

Baltijas valstu uzraudzības iestāžu kopīgās pārbaudes secinājumi par personas datu apstrādes atbilstību īstermiņa transportlīdzekļu nomas jomā

I. VISPĀRĪGA INFORMĀCIJA

Baltijas valstu uzraudzības iestādes (Lietuvas Datu aizsardzības inspekcija, Latvijas Datu valsts inspekcija, Igaunijas Valsts datu aizsardzības inspekcija, turpmāk - uzraudzības iestādes) vienojās veikt preventīvu pārbaudi par personas datu apstrādes atbilstību īstermiņa transportlīdzekļu nomas jomā.

Uzraudzības iestādes veica preventīvu pārbaudi īstermiņa transportlīdzekļu nomas pakalpojumu jomā, lai izvērtētu, vai pakalpojumu sniedzēji, kas darbojas Igaunijā, Latvijā un Lietuvā un piedāvā īstermiņa transportlīdzekļu nomas pakalpojumus fiziskām personām Baltijas valstīs, ievēro Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvas 95/46 EK (Vispārīgā datu aizsardzības regula) (turpmāk – Datu regula) prasības.

Par koordinēto uzraudzības pasākumu īstenošanu iestādes vienojās 2021. gada sanāsmē, kad tika pieņemts lēmums 2022./2023. gadā Igaunijā, Latvijā un Lietuvā organizēt nozaru uzraudzību ar mērķi izstrādāt ieteikumus personas datu apstrādes un aizsardzības procesu uzlabošanai kādā nozarē.

Uzraudzības iestādes vienojās par šādiem kritērijiem, pēc kuriem tika izvēlēti pakalpojumu sniedzēji pārbaudes veikšanai:

- ✓ Tie piedāvā transportlīdzekļu, tostarp elektrisko motorolleru, īstermiņa nomu (automobiļu koplietošanu);
- ✓ Galvenais pakalpojumu saņēmējs ir fiziska persona;
- ✓ Darbības vieta - Baltijas valstis.

II. Pārbaudes darbības joma

Visas uzraudzības iestādes ievēroja vismaz dažus no turpmāk minētajiem kritērijiem, vienlaikus saglabājot katras iestādes autonomiju attiecībā uz papildu apsvērumu iekļaušanu mērķauditorijas atlasē. Tika nodrošināta galveno pārbaudes aspektu saglabāšana: personas datu apstrāde, īstermiņa transportlīdzekļu nomas pakalpojumu sniegšana fiziskām personām un atbilstība Datu regulas prasībām.

- ✓ Uzņēmumi, kas sniedz pakalpojumus visās Baltijas valstīs, un tādi uzņēmumi, kas sniedz pakalpojumus vismaz divās Baltijas valstīs.
- ✓ uzņēmumi, kuru pārzinis vai kopīgais pārzinis (personas, kas atbildīgas par personas datu aizsardzību, kā noteikts Datu regulas 4. panta 7. un 8. punktā) atrodas vienā no Baltijas valstīm (konkrēto uzņēmumu pārbaudi ierosina valsts, kurā atrodas galvenā uzņēmējdarbības vieta);
- ✓ uzņēmumi par kuriem tiek iesniegta lielākā daļa sūdzību/pieteikumu (salīdzinājumā ar citiem tā paša tirgus uzņēmumiem);
- ✓ uzņēmumi, kas aizņem lielāko daļu no transportlīdzekļu nomas pakalpojumu tirgus;
- ✓ uzņēmumi, kurus (daļēji) finansē patērētāji (Tuul Mobility OÜ ir publiski emitējis obligācijas);
- ✓ Uzņēmumi, kas pazīstami ar to, ka izmanto plaša mēroga uz patērētājiem orientētu reklāmu.

Ņemot vērā minētos kritērijus, uzraudzības iestādes izvēlējās astoņus uzņēmumus, kas sniedz īstermiņa transportlīdzekļu nomas pakalpojumus Baltijas valstu teritorijā (turpmāk – uzņēmumi):

1. SIA "TRANSPORTS" (SIXT);
2. Ltd. SLYFOX (CARGURU);
3. SIA RIDE;
4. SIA "ETERNA ELECT" (Skoka);
5. UAB "Prime leasing" (CityBee).
6. Bolt Operations OÜ;
7. ELMO Rent AS (pakalpojumi ir pārtraukti līdz ziņojuma sniegšanai);
8. Tuul Mobilitāte OÜ.

Pārbaudes ietvaros tika izvērtēts, vai personas dati, ko uzņēmumi apstrādā:

- ✓ ir atbilstoši (Datu regulas 5. panta 1. punkta c) apakšpunkts);
- ✓ tiek apstrādāti saskaņā ar mērķi (Datu regulas 5. panta 1. punkta b) apakšpunkts);
- ✓ atbilst glabāšanas ierobežojuma principam (Datu regulas 5. panta 1. punkta e) apakšpunkts);
- ✓ ir atbilstošs tiesiskais pamats (Datu regulas 6. pants).

Veicot koordinētas uzraudzības darbības uzraudzības iestāžu mītnes valstīs, uzraudzības iestādes ir nonākušas pie salīdzinoši līdzīgiem secinājumiem par nekonsekveni uzņēmumu personas datu apstrādē transportlīdzekļu īstermiņa nomas jomā, kas atrodami tālāk sadaļā.

III. INSPEKCIJAS SECINĀJUMI

1. Atbilstoša tiesiskā pamata noteikšana.

Viena no būtiskākajām neatbilstībām, kas konstatēta transportlīdzekļu nomas pakalpojumu sniedzēju personas datu apstrādē, ir neatbilstoša tiesiskā pamata izvēle vai nespēja pietiekami pamatot, kamdēļ šāds pamats ir izvēlēts. Dažkārt tiesiskais pamats un apstrādāto personas datu apjoms, kas norādīts privātuma politikā vai datu apstrādes noteikumos, nesakrīt ar informāciju, ko uzņēmumi sniedza uzraudzības iestādēm. Tāpat tika konstatēti gadījumi, kad visām apstrādes darbībām tika piemērots viens tiesiskais pamats, pat attiecībā uz darbībām, kurām šis pamats nebija piemērots. Personas datu apstrādes tiesiskais pamats, kuru uzņēmumi izmantoja visvairāk, ir līguma, kura līgumslēdzēja puse ir datu subjekts, izpilde vai nepieciešamība veikt pasākumus pirms līguma noslēgšanas (Datu regulas 6. panta 1. punkta b) apakšpunkts). Šis tiesiskais pamats tika izmantots arī personas datu apstrādei, kas nav nepieciešama līguma izpildei. Dažiem apstrādes veidiem pareizais tiesiskais pamats būtu leģitīmas intereses (Datu regulas 6. panta 1. punkta f) apakšpunkts). Nepareizi izvēloties tiesisko pamatu, daži uzņēmumi nav veikuši Datu regulas 6. panta 1. punkta f) apakšpunktā paredzēto leģitīmo interešu izvērtēšanas pārbaudi, kā rezultātā nav nodrošināta atbilstoša personas datu apstrādes pamatojuma izvērtēšana.

2. Datu apjoms.

Lai gan pieprasīto personas datu apjoms katram klientam ir atšķirīgs, kopējais informācijas apjoms, kas uzņēmumiem ir nepieciešams, lai sniegtu pakalpojumus klientiem, ir

līdzīgs. Daži uzņēmumi atsevišķi nepieprasa konkrētu informāciju no klienta, tādējādi pieprasot mazāku datu apjomu kā obligāto aizpildīto informāciju, piemēram, nepieprasa sociālās apdrošināšanas numuru vai dzimšanas datumu. Tomēr minētā informācija tiek iegūta netiešā veidā, piemēram, lūdzot nosūtīt vadītāja apliecības kopiju, kurā ir iepriekš minētie dati.

Dažos gadījumos pieprasīto personas datu apjoms, ja persona vēlas saņemt pakalpojumu un tai ir jāiesniedz pieprasījums, atšķiras no datu apjoma, kas nepieciešams, lai saņemtu pakalpojumu, kas noteikts uzņēmumu tīmekļa vietņu privātuma politikās.

3. Pārredzamība.

Vairākos uzņēmumos tika konstatēti pārkāpumi attiecībā uz pārredzamības principa ievērošanu, kas izpaudās kā nespēja nodrošināt datu subjektiem skaidru un jēgpilnu informāciju par viņu personas datu apstrādi. Tika konstatēts, ka:

- ✓ Uzņēmuma privātuma politika un pakalpojumu sniegšanas noteikumi neietver visu Datu regulas III nodaļā minēto informāciju par personas datu apstrādi;
- ✓ Ne uzņēmuma privātuma politikā, ne pakalpojumu sniegšanas noteikumos nav skaidri norādīts, kādos gadījumos un kādā veidā tiek vai var tikt pārbaudīti klienta dokumenti, kas apliecina transportlīdzekļa vadīšanas tiesības, lai pārliecinātos par autovadītāja apliecības derīgumu;
- ✓ Pārbaudes laikā tika konstatēts, ka uzņēmumi apstrādes ierakstos nošķir "aizdomīgus" klientus, bet informācija par klientu klasificēšanu par "aizdomīgiem" nav sniegta ne privātuma politikā, ne uzņēmuma pakalpojumu sniegšanas noteikumos. Noteiktās situācijās uzraudzības iestādei sniegtā informācija bija nepilnīga un neatbilda uzņēmuma privātuma politikā un pakalpojumu sniegšanas noteikumos publicētajai informācijai.

4. Glabāšanas periodi.

Lai gan vairumā gadījumu šajā aspektā netika konstatētas neatbilstības personas datu apstrādē, dažos gadījumos uzņēmumu norādītie glabāšanas periodi noteikti bija pārāk neskaidri (piemēram, dati tiek glabāti tik ilgi, cik tas ir nepieciešams vai atļauts saskaņā ar piemērojamiem tiesību aktiem, vai lai sasniegtu privātuma politikā norādītos mērķus). Tāpēc no atbilžu kopuma un publiski pieejamās informācijas nav skaidrs, cik ilgi un kādu iemeslu dēļ tiek glabāti noteikta veida dati. Dažos uzņēmumos tika konstatētas neatbilstības tehniskajās prasībās, kas zināmā mērā ir saistītas ar uzglabāšanas laiku. Proti, klientu personas dati netika dzēsti noteiktos apstākļos. Lai gan neatbilstība ir novērsta, šādas situācijas nerastos, ja

uzņēmums būtu veicis visus nepieciešamos tehniskos pasākumus, lai nodrošinātu savlaicīgu datu apstrādes atbilstību, tostarp apstrādes darbību periodisku pārskatīšanu.

5. Biometriskie dati

Ņemot vērā uzņēmumu sniegtās atbildes, var secināt, ka vairumā gadījumu klientu identifikācija, kā arī personas datu turpmāka apstrāde notiek, neizmantojot biometriskos datus. Tomēr dažos gadījumos, lai apstiprinātu identitāti, klienta sejas attēla dati (cita starpā) tiek apstrādāti, pamatojoties uz datu subjektu piekrišanu (Datu regulas 9. panta 2. punkta a) apakšpunkts). Lai izpildītu Datu regulas 7. panta prasības un nodrošinātu, ka piekrišana tiek sniegta brīvi un datu subjektam ir izvēles iespējas attiecībā uz piekrišanas sniegšanu, uzņēmumi privātuma politikā iekļauj informāciju par iespēju neizmantot biometriskos datus, t. i., klienti var sazināties ar uzņēmumu, kas var piedāvāt alternatīvu biometriskajiem datiem. Tomēr ne uzņēmuma pakalpojumu sniegšanas noteikumi, ne privātuma politika nenodrošina klientiem līdzvērtīgu, brīvi izvēlētu alternatīvu, kas ļauj neizmantot biometriskos datus.

VI. IETEIKUMI

1. Atbilstoša tiesiskā pamata noteikšana.

Datu regulas 6. panta 1. punkta b) apakšpunkts ir jāinterpretē šauri. Tas nav piemērojams gadījumos, kad apstrāde nav nepieciešama līguma izpildei, bet uzņēmums to vienpusēji nosaka uzņēmuma interešu izpildei. Turklāt tas, ka uz daļu no datu apstrādes attiecas līgums, nenozīmē, ka šāda apstrāde ir nepieciešama tās veikšanai. Piemēram, 6. panta 1. punkta b) apakšpunkts nav piemērots tiesiskais pamats klientu profilēšanai vai komerciālu paziņojumu nosūtīšanai. Pat ja šādas apstrādes darbības ir īpaši norādītas līguma smalkajā drukā, tas nenozīmē, ka datu apstrāde ir "nepieciešama" līguma izpildei.

No otras puses, gadījumos, kad apstrādi neuzskata par nepieciešamu līguma izpildei un pakalpojumu var sniegt, neveicot konkrēto apstrādi, būtu jānosaka cits tiesiskais pamats. Uzņēmumi pēc katras apstrādes veida izvērtēšanas var izmantot citu Datu regulas noteikto tiesisko pamatu, piemēram, legītīmās intereses (6. panta 1. punkta f) apakšpunkts) vai piekrišanu (6. panta 1. punkta a) apakšpunkts), ja ir izpildīti attiecīgie nosacījumi.

Datu regulas 6. panta 1. punkta f) apakšpunkts (apstrāde ir nepieciešama pārziņa vai trešās personas legitīmajām interesēm, izņemot gadījumus, kad datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama personas datu aizsardzība, ir svarīgākas par šādām interesēm, jo

īpaši, ja datu subjekts ir bērns) attiecas uz situācijām, kad apstrāde ir netieši saistīta ar tāda līguma izpildi, kura līgumslēdzēja puse ir datu subjekts.

Saistībā ar transportlīdzekļu nomu tā varētu būt transportlīdzekļa atrašanās vietas (GPS), transportlīdzekļu uzraudzības un zādzību novēršanas datu apstrāde. Tomēr GPS izmantošanai ir atšķirīgs tiesiskais pamats atkarībā no datu apstrādes nolūka. Piemēram, Datu regulas 6. panta 1. punkta b) apakšpunktu varētu piemērot, lai noskaidrotu tā klienta identitāti, kurš ir pārkāpis Ceļu satiksmes noteikumus un tādējādi pārkāpis līgumu. Datu regulas 6. panta 1. punkta c) apakšpunkts attiecas arī uz uzņēmuma pienākumu paziņot personas datus administratīva pārkāpuma gadījumā. Un GPS izmantošana klienta ierīcē ietilpst 6. panta 1. punkta a) apakšpunktā, ja datu apstrādes mērķis ir nodrošināt klientam precīzus attālumus no viņa atrašanās vietas līdz transportlīdzeklim.

Ja klientu biometriskos datus apstrādā, pamatojoties uz piekrišanu, tai ir jāatbilst “derīgas” piekrišanas elementiem.¹ Datu subjekta “piekrišana” ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei (Datu regulas 4. panta 11. punkts). Cita starpā jāatzīmē, ka elements “brīvprātīga” nozīmē datu subjektu reālu izvēli un kontroli. Vispārīgais noteikums Datu regulas paredz, ka tad, ja datu subjektam nav reālas izvēles, viņš jūtas spiests sniegt piekrišanu vai viņam radīsies negatīvas sekas, ja viņš nepiekrīt, piekrišana nebūs spēkā.² Jāatzīmē, ka, lai nodrošinātu piekrišanas brīvprātīgumu, datu pārzinim būtu jānodrošina alternatīva, nevis pārāk apgrūtināša identitātes pārbaudes metode.

Tālāk redzamajā tabulā ir apkopoti visbiežāk konstatētie personas dati un personas datu apstrādes nolūki, kā arī to iespējamais tiesiskais pamats. Jāņem vērā, ka katra situācija ir jāizvērtē individuāli, un atbilstošākais tiesiskais pamats var atšķirties atkarībā no konkrētajiem apstākļiem.

¹ Sk. Eiropas Datu aizsardzības kolēģijas Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679.

² Sk. Eiropas Datu aizsardzības kolēģijas Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulas 2016/679 13. apsvērumu.

Personas dati**Tiesiskais pamats (Datu regulas 6. pants)**

Personas identifikācijas dati (vārds, uzvārds, personas kods / identifikācijas numurs, dzimšanas datums), sejas attēls (biometriskie dati)	6. panta 1. punkta b) apakšpunkts - lai identificētu personas identitāti, lai noslēgtu līgumu 9. panta 2. punkta a) apakšpunkts – sejas atpazīšanas rīka izmantošana
Atrašanās vietas dati (GPS dati)	6. panta 1. punkta f) apakšpunkts Autostāvvietas uzraudzība, zādzību novēršana 6. panta 1. punkta b) apakšpunkts Noteikt tā klienta identitāti, kurš izdarījis ceļu satiksmes noteikumu pārkāpumu un līdz ar to pārkāpis līgumu 6. panta 1. punkta c) apakšpunkts Pienākums paziņot personas datus administratīva pārkāpuma gadījumā 6. panta 1. punkta a) apakšpunkts Nodrošināt klientam precīzus attālumus no viņa atrašanās vietas līdz transportlīdzekļiem
Dzīvesvietas pasta adrese (pilsēta, iela, mājas Nr., dzīvokļa Nr.)	6. panta 1. punkta b) apakšpunkts Lai nosūtītu oficiālos paziņojumus
Kontaktinformācija (tālruna numurs, e-pasta adrese)	6. panta 1. punkta b) apakšpunkts Saziņai saistībā ar līguma izpildi (piemēram, lai informētu par jauniem pieejamiem transportlīdzekļiem, izmaiņām maksājumu politikā utt.) 6. panta 1. punkta f) apakšpunkts Saziņai, lai samazinātu ceļu satiksmes negadījumu skaitu ātruma pārsniegšanas dēļ (automatizēti zvani klientiem, kuri pārsniedz ātruma ierobežojumu) 6. panta 1. punkta a) apakšpunkts Komercepaziņojumu nosūtīšana
Informācija par autovadītāja apliecību (fotoattēls, apliecības numurs, derīguma termiņš, pašreizējās vadītāja apliecības kategorijas)	6. panta 1. punkta b) apakšpunkts Pārbaudīt personas tiesības vadīt transportlīdzekli un spēkā esošās transportlīdzekļu vadīšanas tiesību kategorijas
Informācija par saņemtajiem administratīvajiem pārkāpumiem	6. panta 1. punkta b), c) un f) apakšpunkts Interesu aizsardzībai un līguma noteikumu pārvaldībai
Informācija par noslēgtu līgumu	6. panta 1. punkta b) apakšpunkts

(noslēgts līgums, izvēlēts pakalpojums, nosacījumi)	Lai kontrolētu un pārvaldītu līgumattiecības saistībā ar pakalpojuma sniegšanu, kā arī nodrošinātu nepieciešamo rīcību situācijās, kas var rasties pēc pakalpojuma termiņa beigām.
Informācija par ceļu satiksmes negadījumiem	6. panta 1. punkta f) apakšpunkts Interesu aizsardzībai, nelaimes gadījumu izvērtēšanai, pakalpojumu kvalitātes uzlabošanai, apdrošināšanas atlīdzības pieprasīšanai
Rēķinu/maksājumu dati Kartes turētāja vārds, uzvārds, kartes numurs, derīguma termiņš un CVC numurs	6. panta 1. punkta b) apakšpunkts Lai saņemtu samaksu par sniegto pakalpojumu 6. panta 1. punkta c) apakšpunkts Lai nodrošinātu maksājumu plūsmu

2. Datu apjoms

Datu minimizēšana jānodrošina jau personas datu apstrādes sākuma posmā, izvairoties no tādu datu vākšanas, kuru apstrāde nav obligāta. Noteiktais mērķis ir jāīsteno, izmantojot tikai minimālo datu apjomu, kas nepieciešams tā sasniegšanai. Tas nozīmē, ka nedrīkst apkopot vairāk datu, nekā ir būtiski nepieciešams pakalpojuma sniegšanai.

Lai noteiktu atbilstošu datu apjomu, jāņem vērā šādi aspekti:

- ✓ Apstrādātajiem personas datiem jābūt atbilstošiem un nepārmērīgiem, ņemot vērā nolūkus, kādos tie tiek apstrādāti;
- ✓ Daži datu ievades lauki būtu jāizstrādā tā, lai tie nedotu lieku vietu tādu datu ievadišanai, kas nav nepieciešami;
- ✓ Nevajadzīgie personas dati ir jādzēš pēc noteiktā laika;
- ✓ Jāveic periodiskas pārbaudes attiecībā uz apstrādājamo personas datu apjomu, to nepieciešamību.

3. Pārredzamība

Ņemot vērā Datu regulas noteikto pārredzamības principu, pārzinim ir jānodrošina personas datu apstrāde, kas ļauj datu subjektam saprast, kādi dati tiek apstrādāti, kādam nolūkam un ar kādu tiesisko pamatu.

Datu subjektiem jābūt piekļuvei visai informācijai par viņu personas datiem, kas tiek vākti, izmantoti, skatīti vai citādi apstrādāti, un par to, cik lielā mērā personas dati tiek vai tiks apstrādāti. Pārredzamības principa pamatā ir prasība, ka visai ar minēto personas datu apstrādi saistītajai informācijai un saziņai ir jābūt viegli pieejamai un viegli saprotamai un ka ir jāizmanto skaidra un

vienkārša valoda. Minētais princips jo īpaši attiecas uz datu subjektu informēšanu par pārziņa identitāti un apstrādes nolūkiem, kā arī uz papildu informāciju, lai nodrošinātu godprātīgu un pārredzamu apstrādi attiecīgajām fiziskajām personām un viņu tiesībām saņemt apstiprinājumu un paziņojumu par to, kuri no viņu personas datiem tiek apstrādāti. Personas būtu jāinformē par riskiem, noteikumiem, aizsardzības pasākumiem un tiesībām, kas saistītas ar personas datu apstrādi, un par to, kā īstenot savas tiesības saistībā ar šādu apstrādi.

Lai īstenotu pārredzamības principu saskaņā ar Datu regulas prasībām, pārzinim ir jāveic šādas darbības:

- ✓ Informācijai par personas datu apstrādi jābūt lietotājam viegli pieejamai un viegli saprotamai skaidrā un vienkāršā valodā. Informācijai jābūt pieejamai tās valsts valodā, kurā darbojas pārzinis. Ja ir vairāki, tad visās valodās. Ja administrators darbojas vairākās valstīs, informācijai jābūt pieejamai katras valsts valodā;
- ✓ Privātuma politikā norādītajai informācijai ir jāatbilst apstrādei, ko pārzinis veic praksē attiecībā uz personas datu apjomu, nolūkiem, tiesiskajiem pamatiem. Privātuma politikā norādītajai informācijai ir jāatspoguļo pārziņa praktiskā rīcība un ar datiem veiktās darbības. Ja apstrādes darbības mainās, attiecīgi jāmaina privātuma politika.
- ✓ Privātuma politikā jānorāda informācija, kas datu subjektam ļauj pilnībā saprast, kas ir pārzinis, kādi dati tiek apstrādāti, kādi ir apstrādes nolūki un tiesiskais pamats, kā arī kā datu subjekts var īstenot savas tiesības. Pamatinformācijai jābūt šādai:
 - uzņēmuma nosaukums un kontaktinformācija;
 - datu aizsardzības speciālista kontaktinformācija (jānorāda e-pasta adrese, kur ar pārzini var sazināties ar jautājumiem par datu aizsardzību vai ar datu subjekta datu piekļuves pieprasījumu);
 - apstrādes nolūks;
 - apstrādāto datu veidi;
 - apstrādes tiesiskais pamats (viens no Datu regulas 6. panta 1. punktā minētajiem tiesiskajiem pamatiem);
 - datu vākšanas avots;
 - datu saņēmēji vai to kategorijas;
 - datu glabāšanas periods/prasības;
 - vai dati tiek nosūtīti trešām valstīm vai starptautiskām organizācijām;
 - norādījumi par to, kā dzēst personas datus.
- ✓ Privātuma politikā ietvertā informācija ir regulāri jāatjaunina, tai ir jāatbilst uzņēmuma pašreizējai personas datu apstrādei;

- ✓ Privātuma politika būtu jāpublicē tīmekļa vietnē vai lietotnē viegli pieejamā vietā.

4. Datu glabāšanas periods

Katram personas datu apstrādes periodam vajadzētu būt skaidram, likumīgam un noteiktam jau personas datu vākšanas laikā. Būtu jāizvērtē datu glabāšanas ilgums, nodrošinot, ka personas datu glabāšanas periods ir stingri ierobežots līdz minimumam. Personas datiem būtu jāietver tikai tas, kas ir nepieciešams nolūkiem, kādos tos apstrādā. Lai varētu laikus identificēt datu apstrādes neatbilstības, uzņēmumiem būtu periodiski jāpārskata savas iekšējās datu apstrādes politikas atbilstība apstrādes darbībām. Tas ir īpaši svarīgi gadījumos, kad ir notikušas apstrādes darbības vai ir sāкта apstrāde jaunam nolūkam. Tas pats attiecas uz tehniskajiem pasākumiem, t. i., to atbilstība būtu periodiski jāpārskata, ņemot vērā pieejamo tehnoloģiju progresu.

Tāpat ne mazāk svarīga ir darbinieku ikgadējā apmācība personas datu apstrādes jomā. Kvalificēts un zinošs darbinieks spēs savlaicīgi identificēt un novērst datu apstrādes neatbilstības. Turklāt regulāra darbinieku apmācība palīdzēs darbiniekiem savā darbā ievērot personas datu apstrādes principus, kas ļaus uzņēmējiem ilgtermiņā izvairīties no finansiāliem un/vai reputācijas zaudējumiem.

Lai īstenotu glabāšanas principu saskaņā ar Datu regulas prasībām, pārzinim ir jāveic šādas darbības:

- ✓ personas dati nebūtu jāglabā ilgāk, nekā tas ir nepieciešams nolūkiem, kādos tos apstrādā;
- ✓ jāizveido atbilstoši mehānismi (noteikumi, procedūras) personas datu automātiskai dzēšanai;
- ✓ ja tas nav iespējams un datus dzēš manuāli, būtu jāveic periodiskas pārbaudes par datu dzēšanas termiņu ievērošanu;
- ✓ personas datu glabāšanas noteikumu/nepieciešamības periodiska pārskatīšana (maksimālais termiņš);
- ✓ jānodrošina darbinieku ikgadēja apmācība personas datu apstrādes jomā;
- ✓ periodiski jāpārskata drošības iestatījumi un piekļuves tiesības;
- ✓ jānosaka skaidri un saprotami glabāšanas periodi. Ja glabāšanas termiņš ir definēts normatīvajā aktā, tad konkrētais termiņš ir jānorāda privātuma politikā.

5. Biometriskie dati

Apstrādājot klienta īpašās kategorijas datus, piemēram, sejas attēla datus, pārzinim ir jānodrošina ne tikai tiesiskais pamats atbilstoši Datu regulas 6. pantam, bet arī jāatsaucas uz kādu no Datu regulas 9. pantā noteiktajiem izņēmumiem, kas atļauj īpašās kategorijas datu apstrādi, neskatoties uz vispārējo aizliegumu.

Biometrisko datu (sejas attēla datu) izmantošana uzņēmumos ir juridiski iespējama tikai ar nepārprotamu piekrišanu. Nepārprotama piekrišana ir viens no izņēmumiem no aizlieguma apstrādāt īpašu kategoriju datus. Tomēr, lai datu subjekta sniegtā piekrišana būtu spēkā, tai ir jāatbilst Datu regulas 7. panta noteikumiem. Tas nozīmē, ka piekrišanai jābūt:

- ✓ brīvi sniegtai;
- ✓ konkrētam mērķim;
- ✓ apzinātai;
- ✓ nepārprotama norāde uz datu subjekta vēlmēm, ar kuru viņš skaidri apstiprinošas darbības veidā dod piekrišanu savu personas datu apstrādei.

Datu subjektiem jābūt nodrošinātai reālai izvēles un kontroles iespējai attiecībā uz savu personas datu apstrādi. Gadījumos, kad datu subjektam nav faktiskas iespējas izvēlēties, kad viņš jūt, ka piekrišana tiek uzspiesta, vai baidās, ka tās nesniegšana radīs negatīvas sekas, piekrišana nav uzskatāma par derīgu. Ja piekrišana tiek noteikta kā neapspriežama pakalpojuma vai līguma daļa, tā netiek uzskatīta par brīvprātīgi sniegtu.

Tādēļ uzņēmumiem ir jāspēj nodrošināt, ka piekrišana tiek sniegta brīvi un ka pastāv reāla alternatīva, ko var izmantot gadījumos, kad datu subjekts nevēlas dot savu piekrišanu vai ir to atsaucis. Kā biometrisku datu alternatīvas izmantošanas piemēru iestādes apsver dokumentu verifikāciju klātienē vai videozvana verifikāciju.

Iestādes neizslēdz citas alternatīvas, tomēr tās uzsver, ka šajos gadījumos ir svarīgi nodrošināt, lai tas neradītu pārmērīgi lielu administratīvo vai citu slogu, tādējādi ietekmējot datu subjektu dot savu piekrišanu.