Datu valsts inspekcija

PERSONAS DATU APSTRĀDE TELEMĀRKETINGA JOMĀ APSTRĀDĀTĀJA STATUSĀ

Vadlīnijas

2023

Saīsinājumi

Inspekcija – Datu valsts inspekcija
Datu regula – Eiropas Parlamenta un Padomes 2016. gada 27. aprīļa Regula Nr. 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula)
ISPL – Informācijas sabiedrības pakalpojumu likums
E–privātuma direktīva – Eiropas Parlamenta un Padomes 2002. gada 12. jūlija direktīva 2002/58/EK par personas datu apstrādi un privātās dzīves aizsardzību elektronisko komunikāciju nozarē (direktīva par privāto dzīvi un elektronisko komunikāciju)
IT – informācijas tehnoloģijas

Vadlīnijās papildus uzmanības pievēršanai tiek izmantots šāds apzīmējums:

Pievērs uzmanību!

Saturs

IEVADS....4
1. TELEMĀRKETINGA REGULĒJOŠO NORMATĪVO AKTU MIJIEDARBĪBA....4
2. APSTRĀDĀTĀJA DEFINĪCIJA....5
3. TIESISKĀS ATTIECĪBAS STARP PĀRZINI UN APSTRĀDĀTĀJU....7
4. "APAKŠAPSTRĀDĀTĀJA" PIESAISTE....9
5. KOMERCIĀLA PAZIŅOJUMA SŪTĪŠANAS TIESISKIE ASPEKTI....10
5.1. Tiesiskais pamats....12
5.2. Informācijas avoti un datubāzes....15
6. APSTRĀDES DROŠĪBA....17
6.1. Vairāklīmeņu drošība....17
6.2. Darbs attālināti....20
6.3. Mākoņpakalpojumi....21

IEVADS

Komerciālas informācijas sūtīšana elektroniskā veidā mūsdienās kļūst arvien izplatītāka. Attīstoties tehnoloģijām un mārketinga metodēm, komerciālas informācijas nosūtīšana, jo īpaši zvanu un īsziņu vai multiziņu veidā, tās saņēmējiem nereti kļūst apgrūtinoša un nevēlama, vienlaikus skarot to tiesības uz privātumu.

Telemārketings pēc būtības ir tirdzniecība un reklāma, izmantojot telefona sakarus, viena no teledarba formām.[1] Praksē telemārketingu nereti izvēlas kā papildu līdzekli, lai elektroniska komerciāla paziņojuma veidā uzņēmumi informētu personas par jaunām precēm vai pakalpojumiem, ar mērķi galvenokārt palielināt pārdošanas apjomus un gūt finansiālu labumu.

Vadlīniju mērķis ir veicināt Datu regulas un ISPL prasību izpildi uzņēmumos, kuru darbības veids ir saistīts ar telemārketingu.

Vadlīnijām ir ieteikuma raksturs, un to mērķauditorija ir uzņēmumi, kuru darbības veids ir saistīts ar telemārketingu, tostarp izejošo zvanu centru darbību, – komersanti, organizācijas vai citas personas, kas veic komercdarbību, saimniecisko darbību un sūta komerciālus paziņojumus apstrādātāja statusā, lai reklamētu preces un pakalpojumus citu personu (pārziņu) vārdā. Tomēr vadlīnijas varētu būt noderīgas ikvienam interesentam, tai skaitā komerciālu paziņojumu saņēmējiem.

[1] Termina skaidrojums pieejams pēc saites: https://tezaurs.lv/telem%C4%81rketings

[2] Papildus informāciju skatīt: The European Data Protection Board (EDPB) Opinion 5/2019 on the interplay between the ePrivacy Directive and the GDPR, in particular regarding the competence, tasks and powers of data protection authorities: https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-52019-interplay-between-eprivacy_en

1. TELEMĀRKETINGA REGULĒJOŠO NORMATĪVO AKTU MIJIEDARBĪBA

Uz personas datu apstrādi, kas veikta telemārketinga ietvaros, attiecināmi divi normatīvie akti, kurus uzrauga Inspekcija, proti, ISPL, kas pieņemts, lai tai skaitā transponētu E–privātuma direktīvu, kā arī Datu regula.

E–privātuma direktīvas un Datu regulas savstarpējo mijiedarbību ir izvērsti analizējusi Eiropas datu aizsardzības kolēģija (EDAK) savā 2019. gada 12. marta viedoklī Nr. 5/2019 par mijiedarbību starp E–privātuma direktīvu un Datu regulu, īpaši attiecībā uz datu aizsardzības iestāžu kompetenci, uzdevumiem un pilnvarām.[2]

Datu regulas 95. pantā un 173. apsvērumā norādītā saikne starp šiem normatīvajiem aktiem, kas apstiprina vispārējā tiesību akta (Datu regulas) un speciālā tiesību akta (ISPL) attiecības.

E–privātuma direktīvas 2. panta f) apakšpunktā norādīts, ka "lietotāja vai abonenta "piekrišana" atbilst datu subjekta piekrišanai Direktīvā 95/46/EK. E–privātuma direktīvas 17. apsvērumā skaidrots: "šajā direktīvā jēdzienam lietotāja vai abonenta piekrišana, neatkarīgi no tā, vai tas ir fiziska vai juridiska persona, jābūt tādai pašai nozīmei, kāda tā ir jēdzienam informācijas objekta piekrišana, kā noteikts un precizēts Direktīvā 95/46/EK. Piekrišanu var sniegt ar jebkuru pienācīgu metodi, kas ļauj lietotājam brīvi sniegt konkrētu un

informētu norādi par savu vēlmi, tostarp atzīmēšanu ar ķeksīti interneta tīmekļa vietnē." Ievērojot Datu regulas 94. pantā noteikto, ka atsauces uz atcelto direktīvu 95/46/EK uzskata par atsaucēm uz šo regulu, uzskatāms, ka E–privātuma direktīvas transponējošo tiesību aktu kontekstā jēdziens "piekrišana" ir analogs Datu regulas 4. panta 11. punktā definētajam "piekrišanas" jēdzienam.

Saskaņā ar Datu regulas 4. panta 11. punktu 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. Līdz ar to piekrišana ir jādod ar skaidri apstiprinošu darbību, kas nozīmē brīvi sniegtu, konkrētu, apzinātu un viennozīmīgu norādi par datu subjekta piekrišanu ar viņu saistīto personas datu apstrādei, piemēram, ar rakstisku, tostarp elektronisku, vai mutisku paziņojumu.

2. APSTRĀDĀTĀJA DEFINĪCIJA

Arī telemārketinga jomā pārziņa jēdzienam un tā mijiedarbībai ar apstrādātāja jēdzienu ir principiāla nozīme Datu regulas piemērošanā, jo tie nosaka, kuras personas atbild par datu aizsardzības noteikumu ievērošanu, kā datu subjekti var īstenot savas tiesības, kuri ir piemērojamie dalībvalstu tiesību akti, un kā var darboties kompetentās datu aizsardzības iestādes.

Datu regulas 4. panta 8. punkts noteic, ka "apstrādātājs" ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus.

Lai personu varētu uzskatīt par apstrādātāju, tai jāatbilst diviem pamatnosacījumiem:

→ tai jābūt atsevišķam tiesību subjektam attiecībā pret pārzini[3];

→ un jāapstrādā personas dati tā uzdevumā.

Praksē parasti noslēgtā līguma noteikumi palīdz identificēt un atšķirt apstrādātāju no pārziņa.

Līdz ar to apstrādātāja pastāvēšana ir atkarīga no lēmuma, ko pieņem pārzinis, kurš var izvēlēties, vai nu apstrādāt datus savā organizācijā, piemēram, uzticot šo darbu darbiniekiem, kas ir pilnvaroti apstrādāt datus pārziņa tiešā vadībā, vai ar līgumu pilnīgi vai daļēji uzticēt ar datu apstrādi saistītās darbības trešajai personai, kas būs uzskatāma par apstrādātāju.

Izšķirošais elements, nodalot pārziņa un apstrādātāja lomas, ir ietekme uz datu apstrādes nolūku un tās līdzekļu būtiskajiem elementiem. Rīkoties kāda vārdā nozīmē apmierināt kāda intereses, un tas sasaucas ar juridisko jēdzienu "deleģēšana". Vienlaikus tas var nozīmēt arī zināmu rīcības brīvību, proti, apstrādātāja tiesības izvēlēties piemērotākos tehniskos un organizatoriskos līdzekļus.

[3] Saskaņā ar Datu regulas 4.panta 7.punktu, par personas datu apstrādes atbilstību Datu regulai ir atbildīgs "pārzinis" – fiziskā vai juridiskā persona, valsts vai pašvaldību institūcija, kura nosaka personas datu apstrādes nolūkus un līdzekļus.

Darboties kāda uzdevumā nozīmē arī to, ka apstrādātājs nedrīkst veikt apstrādi pats saviem nolūkiem. Kā norādīts Datu regulas 28. panta 10. punktā, apstrādātājs pārkāpj Datu regulu, ja pārsniedz pārziņa norādījumus un sāk noteikt pats savus apstrādes nolūkus un līdzekļus. Apstrādātājs attiecībā uz šo apstrādi tiks uzskatīts par pārzini, un viņam var piemērot sankcijas par pārziņa norādījumu pārsniegšanu.

Ja apstrādātājs pārkāpj Datu regulu, nosakot apstrādes nolūkus un līdzekļus, to atzīst par pārzini attiecībā uz minēto apstrādi (Datu regulas 28. panta 10. punkts).

Piemērs - Uzņēmums X dažādiem uzņēmumiem sniedz mārketinga pakalpojumus. Tas noslēdz līgumu ar uzņēmumu Y, noslēdzot Datu regulas 28. panta 3. punktam atbilstošu līgumu. Tomēr uzņēmums X nolemj izmantot uzņēmuma Y datubāzi arī citiem nolūkiem, nevis kā paredzējis pārzinis – uzņēmums Y. Lēmums pievienot papildu nolūku tam nolūkam, kuram personas dati tika nodoti, pārveido uzņēmumu X par pārzini uz šo apstrādes darbību kopumu, un datu apstrāde šim nolūkam būtu Datu regulas pārkāpums.

Apstrādātāja loma iespējama, pat ja personas datu apstrāde nav pakalpojuma galvenais vai primārais objekts, ar nosacījumu, ka klients praksē joprojām nosaka apstrādes nolūkus un līdzekļus. Tomēr vienlaikus jāizvērtē, vai apstrādātājs ļauj klientam īstenot pietiekamu kontroles pakāpi.

Piemērs – Uzņēmums A saņem no uzņēmuma Y ienākošo zvanu centra pakalpojumu. Līdz ar to uzņēmumam Y ir vajadzīga piekļuve uzņēmuma A klientu datubāzēm, lai sniegtu tiem atbalstu. Uzņēmums Y datus neapstrādā citos nolūkos, kā norādījis uzņēmums A, līdz ar to tas ir uzskatāms par apstrādātāju. Uzņēmumi A un Y savstarpēji noslēdz līgumu.

Apstrādātājs var piedāvāt arī iepriekš izstrādātu pakalpojumu, tomēr vienlaikus jāatceras, ka tieši pārzinis pieņem galīgo lēmumu attiecībā uz apstrādes būtiskajiem aspektiem.[4]

Piemērs — Uzņēmums X piedāvā mākoņpakalpojumus uzņēmumam B. Uzņēmums X vēlas slēgt standarta vienošanos, kāda tiek piedāvāta visā pasaulē, t.sk. ārpus Eiropas Savienības. Uzņēmumam B jebkurā gadījumā jāpārliecinās, lai šī vienošanās atbilst tostarp Datu regulas 28. panta 3. punktam. Vienlaikus uzņēmumam B jābūt pārliecinātam, ka mākoņpakalpojumu sniedzējs (uzņēmums X) tai skaitā ievēros datu glabāšanas termiņus, to dzēšanu veiks atbilstoši uzņēmuma B norādījumiem, u.c,

[4] Papildu informāciju skatīt: Eiropas Datu aizsardzības kolēģijas (EDAK) 2020. gada jūlija pamatnostādnes par pārziņa un apstrādātāja jēdzieniem VDAR (Pieņemts 2021. gada 7. jūlijā): https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_lv

3. TIESISKĀS ATTIECĪBAS STARP PĀRZINI UN APSTRĀDĀTĀJU

Kā jebkurai datu apstrādei, arī šai pārzinis piemēro atbilstošu datu apstrādes mērķi un tiesisku pamatu, kas pieļauj minēto pakalpojumu sniegšanu. Ja apstrādātājam pastāv proaktīvs pienākums sekot apstrādes likumībai - tad šos aspektus apstrādātājam jāpārbauda noslēgtā līguma izpildes gaitā.

Personas datu apstrādes nolūkus un līdzekļus nosaka pārzinis, nevis apstrādātājs. Datu apstrādātājs personas datus apstrādā tikai pārziņa uzdevumā.

Apstrādātāji ir atbildīgi par kaitējumu, kas nodarīts ar apstrādi, tikai tad, ja tie nav izpildījuši Datu regulā paredzētos pienākumus, kas konkrēti adresēti apstrādātājam, vai ja tie rīkojušies neatbilstoši vai pretēji pārziņa likumīgiem norādījumiem.

Apstrādi, ko veic apstrādātājs, reglamentē ar līgumu vai ar citu juridisku aktu saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kas ir saistošs apstrādātājam un pārzinim (Datu regulas 28. pants 3. punkts). Tos jānoslēdz rakstveidā, tostarp elektroniski[5]. Atbildīgs ir gan pārzinis, gan apstrādātājs. Līgumi, kas noslēgti pirms Datu regulas spēkā stāšanās dienas, bija jāatjaunina, ņemot vērā Datu regulas 28. panta 3.punktu.

Līgumus starp pārziņiem un apstrādātājiem dažkārt var vienpusēji sagatavot kāda viena puse. Izpildot norādīto pienākumu, pārzinis un apstrādātājs līgumā iekļauj visus obligātos elementus, var arī pilnībā vai daļēji izmantot līguma standartklauzulas[6], kas saistītas ar pienākumiem, kuri noteikti Datu regulas 28. pantā[7].

Tā kā Datu regula paredz skaidru pienākumu slēgt rakstisku līgumu, ja nav spēkā cita atbilstoša juridiska akta, līguma neesamība ir Datu regulas pārkāpums.

Īpaši vēršam uzmanību uz sekojošiem apstrādātāja pienākumiem attiecībā pret pārzini, tostarp:

[5] Datu regulas 28. panta 9. punkts.

[6] Papildu informāciju skatīt: COMMISSION IMPLEMENTING DECISION on standard contractual clauses between controllers and processors under Article 28 (7) of Regulation (EU) 2016/679 and Article 29 (7) of Regulation (EU) 2018/1725: https://commission.europa.eu/publications/standard-contractual-clauses-controllers-and-processors-eueea_en

[7] Datu regulas 28. panta 6. punkts. Kā norāda arī Eiropas Datu aizsardzības kolēģija (EDAK), līguma standartklauzulas, ar ko nodrošina atbilstību Datu regulas 28. pantam, nav tās pašas standarta līguma klauzulas, kas minētas 46. panta 2. punktā. Pirmās klauzulas detalizēti nosaka un paskaidro, kā tiks izpildīti 28. panta 3. un 4. punkta noteikumi, bet otrās nodrošina atbilstošus aizsardzības pasākumus gadījumos, kad personas dati tiek pārsūtīti uz trešo valsti vai starptautisku organizāciju, ja nav atbilstoša lēmuma saskaņā ar 45. panta 3. punktu.

→ apstrādātājs drīkst apstrādāt datus tikai saskaņā ar pārziņa dokumentētiem norādījumiem (Datu regulas 28. panta 3. punkta a) apakšpunkts);

→ jānodrošina, ka personas, kuras ir pilnvarotas apstrādāt datus, ir apņēmušās ievērot konfidencialitāti vai tām ir noteikts attiecīgs likumisks pienākums ievērot konfidencialitāti (Datu regulas 28. panta 3. punkta b) apakšpunkts);

→ jāievēro 28. panta 2. un 4. punktā minētie nosacījumi, saskaņā ar kuriem tiek piesaistīts cits apstrādātājs (Datu regulas 28. panta 3. punkta d) apakšpunkts);

→ jāpalīdz pārzinim [..] izpildīt savu pienākumu atbildēt uz pieprasījumiem par [..] datu subjekta tiesību īstenošanu (Datu regulas 28. panta 3. punkta e) apakšpunkts);

→ jāpalīdz pārzinim nodrošināt 32. līdz 36. pantā minēto pienākumu izpildi (Datu regulas 28. panta 3. punkta f) apakšpunkts);

→ pēc apstrādes pakalpojumu sniegšanas pabeigšanas apstrādātājam pēc pārziņa izvēles jādzēš vai jāatdod visi personas dati pārzinim un jādzēš esošās kopijas (Datu regulas 28. panta 3. punkta g) apakšpunkts);

→ jādara pārzinim pieejama visa informācija, kas nepieciešama, lai apliecinātu, ka tiek pildīti 28. pantā paredzētie pienākumi, un lai ļautu pārzinim vai citam pārziņa pilnvarotam revidentam veikt revīzijas, tostarp pārbaudes, un sniegtu tajās ieguldījumu (Datu regulas 28. panta 3. punkta h) apakšpunkts);

→ apstrādātājam jāuztur visu pārziņa vārdā veikto apstrādes darbību kategoriju reģistrs (Datu regulas 30. panta 2. punkts);

→ jāīsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam (Datu regulas 32. pants);

→ tiklīdz apstrādātājam kļuvis zināms personas datu aizsardzības pārkāpums, bez nepamatotas kavēšanās jāpaziņo par to pārzinim (Datu regulas 33. panta 2. punkts);

→ jāievēro noteikumi par datu pārsūtīšanu uz trešām valstīm vai starptautiskām organizācijām (Datu regulas V nodaļa).

Sagatavojot līgumu jāņem vērā konkrētos apstrādātāja uzdevumus un pienākumus saistībā ar veicamo apstrādi un risku datu subjekta tiesībām un brīvībām[8].

Datu regulas 28. panta 3. punkts noteic, ka līgumā starp pārzini un apstrādātāju jāiekļauj vismaz šāda informācija:

→ apstrādes priekšmets;
→ apstrādes ilgums;
→ apstrādes veids;
→ personas datu veidi;
→ datu subjektu kategorijas;
→ pārziņa pienākumi un tiesības;
→ cita būtiska informācija attiecībā uz apstrādes riskiem un papildus piemērojamām prasībām.[9]

Noslēgtajā līgumā par apstrādi nevajadzētu atkārtot Datu regulas noteikumus. Jāiekļauj specifiskāku, konkrētāku

[8] Skat. Datu regulas 81. apsvērumu.

[9] Papildu informāciju skatīt: Eiropas Datu aizsardzības kolēģijas (EDAK) 2020. gada jūlija pamatnostādnes par pārziņa un apstrādātāja jēdzieniem VDAR (Pieņemts 2021. gada 7. jūlijā): https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_lv

informāciju par to, kā tiks izpildītas prasības un kāds drošības līmenis ir nepieciešams to personas datu apstrādei, kas ir līguma par apstrādi priekšmets.[10]

Attiecībā uz pārziņa sniegtiem nelikumīgiem norādījumiem, Eiropas datu aizsardzības kolēģija (EDAK) un Eiropas Datu aizsardzības uzraudzītājs (EDAU) uzskata, ka līgumā starp pārzini un apstrādātāju būtu jāiekļauj precīzāka informācija par sekām un risinājumiem, kas paredzēti gadījumā, ja apstrādātājs informē pārzini, ka, viņaprāt, norādījums pārkāpj Datu regulu vai citus piemērojamos datu aizsardzības noteikumus[11]. Tomēr pašlaik minētajam ir tikai ieteikuma raksturs.

4. "APAKŠAPSTRĀDĀTĀJA" PIESAISTE

Iespējami gadījumi, kad apstrādātāji procesā piesaista citu dalībnieku, tam uzticot darbības, kas ietver personas datu apstrādi. Lai pārliecinātos, vai šī persona būtu uzskatāma par "apakšapstrādātāju", analīze jāveic saskaņā ar iepriekš minēto saistībā ar apstrādātāja jēdzienu.

Saskaņā ar Datu regulas 28. panta 4. punktu "apakšapstrādātāja" piesaisti jāparedz līgumā vai citā juridiskā dokumentā, kas regulē apstrādi, vienlaikus paredzot pienākumus, kurus pārzinis uzlicis pirmajam apstrādātājam. Vienlaikus pietiekami jāgarantē, ka tiks piemēroti tehniskie un organizatoriskie pasākumi tādā veidā, lai apstrādē tiktu ievērotas Datu regulā noteiktās prasības.

Līgumā starp pārzini un apstrādātāju tostarp jāparedz, ka apstrādātājs ievēro Datu regulas 28. panta 2. un 4. punktā minētos nosacījumus, saskaņā ar kuriem tiek piesaistīts cits apstrādātājs.

Arī šajā gadījumā pārzinis saglabā tiesības noteikt personas datu apstrādes nolūkus un līdzekļus.

Datu regulas 28. panta 2. punkts paredz, ka apstrādātājs drīkst piesaistīt citu apstrādātāju tikai ar iepriekšēju konkrētu vai vispārēju rakstisku pārziņa atļauju.

Ja pārzinis izvēlas dot **konkrētu atļauju**, viņam rakstveidā jānorāda, uz kuru apakšapstrādātāju, un kuru apstrādes darbību šī atļauja attiecas. Pirms jebkuru turpmāku izmaiņu veikšanas, tās ir jāapstiprina pārzinim. Ja apstrādātājs uz konkrētas atļaujas pieprasījumu nesaņem atbildi noteiktajā termiņā, šis pieprasījums ir uzskatāms par noraidītu. Pārzinim jāpieņem lēmums par atļaujas piešķiršanu vai atteikšanu, ņemot vērā savu pienākumu izmantot tikai tādus apstrādātājus, kas sniedz "pietiekamas garantijas".

[10] 2020. gada jūlija pamatnostādnes par pārziņa un apstrādātāja jēdzieniem VDAR (Pieņemts 2021. gada 7. jūlijā): https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_lv

[11] Papildu informāciju skatīt: EDAK un EDAU Kopīgais atzinums 1/2021 par Eiropas Komisijas Īstenošanas lēmumu par standartklauzulām līgumos starp pārziņiem un apstrādātājiemjautājumos, kas minēti Regulas (ES): https://edpb.europa.eu/system/files/2021-04/edpb-edpsjointopinion01_2021_sccs_c_p_lv.pdf 2016/679 28. panta 7. punktā un Regulas (ES) 2018/1725 29. panta 7. punktā

Pārzinis var dot arī **vispārēju atļauju** izmantot apakšapstrādātājus (līgumā iekļaujot tā pielikumā sarakstu ar šādiem apakšapstrādātājiem), kas jāpapildina ar kritērijiem, kuri noteiks apstrādātāja izvēli (piemēram, garantijas attiecībā uz tehniskiem un organizatoriskiem pasākumiem, ekspertu zināšanas, uzticamība un resursi)[12]. Šādā gadījumā apstrādātājam laikus jāinformē pārzinis par jebkuru paredzēto apakšapstrādātāja(-u) pievienošanu vai nomaiņu, lai nodrošinātu pārzinim iespēju iesniegt iebildumus.

Turklāt vispārējas rakstiskas atļaujas gadījumā apstrādātājs informē pārzini par jebkādām iecerētām pārmaiņām saistībā ar papildu apstrādātāju vai apstrādātāja aizstāšanu, tādējādi sniedzot pārzinim iespēju iebilst pret šādām izmaiņām.

Apstrādātājs jebkurā gadījumā ir pilnībā atbildīgs pret pārzini par "apakšapstrādātāju" pienākumu izpildi (Datu regulas 28. panta 4. punkts). Jānodrošina, ka apstrādātājs ierosina tikai tādus "apakšapstrādātājus", kuri sniedz pietiekamas garantijas.[13]

Piemērs – Uzņēmums X, kura darbības veids ir saistīts ar telemārketingu, tostarp izejošo zvanu centru darbību, apstrādā personas datus klienta Y uzdevumā, veicot zvanus klientiem tā vārdā. Lai veiktu zvanus, uzņēmums X ar pārziņa – klienta Y - saskaņojumu piesaista ārpakalpojumu, proti, informācijas sistēmu drošības speciālistu B, kuram tiešo darba pienākumu veikšanas ietvaros ir pieeja klienta Y datubāzēm, kas satur personas datus. Informācijas sistēmu drošības speciālists B ir uzskatāms par "apakšapstrādātāju". Tā piesaistei ir noslēgts līgums.

5. KOMERCIĀLA PAZIŅOJUMA SŪTĪŠANAS TIESISKIE ASPEKTI

Komerciālu paziņojumu nosūtīšanas tiesiskais ietvars telemārketinga veikšanai pamatā ir noteikts ISPL 8. un 9. pantā. Šajās vadlīnijās uzmanība vērsta tieši uz komerciālu paziņojumu sūtīšanu fiziskām, nevis juridiskām personām, uz ko attiecināmas daudz stingrākas prasības.

Veicot komerciālu paziņojumu sūtīšanu fiziskai personai, izmantojot telefonsakarus, un tās uzraudzību, būtiski ir izprast termina "komerciāls paziņojums" nozīmi. ISPL 1.panta pirmās daļas 3.punkts noteic, ka tas ir jebkāds paziņojums elektroniskā veidā, kas paredzēts tiešai vai netiešai preču vai pakalpojumu reklamēšanai vai arī tāda komersanta, organizācijas vai personas tēla reklamēšanai, kas veic komercdarbību, saimniecisku darbību vai reglamentēto profesionālo darbību. Par komerciālo paziņojumu neuzskata informāciju, kas dod iespēju tieši piekļūt vispārējai informācijai par pakalpojuma sniedzēju un tā darbību (domēna vārds vai elektroniskā pasta adrese).

[12] Šis pienākums izriet no pārskatatbildības principa, kas minēts Datu regulas 24. pantā, un no pienākuma ievērot Datu regulas 28. panta 1. punkta, 32. panta un V nodaļas noteikumus.

[13] Papildu informāciju skatīt: Eiropas Datu aizsardzības kolēģijas (EDAK) 2020. gada jūlija pamatnostādnes par pārziņa un apstrādātāja jēdzieniem VDAR (Pieņemts 2021. gada 7. jūlijā): https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-072020-concepts-controller-and-processor-gdpr_lv

Minētā definīcija ietver trīs pamatelementus:

→ jebkāds paziņojums;

→ elektroniskā veidā;

→ paredzēts tiešai vai netiešai preču vai pakalpojumu reklamēšanai vai arī tāda komersanta, organizācijas vai personas tēla reklamēšanai, kas veic komercdarbību, saimniecisku darbību vai reglamentēto profesionālo darbību.

Informācija ir atzīstama par komerciālu paziņojumu ISPL izpratnē, ja vienlaicīgi pastāv visi trīs iepriekš minētie elementi. Šie elementi ir savstarpēji saistīti un viens otru papildina vai ierobežo.

Minētā definīcija satur gan pozitīvo daļu, pirmajā teikumā nosakot, kas ir komerciāls paziņojums, gan negatīvo daļu, otrajā teikumā nosakot, kas nav komerciāls paziņojums. No komerciāla paziņojuma definīcijas izriet, ka komerciāls paziņojums ir jebkāds paziņojums, kas sniegts elektroniskā veidā, ar konkrētu mērķi - tieši vai netieši reklamēt komersanta, organizācijas vai personas preces, pakalpojumus vai tēlu. Līdz ar to, paziņojums uzskatāms par komerciālu, ja tā tiešais vai netiešais mērķis ir veicināt komersanta vai pakalpojumu sniedzēja piedāvāto preču vai pakalpojumu popularitāti vai pieprasījumu pēc tiem. Vienlaikus no definīcijas negatīvās daļas, kas ietverta tās otrajā teikumā, izriet, ka par komerciālu paziņojumu nav uzskatāma informācija, kas dod iespēju potenciālajam klientam pašam tieši piekļūt vispārējai informācijai par pakalpojuma sniedzēju un tā darbību, piemēram, domēna vārds vai elektroniskā pasta adrese.

Savukārt ISPL 8. panta pirmā daļa noteic, ka komerciāls paziņojums atbilst vispārējām Reklāmas likuma[14] prasībām, kā arī šādām prasībām:

→ tas ir skaidri atpazīstams kā komerciāls paziņojums;

→ ir skaidri nosakāma persona, kuras vārdā šis komerciālais paziņojums izplatīts;

→ ir precīzi formulēts piedāvājuma saturs un pakalpojuma saņemšanas noteikumi;

→ atlaides, prēmijas un balvas ir skaidri atpazīstamas, un to saņemšanas noteikumi ir skaidri izklāstīti;

→ reklāmas sacensības, loterijas vai spēles ir skaidri atpazīstamas, un attiecīgie dalības noteikumi ir viegli pieejami, kā arī skaidri un nepārprotami izklāstīti;

→ pakalpojuma saņēmējam ir dota iespēja atteikties no turpmāku komerciālu paziņojumu saņemšanas.

No ISPL 9. panta sestās daļas izriet, ka pirms komerciāla paziņojuma sūtīšanas ir svarīgi identificēt, vai komerciālā paziņojuma saņēmējs būs fiziskā vai juridiskā persona, jo tas tiešā veidā ietekmē prasības, kas komersantam jāievēro, tiesiskai komerciāla paziņojuma sūtīšanai.

Ja komerciāls paziņojums tiek sūtīts identificētai vai identificējamai fiziskai personai, komerciālā paziņojuma sūtītājam papildus ISPL ir jāievēro arī Datu regula.

Uzņēmumu, kas nodrošina telemārketinga pakalpojumus, rīcībā var nonākt informācija – tostarp fizisku personu dati, dažkārt arī ziņas par to, kādas preces šī persona visbiežāk iegādājas u.c.[15] Pieejas tiesībām datiem darbiniekiem jābūt priviliģētām, atbilstoši tiešajiem darba

[14] Reklāmas likums pieejams pēc saites : https://likumi.lv/ta/id/163

[15] Saskaņā ar Datu regulas 4. panta 1. punktu, personas dati ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku

pienākumiem. Šo personas datu vākšana, glabāšana vai izmantošana ir uzskatāma par apstrādi[16] Datu regulas izpratnē.

Piemēram, telefona numuru, apvienojot ar citu informāciju, kā rezultātā iespējams identificēt fizisko personu, uzskata par personas datiem.

Katra aizliegta komerciāla paziņojuma sūtīšana ir atsevišķs pārkāpums[17]. Vērtējot, kura persona ir atbildīga par aizliegta komerciāla paziņojuma sūtīšanu gadījumā, ja sūtīšanā ir iesaistītas vairākas personas, piemēram, komersants, kura vārdā un uzdevumā komerciālo paziņojumu sūta tā darbinieks, apakšuzņēmējs vai cita pilnvarotā persona, tiek ņemts vērā tostarp Civillikumā noteiktais regulējums, kā arī vienošanās, kuras noslēgtas starp iepriekš minētajām personām. Neskatoties uz iepriekš minēto, Inspekcija norāda, ka personai, kuras vārdā, uzdevumā un interesēs komerciāls paziņojums tiek sūtīts, ir jādara viss iespējamais, lai personas, kuras faktiski komerciālu paziņojumu sūta, ievērotu ISPL un Datu regulas noteikumus.

5.1. Tiesiskais pamats

Komunikācija, izmantojot komerciāla paziņojuma sūtīšanai publiski pieejamus elektronisko sakaru pakalpojumus, var notikt, ja pakalpojuma saņēmējs (fiziska persona) iepriekš ir devis brīvu un nepārprotamu piekrišanu, izņemot ISPL 9. panta pirmajā un otrajā daļā minētos gadījumus[18]. Tātad apstrādātājs drīkst nosūtīt komerciālu paziņojumu fiziskai personai tikai tad, kad tam iepriekš ir nodrošināta atbilstoša piekrišana.

Interpretējot ISPL terminu "brīva un nepārprotama piekrišana", jāņem vērā Datu regulas 4. panta 11. punktā definēto "piekrišanas" jēdzienu.

ISPL noteiktās prasības attiecināmas uz visiem komerciālu paziņojumu sūtīšanas gadījumiem, pat ja zvanītāja rīcībā ir tikai telefona numurs, kas bez papildu informācijas neļauj identificēt konkrēto fizisko personu.

Piekrišana ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta (komerciāla paziņojuma saņēmēja) vēlmēm, ar kuru viņš paziņojuma vai

---

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.

[16] Datu regulas 4. panta 2. punktā noteikts, ka "apstrāde" ir jebkura ar personas datiem vai personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana.

[17] ISPL 9. panta piektā daļa.

[18] ISPL 9.panta trešā daļa.

skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei[19].

Jāievēro, ka iegūstamajai piekrišanai, tostarp telemārketinga ietvaros, ir jāatbilst sekojošām prasībām:

→ **Brīvi sniegta piekrišana.** Norāda uz reālu izvēles iespēju pār komerciālu paziņojumu saņemšanu, ar negatīvu seku neiestāšanās risku.

→ **Nepārprotama piekrišana.** Komerciālā paziņojuma iespējamā saņēmēja klusēšana vai iespējas atteikties no komerciālu paziņojumu saņemšanas neizmantošana nav atzīstama par nepārprotamu piekrišanu, un līdz ar to šāda piekrišana nav atbilstoša ISPL un Datu regulai.

→ **Konkrēta piekrišana.** Nosaka, ka jābūt norādītiem konkrētiem apstrādes nolūkiem un apstrādātajiem datiem jābūt adekvātiem, atbilstīgiem un tie nedrīkst būt pārmērīgi attiecībā uz nolūkiem, kādiem tie ir iegūti un/vai tālāk apstrādāti.

→ **Apzināta piekrišana.** Norāda, ka informācijas nodrošināšana pirms piekrišanas saņemšanas ir būtiska, lai fiziskā persona varētu pieņemt apzinātus lēmumus, saprast, kam viņi piekrīt.

→ **Aktīvi sniegta piekrišana.** Norāda, ka piekrišanai jābūt nepārprotami sniegtai ar lietotāja aktīvu darbību, kas apstiprina, ka persona piekrīt komerciālu paziņojumu saņemšanai. Ir skaidri jānorāda, kura darbība norāda uz piekrišanu komerciālu paziņojumu saņemšanai. Jāpārliecinās, ka izvēle, kas izteikta ar aktīvu darbību, patiešām ir balstīta uz skaidru informāciju, ka šīs darbības rezultātā dati tiks izmantoti mārketinga nolūkiem.

Jāspēj uzskatāmi parādīt, ka subjekts ir devis piekrišanu komerciālu paziņojumu saņemšanai un datu apstrādei. Īpaša uzmanība jāpievērš gadījumiem, kad piekrišana tiek sniegta mutiski, piemēram, gadījumos, kad sarunu ieraksti pēc noteikta laika tiek dzēsti. Jāņem vērā, ka piekrišanas fakta esamību jāpierāda visu apstrādes laiku, līdz ar to šo informāciju arī attiecīgi jāglabā.

Publiski pieejamā veidā fizisku personu kontaktinformāciju publicē lielākoties citiem mērķiem, nevis kā piekrišanu komerciālu paziņojumu saņemšanai. Izmantojot publiski pieejamu fizisku personu kontaktinformāciju, nepastāv tiesisks pamats komerciāla paziņojuma sūtīšanai ISPL izpratnē un personas datu apstrādei Datu regulas izpratnē.

Nav noteikts konkrēts termiņš, cik ilgi piekrišana ir derīga. Tas, cik ilgi piekrišana ir derīga, ir atkarīgs no konteksta, sākotnējās piekrišanas tvēruma un tā, ko komerciālā paziņojuma saņēmējs sagaida. Ja apstrādes darbības ievērojami mainās vai attīstās, sākotnējā piekrišana vairs nebūs spēkā esoša. Tādā gadījumā ir jāsaņem jauna atļauja komerciālu paziņojumu sūtīšanai.

Jāņem vērā, ka Latvijas Republikā ir atļauts izmantot "*random number generators*" un robota zvanus, ciktāl netiek pārkāpta ISPL 9.panta pirmā daļa. No tās izriet vispārējs aizliegums izmantot automātiskās zvanīšanas sistēmas komerciālu paziņojumu sūtīšanai, nosakot, ka tas ir atļauts tikai gadījumā, ja tam ir iegūta iepriekšēja brīva un nepārprotama

[19] Datu regulas 4. panta 11. punkts.

piekrišana. Tādējādi, komerciālu paziņojumu sūtīšana ISPL 9. panta pirmajā daļā norādītajā veidā ir likumīga tikai gadījumā, ja konkrētā persona iepriekš ir devusi savu brīvu un nepārprotamu piekrišanu tam, ka tiks traucēta ar automatizētām zvanīšanas iekārtām, lai tādā veidā saņemtu komerciālu paziņojumu. No ISPL 9. panta pirmās daļas izriet, ka iepriekšēja piekrišana ir nepieciešama ne tikai paša komerciālā paziņojuma sniegšanai kā tādai, bet arī veidam kādā tas tiek sūtīts. Tas nozīmē to, ka faktiski klients, kura vārdā tiek veikti, piemēram, zvani, dod uzdevumu šīs metodes izmantošanai, vienlaikus nodrošinot atbilstošu komerciālā paziņojuma saņēmēja piekrišanu.

No ISPL 8. panta pirmās daļas 6. punkta izriet vēl viens tiesiskas komerciālu paziņojumu sūtīšanas priekšnoteikums – sūtot komerciālu paziņojumu elektroniskā veidā, komersantam vai pakalpojumu sniedzējam ir jānodrošina saņēmējam iespēja atteikties no komerciāla paziņojuma saņemšanas. Jāievēro arī tas, ka atteikšanās nedrīkstētu būt sarežģītāka kā piekrišanas došana.

Tātad komerciālu paziņojumu saņēmējs var jebkurā laikā atsaukt savu piekrišanu tikpat viegli, kā to sniedzis. Šim nolūkam, tas piekrišanas iegūšanas brīdī ir jāinformē arī par tās atsaukšanas iespējām.

Datu regula nenosaka, ka piekrišanas sniegšana un atsaukšana vienmēr ir jāveic, izmantojot vienu un to pašu rīcību. Tomēr, ja piekrišana tiek iegūta, piemēram, izmantojot elektroniskus līdzekļus un tikai ar vienu peles klikšķi, subjektiem praksē ir jābūt iespējai tikpat viegli atsaukt šo piekrišanu. Atteikšanās iespēju vēlams nodrošināt vismaz tādā pašā veidā, kādā komerciāls paziņojums ir nosūtīts, vai vēl vieglākā veidā.

Piemērs – Uzņēmuma X tīmekļa vietnes dialoglogā tiek pieprasīta piekrišana izmantot klienta kontaktinformāciju mārketinga nolūkos. Šim nolūkam klienti var izvēlēties atzīmēt "Jā" vai "Nē". Pārzinis informē klientus, ka viņiem ir iespēja atsaukt piekrišanu. Lai to izdarītu, viņiem pa maksas tālruni jāsazinās ar zvanu centru darba dienās no plkst. 9:00 līdz 15:00. Šajā gadījumā pārzinis neizpilda Datu regulas 7. panta 3. punkta prasības. Konkrētajā gadījumā personai prasa veikt tālruņa zvanu par maksu, turklāt noteiktā darba laikā, kas ir apgrūtinošāk, nekā viens peles klikšķis, kas bija nepieciešams, lai sniegtu piekrišanu konkrētajā tīmekļa vietnē.

ISPL 9. panta ceturtā daļa noteic, ka elektronisko pastu vai cita veida komunikāciju, izmantojot publiski pieejamus elektronisko sakaru pakalpojumus, aizliegts izmantot komerciāla paziņojuma sūtīšanai, ja tiek lietota nederīga elektroniskā pasta adrese, nederīgs tālruņa vai faksa numurs, uz kuru pakalpojuma saņēmējs varētu sūtīt pieprasījumu pārtraukt komunikāciju, vai ja netiek ņemta vērā pakalpojuma saņēmēja atteikšanās no turpmāku komerciālu paziņojumu saņemšanas. Iepriekš minētais ir saistošs visām personām, kuras sūta komerciālus paziņojumus ISPL izpratnē, neatkarīgi no sūtīšanas veida, ja vien ISPL nav noteikts tiešs izņēmums attiecībā uz konkrētu veidu.

Prasība par piekrišanas vienkāršu atsaukšanu Datu regulā tiek aprakstīta kā nepieciešams spēkā esošas piekrišanas aspekts. Ja atsaukšanas tiesības neatbilst Datu regulas prasībām, tad piekrišanas mehānisms neatbilst Datu

regulai.[20]

Ja fiziskā persona, piemēram, zvana laikā atsauc piekrišanu turpmākai komerciālu zvanu saņemšanai un datu apstrādei, tad arī apstrādātājam ir pienākums to ievērot, par minēto bez kavēšanās informējot konkrēto pārzini.

Praksē nereti informāciju par piekrišanas atsaukšanu fiksē klientu iesniegtajās datubāzēs, tomēr šāda risinājuma izmantošanas gadījumā ir nepieciešams pārliecināties, ka informācija korekti tiek ielasīta arī pārziņa pusē. Savukārt, ja informācija tiek nosūtīta, piemēram, izmantojot elektronisko pastu, tad jāpārliecinās par tās saņemšanu, lai dati tiktu dzēsti un konkrētais telefona numurs vairs netiktu izmantots mārketinga nolūkiem. Īpaša uzmanība informācijas apmaiņai par konkrēto fizisko personu jāpievērš, kad vienlaikus tiek realizētas vairākas kampaņas pie dažādiem telemārketinga pakalpojumu sniedzējiem, lai nodrošinātu datu integritāti. Komerciālo paziņojumu sūtītājiem informāciju par atteikuma saņemšanu ir būtiski nodot visām personām, kas ir iesaistītas komerciālo paziņojumu sūtīšanā attiecīgā uzņēmuma vārdā, piemēram, darbiniekiem un apakšuzņēmējiem.

Jāņem vērā, ka apstrādes ietvaros arī zvanu ierakstu veikšanai un glabāšanai, kuru visbiežāk veic tieši telemārketinga pakalpojumu sniedzējs kvalitātes kontrolei, ir jāpiemēro atbilstošs tiesiskais pamats saskaņā ar Datu regulu. Turklāt sazvanīto personu ir jāinformē par ieraksta veikšanu.

5.2. Informācijas avoti un datubāzes

Īpašu uzmanību jāvērš arī uz izmantotajiem informācijas avotiem mērķēta telemārketinga veikšanai, un datubāzēm, kuras satur fizisku personu datus.

Pastāvot pārziņa un apstrādātāja tiesiskajām attiecībām, klienti – pārziņi – nodod uzņēmumu rīcībā savu datubāzi ar fizisko personu datiem, un konkrētais uzņēmums kā apstrādātājs attiecīgi izmanto šo klienta nodrošināto datubāzi noteiktā uzdevumā.

Jāievēro, lai pārziņa izsniegto datubāzi apstrādātājs izmantotu tikai noteiktajam mērķim, proti saziņai ar klientu loku konkrētās kampaņas ietvaros. Ir jānodala dažādu klientu datubāzes. Tas nozīmē, ka viena klienta izsniegto datubāzi nedrīkst izmantot cita klienta interesēs. Rīkojoties pretēji norādījumiem, apstrādātājs kļūtu par pārzini, jo tas pārsniegtu pārziņa norādījumus, nosakot pats savus apstrādes nolūkus un līdzekļus. Papildu riskus radītu arī tas, ka šim mērķim nav iegūta atbilstoša piekrišana.

Tāpat jāņem vērā, ka iegūstot un uzglabājot informāciju par datu subjektu datubāzēs, jāievēro datu minimizēšanas princips, kā arī citi principi saskaņā ar Datu regulas 5. pantu.

[20] Papildu informāciju skatīt: Eiropas Datu aizsardzības kolēģijas (EDAK) Pamatnostādnes 05/2020 par piekrišanu saskaņā ar Regulu 2016/679: https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_lv

Klienti kā pārziņi uzņemas atbildību par telemārketinga uzņēmumiem kā apstrādātājiem iesniegtās datubāzes saturu, tomēr arī apstrādātājam ir jāņem vērā personas tiesības uz datu aizsardzību, tostarp, ja tā iebilst komerciālu paziņojumu saņemšanai.

Dažkārt telemārketinga veikšanai tiek izmantotas dažādas publiski pieejamas datubāzes, tomēr jāņem vērā, ka gadījumos, kad, piemēram, zvana veikšanai tiek izmantota juridiskas personas kontaktinformācija, jāpārliecinās, ka tādējādi tomēr netiek veikta komerciālu paziņojumu sūtīšana fiziskajām personām, kā arī personas datu apstrāde Datu regulas izpratnē.

Piemērs – Uzņēmums A veic telemārketinga zvanu, izmantojot juridiskās personas – uzņēmuma B – kontaktinformāciju, kas iekļauta Latvijas Republikas Uzņēmumu Reģistra informācijas atkalizmantotāja datubāzē. Uz telefona zvanu atbild uzņēmuma B sekretāre, kurai uzreiz tiek izteikts piedāvājums iegādāties preci, kura ir domāta fiziskai personai, nevis juridiskai personai. Piekrišana komerciālu paziņojumu saņemšanai netiek prasīta. Sekretāre tomēr nolemj iegādāties piedāvāto preci un uzņēmumam A telefoniski sniedz savus personas datus. Rezultātā ar fizisku personu tiek noslēgts preces iegādes līgums. Piedāvājums juridiskai personai nemaz netiek izteikts, jo pats piedāvājums nav domāts juridiskajām personām, bet juridisko personu saziņas līdzekļi tiek izmantoti, lai uzrunātu fiziskās personas. Konkrētajā situācijā uzņēmums A negodprātīgi izmanto juridiskas personas kontaktinformāciju, ar mērķi izteikt komerciālu paziņojumu tikai fiziskai personai, kura pacēlusi klausuli. Turklāt piekrišana komerciālu paziņojumu saņemšanai netiek iegūta. Uzņēmumam A jāveic telemārketinga zvani tādā veidā, lai netiktu pārkāpti ISPL 9. panta aizliegumi un ierobežojumi, kas attiecas uz komerciālu paziņojumu sūtīšanu fiziskajām personām.

Veicot "aukstos zvanus"[21], kad telefona numurs tiek salikts (ģenerēts) jauktā secībā no dažādiem numerācijas diapazoniem, ir jāizvērtē, vai tiek ievērotas ISPL prasības, kā arī Datu regula, kad tiek uzsākts veikt personas datu apstrādi, tostarp attiecībā uz tiesiskā pamata nodrošināšanu u.c.

Jāņem vērā arī tas, ka ISPL 9. pants neparedz gadījumus, kad, piemēram, zvana mērķis ir vispārīgas piekrišanas iegūšana komerciālu paziņojumu sūtīšanai, turklāt nenoteiktam mērķim.

Nereti klienti datubāzes nodod programmas "Excel" vai "SharePoint" u.c. formātā, šifrētā veidā, izmantojot e–pastu. Īpaši ieteicams, ka šādos gadījumos piekļuve datubāzēm tiek nodrošināta ar vismaz 2 kanālu starpniecību – vienā kanālā uzņēmumam tiek atsūtīta šifrēta datu bāze, savukārt otrā kanālā – parole (piemēram, citā elektroniskajā pastā vai īsziņas veidā uz mobilo telefonu).

Pēc telemārketinga kampaņas beigām, jānodrošina, ka saņemtās datubāzes un tajās esošie personas dati tiek neatgriezeniski dzēsti (manuāli vai automātiski), un tie netiek

[21] Izmanto tālruni, lai zvanītu, mēģinot pārliecināt potenciālos pircējus, kuriem nav iepriekšējas zināšanas par šo uzņēmumu, iegādāties tā produktus vai pakalpojumus.

izmantoti citos nolūkos. Dzēšanas kārtību un termiņus jāatrunā ar klientiem noslēgtajos pakalpojuma līgumos. Vienlaikus jāparedz un jānodrošina, lai datus pēc dzēšamas nebūtu iespējams atjaunot, tostarp no izveidotajām rezerves kopijām.

6. APSTRĀDES DROŠĪBA

Datu regulas 32. pants noteic, ka, ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un smaguma pakāpes risku attiecībā uz fizisku personu tiesībām un brīvībām, pārzinis un apstrādātājs īsteno atbilstīgus tehniskus un organizatoriskus pasākumus, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam. Tajā skaitā, īsteno b) apakšpunktā minēto spēju nodrošināt apstrādes sistēmu un pakalpojumu nepārtrauktu konfidencialitāti, integritāti, pieejamību un noturību un d) apakšpunktā minēto procesu, regulārai tehnisko un organizatorisko pasākumu efektivitātes testēšanai, izvērtēšanai un novērtēšanai, lai nodrošinātu apstrādes drošību. Datu regulas 32 .panta 2. punkts nosaka, ka, novērtējot atbilstīgo drošības līmeni, pārzinis un apstrādātājs ņem vērā riskus, ko rada apstrāde, jo īpaši, nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.

Arī Datu regulas 83. apsvērumā tiek uzsvērta pārziņa un apstrādātāja atbildība par Datu regulas ievērošanu, proti, lai saglabātu drošību un novērstu tādu apstrādi, kurā tiek pārkāpta šī regula, pārzinim vai apstrādātājam būtu jānovērtē apstrādei raksturīgie riski un jāīsteno pasākumi šo risku mazināšanai, piemēram, šifrēšana. Minētajiem pasākumiem, ņemot vērā tehniskās iespējas un īstenošanas izmaksas, būtu jānodrošina atbilstošs drošības līmenis, tostarp konfidencialitāte, attiecībā uz apstrādei raksturīgo risku un aizsargājamo personas datu īpatnībām. Novērtējot datu drošības risku, vērā būtu jāņem riski, ko rada personas datu apstrāde, piemēram, nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem, kas var izraisīt fizisku, materiālu vai nemateriālu kaitējumu.

Inspekcija vērš uzmanību, ka turpmāk sniegtās rekomendācijas neaptver visus iespējamos pasākumus apstrādes drošības nodrošināšanai.

6.1. Vairāklīmeņu drošība

Drošības paaugstināšanas pasākumiem ieteicams izmantot vairāklīmeņu pieeju, jo viena simtprocentīgi droša risinājuma nav. Efektīva rezultāta sasniegšanai nepieciešama sistēma, kas sastāv no vairākām komponentēm un apvieno dažādus līdzekļus un tehnoloģijas – ja uzbrucējam izdodas apiet vienu, viņu, iespējams, var apturēt pārējās.

Nepieciešamie aizsardzības pasākumi jānosaka, ņemot vērā:

- Fizisko drošību;
- Personāla drošību;
- Dokumentu drošību;
- Automatizēto sistēmu/tīklu drošību;
- Kriptogrāfijas drošību.

Attiecībā uz fizisko drošību jāņem vērā, ka ir jānodrošina, lai trešajai personai iekļūstot uzņēmuma telpās, tai neautorizējoties nebūtu fiziskas piekļuves iekārtām, kurās glabājas personas dati. Var izmantot, piemēram, piekļuves kartes telpām. Arī serverus vēlams izvietot telpās ar ierobežotu piekļuvi (fiziskas pieejas kontrole).

Piemērs – Uzņēmums A ar uzņēmumu B noslēdz līgumu par biroja telpu uzkopšanu. Telpu apkopējiem nav paredzētas tiesības piekļūt klienta - Uzņēmuma A - rīcībā esošajiem personas datiem un tos apstrādāt. Uzņēmums B un tā darbinieki – apkopēji – ir uzskatāmi par trešo personu[22], un uzņēmumam A kā pārzinim ir jānodrošina nepieciešamie tehniskie un organizatoriskie pasākumi, lai nepieļautu trešo personu piekļuvi minētajiem personas datiem.

Attiecībā uz rezerves kopiju uzglabāšanu, jāņem vērā, lai tās nebūtu brīvi pieejamas nepiederošām personām, tās uzglabājot drošā vietā. Jāņem vērā, ka tās jāveido regulāri un jāiznīcina, kad tās vairs nav vajadzīgas.

Regulāri jāaktualizē jautājums, vai vēl nepieciešams veikt personas datu apstrādi, jo, iespējams, datu apstrādes mērķis ir sasniegts un datus var dzēst.

Datortīklu ievainojamības novēršanai, jānodrošina patstāvīga aizsardzība pret ļaunprogrammatūrām un citiem līdzīgiem draudiem. Vienlaikus jāievēro, lai drošības programmatūras un operētājsistēmas tiktu regulāri atjauninātas. Bieži to var iestatīt automātiski.

Sistēmai jābūt spējīgai novērst ārēju nesankcionētu piekļuvi datiem, neļaujot uzbrucējam iekļūt uzņēmuma datu tīklā. To var nodrošināt, piemēram, ar pareizi konfigurēta ugunsmūra palīdzību.

Nepieciešams, lai izmantotā drošības programmatūra ir aktīva un pastāvīgi skenē svarīgākās datnes, direktorijas un diskus. Vēlams ne retāk kā reizi gadā pārbaudīt, vai izmantotie drošības risinājumi atbilst prasībām un aktuālajai situācijai.

Inspekcija rekomendē uzņēmumiem regulāri pārbaudīt drošības programmatūras ziņojumus, sistēmu un aplikāciju žurnālfailus un citas atskaišu sistēmas, kas ir to rīcībā. Vēlams veikt sistēmas ievainojamības un integritātes testus. Konstatējot neatbilstības, nekavējoties jāveic atbilstoši drošības pasākumi lai ievainojamības novērstu.

Ik pēc noteikta laika vēlams pārbaudīt darba datoros izmantoto programmatūru. Tās kuras netiek lietotas, vēlams atinstalēt. Neregulāra atjauninājumu instalācija, var radīt paaugstinātus drošības riskus. Ilgstoši neizmantotām programmām var būt pārtraukts izstrādāt atjauninājumus ievainojamību novēršanai, un tās var kļūt par ievērojamu drošības caurumu.

Informācijas sistēmām jāpiešķir priviliģētas piekļuves tiesības. Katram lietotājam jāpiešķir savi atšķirīgi autentifikācijas līdzekļi – lietotāja vārds un parole. Savukārt, ja sistēmā tiek apstrādāti īpašo kategoriju personas dati, tad būtu

[22] Datu regula paredz arī trešās personas jēdzienu, lai arī tā konkrēti nenosaka to pienākumus vai atbildību attiecībā uz veikto personas datu apstrādi.

vēlams ieviest vairāklīmeņu autentifikāciju, piemēram, ar sertifikātiem, kodu kalkulatoriem vai citiem līdzekļiem.

Sistēmās jānosaka paroļu komplicētības līmenis, jāierobežo maksimālais neveiksmīgu autorizācijas gadījumu skaits, kā arī jāveic regulāra paroļu maiņa.

Lietotāja konti un citi autentifikācijas līdzekļi jābloķē nekavējoties pēc darba tiesisko attiecību izbeigšanas ar konkrētu darbinieku, kā arī darbiniekam esot ilgstošā prombūtnē.

Īpaši ieteicams darbiniekiem regulāri rīkot apmācības personas datu aizsardzības jomā un informācijas sistēmu drošības jautājumos, vienlaikus tos informējot par to atbildību un lomu, kas ir iekļauta arī uzņēmuma iekšējos noteikumos. Darbinieki jāapmāca atpazīt dažādus iespējamos draudus, piemēram, pikšķerēšanas elektroniskā pasta ziņojumus, kā arī jāinformē par rīcību gadījumos, kad notikusi nelikumīga personas datu apstrāde (piemēram, kā atpazīt informācijas drošības incidentus, un kam par tiem ziņot, u.c.), lai pēc iespējas ātrāk būtu iespējams šādu pārkāpumu novērst.

Drošības nolūkos darbiniekiem var aizliegt patstāvīgi uzstādīt trešo pušu lietojumprogrammatūru darba datoros, kā arī izmantot datu nesējus, lai mazinātu iespēju datus izgūt un izmantot citos nolūkos. Iespējami riski, ka darbinieki var datus nokopēt un, piemēram, pārdot citiem uzņēmumiem peļņas nolūkā.

Vēlams ieviest "*A clean desk and clear screen policy*"[23] ("Tīra galda un notīrīta ekrāna politika"), kura būtu jāiekļauj arī uzņēmumu iekšējos noteikumos. Tas tostarp paredz darba datora darbvirsmas bloķēšanu, kad konkrētais darbinieks to neizmanto un pamet darba vietu. Kā arī kontrolēt nevēlamu datu nokopēšanu, u.c.

Drošības nolūkos sistēmās var aktivizēt reģistrācijas žurnālu, fiksējot ikvienu darbību, kas saistīta ar piekļuvi personas datiem (caurlūkošana, izmaiņu veikšana, dzēšana). Reģistrācijas žurnāliem jābūt sasaistītiem ar laika zīmogu, kā arī tie pienācīgi jāaizsargā no viltošanas vai neatļautas piekļuves.

Lai novērstu incidentus vai samazinātu to ietekmi, var nodalīt tīkla iekārtas un ierobežot komunikāciju starp tām. Piemēram, serveri, kas nodrošina organizācijas tīmekļa vietnes darbību, var izvietot atsevišķā apakštīklā no datu servera. Tas nozīmē, ka sekmīgi realizēts uzbrukums negarantē uzbrucējam pieeju citiem datiem.

Efektīvas instrukcijas, plāni un politikas dokumenti būs vērtīgs papildinājums, veicot risku izvērtēšanu un uzlabojot organizācijas pārvaldības procesus kopumā.

Bieži IT sistēmu aizsardzības līmenis ir nepietiekams tikai tāpēc, ka korekti netiek pielietotas esošās drošības procedūras, un ka pašas organizācijas nespēj konstatēt, kur un kāpēc var rasties problēmas. Lai no minētā izvairītos, ieteicams sastādīt pārskatu, kādi personas dati ir uzņēmuma

[23] Ietverta ISO 27001 standartā.

rīcībā, un kādi aizsardzības līdzekļi tiem ir piemēroti. Jāapzina riski visiem rīcībā esošajiem personas datu veidiem. Tāpat jāieplāno rīcība gadījumos, ja notiktu, piemēram, šo datu noplūde vai tie tiktu mainīti, izdzēsti, kā arī, ja tiem būtu liegta piekļuve elektrības pārrāvuma gadījumā, fiziskas servera bojāejas gadījumā, u.c.

Praksē bieži IT sistēmu apkalpošanu uztic apakšapstrādātājiem. Tomēr, pirms piesaistīt IT atbalsta personālu no ārienes, būtu jāpārliecinās par tā reputāciju, kompetences līmeni, spēju ievērot datu aizsardzības principus, konfidencialitātes prasības u.c. Drošības prasības ir jāparedz noslēgtajos līgumos.

Ja iespējams, vēlams caurskatīt pakalpojumu sniedzēju sagatavotās drošības stāvokļa novērtējuma atskaites.

6.2. Darbs attālināti

Tāds pats drošības līmenis kā strādājot uzņēmuma telpās ir jānodrošina arī ierīcēs, kas tiek lietotas ārpus biroja – portatīvajos datoros, mobilajos tālruņos un viedtālruņos, ārējos cietajos diskos u.c. Neskaitāmi datu noplūdes un drošības incidenti notiek gadījumos, kad iekārtas tiek pazaudētas vai nozagtas. Lai samazinātu šādu risku iespējamību, vēlams, lai personas dati uz šīm iekārtām netiek glabāti vispār vai arī šai informācijai nav iespējams piekļūt bez atbilstošas autorizācijas.

Ja darbs tiek veikts attālināti, drošības nolūkos ieteicams, lai sistēmām un datubāzēm attālināti pieslēgties darbinieki var tikai caur šifrētu VPN savienojumu.

Augsti riski pastāv gadījumos, kad personas dati tiek pārsūtīti, piemēram, izmantojot elektronisko pastu. Vēlams izstrādāt drošu informācijas pārsūtīšanas procedūru, to iekļaujot uzņēmuma iekšējā politikā. Tās ietvaros var paredzēt, piemēram, ka nosūtāmie dati jāaizsargā ar paroli un jāšifrē, kā arī, ka atsevišķiem darbinieku amatiem personas datu pārsūtīšana ir aizliegta, u.c.

Datu šifrēšana ir viens no izplatītākajiem paņēmieniem, kā nodrošināt piekļuvi datiem tikai pilnvarotām personām. Datu "atslēgšanai" parasti nepieciešama parole.

Šifrēšanas parolei ir jābūt sarežģītai, lai to nebūtu iespējams uzminēt ar vienkāršiem paroļu uzlaušanas rīkiem. Lai parole būtu pietiekami droša vēlams ievērot sekojošus kritērijus:

→ parolei jābūt veidotai gan no lielajiem, gan arī no mazajiem burtiem;

→ parolei ir jāsatur gan ciparus, gan arī speciālos simbolus (piemēram, !;@;%; u.c.);

→ parolei jābūt pietiekoši garai, lai to nevarētu uzminēt ar paroļu uzbrukuma metodi (uz vadlīniju sagatavošanas brīdi par drošu paroli tiek uzskatīta parole, kuras garums nav īsāks par 16 rakstzīmēm);

→ paroles nedrīkst atkārtoties.

Šifrēt iespējams gan visu datora cieto disku, gan atsevišķas datnes. Gadījumā, kad piekļuvei personas datiem tiek izmantots internets, arī šo savienojumu var šifrēt ar atbilstošiem šifrēšanas protokoliem.

Ņemot vērā iespējas, telemārketinga uzņēmumi var izskatīt iespēju ieviest arī kriptogrāfijas kontroles pasākumus, vienlaikus nodrošinot arī atbilstošu kriptēšanas atslēgu pārvaldību.

Vēlams izstrādāt iekšējās kārtības noteikumus, kas paredz drošības prasību ievērošanu darbam attālināti. Ar tiem jāiepazīstina visi darbinieki, nodrošinot, ka minētie noteikumi jebkurā brīdī būs tiem brīvi pieejami.

6.3. Mākoņpakalpojumi

Mūsdienās īpašu popularitāti ir ieguvusi mākoņpakalpojumu izmantošana, kas dažādos uzņēmumos un organizācijās uzlabo datu pieejamību. Mākoņpakalpojumu sniegšanas ietvaros pakalpojumu sniedzēji veido liela mēroga datu centrus, un nodrošina to kā pakalpojumu.

Tas nozīmē, ka dati fiziski neatrodas konkrētā uzņēmuma telpās vai ierīcēs, kas var radīt paaugstinātus datu drošības riskus. Jebkurā gadījumā ir jāseko līdz, lai dati būtu drošībā. Vēlams pārbaudīt izvēlēto mākoņpakalpojumu sniedzēju, piemēram, tam pieprasīt pakalpojuma kvalitātes sertifikātu u.c. Inspekcija vērš uzmanību uz pienākumu izvērtēt, vai šie dokumenti nodrošina, ka iespējamais datu apstrādes un aizsardzības riska līmenis konkrētajā gadījumā būs pieņemams un Eiropas Savienības normatīvajam regulējumam atbilstošs. Pakalpojuma sniedzējam jāreaģē nekavējoties, ja viņa sniegtajā pakalpojumā vai izmantotajā programmatūrā tiks konstatēta ievainojamība.

Izmantojot šāda veida pakalpojumus, ieteicams, lai pakalpojumu sniedzēja uzglabātie dati tiktu šifrēti uzglabāšanas vietā, nosakot precīzu kārtību, kas un kādā veidā atbild par attiecīgo šifru atslēgām, parolēm un sertifikātiem.

Veicot personas datu apstrādi "mākonī", pakalpojumu sniedzējs kļūst par apstrādātāju, ar kuru jānoslēdz rakstveida līgums.

Izvēlētajam mākoņpakalpojumu sniedzējam būtu jānodrošina uzņēmumam iespējas kontrolēt to, kurš, kad un kādiem datiem piekļūst. Pirms konkrētā pakalpojuma sniedzēja izvēles, vēlams izvērtēt tehniskā atbalsta pieejamību, kā arī, cik lielā mērā makoņpakalojuma sniedzējs spēj rast risinājumu neparedzētos pakalpojumatteices gadījumos, lai spētu nodrošināt tā nepārtrauktību.

Tāpat, ne mazāk būtiski pārliecināties, vai personas dati tādējādi netiktu nodoti (tas ietver arī glabāšanu) uz trešām valstīm. Šādā gadījumā jāņem vērā Datu regulas V nodaļas nosacījumi. Atbilstoši Datu regulas 44. pantam personas datus, kas tiek apstrādāti vai kurus ir paredzēts apstrādāt pēc nosūtīšanas uz trešo valsti vai starptautisku organizāciju, nosūta tikai tad, ja, ņemot vērā citus šīs regulas noteikumus, pārzinis un apstrādātājs ir ievērojuši šajā nodaļā paredzētos nosacījumus, ietverot arī personas datu tālāku nosūtīšanu no trešās valsts vai starptautiskās organizācijas uz citu trešo valsti vai citu starptautisku organizāciju. Piemēro visus šīs nodaļas noteikumus, lai nodrošinātu, ka nemazinās ar šo regulu garantētais fizisku personu aizsardzības līmenis.

Gadījumā, ja plānots lauzt līgumu ar mākoņpakalpojumu sniedzēju, tam visi saņemtie dati un to rezerves kopijas ir neatgriezeniski jāiznīcina.

Datu valsts inspekcija
Elijas iela 17, Rīga, LV-1050
pasts@dvi.gov.lv
t. 67223131
www.dvi.gov.lv