir svarīgi atgādināt, ka cietušajam būtu jāsniedz informācija par visiem persondatiem, ko pārzinis glabā saistībā ar viņa identitāti, arī datiem, kas savākti, pamatojoties

---

<sup>63</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 9. lpp.: "Datu pārnesamības pieprasījuma darbības jomā ir vienīgi persondati. Tāpēc jebkuri dati, kas ir anonīmi vai neattiecas uz datu subjektu, nebūs tā darbības jomā. Tomēr pieprasījuma darbības jomā ir pseidoanonīmi dati, kas skaidri sasaistāmi ar datu subjektu (piemēram, ja viņš ir norādījis attiecīgo identifikatoru, sal. ar 11. panta 2. punktu)."

<sup>64</sup> EST spriedums lietā C-434/16 *Peter Nowak pret Data Protection Commissioner*, 2017, 44. punkts.

<sup>65</sup> 29. panta darba grupas Pamatnostādnes par tiesībām uz datu pārnesamību, ko apstiprinājusi EDAK, 9. lpp.: "Daudzās situācijās datu pārziņi apstrādās informāciju, kas satur vairāku datu subjektu persondatus. Šādā gadījumā datu pārziņiem nevajadzētu pārāk ierobežoti interpretēt frāzi "datu subjekta persondati". Piemēram, telefona sarunu, starppersonu ziņojumapmaiņas vai IP balss pārraides ieraksti var saturēt (abonenta konta vēsturē) informāciju par trešām personām, kas saistītas ar ienākošajiem vai izejošajiem zvaniem. Lai gan tādējādi ieraksti saturēs persondatus par daudziem cilvēkiem, būtu jānodrošina, ka, atbildot uz datu pārnesamības pieprasījumiem, abonenti var saņemt šos ierakstus, jo tie attiecas (arī) uz datu subjektu. Tomēr tad, ja šādus ierakstus pēc tam nosūta jaunam datu pārzinim, šim jaunajam datu pārzinim nevajadzētu tos apstrādāt tādiem mērķiem, kas nelabvēlīgi ietekmē trešo personu tiesības un brīvības (sk. trešo nosacījumu)."

<sup>66</sup> Sk. 34. piemēru 6.2. iedaļā.

uz krāpnieka darbībām. Citiem vārdiem sakot, pat pēc tam, kad pārzinis uzzinājis par identitātes zādzību, persondati, kas ir saistīti ar cietušā identitāti, ir datu subjekta persondati.

**17. piemērs.** Persona krāpnieciski izmanto citas personas identitāti, lai tiešsaistē spēlētu pokeru. Noziedzīgā nodarījuma izdarītājs apmaksā tiešsaistes kazino, izmantojot kredītkarti, ko viņš nozadzis cietušajam. Kad cietušais uzzina par identitātes zādzību, viņš tiešsaistes kazino pakalpojumu sniedzējam lūdz nodrošināt viņam piekļuvi viņa persondatiem un, konkrētāk, spēlētajām tiešsaistes spēlēm un informācijai par kredītkarti, ko izmantojis noziedzīgā nodarījuma izdarītājs.

Starp savāktajiem datiem un noziedzīgajā nodarījumā cietušo pastāv saikne, jo ir izmantota cietušā identitāte. Pēc krāpšanas atklāšanas joprojām pastāv saikne starp cietušo un iepriekš minētajiem persondatiem, ņemot vērā to saturu (cietušā kredītkarte nepārprotami attiecas uz cietušo), nolūku un sekas (piemēram, informāciju par noziedzīgā nodarījuma izdarītāja spēlētajām tiešsaistes spēlēm var izmantot, lai cietušajam izsniegtu rēķinus). Tāpēc tiešsaistes kazino piešķir cietušajam piekļuvi iepriekš minētajiem persondatiem.

108. Attiecīgā gadījumā var izmantot iekšējos savienojumu žurnālus, lai glabātu ierakstus par piekļuvi datnei un izsekotu, kādas darbības veiktas saistībā ar piekļuvi ierakstam, piemēram, drukāšana, kopēšana vai persondatu dzēšana. Šajos žurnālos var iekļaut pieteikšanās laiku, piekļuves datnei iemeslu, kā arī informāciju, kas identificē personu, kurai ir bijusi piekļuve. Ar šo tematu saistīti jautājumi ir ietverti pašlaik izskatāmā lietā EST (C-579/21). Savienojumu žurnālu ieviešana, uzraudzība un pārskatīšana ir pārziņa atbildībā, un tos var pārbaudīt uzraudzības iestādes. Tādējādi pārzinim būtu jāpārliciecinās, ka personas, kas darbojas viņa pakļautībā un kam ir piekļuve persondatiem, neapstrādā persondatus citādi, kā vien saskaņā ar pārziņa norādījumiem, kā noteikts VDAR 29. pantā. Ja persona tomēr apstrādā persondatus citiem nolūkiem, kas nav pārziņa norādījumu izpilde, viņa šādā apstrādē var kļūt par pārzini un pret viņu var ierosināt disciplinārlietu vai kriminālprocesu vai viņai var piemērot administratīvas sankcijas, ko nosaka uzraudzības iestādes. EDAK norāda, ka saskaņā ar VDAR 24. pantu darba devēja pienākums ir izmantot atbilstošus pasākumus, no izglītojošām līdz disciplinārām procedūrām, lai nodrošinātu, ka apstrāde atbilst VDAR un ka nenotiek pārkāpumi.

#### 4.2.2 persondati, kas tiek apstrādāti

109. VDAR 15. panta 1. punktā ir minēti arī persondati, kas tiek apstrādāti. Atsauces laiks to persondatu diapazona noteikšanai, uz kuriem attiecas piekļuves pieprasījums, jau ir izklāstīts 2.3.3. iedaļā. Tomēr formulējums arī liek domāt, ka piekļuves tiesībās nav nošķirti apstrādes darbību mērķi.

**18. piemērs.** Uzņēmums apstrādāja datu subjekta persondatus, lai sagatavotu viņa pirkuma pasūtījumu un organizētu tā nosūtīšanu uz datu subjekta dzīvesvietas adresi. Pēc tam, kad šie sākotnējie nolūki, kuriem persondati tika vākti, vairs nepastāv, pārzinis dažus persondatus glabā tikai tādēļ, lai izpildītu savus juridiskos pienākumus attiecībā uz ierakstu glabāšanu.

Datu subjekts pieprasa piekļuvi saviem persondatiem. Lai izpildītu savu pienākumu saskaņā ar VDAR 15. panta 1. punktu, pārzinim ir jāsniedz datu subjektam pieprasītie persondati, ko pārzinis glabā, lai izpildītu savus juridiskos pienākumus.

110. Jānošķir arhivēti persondati no dublējuma datiem, kas ir persondati, kurus glabā vienīgi, lai atjaunotu datus to zuduma gadījumā. Būtu jānorāda, ka integrētas datu aizsardzības un datu minimizēšanas principu ziņā dublējuma dati būtībā ir līdzīgi datiem reāllaika sistēmā. Ja pastāv nelielas atšķirības starp persondatiem dublējumkopijā un reāllaika sistēmā, tās parasti ir saistītas ar papildu datu vākšanu kopš pēdējās dublēšanas. Dažos gadījumos, samazinot datu apjomu reāllaika sistēmā (piemēram, dažus

datus dzēšot pēc glabāšanas perioda beigām vai pēc dzēšanas pieprasījuma), dublējumkopijā tie tiks pārrakstīti tikai turpmākās dublēšanas laikā. Ja piekļuves pieprasījums tiek iesniegts brīdī, kad dublējumkopijā ir vairāk persondatu, kas attiecas uz datu subjektu, nekā reāllaika sistēmā, vai persondati atšķiras (ko var redzēt, piemēram, reāllaika sistēmas dzēšanas žurnālā, kas ieviests, pilnā mērā ievērojot datu minimizēšanas principu), pārzinim jānodrošina šīs situācijas pārredzamība un, ja tas ir tehniski iespējams, pēc datu subjekta pieprasījuma jānodrošina piekļuve, tai skaitā piekļuve persondatiem, kas tiek glabāti dublējumkopijā. Piemēram, lai datu subjektiem, kuri īsteno savas tiesības, nodrošinātu pārredzamību, dzēšanas žurnāls reāllaika sistēmā var ļaut pārzinim apskatīt, vai dublējumkopijā ir dati, kuru reāllaika sistēmā vairs nav, jo tie nesen ir dzēsti un dublējumkopijā vēl nav pārrakstīti.

#### 4.2.3 Jauna piekļuves pieprasījuma tvērums

111. Jāpiebilst arī tas, ka datu subjektiem ir tiesības piekļūt visiem apstrādātajiem datiem, kas uz viņiem attiecas, vai šādu datu daļām atkarībā no pieprasījuma tvēruma (sk. arī 2.3.1. iedaļu par informācijas pilnīgumu un 3.1.1. iedaļu par pieprasījuma satura analīzi). Līdz ar to, ja pārzinis jau iepriekš ir izpildījis piekļuves pieprasījumu un ja vien pieprasījums nav pārmērīgs, pārzinis nevar samazināt šā jaunā pieprasījuma tvērumu. Tas nozīmē, ka saistībā ar jebkādiem turpmākiem tā paša datu subjekta piekļuves pieprasījumiem pārzinim datu subjekts nebūtu jāinformē tikai par izmaiņām apstrādātajos persondatos vai pašā apstrādē kopš pēdējā pieprasījuma, ja vien datu subjekts tam nav skaidri piekritis. Pretējā gadījumā datu subjektiem būtu pienākums apkopot sniegtos persondatus, lai iegūtu pilnīgu persondatu kopu attiecībā uz viņu informāciju par apstrādi un datu subjektu tiesībām.

#### 4.3 Informācija par apstrādi un datu subjekta tiesībām

112. Papildus piekļuvei pašiem persondatiem pārzinim ir jāsniedz informācija par apstrādi un datu subjekta tiesībām saskaņā ar VDAR 15. panta 1. punkta a) līdz h) apakšpunktu un 15. panta 2. punktu. Lielākā daļa informācijas par šiem konkrētajiem punktiem jau ir apkopota — vismaz vispārīgi — pārziņa apstrādes darbību reģistrā, kas minēts VDAR 30. pantā, un/vai paziņojumā par privātumu, kas izstrādāts saskaņā ar VDAR 12.–14. pantu. Tāpēc vispirms varētu būt lietderīgi 29. panta darba grupas Pārredzamības pamatnostādņēs saskaņā ar Regulu 2016/679<sup>67</sup> iepazīties ar tās informācijas saturu, kas jāsniedz saskaņā ar VDAR 13. un 14. pantu.
113. Lai nodrošinātu atbilstību 15. panta 1. punkta a) līdz h) apakšpunktam un 15. panta 2. punktam, pārziņi var uzmanīgi izmantot sava paziņojuma par privātumu teksta moduļus, ja vien pārziņi pārliecinās, ka tie ir atjaunināti un precīzi attiecībā uz datu subjekta pieprasījumu. Pirms datu apstrādes vai tās sākumā bieži vien vēl nevar nodrošināt noteiktu informāciju, piemēram, konkrētu saņēmēju identifikāciju vai konkrētu datu apstrādes ilgumu. Daļa informācijas, piemēram, tiesības iesniegt sūdzību uzraudzības iestādei (sk. 15. panta 1. punkta f) apakšpunktu), nemainās atkarībā no personas, kas iesniegusi piekļuves pieprasījumu. Tāpēc to var paziņot vispārīgi, kā tas tiek darīts arī paziņojumā par privātumu. Citu veidu informācija, piemēram, informācija par saņēmējiem, datu kategorijām un avotu, var atšķirties atkarībā no tā, kas iesniedz pieprasījumu un kāds ir pieprasījuma tvērums. Tāpēc saistībā ar piekļuves pieprasījumu saskaņā ar 15. pantu jebkura informācija par apstrādi, kas pieejama pārzinim, var būt jāatjaunina un jāpielāgo apstrādes darbībām, ko faktiski veic attiecībā uz datu subjektu, kurš iesniedzis pieprasījumu. Tādējādi atsaukšanās uz privātuma politikas tekstu nebūtu pietiekams veids,

---

<sup>67</sup> 29. panta darba grupas Pārredzamības pamatnostādnes saskaņā ar Regulu 2016/679, WP260 rev.01, 2018. gada 11. aprīlis, kuras apstiprinājusi EDAK (tālāk "29. panta darba grupas Pārredzamības pamatnostādnes, kuras apstiprinājusi EDAK").

kā pārzinis varētu sniegt 15. panta 1. punkta a) līdz h) apakšpunktā un 2. punktā prasīto informāciju, ja vien “pielāgotā un atjauninātā” informācija nav tāda pati kā informācija, kas sniegta apstrādes sākumā. Paskaidrojot, kāda informācija attiecas uz pieprasījuma iesniedzēju personu, pārzinis attiecīgā gadījumā varētu minēt konkrētas darbības (piemēram, “ja esat izmantojis šo pakalpojumu...”, “ja esat apmaksājis rēķinu”), ja vien datu subjektiem ir skaidrs, ka tās uz viņiem attiecas. Tālāk ir izskaidrota vajadzīgā precizējuma pakāpe saistībā ar atsevišķiem informācijas veidiem.

114. Attiecībā uz informāciju par nolūkiem saskaņā ar 15. panta 1. punkta a) apakšpunktu jābūt konkrēti norādītam(-iem) precīzam(-iem) ar pieprasījuma iesniedzēja datu subjekta konkrēto gadījumu saistītajam(-iem) nolūkam(-iem). Nebūtu pietiekami uzskaitīt pārziņa vispārējos nolūkus, neprecizējot pārziņa nolūku(-us) attiecīgajā pieprasījuma iesniedzēja datu subjekta gadījumā. Ja apstrādi veic vairākos nolūkos, pārzinim ir jāprecizē, kuri dati vai kuras datu kategorijas kādā(-os) nolūkā(-os) tiek apstrādāti. Atšķirībā no VDAR 13. panta 1. punkta c) apakšpunkta un 14. panta 1. punkta c) apakšpunkta informācija par apstrādi, kas minēta 15. panta 1. punkta a) apakšpunktā, neietver informāciju par apstrādes juridisko pamatu. Tomēr, tā kā dažu datu subjektu tiesības ir atkarīgas no piemērojamā juridiskā pamata, šī informācija ir svarīga, lai datu subjekti varētu pārliecināties par datu apstrādes likumīgumu un noteikt, kuras datu subjekta tiesības ir piemērojamas konkrētajā situācijā. Tāpēc, lai veicinātu datu subjektu tiesību īstenošanu saskaņā ar VDAR 12. panta 2. punktu, pārzinim ieteicams arī informēt datu subjektu par katrai apstrādes darbībai piemērojamo juridisko pamatu vai norādīt, kur viņš šo informāciju var atrast. Jebkurā gadījumā pārredzamas apstrādes princips paredz, ka informācijai par apstrādes juridisko pamatu datu subjektam jābūt viegli pieejamai (piemēram, paziņojumā par privātumu).
115. Datu subjekta situācijai var būt jāpielāgo arī informācija par datu kategorijām (15. panta 1. punkta b) apakšpunkts), lai kategorijas, kas uz pieprasījuma iesniedzēju neattiecas, tiktu izslēgtas.

**19. piemērs.** Saistībā ar VDAR 13./14. pantā minēto informāciju viesnīca paziņo, ka apstrādā vairākas klientu datu kategorijas (identifikācijas datus, kontaktinformāciju, bankas datus, kredītkartes numuru utt.). Ja piekļuves pieprasījums ir iesniegts, pamatojoties uz 15. pantu, tad papildus tam, ka pieprasījuma iesniedzējam datu subjektam tiek nodrošināta piekļuve faktiskajiem apstrādātajiem datiem (2. komponents), viņš saskaņā ar 15. panta 1. punkta b) apakšpunktu ir jāinformē arī par konkrētajām datu kategorijām, kas tiek apstrādātas konkrētajā gadījumā (piem., neiekļaujot bankas datus vai kredītkartes datus, ja maksājums veikts skaidrā naudā).

116. Informācijā par “saņēmējiem vai saņēmēju kategorijām” (15. panta 1. punkta c) apakšpunkts) vispirms ir jāņem vērā VDAR 4. panta 9. punktā sniegtā saņēmēja definīcija. Saņēmēja definīcijas pamatā ir persondatu izpaušana fiziskai vai juridiskai personai, publiskai iestādei, aģentūrai vai citai struktūrai<sup>68</sup>. No VDAR 4. panta 9. punkta izriet, ka publiskās iestādes, kas rīkojas saistībā ar konkrētu izmeklēšanu, uz kuru attiecas īpaši valsts noteikumi, nav uzskatāmas par saņēmējiem.
117. Attiecībā uz jautājumu, vai pārzinis var brīvi izvēlēties starp informāciju par saņēmējiem vai par saņēmēju kategorijām, jānorāda, ka “atšķirībā no VDAR 13. un 14. panta, kuros ir noteikts pārziņa pienākums (..), VDAR 15. pantā ir paredzētas īstenas datu subjekta piekļuves tiesības, tāpēc šim subjektam ir jābūt iespējai izvēlēties saņemt informāciju vai nu — ja tas ir iespējams — par

---

<sup>68</sup> Būtu jānorāda arī tas, ka vienā un tajā pašā uzņēmumā var būt dažādi pārziņi, kā definēts VDAR 4. panta 7. punktā. Šajā kontekstā ir iespējams, ka viens saņēmējs izpauž datus otram saņēmējam tajā pašā uzņēmumā.

konkrētajiem saņēmējiem, kuriem minētie dati ir vai tiks izpausti, vai arī par saņēmēju kategorijām.”<sup>69</sup> Jāatgādina arī, ka atbilstīgi norādītajam iepriekš minētajās Pārredzamības pamatnostādnes<sup>70</sup> jau saskaņā ar VDAR 13. un 14. pantu informācijai par saņēmējiem vai saņēmēju kategorijām, ievērojot pārredzamības un godprātības principus, vajadzētu būt pēc iespējas konkrētākai. Saskaņā ar 15. pantu, ja datu subjekts nav izvēlējis citādi, pārzinim ir pienākums nosaukt faktiskos saņēmējus, izņemot gadījumus, kad minētos saņēmējus nav iespējams identificēt vai pārzinis uzskatāmi parāda, ka datu subjekta piekļuves pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi VDAR 12. panta 5. punkta nozīmē<sup>71</sup>, <sup>72</sup>. Šajā saistībā EDAK atgādina, ka informācijas par faktiskajiem saņēmējiem glabāšana ir nepieciešama, lai cita starpā varētu izpildīt pārziņa pienākumus saskaņā ar VDAR 5. panta 2. punktu un 19. pantu.

**20. piemērs.** Paziņojumā par privātumu darba devējs saskaņā ar VDAR 13. panta 1. punkta e) apakšpunktu un 14. panta 1. punkta e) apakšpunktu sniedz informāciju par to, kuras datu kategorijas komandējumu gadījumā tiek nodotas “ceļojumu aģentūrām” vai “viesnīcām”. Ja darbinieks pēc komandējuma iesniedz pieprasījumu par piekļuvi persondatiem, darba devējam attiecībā uz persondatu saņēmējiem saskaņā ar 15. panta 1. punkta c) apakšpunktu savā atbildē būtu jānorāda ceļojumu aģentūra(-as) un viesnīca(-as), kas saņēmušas datus. Lai gan darba devējs savā paziņojumā par privātumu likumīgi minēja saņēmēju kategorijas saskaņā ar 13. un 14. pantu, jo šajā posmā saņēmējus vēl nebija iespējams nosaukt, viņam, ja vien darbinieks nav izvēlējis citādi, būtu jāsniedz informācija par konkrētiem saņēmējiem (ceļojumu aģentūru, viesnīcu u. c. nosaukumi), kad darbinieks iesniedz piekļuves pieprasījumu.

Ja pārzinis, ievērojot iepriekš minētos nosacījumus, var norādīt saņēmēju kategorijas, informācijai vajadzētu būt pēc iespējas precīzākai, norādot saņēmēja veidu (t. i., atsaucoties uz tā veiktajām darbībām), nozari, sektoru un apakšsektoru, kā arī saņēmēju atrašanās vietu<sup>73</sup>.

118. Saskaņā ar 15. panta 1. punkta d) apakšpunktu, ja iespējams, ir jāsniedz informācija par paredzēto laikposmu, cik ilgi persondati tiks glabāti. Pretējā gadījumā jānorāda kritēriji, ko izmanto minētā laikposma noteikšanai. Pārziņa sniegtajai informācijai jābūt pietiekami precīzai, lai datu subjekts varētu zināt, cik ilgi viņa dati tiks glabāti. Ja nav iespējams norādīt dzēšanas laiku, norāda glabāšanas periodu ilgumu un šā perioda sākumu vai izraisītājnotikumu (piemēram, līguma izbeigšana, garantijas perioda beigas u. c.). Vienīgi ar tādu norādi kā “dzēšana pēc tiesību aktos noteiktā glabāšanas laika beigām”, ir nepietiekami. Norādēs par datu glabāšanas termiņiem galvenā uzmanība būs jāpievērš konkrētajiem datiem, kas attiecas uz datu subjektu. Ja uz datu subjekta persondatiem attiecas dažādi dzēšanas periodi (piemēram, tāpēc, ka ne uz visiem datiem attiecas juridiski glabāšanas pienākumi), dzēšanas termiņus norāda saistībā ar attiecīgajām apstrādes darbībām un datu kategorijām.
119. Lai gan informācija par tiesībām iesniegt sūdzību uzraudzības iestādei (15. panta 1. punkta f) apakšpunkts) nav atkarīga no konkrētajiem apstākļiem, 15. panta 1. punkta e) apakšpunktā minētās datu subjekta tiesības atšķiras atkarībā no apstrādes juridiskā pamata. Attiecībā uz pārziņa pienākumu veicināt datu subjekta tiesību īstenošanu saskaņā ar VDAR 12. panta 2. punktu — pārziņa atbilde par

<sup>69</sup> EST, C-154/21(*Österreichische Post AG*), 36. punkts.

<sup>70</sup> 29. panta darba grupas Pārredzamības pamatnostādnes saskaņā ar Regulu 2016/679, WP260 rev.01, 2018. gada 11. aprīlis, kuras apstiprinājusi EDAK (tālāk “29. panta darba grupas Pārredzamības pamatnostādnes, kuras apstiprinājusi EDAK”), 37. lpp. (pielikums).

<sup>71</sup> EST, C-154/21 (*Österreichische Post AG*).

<sup>72</sup> Tas vien, ka dati ir izpausti lielam skaitam saņēmēju, pats par sevi nepadara pieprasījumu par pārmērīgu, sk. 6. iedaļas 188. punktu.

<sup>73</sup> 29. panta darba grupas Pārredzamības pamatnostādnes, kuras apstiprinājusi EDAK, 37. lpp. (pielikums).

minētajām tiesībām ir individuāli jāpielāgo datu subjekta gadījumam, un tai jābūt saistītai ar attiecīgajām apstrādes darbībām. Būtu jāizvairās sniegt informāciju par tiesībām, kas datu subjektam konkrētajā situācijā nav piemērojamas.

120. Saskaņā ar 15. panta 1. punkta g) apakšpunktu ir jāsniedz “visa pieejamā informācija” par datu avotu, ja persondati netiek vākti no datu subjekta. Pieejamās informācijas apjoms laika gaitā var mainīties.

**21. piemērs.** Liela uzņēmuma privātuma politikā ir noteikts:

“Kredībspējas pārbaudes mums palīdz novērst problēmas maksājumu darījumos. Tās garantē mūsu uzņēmuma aizsardzību pret finanšu riskiem, kas var ietekmēt arī pārdošanas cenas vidējā termiņā un ilgtermiņā. Kredībspējas pārbaude noteikti tiek veikta, kad gatavojamies sūtīt preces, vienlaikus nesaņemot attiecīgo pirkuma summu, piemēram, ja pirkums veikts uz kredīta. Neveicot kredībspējas pārbaudi, ir iespējama tikai priekšapmaksā (tūlītējs bankas pārskaitījums, tiešsaistes maksājumu pakalpojumu sniedzējs, kredītkarte).

Lai pārbaudītu kredībspēju, mēs nosūtīsim jūsu vārdu, uzvārdu, adresi un dzimšanas datumu šādiem pakalpojumu sniedzējiem, piemēram: 1) finanšu informācijas aģentūra X, 2) darījumdarbības informācijas sniedzējs Y, 3) komercakredītu atsauces aģentūra Z.

Dati iepriekš minētajām kredītiestādēm tiek nodoti tikai juridiski pieļaujamajās robežās un tikai, lai analizētu jūsu līdzšinējo maksāšanas praksi, kā arī lai novērtētu saistību neizpildes risku, pamatojoties uz matemātiskām un statistiskām procedūrām, kurās izmanto adreses datus, kā arī lai pārbaudītu jūsu adresi (pārbaude piegādes nolūkā). Atkarībā no kredībspējas pārbaudes rezultātiem mēs, iespējams, vairs nevarēsim jums piedāvāt atsevišķas maksāšanas metodes, piemēram, rēķina apmaksu pēc iegādes.”

Tādējādi paziņojumā par privātumu ir vispārīgi minēta iespēja saņemt informāciju no uzskaitītajām ekonomiskās informācijas iestādēm saskaņā ar VDAR 13. un 14. pantu. Ja *ex ante* nav skaidrs, kurš no uzņēmumiem iesaistīsies apstrādē, privātuma politikā ir pietiekami norādīt atbilstīgo uzņēmumu nosaukumus. Saistībā ar pieprasījumu, kura pamatā ir 15. pants, papildus informācijai par to, ka ir iegūti kredībspējas dati, vēl (*ex post*) būtu jāatklāj arī, kurš no minētajiem uzņēmumiem ir bijis tieši iesaistīts. VDAR 15. panta 1. punkta g) apakšpunktā ir skaidri noteikts, ka informācija par datu apstrādi ietver “visu pieejamo informāciju par datu avotu”, ja persondati netiek vākti no datu subjekta.

121. VDAR 15. panta 1. punkta h) apakšpunktā ir noteikts, ka katram datu subjektam vajadzētu būt tiesībām saņemt jēgpilnu informāciju, *inter alia*, par to, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, un par tajā ietverto loģiku, kā arī šādas apstrādes iespējamo nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu<sup>74</sup>. Ja iespējams, informācijai saskaņā ar 15. panta 1. punkta h) apakšpunktu jābūt konkrētākai attiecībā uz pamatojumu, kura rezultātā tiek pieņemti konkrēti lēmumi par datu subjektu, kas lūdzis piekļuvi.
122. Saskaņā ar VDAR 13. panta 1. punkta f) apakšpunktu un 14. panta 1. punkta f) apakšpunktu ir jāsniedz informācija par paredzētu datu nosūtīšanu uz trešo valsti vai starptautisku organizāciju, tai skaitā par to, ka pastāv Komisijas lēmums par aizsardzības līmeņa pietiekamību vai piemērotas garantijas. Saistībā ar piekļuves pieprasījumu saskaņā ar 15. pantu — 15. panta 2. punktā ir paredzēts sniegt

<sup>74</sup> Šajā saistībā sk. Pārredzamības pamatnostādņu saskaņā ar Regulu 2016/679 (WP 260) 41. punktu, kurā iekļauta atsauce uz Pamatnostādņiem par automatizētu individuālu lēmumu pieņemšanu un profilēšanu Regulas 2016/679 nolūkiem (WP 251).

informāciju par atbilstošām garantijām saskaņā ar VDAR 46. pantu tikai gadījumos, kad faktiski notiek nosūtīšana uz trešo valsti vai starptautisku organizāciju.

## 5 KĀ PĀRZINIS VAR NODROŠINĀT PIEKĻUVI?

123. VDAR nav ļoti preskriptīva attiecībā uz to, kā pārzinim ir jānodrošina piekļuve. Dažās situācijās, piemēram, ja nelielai organizācijai ir ierobežota informācija par datu subjektu, piekļuves tiesības var būt piemērojamas viegli un vienkārši. Citās situācijās piekļuves tiesību īstenošana ir sarežģītāka, jo sarežģītāka ir datu apstrāde saistībā ar datu subjektu skaitu, apstrādāto datu kategorijām, kā arī datu plūsmu dažādās organizācijās un starp tām. Ņemot vērā atšķirības persondatu apstrādē, var attiecīgi atšķirties atbilstošais piekļuves nodrošināšanas veids.
124. Šis iedaļas mērķis ir sniegt dažus norādījumus un praktiskus piemērus par dažādiem veidiem, kā pārziņi var izpildīt piekļuves pieprasījumu, kā arī par VDAR 12. panta 1. punkta nozīmi saistībā ar piekļuves tiesībām. Šajā iedaļā tiks sniegti arī daži norādījumi par to, kas tiek uzskatīts par plaši izmantotu elektronisko formātu, kā arī par piekļuves nodrošināšanas termiņiem saskaņā ar VDAR 12. panta 3. punktu.

### 5.1 Kā pārzinis var izgūt pieprasītos datus?

125. Datu subjektiem vajadzētu būt piekļuvei visai informācijai, ko pārzinis attiecībā uz viņiem apstrādā. Tas nozīmē, piemēram, ka pārzinim ir pienākums meklēt persondatus savās IT sistēmās un ar IT nesaistītās kartotēkās. Veicot šādu meklēšanu, pārzinim būtu jāizmanto organizācijā pieejamā informācija par datu subjektu, un rezultātā viņš, visticamāk, atradīs atbilstības sistēmās atkarībā no tā, kā informācija tiek strukturēta<sup>75</sup>. Piemēram, ja informācija tiek šķirota datnēs pēc nosaukuma vai atsauces numura, meklēšanu var ierobežot līdz šiem faktoriem. Tomēr, ja datu struktūra ir atkarīga no citiem faktoriem, piemēram, ģimenes attiecībām vai profesionālajiem nosaukumiem, vai jebkāda veida tiešiem vai netiešiem identifikatoriem (piemēram, klienta numura, lietotājvārda vai IP adreses), meklēšana ir jāpaplašina, lai tos iekļautu, ja vien pārzinim ir arī šī ar datu subjektu saistītā informācija vai arī šo informāciju viņam sniedz datu subjekts. Tas pats attiecas uz gadījumiem, kad datu subjekta persondatus var saturēt ieraksti par trešām personām. Tomēr pārzinis nevar pieprasīt datu subjektam sniegt vairāk informācijas, nekā vajadzīgs, lai datu subjektu identificētu. Ja pārzinis datu apstrādes darbībām izmanto apstrādātāju, meklēšana, protams, ir jāpaplašina, lai iekļautu arī persondatus, ko apstrādā apstrādātājs.
126. Saskaņā ar VDAR 25. pantu par integrētu datu aizsardzību un datu aizsardzību pēc noklusējuma pārzinim (un visiem apstrādātājiem, ko tas izmanto) jau vajadzētu būt ieviesušam funkcijas, kas nodrošina datu subjekta tiesību ievērošanu. Šajā kontekstā tas nozīmē, ka vajadzētu būt atbilstošiem veidiem, kādos, apstrādājot pieprasījumu, atrast un izgūt informāciju par datu subjektu. Tomēr būtu jānorāda, ka pārmērīga interpretācija šajā saistībā varētu radīt informācijas atrašanas un izgūšanas funkcijas, kas pašas par sevi rada risku datu subjektu privātumam. Tāpēc ir svarīgi paturēt prātā, ka arī datu izguves process būtu jāizstrādā datu aizsardzībai nekaitīgā veidā, lai tas neapdraudētu citu personu, piemēram, pārziņa darbinieku, privātumu.

### 5.2 Atbilstoši pasākumi piekļuves nodrošināšanai

---

<sup>75</sup> Šādā meklēšanā, protams, būtu jāiekļauj arī apstrādātāja rīcībā esošā informācija, sk. VDAR 28. panta 3. punkta e) apakšpunkts.



### 5.2.1 "Atbilstošu pasākumu" veikšana

127. VDAR 12. pantā ir noteiktas prasības attiecībā uz piekļuves nodrošināšanu, t. i., apstiprinājuma, persondatu un papildu informācijas sniegšanu saskaņā ar 15. pantu, kā arī precizēts piekļuves tiesību nodrošināšanas formāts, veids un termiņš. 29. panta darba grupas Pārredzamības pamatnostādnes saskaņā ar Regulu 2016/679<sup>76</sup> ir sniegti papildu norādījumi attiecībā uz 12. pantu, galvenokārt saistībā ar VDAR 13. un 14. pantu, bet arī saistībā ar 15. pantu un pārredzamību kopumā. Tādējādi minētajās pamatnostādnes definēto bieži var vienādi piemērot arī attiecībā uz piekļuves nodrošināšanu saskaņā ar 15. pantu.
128. VDAR 12. panta 1. punktā ir noteikts, ka pārzinis veic atbilstošus pasākumus, lai kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu, nodrošinātu 15. pantā minēto saziņu ar datu subjektu attiecībā uz apstrādi. VDAR 12. panta 2. punktā ir noteikts, ka pārzinis veicina datu subjekta piekļuves tiesību izmantošanu. Precīzākas prasības šajā saistībā būs jāizvērtē katrā gadījumā atsevišķi. Pieņemot lēmumu par to, kādi pasākumi ir atbilstoši, pārziņiem ir jāņem vērā visi attiecīgie apstākļi, tai skaitā, bet ne tikai, apstrādāto datu apjoms, datu apstrādes sarežģītība un pārziņiem zināmā informācija par datu subjektiem, piemēram, vai lielākā daļa datu subjektu ir bērni, vecāka gadagājuma cilvēki vai personas ar invaliditāti. Turklāt gadījumos, kad pārzinis tiek informēts par pieprasījuma iesniedzēja datu subjekta konkrētajām vajadzībām, par kurām, piemēram, iekļauta papildu informācija iesniegtajā pieprasījumā, pārzinim šie apstākļi ir jāņem vērā. Līdz ar to atbilstošie pasākumi atšķirsies.
129. Veicot novērtējumu, ir svarīgi paturēt prātā to, ka termins "atbilstošs" nekad nebūtu jāsaprot kā veids, kādā ierobežot to datu apjomu, uz kuriem attiecas piekļuves tiesības. Termins "atbilstošs" nenozīmē, ka centienus sniegt informāciju var līdzsvarot, piemēram, ar jebkādam interesēm, kas datu subjektam varētu būt persondatu iegūšanā. Tā vietā novērtējuma mērķim vajadzētu būt vispiemērotākās metodes izvēlei, lai sniegtu visu informāciju, uz kuru attiecas šīs tiesības, atkarībā no katra gadījuma konkrētajiem apstākļiem. Tādējādi pārzinim, kurš apstrādā lielu datu apjomu lielā mērogā, ir jāpiekrīt pielikt lielas pūles, lai datu subjektiem nodrošinātu piekļuves tiesības kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot vienkāršu un skaidru valodu.
130. Atbildot uz pieprasījumu par piekļuvi datiem, jāizvairās no datu subjekta novirzīšanas uz dažādiem avotiem. Kā iepriekš norādīts 29. panta darba grupas Pārredzamības pamatnostādnes (attiecībā uz jēdzienu "sniedz", kas minēts VDAR 13. un 14. pantā), jēdziens "sniedz" nozīmē, ka "*datu subjektam nevajadzētu būt spiestam aktīvi meklēt citā informācijā to informāciju, uz kuru attiecas šie panti, piemēram, tīmekļa vietnes vai lietotnes lietošanas nosacījumos*"<sup>77</sup>. Tāpēc un ievērojot pārredzamības principu, datu subjektiem no pārziņa ir jāiegūst 15. panta 1. punktā, 15. panta 2. punktā un 15. panta 3. punktā noteiktā informācija un persondati tādā veidā, kas nodrošina pilnīgu piekļuvi pieprasītajai informācijai. Īpašos apstākļos informācijas apmaiņa ar pārzini būtu neatbilstoša vai pat nelikumīga, piemēram, ja informācija ir sensitīva (ja tā attiecas, piem., uz trauksmes celšanu). Šādos gadījumos, atbildot uz datu subjektu piekļuves pieprasījumu, informāciju būtu lietderīgi sadalīt vairākās atbildēs. Pārziņa izvēlētajai metodei ir faktiski jānodrošina datu subjektam pieprasītie dati un informācija, tāpēc atbilstoša rīcība nebūtu tikai likt datu subjektam pārbaudīt pieprasītos datus, kas saglabāti viņa paša ierīcē, arī, piemēram, pārbaudīt klikšķināšanas plūsmas vēsturi un IP adreses viņa mobilajā tālrunī.

---

<sup>76</sup> 29. panta darba grupas Pārredzamības pamatnostādnes saskaņā ar Regulu 2016/679, WP260 rev.01, 2018. gada 11. aprīlis, kuras apstiprinājusi EDAK (tālāk "29. panta darba grupas Pārredzamības pamatnostādnes, kuras apstiprinājusi EDAK").

<sup>77</sup> 29. panta darba grupas Pārredzamības pamatnostādnes, kuras apstiprinājusi EDAK, 33. punkts.

131. Saskaņā ar pārskatatbildības principu pārzinim ir jādokumentē sava pieeja, lai varētu uzskatāmi parādīt saskaņā ar 15. pantu vajadzīgās informācijas sniegšanai izvēlēto līdzekļu atbilstību attiecīgajiem apstākļiem.

#### 5.2.2 Dažādi piekļuves nodrošināšanas līdzekļi

132. Kā jau skaidrots iepriekš 2.2.2. iedaļā, datu subjektiem, iesniedzot piekļuves pieprasījumu, ir tiesības saņemt apstrādē esošo viņu persondatu kopiju saskaņā ar 15. panta 3. punktu kopā ar papildu informāciju, un to uzskata par galveno veidu, kā nodrošināt piekļuvi persondatiem.
133. Tomēr dažos gadījumos pārzinim varētu būt lietderīgi nodrošināt piekļuvi citos veidos, nevis sniedzot kopiju. Šāda nepastāvīga kārtība attiecībā uz piekļuvi datiem varētu būt, piemēram, mutiska informācija, datņu pārbaude, piekļuve uz vietas vai attālināti bez iespējas datus lejuplādēt. Šī kārtība var būt piemērots piekļuves piešķiršanas veids, piemēram, gadījumos, kad tas ir datu subjekta interesēs vai kad datu subjekts to lūdz. Piekļuve uz vietas kā sākotnējs pasākums varētu būt atbilstoša arī tad, ja pārzinis apstrādā lielu daudzumu nedigitalizētu datu, lai datu subjekts iegūtu informāciju par to, kādi persondati tiek apstrādāti, un varētu pieņemt šajā informācijā balstītu lēmumu par to, kādus persondatus viņš vēlas saņemt kopijā. Nepastāvīgi piekļuves veidi konkrētās situācijās var būt pietiekami un piemēroti; piemēram, tā var apmierināt datu subjektu vajadzību pārbaudīt, vai pārziņa apstrādātie dati ir pareizi, dodot datu subjektiem iespēju aplūkot sākotnējos datus. Pārzinim nav pienākuma sniegt informāciju citos veidos, kā vien nodrošinot kopiju, bet, izskatot šādu pieprasījumu, tam būtu jāizmanto saprātīga pieeja. Piekļuves nodrošināšana citos veidos, kas nav kopijas nodrošināšana, neizslēdz datu subjektu tiesības saņemt arī kopiju, ja vien viņi izvēlas to nedarīt.
134. Pārzinis atkarībā no konkrētās situācijas var izvēlēties no dažādajiem veidiem, kādos sniegt apstrādē esošo datu kopiju un papildu informāciju, piemēram, pa e-pastu, pa pastu vai pašapkalpošanās rīkā. Ja datu subjekts pieprasījumu iesniedz elektroniskā formā un ja vien datu subjekts nepieprasa citādi, informāciju sniedz plaši izmantotā elektroniskā formātā, kā noteikts 15. panta 3. punktā. Jebkurā gadījumā pārzinim, sniedzot informāciju e-pastā vai tiešsaistes pašapkalpošanās rīkos, ir jāparedz piemēroti tehniskie un organizatoriskie pasākumi, tai skaitā pienācīga šifrēšana.
135. Situācijā, kad pārzinis pieprasījuma iesniedzējas persondatus apstrādā tikai nelielā apjomā, persondatu kopiju un papildu informāciju var un vajadzētu sniegt, izmantojot vienkāršu procedūru.

**22. piemērs.** Vietējā grāmatnīcā tiek reģistrēti to klientu vārdi, uzvārdi un adreses, kuri ir pasūtījuši piegādi mājās. Klients apmeklē grāmatnīcu un iesniedz piekļuves pieprasījumu. Šādā situācijā pietiktu ar klienta persondatu izdrukāšanu tieši no uzņēmuma sistēmas, vienlaikus sniedzot arī 15. panta 1. un 2. punktā minēto papildu informāciju.

**23. piemērs.** Ziedotājs, kas ik mēnesi veic ziedojumus labdarības organizācijai, iesniedz piekļuves pieprasījumu pa e-pastu. Labdarības organizācijas rīcībā ir informācija par pēdējo divpadsmit mēnešu laikā veiktajiem ziedojumiem, kā arī ziedotāju vārdi un uzvārdi un e-pasta adreses. Pārzinis varētu sniegt persondatu kopiju un papildu informāciju, atbildot uz e-pasta vēstuli, ja vien tas piemēro visus vajadzīgos aizsardzības pasākumus, ņemot vērā, piemēram, datu raksturu.

136. Izmantot piekļuves pieprasījumu manuālu apstrādi var pat pārziņi, kas apstrādā lielu datu apjomu. Ja pārzinis apstrādā datus vairākos dažādos departamentos, tad, lai varētu atbildēt uz datu subjekta pieprasījumu, tam ir jāsavāc persondati no katra departamenta.

**24. piemērs.** Pārzinis ir iecēlis administratoru, kas risina praktiskos jautājumus saistībā ar piekļuves pieprasījumiem. Pēc pieprasījuma saņemšanas administrators pa e-pastu nosūta pieprasījumu dažādajiem organizācijas departamentiem, lūdzot tos apkopot persondatus par datu subjektu. Katra departamenta pārstāvji sniedz administratoram tos persondatus, kurus apstrādā viņu departaments. Pēc tam administrators visus savāktos persondatus kopā ar vajadzīgo papildu informāciju nosūta datu subjektam, piemēram, attiecīgā gadījumā pa e-pastu.

137. Lai gan manuālus piekļuves pieprasījumu apstrādes procesus varētu uzskatīt par atbilstošiem, daži pārzini, apstrādājot datu subjektu pieprasījumus, var gūt labumu no automatizētu procesu izmantošanas. Tas varētu attiekties, piemēram, uz pārziniem, kuri saņem lielu skaitu pieprasījumu. Viens no veidiem, kā sniegt informāciju saskaņā ar 15. pantu, ir nodrošināt datu subjektam pašapkalpošanās rīkus. Tas varētu veicināt datu subjektu piekļuves pieprasījumu efektīvu un savlaicīgu izskatīšanu, kā arī ļaut pārzinim pašapkalpošanās rīkā iekļaut pārbaudes mehānismu.

**25. piemērs.** Sociālo mediju pakalpojumā ir ieviests automatizēts piekļuves pieprasījumu apstrādes process, kas datu subjektam ļauj piekļūt saviem persondatiem no sava lietotāja konta. Lai izgūtu persondatus, sociālo mediju pakalpojuma lietotāji pēc pieteikšanās savā lietotāja kontā var izvēlēties iespēju "Iejupielādēt savus persondatus". Šī pašapkalpošanās iespēja ļauj lietotājiem lejupielādēt datni ar viņu persondatiem tieši no lietotāja konta savā datorā.

138. Pašapkalpošanās rīku izmantošanai nekad nevajadzētu ierobežot saņemto persondatu apjomu. Ja pašapkalpošanās rīkā nevar nodrošināt visu 15. pantā minēto informāciju, pārējā informācija ir jānodrošina citā veidā. Pārzinis var mudināt datu subjektu izmantot pašapkalpošanās rīku, ko tas ieviesis piekļuves pieprasījumu apstrādei. Tomēr būtu jānorāda, ka pārzinim ir jāizskata arī tie piekļuves pieprasījumi, kas netiek nosūtīti, izmantojot izveidoto saziņas kanālu<sup>78</sup>.

### 5.2.3 Piekļuves nodrošināšana "kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu"

139. Saskaņā ar VDAR 12. panta 1. punktu pārzinis veic atbilstošus pasākumus, lai kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu, nodrošinātu piekļuvi saskaņā ar 15. pantu.
140. Prasība, ka piekļuve datu subjektam jānodrošina kodolīgā un pārredzamā veidā, nozīmē to, ka pārzinu sniegtajai informācijai vajadzētu būt efektīvai un kodolīgai, lai datu subjekts — jo īpaši, ja tas ir bērns, — to varētu viegli saprast. Izvēloties līdzekļus piekļuves nodrošināšanai saskaņā ar 15. pantu, pārzinim ir jāņem vērā datu apjoms un sarežģītība.

**26. piemērs.** Sociālo mediju pakalpojumu sniedzējs apstrādā lielu informācijas apjomu par datu subjektu. Liela daļa no šiem persondatiem ir informācija, kas ietverta simtiem lapu apjomīgās žurnāldatnēs, kurās tiek reģistrētas datu subjekta darbības tīmekļa vietnē. Ja datu subjekti pieprasa piekļuvi saviem persondatiem, uz šajās žurnāldatnēs ietvertajiem persondatiem patiešām attiecas piekļuves tiesības. Tādējādi piekļuves tiesības formāli var tikt īstenotas, datu subjektam nodrošinot šīs simtiem lapu apjomīgās žurnāldatnes. Tomēr, neveicot pasākumus nolūkā atvieglot žurnāldatnēs iekļautās informācijas saprotamību, datu subjekta piekļuves tiesības praksē varētu nebūt ievērotas, jo no žurnāldatnēm nevar viegli iegūt informāciju un tāpēc netiek izpildīta VDAR 12. panta 1. punkta

<sup>78</sup> Sk. 3.1.2. iedaļu.

prasība. Tāpēc pārzinim, izvēloties veidu, kādā informācija un persondati tiek sniegti datu subjektam, ir jābūt uzmanīgam un rūpīgam.

141. Ņemot vērā iepriekšējā piemērā minētos apstākļus, vairāku līmeņu pieejas izmantošana, kas līdzīga vairāku līmeņu pieejai, kura atbalstīta Pārredzamības pamatnostādnes attiecībā uz paziņojumiem par privātumu<sup>79</sup>, varētu būt atbilstošs pasākums, lai izpildītu gan VDAR 15. panta, gan 12. panta 1. punkta prasības. Tas tiks sīkāk izklāstīts 5.2.4. iedaļā. Prasība, ka informācijai jābūt “saprotamai”, nozīmē, ka tā būtu jāsaprot paredzētajai auditorijai<sup>80</sup>, vienlaikus paturot prātā jebkādas konkrētas vajadzības, kas varētu būt datu subjektam un kas ir zināmas pārzinim<sup>81</sup>. Tā kā piekļuves tiesības bieži vien ļauj īstenot citas datu subjekta tiesības, ir ļoti svarīgi, lai sniegtā informācija būtu saprotama un skaidra. Tas ir tāpēc, ka datu subjekti varēs apsvērt, vai izmantot savas tiesības, piemēram, uz labošanu saskaņā ar VDAR 16. pantu, tikai tad, kad viņi zinās, kādi persondati tiek apstrādāti kādos nolūkos utt. Tādējādi pārzinim varētu būt jāsniedz datu subjektam papildu informācija, kas paskaidro sniegtos datus. Būtu jāuzsver, ka datu apstrādes sarežģītība liek pārzinim nodrošināt līdzekļus, kas datus padara saprotamus, un to nevar izmantot par argumentu, lai ierobežotu piekļuvi visiem datiem. Arī pārziņa pienākumu sniegt datus kodolīgā veidā nevar izmantot par argumentu, lai ierobežotu piekļuvi visiem datiem.

**27. piemērs.** E-komercijas tīmekļa vietnē tirgvedības nolūkos tiek vākti dati par tajā aplūkotajām vai iegādātajām precēm. Daļa šo datu būs dati neapstrādātā formātā<sup>82</sup>, kas nav analizēti un lasītājam var nebūt tieši noderīgi (kodi, darbību vēsture utt.). Piekļuves tiesības attiecas arī uz šādiem datiem, kas saistīti ar datu subjektu darbībām, un līdz ar to, atbildot uz datu subjekta pieprasījumu, tie viņam būtu jānodrošina. Sniedzot datus neapstrādātā formātā, ir svarīgi, lai pārzinis veiktu vajadzīgos pasākumus nolūkā nodrošināt, ka datu subjekts datus saprot, piemēram, sniedzot skaidrojošu dokumentu, kurā neapstrādātais formāts ir pārveidots lietotājam ērtā formātā. Šādā dokumentā varētu paskaidrot arī saīsinājumu un citu akronīmu nozīmi, piemēram, “A” nozīmē, ka pirkums ir pārtraukts, bet “B” nozīmē, ka pirkums ir noticis.

142. “Vieglas pieejamības” elements nozīmē, ka 15. pantā minētajai informācijai vajadzētu būt sniegtai tā, lai datu subjektam tai būtu viegli piekļūt. Tas attiecas, piemēram, uz izkārtojumu, attiecīgajiem virsrakstiem un sadalījumu rindkopās. Informācija vienmēr būtu jāsniedz vienkāršā un skaidrā valodā. Pārzinim, kas valstī piedāvā pakalpojumu, būtu arī jāsniedz atbildes valodā, ko attiecīgajā valstī saprot datu subjekti. Ieteicams izmantot arī standartizētas ikonas, ja tās atvieglo informācijas saprotamību un pieejamību. Ja informācijas pieprasījums attiecas uz datu subjektiem ar redzes traucējumiem vai citiem datu subjektiem, kuriem var būt grūti piekļūt informācijai vai to saprast, pārzinim ir jāveic pasākumi, lai vajadzības gadījumā veicinātu sniegtās informācijas, arī mutiskās informācijas, saprotamību<sup>83</sup>. Pārzinim būtu īpaši jā rūpējas par to, lai savas tiesības varētu izmantot vecāka gadagājuma cilvēki, bērni, personas ar redzes traucējumiem vai personas ar kognitīviem vai citiem traucējumiem, piemēram, proaktīvi nodrošinot viegli pieejamus elementus, lai veicinātu šo tiesību īstenošanu.

<sup>79</sup> 29. panta darba grupas Pārredzamības pamatnostādnes, kuras apstiprinājusi EDAK, 35. punkts.

<sup>80</sup> Saprotamība ir cieši saistīta ar prasību izmantot vienkāršu un skaidru valodu (29. darba grupas Pārredzamības pamatnostādnes, kuras apstiprinājusi EDAK, 9. punkts). Tas, kas 12.–16. punktā ir teikts par vienkāršu un skaidru valodu attiecībā uz VDAR 13. un 14. pantā minēto informāciju, attiecas arī uz saziņu saskaņā ar 15. pantu.

<sup>81</sup> Sk. 128. punktu.

<sup>82</sup> Piemērā minētais neapstrādātais formāts ir jāsaprot kā neanalizēti dati, kas ir apstrādes pamatā, nevis kā zemākā līmeņa neapstrādāti dati, kuri var būt tikai mašīnlasāmi (piemēram, “biti”).

<sup>83</sup> Sk. 29. panta darba grupas Pārredzamības pamatnostādņu, kuras apstiprinājusi EDAK, 21. punktu.

#### 5.2.4 Lielam informācijas daudzumam ir vajadzīgas īpašas prasības attiecībā uz to, kā tiek sniegta informācija

143. Neatkarīgi no piekļuves nodrošināšanai izmantotajiem līdzekļiem var rasties pretruna starp informācijas apjomu, kas pārzinim jānodrošina datu subjektiem, un prasību, ka informācijai jābūt kodolīgai. Viens no veidiem, kā tos abus nodrošināt, un atbilstoša pasākuma piemērs atsevišķiem pārziniem, kad jāsniedz liels datu apjoms, ir vairāku līmeņu pieejas izmantošana. Šī pieeja datu subjektiem var atvieglot datu saprotamību. Tomēr būtu jāuzsver, ka šo pieeju var izmantot tikai noteiktos apstākļos, un tā jāīsteno tā, lai netiktu ierobežotas piekļuves tiesības, kā paskaidrots tālāk. Turklāt vairāku līmeņu pieejas izmantošanai nevajadzētu radīt papildu slogu datu subjektam. Tāpēc vispiemērotākā tā būtu, nodrošinot piekļuvi tiešsaistes kontekstā. Vairāku līmeņu pieeja ir tikai veids, kā sniegt informāciju saskaņā ar 15. pantu tādā veidā, kas atbilst arī VDAR 12. panta 1. punkta prasībām, un to nevajadzētu jaukt ar iespēju pārziniem pieprasīt, lai datu subjekts precizētu informāciju vai apstrādes darbības, uz kurām attiecas pieprasījums, kā noteikts VDAR 63. apsvērumā<sup>84</sup>.
144. Vairāku līmeņu pieeja attiecībā uz piekļuves tiesībām nozīmē to, ka konkrētos apstākļos pārzinis 15. pantā noteiktos persondatus un papildu informāciju var sniegt dažādos līmeņos. Pirmajā līmenī būtu jāiekļauj informācija par apstrādi un datu subjekta tiesībām saskaņā ar 15. panta 1. punkta a)–h) apakšpunktu un 15. panta 2. punktu, kā arī apstrādāto persondatu pirmā daļa. Otrajā līmenī būtu jāsniedz vairāk persondatu.
145. Pieņemot lēmumu par to, kāda informācija dažādajos līmeņos būtu jāsniedz, pārzinim būtu jāapdomā, kādu informāciju datu subjekts kopumā uzskatītu par visbūtiskāko. Saskaņā ar godprātības principu pirmajā līmenī būtu jāiekļauj arī informācija par apstrādi, kas datu subjektu ietekmē visvairāk<sup>85</sup>. Attiecībā uz iepriekš minētā pamatojumu pārziniem jāspēj uzskatāmi parādīt pārskatatbildību.

**28. piemērs.** Pārzinis analizē lielas datu kopas, lai sakārtotu klientus dažādos segmentos atkarībā no viņu rīcības tiešsaistē. Šajā situācijā var pieņemt, ka datu subjektiem vissvarīgākā ir informācija par to, kurā segmentā viņi ir ievietoti. Tāpēc šī informācija būtu jāiekļauj pirmajā līmenī. Arī dati neapstrādātā formātā<sup>86</sup>, kas vēl nav analizēti vai tālāk apstrādāti, piemēram, lietotāja darbība tīmekļa vietnē, ir persondati, uz kuriem attiecas piekļuves tiesības, tomēr dažos gadījumos varētu pietikt ar šīs informācijas sniegšanu citā līmenī.

146. Lai vairāku līmeņu pieejas izmantošanu uzskatītu par atbilstošu pasākumu, datu subjekts jau pašā sākumā ir jāinformē par to, ka 15. pantā minētā informācija ir strukturēta dažādos līmeņos, un viņam jāsniedz apraksts par to, kādi persondati un informācija tiks ietverti dažādajos līmeņos. Tādējādi datu subjektam būs vieglāk izlemt, kuriem līmeņiem viņš vēlas piekļūt. Aprakstā būtu objektīvi jāatspoguļo visas persondatu kategorijas, ko pārzinis faktiski apstrādā. Ir arī skaidri jānosaka, kā datu subjekts var iegūt piekļuvi dažādajiem līmeņiem. Piekļuve dažādajiem līmeņiem datu subjektam nerada nesamērīgas pūles, un, lai to iegūtu, datu subjektam nav jāiesniedz jauns pieprasījums. Tas nozīmē, ka datu subjektiem ir jāvar izvēlēties, vai piekļūt visiem līmeņiem uzreiz vai arī piekļūt vienam vai diviem līmeņiem, ja viņiem ar to pietiek.

**29. piemērs.** Datu subjekts iesniedz piekļuves pieprasījumu videostraumēšanas pakalpojuma sniedzējam. Pieprasījums tiek iesniegts, izmantojot iespēju, kas pieejama, kad datu subjekts ir pieteicies savā kontā. Datu subjektam ir divas iespējas, kas tīmekļa vietnē redzamas pogu veidā. Pirmā

<sup>84</sup> Sk. arī 2.3.1. iedaļu.

<sup>85</sup> Sk. 29. panta darba grupas Pārredzamības pamatnostādņu, kuras apstiprinājusi EDAK, 36. punktu.

<sup>86</sup> Sk. 82. zemsvītras piezīmi.

iespēja ir lejupieplādēt persondatu pirmo daļu un papildu informāciju. Tā ietver, piemēram, neseno straumēšanas vēsturi, konta informāciju un maksājumu informāciju. Otrā iespēja ir lejuplādēt persondatu otro daļu, kas satur tehniskas žurnāldatnes par datu subjektu darbībām un konta vēsturisko informāciju. Šajā gadījumā pārzinis ir jāvis datu subjektiem īstenot viņu tiesības tādā veidā, kas datu subjektam nerada papildu slogu.

**1. variants.** Ja datu subjekts izvēlas tikai pogu, kura paredzēta persondatu pirmās daļas lejupielādēšanai, pārzinim ir pienākums sniegt tikai datu pirmo daļu.

**2. variants.** Ja datu subjekts izvēlas pogas, kuras attiecas gan uz datu pirmo, gan otro daļu, pārzinis nevar paziņot tikai datu pirmo daļu un pirms datu otrās daļas paziņošanas pieprasīt jaunu apstiprinājumu. Tā vietā datu subjektam ir jānodrošina abas datu daļas, kā tas izriet no iesniegtā pieprasījuma.

147. Vairāku līmeņu pieejas izmantošana netiks uzskatīta par atbilstošu visiem pārziniem vai visās situācijās. Tā būtu jāizmanto tikai gadījumos, kad datu subjektam būtu grūti saprast informāciju, ja tā tiktu sniegta pilnā apjomā. Citiem vārdiem sakot, pārzinim jāspēj uzskatāmi parādīt, ka vairāku līmeņu pieejas izmantošana datu subjektam sniedz pievienoto vērtību, palīdzot viņam saprast sniegto informāciju. Tāpēc vairāku līmeņu pieeja tiktu uzskatīta par atbilstošu tikai tad, ja pārzinis apstrādā lielu daudzumu persondatu par datu subjektu, kas iesniedzis pieprasījumu, un ja datu subjektam rastos acīmredzamas grūtības aptvert vai saprast informāciju, ja tā visa tiktu sniegta vienā reizē. Tas, ka pārzinim būtu jāpieliek lielas pūles un jāizmanto daudz resursu, lai sniegtu informāciju saskaņā ar 15. pantu, pats par sevi nav arguments vairāku līmeņu pieejas izmantošanai.

#### 5.2.5 Formāts

148. Saskaņā ar VDAR 12. panta 1. punktu informāciju, kas minēta 15. pantā, sniedz rakstiski vai citā veidā, tostarp vajadzības gadījumā elektroniski. Attiecībā uz piekļuvi apstrādē esošajiem persondatiem 15. panta 3. punktā ir noteikts, ka tad, ja datu subjekts pieprasījumu iesniedz elektroniskā formā un ja vien datu subjekts nepieprasa citādi, informāciju sniedz plaši izmantotā elektroniskā formātā. VDAR nav precizēts, kas ir plaši izmantots elektroniskais formāts. Tādējādi ir vairāki iespējamie formāti, ko var izmantot. Tas, ko uzskata par plaši izmantotu elektronisko formātu, arī mainīsies laika gaitā.
149. Formātam, ko varētu uzskatīt par plaši izmantotu elektronisko formātu, būtu jābalstās uz objektīvu novērtējumu, nevis uz to, kādu formātu pārzinis izmanto savās ikdienas darbībās. Lai noteiktu, kāds formāts konkrētajā situācijā uzskatāms par plaši izmantotu formātu, pārzinim būs jānovērtē, vai pārzina darbības jomā vai konkrētajā kontekstā parasti tiek izmantoti īpaši formāti. Ja tādus formātus parasti neizmanto, par plaši izmantotiem elektroniskiem formātiem kopumā būtu jāuzskata atvērti formāti, kas noteikti starptautiskā standartā, piemēram, ISO. Tomēr EDAK neizslēdz iespēju, ka par plaši izmantotiem formātiem 15. panta 3. punkta nozīmē var uzskatīt arī citus formātus. EDAK uzskata, ka, novērtējot, vai formāts ir plaši izmantots elektroniskais formāts, ir svarīgi noteikt, cik viegli persona var piekļūt šādā formātā sniegtajai informācijai. Šajā saistībā būtu jānorāda, kādu informāciju pārzinis ir sniedzis datu subjektam par to, kā piekļūt datnei, kas nodrošināta konkrētā formātā, piemēram, kādas programmas vai programmatūru varētu izmantot, lai formātu padarītu pieejamāku datu subjektam. Tomēr datu subjektam nevajadzētu būt pienākumam iegādāties programmatūru, lai piekļūtu informācijai.
150. Pieņemot lēmumu par formātu, kādā būtu jāsniedz persondatu kopija un informācija saskaņā ar 15. pantu, pārzinim jāpatur prātā, ka formātam jābūt tādā, lai informāciju varētu sniegt gan saprotamā, gan viegli pieejamā veidā. Svarīgi, lai datu subjektam informācija tiktu sniegta aptverošā, pastāvīgā formātā (teksta, elektroniskā). Tā kā informācijai laika gaitā būtu jā saglabājas, būtībā

priekšroka dodama rakstiskai informācijai, arī elektroniskā formātā, salīdzinot ar citiem formātiem. Persondatu kopiju attiecīgā gadījumā varētu glabāt elektroniskā atmiņas ierīcē, piemēram, CD vai USB.

151. Būtu jānorāda, ka, lai pārzinis varētu uzskatīt, ka datu subjektiem ir nodrošināta persondatu kopija, nepietiek ar to, ka viņiem ir nodrošināta piekļuve viņu persondatiem. Lai izpildītu prasību nodrošināt persondatu kopiju un gadījumā, kad dati tiek sniegti elektroniski/digitāli, datu subjektiem jābūt iespējai savus datus lejupielādēt plaši izmantotā elektroniskā formātā.
152. Pārziņa pienākums ir pieņemt lēmumu par atbilstošo formātu, kādā tiks nodrošināti persondati. Pārzinis var (lai gan tas nav obligāti) nodrošināt dokumentus, kas satur persondatus par datu subjektiem, kuri iesnieguši pieprasījumu, to sākotnējā formātā. Piemēram, pārzinis katrā atsevišķā gadījumā varētu nodrošināt piekļuvi datu nesēja kopijai kā tādai, ņemot vērā pārredzamības nepieciešamību (piemēram, lai pārbaudītu pārziņa rīcībā esošo datu precizitāti, ja tiek pieprasīta piekļuve medicīniskajai kartei vai audioierakstam, kura pieraksts tiek apstrīdēts). Tomēr, interpretējot Direktīvā 95/46/EK paredzētās piekļuves tiesības, EST norādīja, ka "lai [piekļuves tiesības] varētu uzskatīt par īstenotām, pietiek uzturēšanās atļaujas pieprasītājam izsniegt saprotamā formā ietvertu šo datu apkopojumu, proti, tādā formā, lai datu subjekts varētu iepazīties ar šiem datiem un pārliecināties, vai tie ir pareizi un tiek apstrādāti direktīvai atbilstošā veidā, lai attiecīgā gadījumā īstenotu savas tiesības, kas tam paredzētas"<sup>87</sup>. Atšķirībā no minētās direktīvas VDAR ir skaidri ietverts pienākums nodrošināt datu subjektam apstrādē esošo persondatu kopiju. Tomēr tas nozīmē, ka datu subjektam ne vienmēr ir tiesības saņemt persondatus saturošo dokumentu kopiju, bet gan ka viņam ir tiesības saņemt šajos dokumentos apstrādāto persondatu neizmainītu kopiju.<sup>88</sup> Šādu persondatu kopiju varētu nodrošināt, izmantojot apkopojumu, kas satur visus persondatus, uz kuriem attiecas piekļuves tiesības, ja vien šis apkopojums ļauj datu subjektam uzzināt par apstrādi un pārliecināties par tās likumīgumu. Tādējādi šajā jautājumā nav pretrunu starp VDAR formulējumu un EST nolēmumu. Nolēmumā ietvertais kopsavilkums nebūtu nepareizi jāinterpretē tādējādi, ka apkopojums neaptver visus datus, uz kuriem attiecas piekļuves tiesības, bet ir tikai veids, kā sniegt visus šos datus, nedodot piekļuvi pamatā esošajiem dokumentiem, kas satur persondatus. Tā kā apkopojumā jāiekļauj persondatu kopija, būtu jāuzsver, ka to nevar sagatavot tā, lai kaut kādā veidā tiktu mainīts informācijas saturs.

**30. piemērs.** Datu subjekts daudzus gadus ir bijis apdrošināts apdrošināšanas sabiedrībā. Ir bijuši vairāki apdrošināšanas gadījumi. Par katru gadījumu starp datu subjektu un apdrošināšanas sabiedrību ir notikusi sarakste e-pastā. Tā kā datu subjektam bija jāsniedz informācija par katra gadījuma konkrētajiem apstākļiem, sarakste satur daudz personiska rakstura informācijas par datu subjektu (par viņa vaļaspriekiem, dzīvokļa biedriem, ikdienas paradumiem utt.). Dažās lietās radās domstarpības par apdrošināšanas sabiedrības pienākumu datu subjektam izmaksāt kompensāciju, kā rezultātā notika apjomīga savstarpēja saziņa. Apdrošināšanas sabiedrība visu šo saraksti glabā. Datu subjekts iesniedz piekļuves pieprasījumu. Šādā situācijā pārzinim nav obligāti jāsniedz e-pasta vēstules to sākotnējā formā, nosūtot tās datu subjektam. Tā vietā pārzinis varētu izvēlēties e-pastā veikto saraksti, kura satur datu subjekta persondatus, apkopot datnē, ko nodrošina datu subjektam.

153. Neatkarīgi no formāta, kādā pārzinis nodrošina persondatus, piemēram, sniedzot faktiskos dokumentus, kas satur persondatus, vai persondatu apkopojumu, informācija atbilst VDAR 12. pantā noteiktajām pārredzamības prasībām. Dažos gadījumos veids, kā šīs prasības izpildīt, varētu būt dažu veidu datu apkopšana un/vai izgūšana tādā veidā, kas informāciju padara viegli saprotamu. Citos

<sup>87</sup> EST, apvienotās lietas C-141/12 un 372/12, *YS* u. c., 60. punkts.

<sup>88</sup> Ar šo tematu saistīti jautājumi ir ietverti pašlaik EST izskatāmās lietās (C-487/21 un C-307/21).



gadījumos informācija ir labāk saprotama, nodrošinot persondatus saturošā dokumenta kopiju. Tāpēc lēmums par to, kurš formāts ir vispiemērotākais, ir jāpieņem katrā gadījumā atsevišķi.

154. Šajā kontekstā ir svarīgi atcerēties, ka pastāv atšķirība starp tiesībām iegūt piekļuvi saskaņā ar VDAR 15. pantu un tiesībām saņemt tādu administratīvo dokumentu kopijas, kurus reglamentē valsts tiesību akti, jo otrās minētās ir tiesības saņemt konkrētā dokumenta kopiju. Tas nenozīmē, ka VDAR 15. pantā paredzētās piekļuves tiesības izslēdz iespēju saņemt persondatus saturošā dokumenta/mediju kopiju.
155. Dažos gadījumos persondati paši par sevi nosaka prasības, kādā formātā tie būtu jāsniedz. Piemēram, ja persondati ir datu subjekta ar roku rakstīta informācija, datu subjektam var būt nepieciešams saņemt šīs ar roku rakstītās informācijas fotokopiju, jo rokraksts pats par sevi ir persondati. Tas jo īpaši varētu attiekties uz gadījumiem, kad rokraksts ir svarīgs elements apstrādē, piemēram, rokrakstu analizē. Tas pats vispārīgi attiecas uz audioierakstiem, jo datu subjekta balss pati par sevi ir persondati. Tomēr dažos gadījumos, piemēram, ja datu subjekts un pārzinis par to vienojas, piekļuvi var nodrošināt sarunas pieraksta veidā.
156. Būtu jānorāda, ka noteikumi par prasībām attiecībā uz formātu piekļuves tiesību un tiesību uz datu pārnesamību gadījumā atšķiras. Lai gan tiesības uz datu pārnesamību saskaņā ar VDAR 20. pantu paredz, ka informācija jāsniedz mašīnlasāmā formātā, 15. pantā minētās tiesības uz informāciju to neparedz. Tādējādi formāti, kas tiek uzskatīti par neatbilstošiem, izpildot datu pārnesamības pieprasījumu, piemēram, pdf datnes, joprojām varētu būt piemēroti, izpildot piekļuves pieprasījumu.

### 5.3 Piekļuves nodrošināšanas termiņi

157. VDAR 12. panta 3. punktā ir noteikts, ka pārzinis bez nepamatotas kavēšanās un jebkurā gadījumā mēneša laikā pēc pieprasījuma saņemšanas datu subjektu informē par darbību, kas pēc pieprasījuma veikta saskaņā ar 15. pantu. Vajadzības gadījumā minēto laikposmu var pagarināt vēl uz diviem mēnešiem, ņemot vērā pieprasījumu sarežģītību un skaitu, ja datu subjekts par šādas kavēšanās iemesliem ir informēts mēneša laikā pēc pieprasījuma saņemšanas. Šo pienākumu informēt datu subjektu par pagarinājumu un tā iemesliem nevajadzētu jaukt ar informāciju, kas jāsniedz bez kavēšanās un vēlākais mēneša laikā, ja pārzinis neveic pieprasīto darbību, kā sīki izklāstīts VDAR 12. panta 4. punktā.
158. Pārzinis reaģē un parasti sniedz informāciju saskaņā ar 15. pantu bez nepamatotas kavēšanās, un tas nozīmē, ka informācija būtu jāsniedz pēc iespējas ātrāk. Tas nozīmē, ka, ja pieprasīto informāciju ir iespējams sniegt laikposmā, kas īsāks par vienu mēnesi, pārzinim tas būtu jā dara. EDAK arī uzskata, ka termiņš, kādā jāsniedz atbilde uz pieprasījumu, dažās situācijās ir jāpielāgo glabāšanas periodam, lai varētu nodrošināt piekļuvi<sup>89</sup>.
159. Termiņš sākas, kad pārzinis ir saņēmis pieprasījumu saskaņā ar 15. pantu, t. i., kad pieprasījums sasniedz pārzini pa kādu no tā oficiālajiem kanāliem<sup>90</sup>. Nav nepieciešams, lai pārzinis faktiski zinātu par pieprasījumu. Tomēr, ja pārzinim ir jāsažinās ar datu subjektu, jo nav skaidra pieprasījuma iesniedzēja personas identitāte, termiņš var tikt apturēts līdz brīdim, kad pārzinis no datu subjekta ir saņēmis vajadzīgo informāciju, ja vien pārzinis papildu informāciju ir pieprasījis bez nepamatotas kavēšanās.

---

<sup>89</sup> Skatīt 2.3.3. iedaļu.

<sup>90</sup> Dažās dalībvalstīs pastāv valsts tiesību akti, kas nosaka, kad ziņojums uzskatāms par saņemtu, ņemot vērā nedēļas nogales un valsts svētku dienas.



Tas pats attiecas uz gadījumiem, kad pārzinis datu subjektam ir lūdzis precizēt apstrādes darbības, uz kurām attiecas pieprasījums, ja ir izpildīti 63. apsvērumā izklāstītie nosacījumi<sup>91</sup>.

**31. piemērs.** Pēc pieprasījuma saņemšanas pārzinis nekavējoties reaģē un lūdz informāciju, kas viņam vajadzīga, lai apstiprinātu pieprasījuma iesniedzēja personas identitāti. Persona sniedz atbildi tikai pēc vairākām dienām, bet informācija, ko datu subjekts nosūta identitātes pārbaudei, nešķiet pietiekama, tāpēc pārzinim jādūdz skaidrojumi. Šādā situācijā apturēšana ilgs līdz brīdim, kad pārzinis būs ieguvis pietiekami informācijas, lai pārbaudītu datu subjekta identitāti.

160. Termiņš, kurā jāsniedz atbilde uz piekļuves pieprasījumu, ir jāaprēķina saskaņā ar Regulu Nr. 1182/71<sup>92</sup>.

**32. piemērs.** Organizācija saņem pieprasījumu 5. martā. Termiņš sākas tajā pašā dienā. Tādējādi organizācijai pieprasījums ir jāizpilda vēlākais līdz 5. aprīlim (ieskaitot).

**33. piemērs.** Ja organizācija saņem pieprasījumu 31. augustā, bet nākamais mēnesis ir īsāks un atbilstīga datuma nav, tad atbildes sniegšanas datums ir vēlākais nākamā mēneša pēdējā diena, tātad 30. septembris.

161. Ja šā laikposma pēdējā diena iekrīt nedēļas nogalē vai valsts svētku dienā, pārzinim ir jāsniedz atbilde līdz nākamajai darbdienai.

162. Noteiktos apstākļos pārzinis vajadzības gadījumā var pagarināt termiņu, kurā jāsniedz atbilde uz piekļuves pieprasījumu, vēl par diviem mēnešiem, ņemot vērā pieprasījumu sarežģītību un skaitu. Būtu jāuzsver, ka šī iespēja ir izņēmums no vispārējā noteikuma un to nevajadzētu izmantot pārmērīgi. Ja pārzini bieži ir spiesti termiņu pagarināt, tas varētu liecināt par nepieciešamību pilnveidot savas vispārīgās procedūras pieprasījumu apstrādei.

163. Kas ir sarežģīts pieprasījums, ir atkarīgs no katras lietas konkrētajiem apstākļiem. Daži no faktoriem, ko varētu uzskatīt par būtiskiem, ir, piemēram, šādi:

- pārziņa apstrādāto datu apjoms;
- tas, kā informācija tiek glabāta, jo īpaši, ja informāciju ir grūti izgūt, piemēram, ja datus apstrādā dažādas organizācijas vienības;
- vajadzība rediģēt informāciju, ja ir spēkā atbrīvojums, piemēram, informāciju par citiem datu subjektiem vai informāciju, kas ir tirdzniecības noslēpums, un
- vajadzība informāciju papildus apstrādāt, lai tā būtu saprotama.

164. Tas vien, ka pieprasījuma izpildē būtu jāpieliek lielas pūles, to nepadara sarežģītu. Tāpat arī tas, ka liels uzņēmums saņem lielu skaitu pieprasījumu, automātiski neizraisītu termiņa pagarināšanu. Taču, ja pārzinis īslaicīgi saņem lielu skaitu pieprasījumu, piemēram, ar savām darbībām saistītas ārkārtējas publicitātes dēļ, to varētu uzskatīt par likumīgu iemeslu, lai pagarinātu atbildes sniegšanas laiku. Tomēr pārzinim, jo īpaši tādām, kas apstrādā lielu datu apjomu, vajadzētu būt ieviestām procedūrām un mehānismiem, lai parastos apstākļos varētu apstrādāt pieprasījumus noteiktajā termiņā.

<sup>91</sup> Skatīt tālāk 2.3.1. iedaļu.

<sup>92</sup> Padomes Regula (EEK, *Euratom*) Nr. 1182/71 (1971. gada 3. jūnijs), ar ko nosaka laikposmiem, datumiem un termiņiem piemērojamus noteikumus.

## 6 PIEKĻUVES TIESĪBU IEROBEŽOJUMI

### 6.1 Vispārīgas piezīmes

165. Uz piekļuves tiesībām attiecas ierobežojumi, kas izriet no VDAR 15. panta 4. punkta (citu personu tiesības un brīvības) un VDAR 12. panta 5. punkta (acīmredzami nepamatoti vai pārmērīgi pieprasījumi). Turklāt piekļuves tiesības var ierobežot Savienības vai dalībvalsts tiesību akti saskaņā ar VDAR 23. pantu. Atkāpes attiecībā uz persondatu apstrādi zinātniskās un vēstures pētniecības vai statistikas nolūkos vai arhivēšanas nolūkos sabiedrības interesēs attiecīgi var pamatot ar VDAR 89. panta 2. punktu un 89. panta 3. punktu, bet atkāpes attiecībā uz apstrādi žurnālistikas vajadzībām vai akadēmiskās, mākslinieciskās vai literārās izpausmes vajadzībām, var pamatot ar VDAR 85. panta 2. punktu.
166. Ir svarīgi norādīt, ka, izņemot iepriekš minētās robežas, atkāpes un iespējamus ierobežojumus, VDAR neparedz nekādus turpmākus izņēmumus vai atkāpes no piekļuves tiesībām. Tas cita starpā nozīmē to, ka uz piekļuves tiesībām neattiecas nekāda vispārēja atruna par proporcionalitāti saistībā ar pūlēm, kas pārzinim jāpieliek, lai izpildītu datu subjektu pieprasījumu saskaņā ar VDAR 15. pantu<sup>93</sup>. Turklāt piekļuves tiesības nav atļauts ierobežot līgumā starp pārzini un datu subjektu.
167. Saskaņā ar 63. apsvērumu datu subjektiem tiek piešķirtas piekļuves tiesības, lai zinātu par apstrādi un pārliecinātos par tās likumīgumu. Piekļuves tiesības cita starpā ļauj datu subjektam atkarībā no apstākļiem panākt persondatu izlabošanu, dzēšanu vai piekļuves noslēgšanu<sup>94</sup>. Tomēr datu subjektiem nav pienākuma norādīt iemeslus vai pamatot savu pieprasījumu. Ja vien tiek izpildītas VDAR 15. panta prasības, pieprasījuma mērķi būtu jāuzskata par nebūtiskiem<sup>95</sup>.

### 6.2 VDAR 15. panta 4. punkts

168. Saskaņā ar VDAR 15. panta 4. punktu tiesības saņemt kopiju nedrīkst nelabvēlīgi ietekmēt citu personu tiesības un brīvības. Skaidrojumi attiecībā uz šo ierobežojumu ir sniegti 63. apsvēruma piektajā un sestajā teikumā. Minētajām tiesībām nevajadzētu nelabvēlīgi ietekmēt citu personu tiesības vai brīvības, tostarp tirdzniecības noslēpumus vai intelektuālā īpašuma tiesības un jo īpaši autortiesības, ar ko aizsargāta programmatūra. Tomēr minēto apsvērumu rezultātam nevajadzētu būt tādām, ka datu subjektam tiek atteikts sniegt jebkādu informāciju. Interpretējot VDAR 15. panta 4. punktu, ir jāievēro īpaša piesardzība, lai nepamatoti nepaplašinātu VDAR 23. pantā noteiktos ierobežojumus, kas ir pieļaujami tikai saskaņā ar stingriem nosacījumiem.
169. VDAR 15. panta 4. punkts attiecas uz tiesībām saņemt datu kopiju, kas ir galvenais veids, kādā piešķir piekļuvi apstrādātajiem datiem (piekļuves tiesību otrais komponents). To arī piemēro un ņem vērā citu personu tiesības un brīvības, ja piekļuvi persondatiem izņēmuma kārtā piešķir, izmantojot citus līdzekļus, kas nav kopija. Piemēram, nav pamatotas atšķirības tajā, vai tirdzniecības noslēpumus ietekmē, datu subjektam nodrošinot kopiju vai piešķirot piekļuvi uz vietas. VDAR 15. panta 4. punkts

---

<sup>93</sup> Ja pārzinis apstrādā lielu informācijas apjomu saistībā ar datu subjektu, kā minēts VDAR 63. apsvērumā, pārzinis var pieprasīt, lai datu subjekts precizētu, uz kuru informāciju vai kurām apstrādes darbībām pieprasījums attiecas. Sk. arī 2.3.1. iedaļu.

<sup>94</sup> EST, apvienotās lietas C-141/12 un C-372/12, YS u. c.

<sup>95</sup> Tas neskar piemērojamos valsts tiesību aktus, kas atbilst VDAR 23. panta prasībām, sk. 6.4. nodaļu.

nav piemērojams papildu informācijai par apstrādi, kā noteikts VDAR 15. panta 1. punkta a)–h) apakšpunktā.

170. Saskaņā ar 63. apsvērumu konfliktējošas tiesības un brīvības ietver tirdzniecības noslēpumus vai intelektuālo īpašumu un jo īpaši autortiesības, ar ko aizsargāta programmatūra. Šīs skaidri minētās tiesības un brīvības būtu jāuzskata tikai par piemēriem, jo principā var uzskatīt, ka jebkurām tiesībām vai brīvībām, kuru pamatā ir Savienības vai dalībvalsts tiesību akti, ir piemērojams VDAR 15. panta 4. punktā noteiktais ierobežojums<sup>96</sup>. Tādējādi arī tiesības uz persondatu aizsardzību (Eiropas Pamattiesību hartas 8. pants) var uzskatīt par skartajām tiesībām VDAR 15. panta 4. punkta nozīmē. Attiecībā uz tiesībām saņemt kopiju — tipisks gadījums, kurā jānovērtē ierobežojums, ir citu personu tiesības uz datu aizsardzību. Turklāt ir jāņem vērā tiesības uz sarakstes konfidencialitāti, piemēram, attiecībā uz privātu saraksti e-pastā nodarbinātības kontekstā<sup>97</sup>. Svarīgi ir norādīt, ka ne visas intereses ir “tiesības un brīvības” saskaņā ar VDAR 15. panta 4. punktu. Piemēram, uzņēmuma ekonomiskās intereses neizpauš persondatus nesasniedz 15. panta 4. punktā minēto atbrīvojuma izmantošanas sliekšni, ja vien netiek skarti tirdzniecības noslēpumi, intelektuālais īpašums vai citas aizsargātas tiesības.
171. “Citas personas” ir jebkura cita persona vai vienība, izņemot datu subjektu, kas izmanto savas piekļuves tiesības. Tādējādi varētu ņemt vērā pārziņa vai apstrādātāja tiesības un brīvības (piemēram, attiecībā uz tirdzniecības noslēpumu un intelektuālā īpašuma konfidencialitātes saglabāšanu). Ja ES likumdevējs būtu vēlējies izslēgt pārziņu vai apstrādātāju tiesības un brīvības, tas būtu izmantojis VDAR 4. panta 10. punktā definēto terminu “trešā persona”.
172. Ar vispārējām bažām par to, ka piekļuves pieprasījuma izpilde varētu ietekmēt citu personu tiesības un brīvības, nepietiek, lai atsauktos uz VDAR 15. panta 4. punktu. Pārzinim ir jāspēj uzskatāmi parādīt, ka citu personu tiesības vai brīvības konkrētajā situācijā faktiski tiktu ietekmētas.

**34. piemērs.** Persona, kas tagad ir pilngadīga, vairākus gadus pagātnē atradās jauniešu sociālā dienesta aprūpē. Attiecīgās datnes, iespējams, var saturēt sensitīvu informāciju par citām personām (vecākiem, sociālajiem darbiniekiem, citiem nepilngadīgajiem). Tomēr informācijas pieprasījumu no datu subjekta šā iemesla dēļ parasti nevar noraidīt, atsaucoties uz VDAR 15. panta 4. punktu. Gluži pretēji, jauniešu sociālajam dienestam kā pārzinim ir detalizēti jāizvērtē un uzskatāmi jāparāda citu personu tiesības un brīvības. Atkarībā no attiecīgajām interesēm un to relatīvā nozīmīguma šādas konkrētas informācijas sniegšanu var noraidīt (piemēram, rediģējot vārdus un uzvārdus).

173. Ņemot vērā VDAR 4. apsvērumu un Eiropas Pamattiesību hartas 52. panta 1. punkta pamatojumu, tiesības uz persondatu aizsardzību nav absolūta prerogatīva<sup>98</sup>. Tādējādi arī piekļuves tiesību īstenošana ir jālīdzsvaro ar citām pamattiesībām saskaņā ar proporcionalitātes principu. Ja saskaņā ar VDAR 15. panta 4. punktu veiktais novērtējums pierāda, ka pieprasījuma izpildei ir nelabvēlīga (negatīva) ietekme uz citu dalībnieku tiesībām un brīvībām (1. posms), ir jāizvērtē visu dalībnieku intereses, ņemot vērā lietas konkrētos apstākļus un jo īpaši to risku iespējamību un smagumu, ko rada datu paziņošana. Pārzinim būtu jācenšas saskaņot konfliktējošās tiesības (2. posms), piemēram, īstenojot atbilstošus pasākumus, lai mazinātu risku citu personu tiesībām un brīvībām. Kā uzsvērts

<sup>96</sup> Konfliktējošo tiesību un brīvību nozīmīgums vai prioritāte nav jēdziena “tiesības un brīvības” definīcijas jautājums. Tomēr šādu interešu līdzsvarošana ir daļa no novērtējuma otrā posma saistībā ar to, vai ir piemērojams 15. panta 4. punkts. Sk. tālāk 173. punktu.

<sup>97</sup> ECT, *Bărbulescu* pret Rumāniju, Nr. 61496/08, 80. punkts, 2017. gada 5. septembris.

<sup>98</sup> Sk., piemēram, arī 48. punktu EST apvienotajās lietās C-92/09 un C-93/09, *Volker und Markus Schecke GbR* un *Hartmut Eifert* pret *Land Hessen* [GC], 2010. gada 9. novembris.

63. apsvērumā, citu personu tiesību un brīvību aizsardzības saskaņā ar VDAR 15. panta 4. punktu rezultātam nevajadzētu būt tādām, ka datu subjektam tiek atteikts sniegt jebkādu informāciju. Tas nozīmē, ka, piemēram, gadījumos, kad ir piemērojams ierobežojums, tā vietā, lai atteiktos sniegt persondatu kopiju, informācija par citiem, cik vien iespējams, jāpadara nesalasāma. Tomēr, ja nav iespējams rast risinājumu attiecīgo tiesību saskaņošanai, pārzinim nākamajā posmā ir jāizlemj, kuras no konfliktējošajām tiesībām un brīvībām ir pārākas (3. posms).

**35. piemērs.** Mazumtirgotājs saviem klientiem piedāvā iespēju pasūtīt produktus, izmantojot tā klientu apkalpošanas tālruņa līniju. Kā pierādījumu komercdarījumiem mazumtirgotājs saglabā zvanu ierakstu saskaņā ar piemērojamo tiesību aktu stingrajām prasībām. Klients vēlas saņemt savas sarunas ar klientu apkalpošanas aģentu kopiju. Pirmajā posmā mazumtirgotājs analizē pieprasījumu un saprot, ka ieraksts satur persondatus, kuri attiecas arī uz kādu citu personu, proti, klientu apkalpošanas aģentu. Otrajā posmā, lai novērtētu, vai kopijas izsniegšana ietekmētu citu personu tiesības un brīvības, mazumtirgotājam ir jālidzvaro konfliktējošās intereses, jo īpaši ņemot vērā to risku iespējamību un smagumu, kas pastāv attiecībā uz klientu apkalpošanas aģenta tiesībām un brīvībām, paziņojot klientam ierakstu. Mazumtirgotājs secina, ka ieraksts satur ļoti ierobežotus persondatus par klientu apkalpošanas aģentu, proti, tikai viņa balsi. Mazumtirgotājs/pārzinis konstatē, ka aģents nav viegli identificējams. Turklāt sarunas saturs ir profesionāla rakstura, un datu subjekts bija sarunu partneris. Pamatojoties uz iepriekš minētajiem apstākļiem, pārzinis objektīvi secina, ka piekļuves tiesības neietekmē nelabvēlīgi klientu apkalpošanas aģenta tiesības un brīvības, un tāpēc pārzinis var nodrošināt datu subjektam pilnu ierakstu, arī tās balss ieraksta daļas, kas attiecas uz klientu apkalpošanas aģentu.

**36. piemērs.** Medicīnas preču veikala kliente, pamatojoties uz VDAR 15. pantu, vēlas piekļūt savu kāju mērījumu rezultātiem. Medicīnas preču veikalā tika veikti datu subjekta kāju mērījumi, lai izgatavotu individuālas medicīniskās kompresijas zeķes. Medicīnas preču veikalam acīmredzot bija liela pieredze, un tas bija izstrādājis īpašu paņēmieni precīzai mērīšanai. Pēc mērījumu veikšanas medicīnas preču veikalā klients vēlas izmantot mērījumu rezultātus, lai zeķes lētāk iegādātos citur (pasūtot tās tiešsaistes veikalā). Medicīnas preču veikals, pamatojoties uz VDAR 15. panta 4. punktu, daļēji atsaka piekļuvi datiem, apgalvojot, ka tā īpašo, precīzo mērīšanas paņēmieni dēļ rezultāti ir aizsargāti kā tirdzniecības noslēpumi. Ja un ciktāl pārzinis var pierādīt, ka:

- informācijas par mērījumu rezultātiem sniegšana datu subjektam nav iespējama, neatklājot to, kā mērījumi tika veikti, un
- informācija par to, kā mērījumi veikti, arī attiecīgā gadījumā precīza mērīšanas vietu noteikšana, ir tirdzniecības noslēpumi,

tas var piemērot VDAR 15. panta 4. punktu.

Pārzinim joprojām būtu jāsniedz iespējami daudz tādas informācijas par mērījumu rezultātiem, kas neatklātu tā tirdzniecības noslēpumu, pat ja tas nozīmētu, ka tam rezultāti ir jāredzīgi un jālabo.

**37. piemērs.** SPĒLĒTĀJS X ir reģistrēts lietotājs spēļu platformā — PLATFORMĀ Y. Kādu dienu SPĒLĒTĀJS X tiek informēts, ka viņa tiešsaistes konts ir ierobežots. Tā kā SPĒLĒTĀJS X vairs nevar pieteikties, viņš lūdz pārzinim piekļuvi visiem persondatiem, kas uz viņu attiecas. Turklāt SPĒLĒTĀJS X pieprasa piekļuvi konta ierobežošanas iemesliem. PLATFORMA Y, kas ir tās tiešsaistes spēļu platformas pārzinis, kurai iesniegts pieprasījums, savos vispārīgajos noteikumos, kas pieejami tās tīmekļa vietnē, informē lietotājus, ka jebkāda veida krāpšanās gadījumā (galvenokārt izmantojot

trešo personu programmatūru) piekļuve platformai tiks uz laiku vai pastāvīgi liegta. Savā privātuma politikā PLATFORMA Y informē lietotājus arī par persondatu apstrādi, ko veic nolūkā atklāt krāpšanos spēlēs, saskaņā ar VDAR 13. pantā noteiktajām prasībām.

PLATFORMAI Y pēc SPĒLĒTĀJA X piekļuves pieprasījuma saņemšanas būtu jānodrošina SPĒLĒTĀJAM X to persondatu kopija, kas par viņu tiek apstrādāti. Attiecībā uz konta ierobežošanas iemeslu PLATFORMAI Y būtu jāapstiprina SPĒLĒTĀJAM X, ka tā ir nolēmusi ierobežot SPĒLĒTĀJA X piekļuvi tiešsaistes spēlēm, jo viņš vienu reizi vai atkārtoti ir krāpies spēlēs un tas ir vispārīgo lietošanas noteikumu pārkāpums. Papildus informācijai, kas sniegta par apstrādi, kuru veic nolūkā atklāt krāpšanos spēlēs, PLATFORMAI Y būtu jāpiešķir SPĒLĒTĀJAM X piekļuve informācijai, ko tā saglabājusi par SPĒLĒTĀJA X krāpšanos spēlēs, kuras dēļ tika noteikts ierobežojums. Konkrēti, PLATFORMAI Y būtu jāsniedz SPĒLĒTĀJAM X informācija, kuras dēļ konts tika ierobežots (piem., žurnāla pārskats, krāpšanās datums un laiks, trešo personu programmatūras atklāšana u. c.), lai datu subjekts (t. i., SPĒLĒTĀJS X) varētu pārbaudīt, vai datu apstrāde ir bijusi pareiza.

Tomēr saskaņā ar VDAR 15. panta 4. punktu un VDAR 63. apsvērumu PLATFORMAI Y nav pienākuma atklāt nevienu pretkrāpšanās programmatūras tehniskās darbības daļu, pat ja šī informācija attiecas uz SPĒLĒTĀJU X, ja vien to var uzskatīt par tirdzniecības noslēpumu. Nepieciešamās interešu līdzsvaros saskaņā ar VDAR 15. panta 4. punktu rezultātā šos persondatus liedz izpaust PLATFORMAS Y tirdzniecības noslēpumi, jo zināšanas par pretkrāpšanās programmatūras tehnisko darbību varētu arī ļaut lietotājam turpmāk izvairīties no krāpšanas atklāšanas<sup>99</sup>.

174. Ja pārziņi saskaņā ar VDAR 15.panta 4. punktu pilnīgi vai daļēji atsakās atbildēt uz piekļuves tiesību pieprasījumu, tiem bez kavēšanās un vēlākais mēneša laikā jāinformē datu subjekts par iemesliem (VDAR 12. panta 4. punkts). Paskaidrojumā ir jāmin konkrētie apstākļi, lai datu subjekti varētu novērtēt, vai viņi atteikumu vēlas apstrīdēt. Tajā jāiekļauj informācija par iespēju iesniegt sūdzību uzraudzības iestādē (VDAR 77. pants) un vērsties tiesā (VDAR 79. pants).

### 6.3 VDAR 12. panta 5. punkts

175. VDAR 12. panta 5. punkts ļauj pārziņiem nepildīt piekļuves tiesību pieprasījumus, kas ir acīmredzami nepamatoti vai pārmērīgi. Šie jēdzieni ir jāinterpretē šauri, jo nedrīkst apdraudēt pārredzamības principu un principu, ka datu subjektu tiesības tiek īstenotas bez maksas.
176. Pārziņiem jāspēj personai uzskatāmi parādīt, kāpēc tie uzskata, ka pieprasījums ir acīmredzami nepamatots vai pārmērīgs, un, ja tiek lūgts, paskaidrot iemeslus kompetentajai uzraudzības iestādei. Lai pieņemtu lēmumu par to, vai pieprasījums ir acīmredzami nepamatots vai pārmērīgs, katrs pieprasījums būtu jāizskata atsevišķi katrā gadījumā, ņemot vērā kontekstu, kādā tas iesniegts.

#### 6.3.1 Ko nozīmē acīmredzami nepamatots?

177. Piekļuves tiesību pieprasījums ir acīmredzami nepamatots, ja, piemērojot objektīvu pieeju, VDAR 15. panta prasības nav skaidri un acīmredzami izpildītas. Tomēr, kā paskaidrots iepriekš 3. iedaļā, piekļuves tiesību pieprasījumiem ir tikai daži priekšnoteikumi. Tāpēc EDAK uzsver, ka attiecībā uz

---

<sup>99</sup> Personām sniegtās informācijas apjoms būs lielā mērā atkarīgs no konteksta, ņemot vērā pārziņa veidu un pakalpojuma noteikumu pārkāpuma veidu. Dažos gadījumos pārziņis, atbildot uz piekļuves pieprasījumu, kuram piemērojams 15. panta 4. punkts, var sniegt tikai pamatinformāciju.

piekļuves tiesību pieprasījumiem pastāv tikai ļoti ierobežotas iespējas atsaukties uz VDAR 12. panta 5. punkta "acīmredzami nepamatoto" alternatīvu.

178. Turklāt ir svarīgi atgādināt, ka pirms ierobežojuma izmantošanas pārziņiem ir rūpīgi jāizanalizē pieprasījuma saturs un tvērums. Piemēram, pieprasījumu nevajadzētu uzskatīt par acīmredzami nepamatotu, ja tas ir saistīts ar tādu persondatu apstrādi, uz kuriem neattiecas VDAR (šajā gadījumā pieprasījums vispār nebūtu jāizskata kā pieprasījums saskaņā ar 15. pantu).
179. Citi gadījumi, kuros VDAR 12. panta 5. punkta piemērojamība ir apšaubāma, ir pieprasījumi, kas saistīti ar informāciju vai apstrādes darbībām, uz kurām pārziņa veiktās apstrādes darbības nepārprotami un acīmredzami neattiecas.

**38. piemērs.** Datu subjekts pašvaldības iestādei iesniedz pieprasījumu attiecībā uz datiem, ko apstrādā valsts iestāde. Tā vietā, lai apgalvotu, ka pieprasījums ir acīmredzami nepamatots, iestādei piemērotāk un arī vieglāk būtu apstiprināt, ka tā šos datus neapstrādā (VDAR 15. panta pirmais komponents: "vai" persondati tiek apstrādāti)<sup>100</sup>.

180. Pārzinim nevajadzētu pieņemt, ka pieprasījums ir acīmredzami nepamatots tādēļ, ka datu subjekts iepriekš ir iesniedzis pieprasījumus, kas bijuši acīmredzami nepamatoti vai pārmērīgi, vai ja tas ietver neobjektīvu vai neatbilstošu valodu.

### 6.3.2 Ko nozīmē pārmērīgs?

181. Termins "pārmērīgs" VDAR nav definēts. No vienas puses, formulējums "jo īpaši to regulāras atkārtotās dēļ" VDAR 12. panta 5. punktā ļauj secināt, ka galvenais scenārijs šīs VDAR 15. panta daļas piemērošanai ir saistīts ar datu subjekta pieprasījumu piekļuves tiesībām skaitu. No otras puses, no iepriekš minētā formulējuma izriet, ka *a priori* nav izslēgti citi iemesli, kas varētu izraisīt pārmērīgumu.
182. Saskaņā ar VDAR 15. panta 3. punktu attiecībā uz tiesībām saņemt kopiju datu subjekts pārzinim noteikti var iesniegt vairāk nekā vienu pieprasījumu<sup>101</sup>. Tādu pieprasījumu gadījumā, kurus, iespējams, varētu uzskatīt par pārmērīgiem, "pārmērīguma" novērtējums ir atkarīgs no pārziņa veiktās analīzes un tās nozares specifikas, kurā tas darbojas.
183. Turpmāku pieprasījumu gadījumā ir jānovērtē, vai ir pārsniegta saprātīgu intervālu robeža (sk. 63. apsvērumu). Pārziņiem ir rūpīgi jāņem vērā katra gadījuma īpašie apstākļi.
184. Piemēram, sociālo tīklu gadījumā izmaiņas datu kopā būs gaidāmas īsākos intervālos nekā zemes reģistru vai centrālo uzņēmumu reģistru gadījumā. Darījumu partneru gadījumā būtu jāņem vērā tas, cik bieži notiek saziņa ar klientu. Attiecīgi atšķiras arī "saprātīgie intervāli", kuros datu subjekti atkal var īstenot savas piekļuves tiesības. Jo biežāk notiek izmaiņas pārziņa datubāzē, jo biežāk datu subjektiem var tikt ļauts pieprasīt piekļuvi viņu persondatiem, šādiem pieprasījumiem neesot pārmērīgiem. No otras puses, tā paša datu subjekta iesniegtu otru pieprasījumu noteiktos apstākļos varētu uzskatīt par atkārtotu.
185. Pieņemot lēmumu par to, vai ir pagājis saprātīgs intervāls, pārziņiem, ņemot vērā datu subjekta saprātīgās gaidas, būtu jāņem vērā šādi aspekti:

---

<sup>100</sup> Cits jautājums ir, vai iestāde, kurai adresēts piekļuves pieprasījums, ir tiesīga šo pieprasījumu pārsūtīt kompetentajai valsts iestādei.

<sup>101</sup> Saskaņā ar 15. panta 3. punkta otro teikumu pārzinis par pieprasītajām papildu kopijām var iekasēt samērīgu samaksu.

- cik bieži dati tiek mainīti — vai ir maz ticams, ka informācija pieprasījumu iesniegšanas starplaikā ir mainījusies? Ja datu kopums acīmredzami netiek apstrādāts citādi, kā vien glabāts, un datu subjekts par to ir informēts, piemēram, saistībā ar iepriekšēju piekļuves tiesību pieprasījumu, tas varētu liecināt par pārmērīgu pieprasījumu;
- datu raksturs — šis aspekts varētu ietvert to, vai dati ir īpaši sensitīvi;
- apstrādes nolūki — šis aspekts varētu ietvert to, vai datu apstrāde pieprasījuma iesniedzējam varētu radīt nelabvēlīgas sekas (kaitējumu), ja tie tiktu izpausti;
- vai turpmākie pieprasījumi attiecas uz tā paša vai cita veida informāciju vai apstrādes darbībām<sup>102</sup>.

**39. piemērs (galdnieks).** Datu subjekts **ik pēc diviem mēnešiem** iesniedz piekļuves pieprasījumus galdniekam, kas viņam izgatavojis galdu. Galdnieks pilnībā atbildēja uz pirmo pieprasījumu. Pieņemot lēmumu par to, vai ir pagājis saprātīgs intervāls, būtu jāņem vērā, ka galdnieks apstrādā un vāc persondatus tikai reizēm (pirmā aizzīme iepriekš) un nevis savas pamatdarbības ietvaros, un ir vēl jo mazāk iespējams, ka galdnieks bieži sniedz pakalpojumus vienam un tam pašam datu subjektam. Šajā gadījumā galdnieks datu subjektam sniedza ne vairāk kā vienu pakalpojumu, tāpēc ir maz ticams, ka datu kopā, kas attiecas uz datu subjektu, ir notikušas izmaiņas. Jo īpaši ņemot vērā apstrādāto persondatu raksturu un apjomu, ar apstrādi saistītos riskus var uzskatīt par nelieliem (otrā aizzīme iepriekš), piemēram, apstrādes nolūks (rēķinu izrakstīšana un ierakstu glabāšanas pienākuma izpilde) datu subjektam nelabvēlīgas sekas, visticamāk, neradīs (trešā aizzīme iepriekš). Turklāt pieprasījums attiecas uz to pašu informāciju, uz kuru attiecas pēdējais pieprasījums (ceturtā aizzīme iepriekš). Tādējādi šādus pieprasījumus var uzskatīt par pārmērīgiem, jo tie atkārtojas.

**40. piemērs (sociālo mediju platforma).** Sociālo mediju platforma, kuras pamatdarbība ir datu subjekta persondatu vākšana un/vai apstrāde, veic plaša mēroga sarežģītas un pastāvīgas apstrādes darbības. Datu subjekts, kas izmanto platformas pakalpojumus, **ik pēc trim mēnešiem** iesniedz piekļuves pieprasījumus. Šajā gadījumā biežas izmaiņas datu subjekta persondatos ir ļoti iespējamās (pirmā aizzīme iepriekš), plašais savākto datu klāsts ietver izrietošus sensitīvus persondatus (otrā aizzīme iepriekš), ko apstrādā, lai datu subjektam rādītu attiecīgu saturu un tīkla dalībniekus (trešā aizzīme). Šādos apstākļos ik pēc trim mēnešiem iesniegtus piekļuves pieprasījumus principā nevar uzskatīt par pārmērīgiem to atkārtošanās dēļ.

**41. piemērs (kredītaģentūras).** Tāpat kā sociālo tīklu gadījumā, nevar izslēgt, ka izmaiņas kredītaģentūru rīcībā esošajos attiecīgajos datos notiks daudz īsākos intervālos nekā citās jomās (pirmā aizzīme iepriekš). Tās izriet no daudziem faktoriem, par kuriem datu subjekts kā persona, kas nav šādas aģentūras darbinieks, parasti nezina darījumdarbības modeļa sarežģītības dēļ. Tāpēc atbildi uz jautājumu par to, kādu veidu datus pārzinis ir savācis vērtējuma vērtības aprēķināšanai un kuri no tiem pašlaik ir iekļauti aprēķinā, var sniegt tikai pati kredītaģentūra. Turklāt kredītaģentūru veiktā datu apstrāde un no tās izrietošā vērtējuma vērtība var tālejoši ietekmēt datu subjektu attiecībā uz

<sup>102</sup> Ja turpmākais pieprasījums attiecas uz tā paša veida informāciju tvēruma UN laika ziņā, runa nav par pārmērīgumu, bet gan par papildu kopijas pieprasījumu, sk. 2.2.2.2. iedaļu.

plānotajiem juridiskajiem darījumiem, piemēram, pirkuma, nomas vai līzings līgumu noslēgšanu (trešā aizzīme iepriekš).

Nav iespējams vispārīgi noteikt nevienu konkrētu intervālu, kurā turpmāka piekļuves pieprasījuma iesniegšanu varētu uzskatīt par pārmērīgu saskaņā ar VDAR 12. panta 5. punkta otro teikumu. Drīzāk ir jāņem vērā konkrētā gadījuma apstākļi kopumā. Tomēr, ņemot vērā datu apstrādes nozīmi datu subjektu ikdienas dzīvē, var pieņemt, ka **viena gada intervāls** starp sniegto bezmaksas informāciju jebkurā gadījumā būs pārāk liels, lai pieprasījumu uzskatītu par pārmērīgu. Ja intervāls starp iesniegtajiem pieprasījumiem ir ļoti īss, izšķirošajam faktoram vajadzētu būt tam, vai datu subjektam ir iemesls uzskatīt, ka informācija vai apstrāde kopš pēdējā pieprasījuma ir mainījusies. Piemēram, ja datu subjekts ir veicis finanšu darījumu, piemēram, saņēmis aizdevumu, datu subjektam vajadzētu būt tiesīgam pieprasīt piekļuvi kredītinformācijai, pat ja šāds pieprasījums tika iesniegts un uz to tika atbildēts neilgi pirms tam.

186. Ja informācija ir viegli sniedzama, izmantojot elektroniskus līdzekļus vai attālinātu piekļuvi drošai sistēmai, kas nozīmē, ka šādu pieprasījumu izpilde pārzini faktiski neapgrūtina, ir maz ticams, ka turpmākus pieprasījumus var uzskatīt par pārmērīgiem.
187. Ja pieprasījums pārklājas ar iepriekšēju pieprasījumu, tad pieprasījumu, kas pārklājas, parasti var uzskatīt par pārmērīgu, ja un ciktāl tas attiecas uz tieši to pašu informāciju vai apstrādes darbībām un pārzinis vēl nav izpildījis iepriekšējo pieprasījumu, nesasniedzot “nepamatotas kavēšanās” stāvokli (sk. VDAR 12. panta 3. punktu). Tādējādi praksē abus pieprasījumus varētu apvienot.
188. Tas, ka informācijas vai kopijas sniegšana datu subjektam pārzinim prasītu daudz laika un pūļu, pats par sevi pieprasījumu nevar padarīt par pārmērīgu<sup>103</sup>. Liels skaits apstrādes darbību parasti ir saistīts ar lielākām pūlēm, izpildot piekļuves pieprasījumus. Tomēr, kā minēts iepriekš, noteiktos apstākļos pieprasījumus var uzskatīt par pārmērīgiem citu iemeslu dēļ, kas nav to atkārtošanās. EDAK uzskata, ka tas jo īpaši attiecas uz gadījumiem, kad VDAR 15. pants tiek izmantots ļaunprātīgi, proti, uz gadījumiem, kad datu subjekti pārmērīgi izmanto piekļuves tiesības vienīgi ar nolūku pārzinim radīt kaitējumu.
189. Ņemot vērā iepriekš minēto, pieprasījums nebūtu jāuzskata par pārmērīgu, pamatojoties uz to, ka:
- datu subjekts nav norādījis pieprasījuma iemeslus vai pārzinis pieprasījumu uzskata par bezjēdzīgu;
  - datu subjekts lieto nepiemērotu vai nepieklājīgu valodu;
  - datu subjekts plāno izmantot datus, lai iesniegtu turpmākas prasības pret pārzini<sup>104</sup>.
190. No otras puses, pieprasījumu var uzskatīt par pārmērīgu, piemēram, ja:
- persona iesniedz pieprasījumu, bet vienlaikus piedāvā to atsaukt apmaiņā pret kāda veida labumu no pārziņa, vai
  - pieprasījums ir ļaunprātīgs un tiek izmantots, lai aizskartu pārzini vai tā darbiniekus, un tā vienīgais nolūks ir radīt traucējumus, piemēram, pamatojoties uz to, ka:

<sup>103</sup> Bez proporcionalitātes pārbaudes, sk. iepriekš 166. punktu.

<sup>104</sup> Tas neskar piemērojamās valsts tiesību aktus, kas atbilst VDAR 23. panta prasībām, sk. 6.4. nodaļu.



- persona pašā pieprasījumā vai citos paziņojumos ir skaidri norādījusi, ka viņas vienīgais nolūks ir izraisīt traucējumus, vai
- persona kampaņas veidā sistemātiski, piemēram, reizi nedēļā, sūta pārzinim dažādus pieprasījumus nolūkā izraisīt traucējumus un tos izraisot<sup>105</sup>.

### 6.3.3 Sekas

191. Acīmredzami nepamatota vai pārmērīga piekļuves tiesību pieprasījuma gadījumā pārziņi saskaņā ar VDAR 12. panta 5. punktu var vai nu pieprasīt saprātīgu samaksu (ņemot vērā administratīvās izmaksas, kas saistītas ar informācijas vai saziņas nodrošināšanu vai pieprasītās darbības veikšanu), vai atteikties izpildīt pieprasījumu.
192. EDAK norāda, ka, no vienas puses, pārziņiem parasti nav pienākuma pieprasīt saprātīgu samaksu, pirms tie atsakās reaģēt uz pieprasījumu. No otras puses, tie arī nevar pilnīgi brīvi izvēlēties starp abām alternatīvām. Faktiski pārziņiem ir jāpieņem adekvāts lēmums atkarībā no gadījuma konkrētajiem apstākļiem. Lai arī ir grūti iedomāties, ka saprātīgas samaksas iekasēšana ir piemērots pasākums acīmredzami nepamatotu pieprasījumu gadījumā, bieži vien saskaņā ar pārredzamības principu, būs lietderīgāk pieprasīt samaksu par pārmērīgiem pieprasījumiem nekā kompensāciju par administratīvajām izmaksām, ko rada atkārtoti pieprasījumi.
193. Pārziņiem jāspēj uzskatāmi parādīt, ka pieprasījums ir acīmredzami nepamatots vai pārmērīgs (VDAR 12. panta 5. punkta trešais teikums). Tāpēc ir ieteicams nodrošināt, lai attiecīgie fakti tiktu pienācīgi dokumentēti. Saskaņā ar VDAR 12. panta 4. punktu, ja pārziņi pilnīgi vai daļēji atsakās izpildīt piekļuves pieprasījumu, tiem nekavējoties un ne vēlāk kā viena mēneša laikā pēc pieprasījuma saņemšanas ir jāinformē datu subjekts par
  - iemesliem;
  - tiesībām iesniegt sūdzību uzraudzības iestādei;
  - iespēju vērsties tiesā.
194. Pirms saprātīgas samaksas pieprasīšanas, pamatojoties uz VDAR 12. panta 5. punktu, pārziņiem datu subjekti būtu jāinformē par savu nodomu to darīt. Datu subjektiem ir jādod iespēja izlemt, vai viņi atsauks pieprasījumu, lai izvairītos no samaksas.
195. Nepamatotus piekļuves tiesību pieprasījumu noraidījumus var uzskatīt par datu subjektu tiesību pārkāpumiem saskaņā ar VDAR 12.–22. pantu, un tāpēc uz tiem var attiekties kompetento uzraudzības iestāžu korektīvo pilnvaru īstenošana, arī administratīvi naudas sodi, pamatojoties uz VDAR 83. panta 5. punkta b) apakšpunktu. Ja datu subjekti uzskata, ka viņu datu subjekta tiesības ir pārkāptas, viņiem ir tiesības iesniegt sūdzību, pamatojoties uz VDAR 77. pantu.

## 6.4 Iespējamie ierobežojumi Savienības vai dalībvalstu tiesību aktos, pamatojoties uz VDAR 23. pantu, un atkāpes

---

<sup>105</sup> “Sistemātiska sūtīšana kampaņas veidā” nozīmē, ka pieprasījumus, kurus varētu viegli apvienot vienā, datu subjekts mākslīgi sadala ne tikai dažos, bet daudzos atsevišķos elementos ar acīmredzamu nodomu izraisīt traucējumus.

196. VDAR 15. pantā paredzēto pienākumu un tiesību darbības jomu var ierobežot ar leģislatīviem pasākumiem Savienības vai dalībvalstu tiesību aktos<sup>106</sup>.
197. Pārziņiem, kuri plāno izmantot ierobežojumu, pamatojoties uz valsts tiesību aktiem, ir rūpīgi jāpārbauda attiecīgo valsts tiesību aktu prasības. Turklāt ir svarīgi norādīt, ka tādiem piekļuves tiesību ierobežojumiem dalībvalstu (vai Savienības) tiesību aktos, kuru pamatā ir VDAR 23. pants, ir stingri jāatbilst šajā pantā paredzētajiem nosacījumiem. EDAK ir izdevusi Pamatnostādnes 10/2020 par ierobežojumiem saskaņā ar VDAR 23. pantu, kurās šajā saistībā ietverti papildu skaidrojumi. Attiecībā uz piekļuves tiesībām EDAK atgādina, ka pārziņiem ierobežojumi būtu jāatceļ, tiklīdz vairs nepastāv tos pamatojoši apstākļi<sup>107</sup>.
198. Leģislatīvos pasākumos, kas saistīti ar ierobežojumiem saskaņā ar VDAR 23. pantu, var arī paredzēt, ka tiesību īstenošana tiek aizkavēta, tiesības tiek īstenotas daļēji vai ierobežotas ar noteiktām datu kategorijām vai ka tiesības var īstenot netieši, iesaistot neatkarīgu uzraudzības iestādi<sup>108</sup>.

---

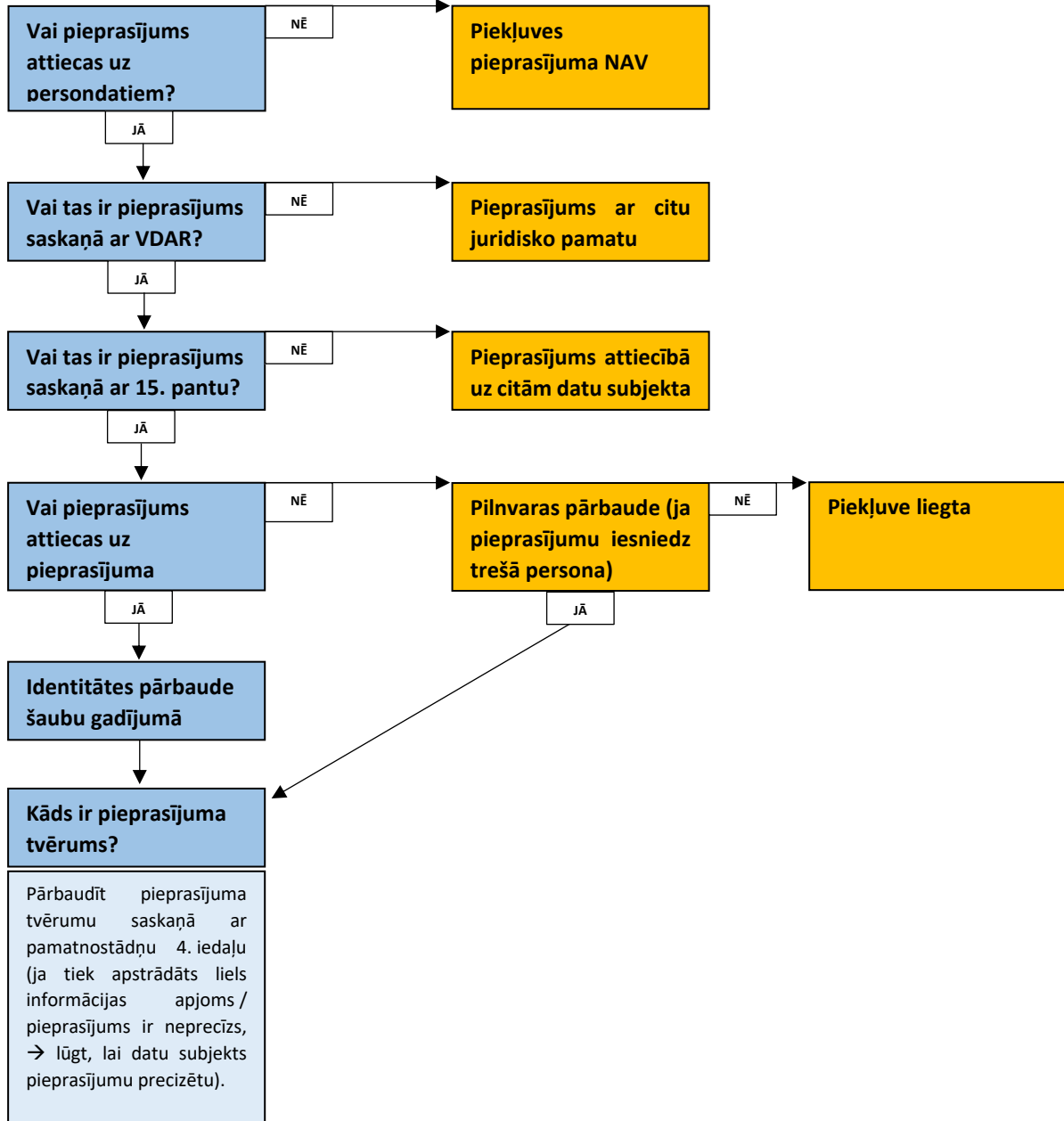
<sup>106</sup> Sk., piem., Vācijas Federālā datu aizsardzības likuma (*BDSG*) 32.–37. pantu, Norvēģijas persondatu likuma 16. un 17. pantu un Zviedrijas Datu aizsardzības likuma 5. nodaļu.

<sup>107</sup> Pamatnostādņu 10/2020 par ierobežojumiem saskaņā ar VDAR 23. pantu (versija 2.0), kas pieņemtas 2021. gada 13. oktobrī, 76. punkts.

<sup>108</sup> Pamatnostādņu 10/2020 par ierobežojumiem saskaņā ar VDAR 23. pantu (versija 2.0), kas pieņemtas 2021. gada 13. oktobrī, 12. punkts. Piemēram, Vācijas Federālā datu aizsardzības likuma 34. panta 3. punktā ir noteikts, ka gadījumā, kad valsts iestāde noteiktu ierobežojumu dēļ datu subjektam nesniedz informāciju, izpildot piekļuves tiesību pieprasījumu, šāda informācija pēc datu subjekta pieprasījuma jāsniedz federālajai uzraudzības iestādei, ja vien (iestādes, uz kuru attiecas pieprasījums) atbildīgā augstākā federālā iestāde konkrētajā gadījumā nenosaka, ka tas apdraudētu federācijas vai federālās zemes drošību. Itālijas Datu aizsardzības kodekss paredz netiešu piekļuvi (ar iestādes starpniecību), ja piekļuve varētu negatīvi ietekmēt vairākas intereses (piemēram, intereses nelikumīgi iegūtu līdzekļu legalizācijas novēršanā), sk. Itālijas Datu aizsardzības kodeksa 2.L pantu.

# PIELIKUMS. PLŪSMKARTE

## 1. posms. Kā interpretēt un novērtēt pieprasījumu?



## 2. posms. Kā atbildēt uz pieprasījumu (1)?

Piekļuves tiesību 3 galvenie komponenti (15. panta struktūra)		
Apstiprinājums par to, vai persondati tiek vai netiek apstrādāti	Piekļuve persondatiem	Papildu informācija par nolūkiem, saņēmējiem u. c. (15. panta 1. punkta a) līdz h) apakšpunkts)

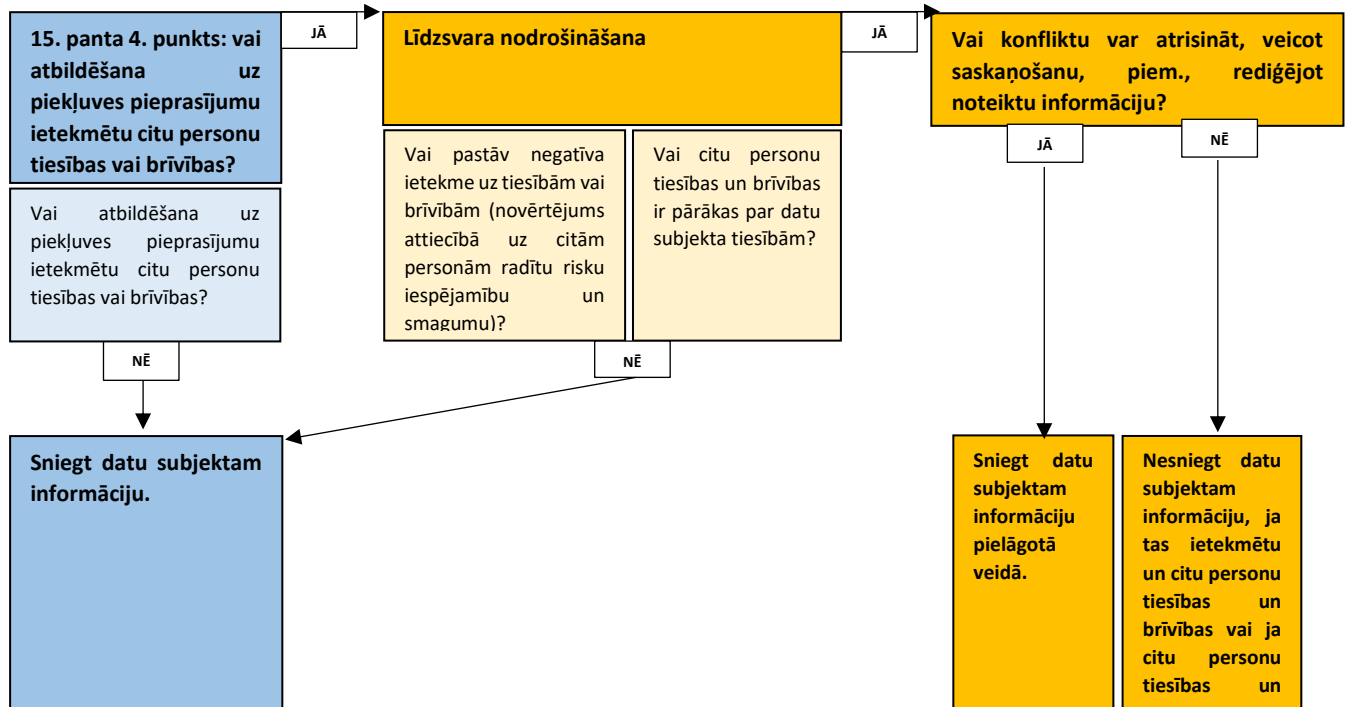
## 2. posms. Kā atbildēt uz pieprasījumu (2)?

Atbilstošu pasākumu veikšana			
12. panta 1. punkts: kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā	12. panta 2. punkts: veicināt piekļuves tiesību īstenošanu		
Izvēlēties starp dažādiem līdzekļiem	Ja nav citas vienošanās, nodrošināt kopiju (15. panta 3. punkts)	Vajadzības gadījumā izmantot vairāku līmeņu pieeju (visatbilstošāk)	Termiņš — bez nepamatotas kavēšanās, jebkurā gadījumā viena mēneša laikā (izņēmuma gadījumos pagarinājums vēl uz diviem mēnešiem)

## 2. posms. Kā atbildēt uz pieprasījumu (3)?

Kā pārzinis var izgūt visus datus par datu subjektu?			
Definēt meklēšanas kritērijus — pamatojoties uz datu subjekta sniegto informāciju, citu pārziņa rīcībā esošo informāciju par datu subjektu un faktoriem, pēc kuriem dati ir strukturēti (piemēram, klienta numurs, IP adrese, profesionālais nosaukums, ģimenes attiecības utt.).	Norādīt visas tehniskās funkcijas, kas var būt pieejamas datu izgūšanai.	Meklēt visās attiecīgajās IT sistēmās un ar IT nesaistītās kartotēkās.	Apkopot, iegūt vai citādi savākt datus, kuri attiecas uz datu subjektu, tādā veidā, kas pilnā mērā atspoguļo apstrādi, t. i., ietver visus datu subjekta persondatus un ļauj datu subjektam zināt par apstrādi un pārliecināties par tās likumīgumu. Informācijas izgūšanu varētu veikt katrā gadījumā atsevišķi vai attiecīgā gadījumā izmantojot pārziņa jau ieviestu integrētu privātuma aizsardzības rīku.

### 3. posms. Ierobežojumu pārbaude (1)



### 3. posms. Ierobežojumu pārbaude (2)

