Datu valsts inspekcija

PERSONAS DATU APSTRĀDE TELEMĀRKETINGA JOMĀ PĀRZIŅA STATUSĀ

VADLĪNIJAS

2026

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
Komersants – uzņēmums, juridiska vai fiziska persona jeb pārzinis, kura mērķis ir komerciālu paziņojumu sūtīšana zvanu veidā esošiem vai potenciālajiem klientiem (tekstā saukts arī par pārzini)

Vadlīnijās papildu uzmanības pievēršanai tiek izmantoti šādi apzīmējumi:

Pievērs uzmanību! – Papildu piezīme tekstā norādītajam teorētiskajam skaidrojumam

Piemērs: Praktisks piemērs, lai uzskatāmāk skaidrotu vadlīnijās ietverto informāciju

SATURS

IEVADS

Komerciālas informācijas sūtīšana elektroniskā veidā mūsdienās nav zaudējusi savu aktualitāti. Attīstoties tehnoloģijām un mārketinga metodēm, komerciālas informācijas nosūtīšana, jo īpaši zvanu 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.

Šo vadlīniju mērķis ir veicināt Datu regulas un ISPL prasību izpildi uzņēmumos, kuri veicina savu attīstību, izmantojot telemārketinga paņēmienus. Tāpat ar vadlīniju sagatavošanu iecerēts izglītot un informēt komersantus par labo praksi, niansēm un noteikumiem, kas jāņem vērā, veicot telemārketingu un nododot šo uzdevumu uz līguma pamata izpildīt citam komersantam - apstrādātājam. Iepazīšanās ar vadlīnijām varētu mudināt komersantus sakārtot savus iekšējos un ārējos procesus, kā arī veicināt godprātīgu attieksmi pret saviem esošajiem un potenciālajiem klientiem.

Apstrādātāja atbildība un darbības robežas attiecībā uz telemārketinga pakalpojumu sniegšanu pie pārziņa jau tika skaidrota Inspekcijas vadlīnijās "Personas datu apstrāde telemārketinga jomā apstrādātāja statusā". Tomēr arī šajās vadlīnijās, ņemot vērā, ka arī pārziņa sasniegto mērķu datu apstrādē un telemārketingā neatņemama loma ir apstrādātājam, to savstarpējās attiecības un atbildība tiks skaidrota atkārtoti.

Vadlīnijām ir rekomendējošs raksturs un tās adresētas uzņēmumiem, kuri savu mārketinga stratēģiju piekopj, īstenojot telemārketingu, tostarp izejošo zvanu centru darbību, sūtot saviem klientiem komerciālus paziņojumus (zvanus), lai reklamētu preces un pakalpojumus – paši vai piesaistot apstrādātāju, uzņēmumu vai personu, kas šīs darbības veic pārziņa vārdā. Tomēr vadlīnijas varētu būt noderīgas ikvienam interesentam, tai skaitā komerciālu paziņojumu saņēmējiem – fiziskām personām. Vadlīnijas ir noderīgas un vispārīgi saistošas arī pārziņiem, kuru darbības ir saistītas ar komerciālu paziņojumu sūtīšanu arī SMS un elektroniskā pasta veidā vai ikvienam sūtījumam, kas veikts, izmantojot elektroniskos sakarus.

Šīs vadlīnijas nav izsmeļošas, un vienlaikus tās atspoguļo Inspekcijas un citu uzraudzības iestāžu, regulatoru un vadlīniju interpretāciju par normatīvajos aktos noteikto, un ir uzskatāmas par labās prakses ceļvedi.

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

1. TELEMĀRKETINGA REGULĒJOŠO NORMATĪVO AKTU MIJIEDARBĪBA

Uz personas datu apstrādi, kas veikta telemārketinga ietvaros, galvenokārt attiecināmi divi normatīvie akti, kuru izpildi uzrauga Inspekcija, proti, ISPL, kas pieņemts, lai tai skaitā transponētu E-privātuma direktīvu, un 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.

Tādējādi prasības piekrišanai piemērojamas gan gadījumā, kad, veicot telemārketinga darbības, sūtot komerciālus paziņojumus klientam, tiek veikta datu apstrāde, un arī tad, kad komersants klientu – komerciāla paziņojuma saņēmēju nevar identificēt kā fizisku personu, piemēram, ja komersanta rīcībā ir tikai personas telefona numurs. Sīkāk par piekrišanas kā tiesiskā pamata būtību skaidrots šo vadlīniju 3.1. apakšnodaļā.

[2] Papildu 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

2. TELEMĀRKETINGA PROCESOS IESAISTĪTĀS LOMAS

Telemārketinga ietvaros veiktā personas datu apstrāde bieži vien ietver vairākus dalībniekus, kuri var pildīt atšķirīgas lomas atkarībā no savstarpēji nolīgtā. Pārziņiem un apstrādātājiem būtu laicīgi jānosaka sasvstarpējo lomu un atbildības sadale, lai spētu nodrošināt datu subjekta tiesību aizsardzību un tiesisku datu apstrādi.

Ja nav pietiekami skaidri noteikta pušu atbildība, pastāv vieta interpretācijām un neskaidrību risks, tādējādi visos gadījumos izšķirošais uzdevums ir nodrošināt pietiekamu skaidrību, lai varētu nodrošināt lomu piemērošanu un apstrāžu atbilstību.

Praksē situācijas nereti var būt komplicētas un savstarpējo pušu loma grūti nosakāma. Situācijās, kad zvanu centrs pats nosaka, kam zvanīt, kādus personas datus vākt un kā tos izmantot savu nolūku sasniegšanai (piemēram, pārdošanai vairākiem klientiem), tas var kļūt par kopīgu vai pat atsevišķu pārzini. Šādā gadījumā tas uzņemas pilnu atbildību par atbilstošu datu subjektu informēšanu, datu apstrādes tiesiskumu un pārējo datu subjektu tiesību nodrošināšanu. Līdz ar to katrā konkrētajā situācijā būtiski ir izvērtēt visus ar apstrādi saistītos aspektus, lai spētu atbilstoši noteikt, kurš ir pārzinis un kurš - apstrādātājs.

2.1. DATU SUBJEKTS JEB KOMERSANTA KLIENTS

Šajās vadlīnijās tiek skaidrots, kā veicami telemārketinga zvani tieši fiziskām personām. Kad komersanta rīcībā ir ne vien klienta telefona numurs, bet arī vārds vai kādi citi personas dati, tad datu aizsardzības kontekstā šo personu sauc par datu subjektu, kurai attiecīgi ir piemērojamas Datu regulā noteiktās datu subjekta tiesības uz datu dzēšanu, iebilšanu pret datu apstrādi, piekrišanas atsaukšanu jebkurā brīdī, datu labošanu u.c. Datu regulas III nodaļā noteiktās tiesības. Savukārt personai, kurai sūta komerciālus paziņojumus telefoniski, apstrādājot vien telefona numuru, ir tiesības uz piekrišanas atsaukšanu jebkurā brīdī. Šīm personām arī ir tiesības būt informētām par to, kā piekrišana komerciālu zvanu saņemšanai tika iegūta, tādējādi komersantam vienmēr ir jābūt spējīgam pierādīt, ka tā patiesi ir iegūta.

2.2. PĀRZINIS

Datu regulas 4. panta 7. punktā noteikts, ka pārzinis ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kas viena pati vai kopīgi ar citām nosaka personas datu apstrādes nolūkus un līdzekļus.

Tādējādi pārzinis ir "persona", kas vienlaikus nosaka, kā datus ir nepieciešams apstrādāt, nosaka datu apstrādes mērķi jeb nolūku, kā arī atbild par šo apstrādi datu subjekta (klienta) un Inspekcijas priekšā, un nepieciešamības gadījumā norīko citu personu, kas tā vārdā veiks klienta datu apstrādi jeb šajā gadījumā – veiks telemārketinga zvanus pārziņa klientiem.

Pārzinis jebkuras datu apstrādes ietvaros, kā arī telemārketinga darbību ietvaros veiktās datu apstrādēs ir juridiska vienība vai fiziska persona, kas atbild par veikto datu apstrādi un tās atbilstību normatīvajam regulējumam.

Ja komersants (tā darbinieks vai pārstāvis) veic zvanu fiziskai personai, zinot tikai tās tālruņa numuru, tad tas nav uzskatāms par pārzini Datu regulas izpratnē, jo netiek apstrādāti personas dati. Tomēr tas atbild par to, ka tiek izpildītas ISPL noteiktās prasības, veicot komerciālus zvanus.

Liekot kopā Datu regulas 4. panta 1. (personas dati), 2. (apstrāde) un 7. punktu (pārzinis) telemārketinga kontekstā, secināms, ka datu apstrāde, ko veic pārzinis, ir visa veida darbības ar informāciju par identificētu vai identificējamu personu, piemēram, tās vārda, pirkumu vēstures un telefona numura izmantošana, lai komersants vai tā pārstāvis veiktu zvanu par jaunu piedāvājumu vai īpašu atlaidi.

Šajā gadījumā komersants ir uzskatāms par datu apstrādes pārzini, kas pats apzinās un atbild par to, kādi dati ir tā rīcībā, kā arī to kādēļ un pamatojoties uz kādu likumisko pamatu tos var apstrādāt[3].

[3] Saskaņā ar Datu regulas 6. panta 1. punktu, lai datu apstrāde būtu likumīga, pārzinis apstrādei piemēro vismaz vienu no šajā punktā minētajiem pamatojumiem.

Gadījumos, kad apstrādes nolūkus, pamatojoties uz rakstveida vienošanos, vieniem un tiem pašiem mērķiem nosaka divi vai vairāki pārziņi, tos datu aizsardzības kontekstā sauc par "kopīgiem pārziņiem"[4].

2.3. APSTRĀDĀTĀJS

Arī telemārketinga jomā pārziņa jēdzienam un tā mijiedarbībai ar apstrādātāja jēdzienu ir principiāla nozīme Datu regulas noteikumu 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. punktā noteikts, ka "apstrādātājs" ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus.

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

→ jābūt atsevišķam tiesību subjektam attiecībā pret pārzini;

→ jāapstrādā personas dati tā uzdevumā.

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

Piemērs: **Uzņēmums G nodarbojas ar galda spēļu tirgošanu savā interneta veikalā. Uzņēmuma vadība kopā ar mārketinga speciālistu nolēmusi, ka pie pasūtījuma veikšanas klientam tiks prasīta piekrišana tā tālruņa numura izmantošanai komerciālu paziņojumu sūtīšanai par aktuāliem Uzņēmuma G piedāvājumiem un publiskām un individuālām atlaidēm. Šāds darbības veids izvēlēts, lai ar šiem paziņojumiem mudinātu pastāvīgos pircējus e-veikalā iepirkties atkal vai ieteikt veikalu draugiem, un tādējādi, vēlams, palielinātu uzņēmuma ienākumus un atpazīstamību tirgū. Tomēr, lai šo mērķi sasniegtu efektīvāk, Uzņēmums noslēdzis sadarbību ar Uzņēmumu P, kas tā vārdā veiks telemārketinga zvanus un informēs klientus par jaunumiem. Uzņēmums P šajā sadarbībā uzskatāms par "apstrādātāju".**

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

Darbinieki, kas strādā pārziņa pakļautībā nav apstrādātāji, tie ir daļa no pārziņa. Apstrādātājs ir atsevišķs uzņēmums, persona, iestāde, kas parasti veic uzdevumus un darbības, kuras pārzinis resursu, zināšanu vai pieredzes trūkuma dēļ nodod izpildei kādam, kas specializējas šajā jomā.

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, lai izpildītu pārziņa uzdevumu un nodrošinātu drošu apstrādi.

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, pats nosakot apstrādes nolūkus un līdzekļus, to atzīst par pārzini attiecībā uz minēto apstrādi (Datu regulas 28. panta 10. punkts). Tāpat tas ir gadījumā, ja pārziņa darbinieks pārkāpj Datu regulu, un ir pierādāms, ka nav saredzama pārziņa vaina vai neizdarība apstrādes pārkāpuma rašanās iemeslā, bet darbinieks apstrādi veicis personisku, sevis noteiktu nolūku ietvaros.

[4] Datu regulas 26. panta 1. punkts.

Piemērs: Uzņēmums X dažādiem uzņēmumiem sniedz mārketinga pakalpojumus. Tas noslēdz Datu regulas 28. panta 3. punktam atbilstošu līgumu ar uzņēmumu Y. Tomēr uzņēmums X nolemj izmantot uzņēmuma Y datubāzi arī saviem nolūkiem sava uzņēmuma popularizēšanai, nevis kā noteicis 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 pārzinis praksē joprojām nosaka apstrādes nolūkus un līdzekļus. Tomēr vienlaikus jāizvērtē, vai apstrādātājs ļauj komersantam (pārzinim) 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 noslēguši līgumu.

Pārzinis var izmantot un apstrādātājs var piedāvāt arī iepriekš izstrādātu pakalpojumu, tomēr vienlaikus jāatceras, ka tieši pārzinis pieņem galīgo lēmumu attiecībā uz apstrādes būtiskajiem aspektiem.[5]

Piemērs: Uzņēmums X piedāvā mākoņpakalpojumus uzņēmumam B. Uzņēmums X vēlas slēgt standarta vienošanos, kāda tiek piedāvāta visā pasaulē, t.sk. ārpus Eiropas Savienības robežām. 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) ievēros arī datu glabāšanas termiņus, to dzēšanu veiks atbilstoši uzņēmuma B norādījumiem, u.tml. Pārliecināties, vai izvēlētais apstrādātājs ir "pārbaudāms" izpētot publiski pieejamo informāciju (tīmekļvietne, publikācijas, viedokļi), kā arī paša potenciālā apstrādātāja sniegto informāciju par datu aizsardzības prakšu piemērošanu, gatavību pildīt pārziņa uzdevumus, apmācīt darbiniekus, nodrošināt ne tikai pakalpojuma faktisku, bet arī likumīgu izpildi.

2.4. 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. Apstrādātājs personas datus apstrādā tikai pārziņa uzdevumā un pēc pārziņa noteiktiem nolūkiem.

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 saistoši apstrādātājam un pārzinim[6]. Tos jānoslēdz rakstveidā, tostarp elektroniski[7]. Pār līguma saistību izpildi atbildīgs ir gan pārzinis, gan apstrādātājs.

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

[5] 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

[6] Datu regulas 28. panta 3. punkts

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

izmantot līguma standartklauzulas[8], kas saistītas ar pienākumiem, kuri noteikti Datu regulas 28. pantā[9]. Tā kā Datu regula paredz skaidru pienākumu slēgt rakstisku līgumu, ja nav spēkā cita atbilstoša juridiska akta, līguma neesamība ir Datu regulas pārkāpums.

Ieteicams arī kā līguma sastāvdaļu, piemēram, līguma pielikuma veidā, sagatavot arī apstrādātājam veicamo sarunu ar klientiem ceļvedi jeb *skriptu*. Tas var būt vispārīgs, bet pietiekami detalizēts apraksts par to, ko jāsatur sarunai ar sazvanīto klientu, vai arī skaidrs sarunas atveidojums par to, kā uzsākama saruna, kas darāms, ja klients atsauc savu piekrišanu datu apstrādei. Šim sarunas plānam jābūt koncentrētam uz datu apstrādes jautājumiem, lai apstrādātājs neapzināti neaizskartu klientu tiesības, tomēr tas, ja nepieciešams, papildināms arī ar saturu, kas tieši saistīts ar komercdarbību un patieso zvana mērķi. Ja sarunas ceļvedi sagatavo apstrādātājs, pārzinim tas rūpīgi jāpārbauda, nepaļaujoties uz apstrādātāja vienpersonisku viedokli.

Īpaši vēršam uzmanību uz šādiem apstrādātāja pienākumiem attiecībā pret pārzini:

→ apstrādātājs drīkst apstrādāt datus tikai saskaņā ar pārziņa dokumentētiem norādījumiem;

→ jānodrošina, ka personas, kuras ir pilnvarotas apstrādāt datus, ir apņēmušās ievērot konfidencialitāti vai tām ir noteikts attiecīgs likumisks pienākums ievērot konfidencialitāti;

→ jāievēro Datu regulas 28. panta 2. un 4. punktā minētie nosacījumi, saskaņā ar kuriem tiek piesaistīts cits apstrādātājs;

→ jāpalīdz pārzinim [..] izpildīt savu pienākumu atbildēt uz pieprasījumiem par [..] datu subjekta tiesību īstenošanu;

→ jāpalīdz pārzinim nodrošināt Datu regulas 32. līdz 36. pantā minēto pienākumu izpildi;

→ pēc apstrādes pakalpojumu sniegšanas pabeigšanas apstrādātājam pēc pārziņa nosacījumiem jādzēš vai jāatdod visi personas dati pārzinim un jādzēš esošās kopijas;

→ jādara pārzinim pieejama visa informācija, kas nepieciešama, lai apliecinātu, ka tiek pildīti Datu regulas 28. pantā paredzētie pienākumi, un lai ļautu pārzinim vai citam pārziņa pilnvarotam revidentam veikt revīzijas, tostarp pārbaudes, un sniegtu tajās ieguldījumu[10];

→ apstrādātājam jāuztur visu pārziņa vārdā veikto apstrādes darbību kategoriju reģistrs[11];

→ jāīsteno atbilstīgi tehniski un organizatoriski pasākumi, lai nodrošinātu tādu drošības līmeni, kas atbilst riskam[12];

→ tiklīdz apstrādātājam kļuvis zināms personas datu aizsardzības pārkāpums, bez nepamatotas kavēšanās jāpaziņo par to pārzinim[13];

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

Sagatavojot līgumu jāņem vērā konkrētie apstrādātāja uzdevumi un pienākumi saistībā ar veicamo apstrādi un risku datu subjekta tiesībām un brīvībām[14].

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;

---

[8] 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

[9] 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.

[10] Apstrādātāja pienākumi attiecībā pret pārzini uzskaitīti Datu regulas 28. panta 3. punktā

[11] Datu regulas 30. panta 2. punkts

[12] Datu regulas 32. pants

[13] Datu regulas 33. panta 2. punkts

[14] Datu regulas 81. apsvērums

→ cita būtiska informācija attiecībā uz apstrādes riskiem un papildus piemērojamām prasībām.[15]

Noslēgtajā līgumā par apstrādi nevajadzētu atkārtot Datu regulas noteikumus. Jāiekļauj specifiskāka, konkrētāka informācija par to, kā tiks izpildītas prasības un kāds drošības līmenis ir nepieciešams to personas datu apstrādei, kas ir līguma par apstrādi priekšmets.[16] Līguma noslēgšanai nevajadzētu būt vien formalitātei, lai abas puses būtu juridiski nodrošinājušās, bet arī, lai apstrādātājam no līguma vien būtu skaidrs, kādos nolūkos pārzinis to norīkojis un kādas ir gan apstrādes, gan sadarbības robežas. Tāpat līguma saturam nevajadzētu būt universālam, bet piemērotam gan katrai sadarbībai, gan katrai apstrādei (-ēm).

Pārzinim nevajadzētu paļauties uz iepriekšēju veiksmīgu sadarbību ar apstrādātāju, līdzšinējo lojalitāti pret pārzini vai apstrādātāja labu attieksmi vai publisko reputāciju, un tādēļ neslēgt ar to līgumu par datu apstrādes veikšanu vai nodrošināt to izteikti formālā veidā. Arī uzticība potenciālā apstrādātāja labai gribai vai zināšanām datu aizsardzībā nav pamats neslēgt savstarpēju līgumu.

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[17]. Tomēr pašlaik minētajam ir tikai ieteikuma raksturs.

2.5. APAKŠAPSTRĀDĀTĀJS

Iespējami gadījumi, kad apstrādātāji procesā piesaista citu dalībnieku, tam uzticot darbības, kas ietver pārziņa uzticēto 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. Arī šajā gadījumā pārzinis saglabā tiesības noteikt personas datu apstrādes nolūkus un līdzekļus.

Vienlaikus pietiekami jāgarantē, ka tiks piemēroti tehniskie un organizatoriskie pasākumi tādā veidā, lai apstrādē tiktu ievērotas Datu regulā noteiktās prasības. Līdzīgi kā pārziņa-apstrādātāja līgumam, arī apstrādātāja un apakšapstrādātāja līgumam jābūt sagatavotam pēc būtības, nevis izmantojot universālu un formālu līguma veidni.

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.

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".

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

---

[15] 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

[16] 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

[17] Papildu informāciju skatīt: EDAK un EDAU Kopīgais atzinums 1/2021 par Eiropas Komisijas Īstenošanas lēmumu par standartklauzulām līgumos starp pārziņiem un apstrādātājiem jautājumos, 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

attiecībā uz tehniskiem un organizatoriskiem pasākumiem, ekspertu zināšanas, uzticamība un resursi)[18]. 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[19]. Jānodrošina, ka apstrādātājs ierosina tikai tādus "apakšapstrādātājus", kuri sniedz pietiekamas garantijas.[20]

Par apakšapstrādātāju nav uzskatāmas personas, kas ir pārziņa vai apstrādātāja darbinieki, bet atsevišķa organizācija, fiziska vai juridiska persona, kas pēc apstrādātāja norīkojuma veiks apstrādātājam no pārziņa uzdotās funkcijas, kuras apstrādātājs nespēj paveikt resursu vai zināšanu trūkuma dēļ.

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

Detalizēta analīze par lomu noteikšanu un dažādu situāciju analīzi datu apstrādē ir veikta Eiropas Datu aizsardzības kolēģijas 2020. gada jūlija pamatnostādnēs par pārziņa un apstrādātāja jēdzieniem VDAR: https://www.edpb.europa.eu/system/files/2023-10/edpb_guidelines_202007_controllerprocessor_final_lv.pdf.

3. APSTRĀDES LIKUMĪBA

Datu regulas kontekstā personas datu apstrāde ir pieļaujama tikai tad, ja tā balstās uz kādu no Datu regulas 6. panta 1. punktā noteiktajiem tiesiskajiem pamatiem. Savukārt ISPL normatīvais ietvars norāda uz nepieciešamību šādu personas datu apstrādi pamatot ar datu subjekta dotu brīvu un nepārprotamu piekrišanu, kas ir atbilstoša Datu regulas prasībām attiecībā uz datu subjekta piekrišanu.

3.1. 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[21]. Tātad apstrādātājs drīkst nosūtīt komerciālu paziņojumu fiziskai personai tikai tad, kad tam iepriekš ir nodrošināta atbilstoša piekrišana[22].

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

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.

---

[18] 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.

[19] Datu regulas 28. panta 4. punkts

[20] 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

[21] ISPL 9.panta trešā daļa.

[22] Ņemot vērā, ka komerciālu paziņojumu sūtīšana zvana veidē pieļaujama vien uz piekrišanas pamata, citu likumisko pamatu analīze šajās vadlīnijās netiks veikta.

Piekrišana ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta (komerciāla paziņojuma saņēmēja) vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei[23].

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.

Publiski pieejamā veidā fizisku personu kontaktinformāciju publicē 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.

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.

Piemērs: **Pie uzņēmuma X persona iegādājās elektropreces, vienlaikus uzņēmuma X tīmekļa vietnē izveidojot klienta profilu. Klients pasūtījuma pieteikumā atzīmēja, ka vēlas saņemt aktuālus jaunumus telefona zvanu veidā par uzņēmuma X atlaidēm un jaunākajām precēm, izmantojot pasūtījuma formā norādīto tālruņa numuru. Tajā pašā nedēļā, kad pasūtījums vēl tika apstrādāts, persona nolēma tomēr piekrišanu atsaukt sarunas laikā ar uzņēmuma X pārstāvi. Pēc šīs piekrišanas atsaukšanas, uzņēmuma X rīcībā joprojām palika personas telefona numurs tādā nolūkā, lai kurjerdienests varētu SMS veidā atsūtīt pakomāta piekļuves informāciju. Tomēr komerciālu paziņojumu izteikšanas nolūkam šis telefona numurs vairs nav izmantojams.**

3.2. PIEKRIŠANAS DERĪGUMA TERMIŅŠ

Attiecībā uz datu glabāšanas ilgumu Datu regulā noteikts, ka datus glabā ne ilgāk kā nepieciešams mērķa jeb nolūka sasniegšanai. Viens kritērijs, kad iegūtā piekrišana ir "dzēšama" jeb dati, kas iegūti uz piekrišanas pamata, ir dzēšami, kad datu subjekts šo piekrišanu atsauc. Kad datu subjekts ir noteicis, ka vairs nevēlas saņemt komerciālus paziņojumus zvanu veidā (šāda iespēja jāparedz ikkatra komerciāla zvana laikā), tad komersantam šāda izvēle ir jārespektē, un tas nedrīkst radīt nelabvēlīgas sekas datu subjektam. Ja komersanta rīcībā līdz šim bija tikai neidentificējamas personas kontaktinformācija – telefona numurs komerciālu piedāvājumu izteikšanai, tad pēc piekrišanas atsaukšanas nekādai informācijai komersanta rīcībā vairs nevajadzētu būt. Savukārt, ja komersanta rīcībā ir arī klienta informācija, kas saistīta ar tā veiktu pasūtījumu, tad šī informācija, neatkarīgi no piekrišanas atsaukšanas, paliek tā rīcībā (citam mērķim), līdz tai iestājas glabāšanas termiņš, bet izmantot to komerciālu paziņojumu izteikšanai gan vairs nav pamata.

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

Ja persona piekrišanu neatsauc, komersantam tik un tā būtu jānosaka periods, cik ilgi piekrišanu un ar to iegūtos datus glabāt. Kaut arī piekrišanai nav noteikta termiņa, tai nevajadzētu būt sniegtai uz bezgalīgu periodu. Tādējādi piekrišanas glabāšanas ilgums atšķirsies no gadījuma uz gadījumu. Ja piekrišana ir prasīta uz konkrētas mārketinga kampaņas īstenošanas laiku, tad pēc šīs kampaņas beigām dati, kas iegūti līdz ar piekrišanu, būtu jādzēš.

Jāņem vērā, ka Latvijā 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 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 komersants, 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 un īstenošanu.

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, piemēram, telefonsarunas laikā.

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. Tāpat zem "klienta kontaktinformācija" var paiet gan klienta telefona numurs, gan e-pasta adrese, līdz ar ko klientam būtu jānodrošina iespēja piekrist katram komunikācijas veidam atsevišķi.

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.[24]

Ja sazvanītā persona zvana laikā atsauc piekrišanu turpmākai komerciālu zvanu saņemšanai un datu apstrādei (ja šajā nolūkā tika apstrādāti arī personas dati), tad arī apstrādātājam ir pienākums to ievērot, par minēto bez kavēšanās informējot arī konkrēto pārzini.

[24] 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

Praksē nereti informāciju par piekrišanas atsaukšanu fiksē apstrādātāju 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.

Zvana veikšana uz automātiski ģenerētu numuru, lai iegūtu personas piekrišanu turpmāku komerciālu paziņojumu sūtīšanai tā paša zvana laikā vai zvanot citreiz, neatbilstu komerciāla paziņojuma sūtīšanas nosacījumiem, jo pašā būtībā galvenais zvana mērķis ir tālāka komerciāla paziņojuma nodošana, bet piekrišanas iegūšana – vien formāla ISPL prasību izpilde.

3.3. DATU DZĒŠANA

Personas datu apstrādes principi nosaka pienākumu pārzinim izmantot personas datus tikai konkrētos, skaidros un leģitīmos nolūkos, un to turpmāka izmantošana netiek ar minētajiem nolūkiem nesavietojamā veidā, tostarp, tos nedrīkst glabāt ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā. Līdz ar to apstrādātājam pēc pakalpojuma sniegšanas pabeigšanas ir jānodrošina visu viņa rīcībā esošo personas datu dzēšana vai atgriešana pārzinim.
Konkrētais datu apstrādes beigu brīdis un turpmāka rīcība un atbildība būtu jānosaka savstarpējā līguma ietvaros, skaidri paredzot:

- datu apstrādes mērķi un termiņu,
- kādi personas dati jādzēš,
- vai tie jānodod pārzinim,
- kāda ir dzēšanas kārtība (piemēram, manuāla vai automātiska),
- vai un kā apstrādātājs informē par dzēšanu,
- vai / kā tiek dzēstas arī rezerves kopijas un *logfaili* (žurnāli).

Pēc telemārketinga kampaņas noslēguma apstrādātājam jāizpilda līgumā ietverts pienākums neatgriezeniski dzēst saņemtās datubāzes, tostarp tajās ietvertos personas datus, piemēram, klientu vārdus, telefona numurus u.c. Šie dati nedrīkst tikt izmantoti citiem nolūkiem, saglabāti ilgāk nekā nepieciešams vai nodoti trešajām pusēm.

Lai izpildītu dzēšanas pienākumu, apstrādātājam jānodrošina, ka:

- dzēšana tiek veikta arī no visām datu glabāšanas vietām,
- ir pierādāma dzēšanas veikšana (piemēram, dzēšanas protokoli vai žurnāli),
- nepieciešamības gadījumā par dzēšanu tiek informēts pārzinis.

Šo pienākumu ieteicams detalizēti atrunāt apstrādes līgumā starp pārzini un apstrādātāju, tostarp noteikt precīzus termiņus, metodes un pienākumus. Līgumam jāsatur arī skaidrs apraksts par to, vai pēc padarītā datus dzēš apstrādātājs vai tos dzēšanai nodot pārzinim.

3.4. SARUNU IERAKSTĪŠANA UN IERAKSTU GLABĀŠANA

Lai uzlabotu klientu apkalpošanas kvalitāti, nereti sastopama prakse telemārketinga pakalpojumu sniegšanas laikā ir arī telefonsarunu ierakstīšana. Lai nerastos riski, kas saistīti ar personas datu apstrādes tiesiskumu, svarīgi sākotnēji nodrošināt, ka šī datu apstrāde notiek saskaņā ar Datu regulas prasībām. Proti, sarunu ierakstīšana drīkst notikt tikai, ja tam ir atbilstošs tiesiskais pamats. Tā kā sarunu ieraksts parasti notiek, lai aizsargātu pārziņa vai apstrādātāja intereses nolūkā uzlabot pakalpojuma sniegšanas vai sarunas kvalitāti, tad šāda datu apstrāde visbiežāk pamatojama ar leģitīmo interešu īstenošanu jeb Datu regulas 6. panta 1. punkta

f) apakšpunktā noteikto likumisko pamatu.[25] Tāpat pirms ierakstīšanas uzsākšanas obligāti jāinformē sazvanītā persona. Piemēram, katra saruna var sākties ar paziņojumu par sarunas ieraksta veikšanu kvalitātes nodrošināšanas nolūkos, izmantojot jau iepriekš ierakstītu paziņojumu vai tādu, kuru katru reizi informāciju pasniedz zvana veicējs, uzņēmuma darbinieks.

- Sarunu ieraksti jāglabā tikai tik ilgi, cik tas ir nepieciešams noteiktajam mērķim. Piemēram, ieraksti, kas kalpo līdzekļiem kvalitātes uzraudzībā, var tikt glabāti ne ilgāk kā 30 dienas.
- Pēc glabāšanas termiņa beigām ir jānodrošina, ka ieraksti tiek neatgriezeniski dzēsti. Būtu jāizmanto automatizētas dzēšanas sistēmas vai manuāli izpildīti dzēšanas procesi, lai varētu pierādīt, ka dati tiešām ir dzēsti.
- Ierakstiem jābūt nodrošinātiem ar autentifikāciju un piekļuves ierobežojumiem, kas nozīmētu, ka tikai pilnvarotām personām būtu iespēja piekļūt ierakstiem.
- Svarīgi ar noteiktu regularitāti veikt iekšējos auditus, lai uzraudzītu glabāšanas termiņu ievērošanu, kā arī laicīgi konstatētu citas apstrādes neatbilstības.
- Datu subjektiem ir tiesības zināt, ka tiek veikta datu apstrāde sarunu ieraksta veidā, un jābūt pieejamai informācijai par šo datu apstrādi.

Pārzinim ir būtiski nodrošināt pārskatāmu un pārredzamu ārēju un iekšēju personas datu apstrādes politiku, kas izriet no sarunu ierakstīšanas un ierakstu glabāšanas, kas veicinās personas datu apstrādes principu ieviešanu uzņēmumā, kā arī datu subjektu uzticību.

3.5. DATU SUBJEKTA TIESĪBU ĪSTENOŠANA

Datu regulas III nodaļā noteiktas datu subjekta tiesības, kuras pārzinim jeb komersantam jānodrošina, veicot personas datu apstrādi. Datu regulas 12. pants pārzinim uzliek ietvaru un norādes kā to sasniegt, proti, informācija jāsniedz kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, izmantojot skaidru un vienkāršu valodu. Datu subjektam jāsniedz visa Datu regulas 13. un 14. pantā minētā informācija un jānodrošina visa Datu regulas 15.–22. pantā un 34. pantā minētā saziņa attiecībā uz apstrādi, jo īpaši attiecībā uz visu informāciju, kas konkrēti paredzēta bērnam.

Saskaņā ar Datu regulas III nodaļu datu subjektam ir tiesības uz informāciju, piekļuves tiesības, tiesības uz labošanu, tiesības datu uz dzēšanu jeb tiesības tikt aizmirstam, tiesības ierobežot datu apstrādi, tiesības uz datu pārnesamību, tiesības iebilst, tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde. Pārzinim ne tikai ir jāīsteno šīs tiesības, kad tas nav pretrunā ar normatīvo regulējumu vai citiem apsvērumiem, bet arī jāinformē datu subjektu par šādu tiesību esamību.

Svarīgi vispirms komersantam iekšēji noteikt kādas apstrādes tiks veiktas, kāds būs to nolūks un tiesiskais pamats. Ņemot vērā nolemto, jāizstrādā procedūras, atbilstoši tiesiskā pamata specifikai. Piemēram, ja tiesiskais pamats būs datu subjekta piekrišana, tad, lai tā būtu spēkā, pārzinim tā jāizstrādā atbilstoši Datu regulas 7. panta prasībām. Tālāk, ņemot vērā noteikto tiesisko pamatu, pārzinim jāsniedz informācija par datu subjekta tiesībām. Tāpat ir jānosaka datu subjekta tiesību īstenošanas procedūra un kārtība – kā tiks informēti datu subjekti atbilstoši Datu regulas 13. un 14. pantā noteiktajām prasībām. Pareiza tiesiskā pamata piemērošana ļaus pārzinim sniegt atbilstošu informācijas apjomu par datu subjekta tiesībām.

Komersantam jānosaka, kādus komunikācijas kanālus datu subjektam izmantot, lai noskaidrotu informāciju par konkrēti savu datu apstrādi pie komersanta, kā tiks risināti datu subjekta tiesību īstenošanas jautājumi, ja datu subjekts savu vēlmi izteiks pie apstrādātāja. Pārzinis var lūgt palīdzību apstrādātājam īstenot datu subjekta tiesības, kad tas vērsies pie apstrādātāja, bet arī var ieviest kārtību, ka, ja datu subjekts vēlas izteikt savu vēlmi, tad tas izdarāms vienīgi pie pārziņa. Būtu jāņem vērā, ka datu subjekta novirzīšana pie vienas vai otras lomas būtu jāizskauž, kad datu subjekts vēlas īstenot tiesības uz savu datu dzēšanu attiecībā uz piekrišanas atsaukšanu. Minētais neatbildīs piekrišanas vienai no pazīmēm, ka to atsaukt ir tikpat viegli, cik to sniegt. Attiecīgi, ja datu subjekts piekrišanu vēlas atsaukt sarunas laikā ar apstrādātāju, šis lūgums ir jāīsteno, nelūdzot datu

[25] Vairāk par leģitīmo interešu īstenošanu kā likumisko pamatu datu apstrādei, skaidrots Eiropas Datu aizsardzības kolēģijas 2024. gada 8. oktobra Pamatnostādnēs 1/2024 par datu apstrādi, pamatojoties uz Datu regulas 6. panta 1. punkta f) apakšpunktu. Pieejams: https://www.edpb.europa.eu/system/files/2024-10/edpb_guidelines_202401_legitimateinterest_en.pdf

subjektam veikt citas papildu darbības. Šādā gadījumā, ievērojot integritātes principu, apstrādātājs informāciju par piekrišanas atsaukšanu nodos arī pārzinim.

Pārzinim ar apstrādātāju būtu arī jāvienojas par to, kādu informāciju un vai par savu datu apstrādi apstrādātāja darbinieks sniegs datu subjektam telefoniski, tai skaitā par pārziņa identitāti un tiesībām atsaukt piekrišanu zvana laikā.

Tāpat datu subjekti var vērsties pie datu aizsardzības speciālista, ja tāds ir iecelts, visos jautājumos, kas saistīti ar viņu personas datu apstrādi un šajā regulā paredzēto tiesību īstenošanu, publicējot datu apstrādes noteikumus, pārzinim būtu arī jāinformē, kā iespējams sazināties ar komersanta datu aizsardzības speciālistu.[26]

Piemērs: **Komersants informāciju par veiktajām datu apstrādēm savā interneta veikalā apkopojis Privātuma politikā, kas publicēta tīmekļa vietnes apakšā. Privātuma politika ir viegli pieejama arī, kad klients veic pirkumu un tam tiek lūgta piekrišana komerciālu zvanu saņemšanai. Attiecīgi klients, ievadot savu telefona numuru lodziņā un ievietojot "ķeksīti" piekrišanai saņemt komerciālus zvanus par komersanta jaunumiem un atlaidēm, var uzreiz interneta pārlūkprogrammas jaunā cilnē atvērt blakus esošo saiti uz komersanta Privātuma politiku. Zem šīs saites plašāk izlasāms par datu subjekta tiesībām, piekrišanas būtību un nolūku.**

[26] Datu regulas 37. panta 7. punkts un 13. panta 1. punkta b) apakšpunkts

4. KOMERCIĀLA PAZIŅOJUMA SŪTĪŠANAS TIESISKIE UN PRAKTISKIE 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 komerciālu paziņojumu sūtīšanu fiziskām personām attiecināmas daudz stingrākas prasības un atbildība.

Komersants var sūtīt komerciālus paziņojumus juridiskai personai līdz brīdim, kamēr nav saņemts atteikums šādu paziņojumu saņemšanai.[27] Uz juridiskas personas telefona numura sūtītu komerciālu paziņojumu (zvanu) neattiecas sākotnējas piekrišanas iegūšana, tomēr nav pieļaujams izmantot juridiskas personas kontaktinformāciju, lai izteiktu piedāvājumu zvana saņēmējam kā fiziskai personai.

Šajā sadaļā vispirms būtu jāapskata komercdarbības būtība, kuras ietvaros tiek sūtīti komerciāli paziņojumi. Komercdarbība ir saimnieciska darbība, kuru savā vārdā peļņas gūšanas nolūkā veic komersants[28]. Attiecīgi komercdarbības pamatā nav labdarība, brīvprātīgais darbs vai bezmaksas pakalpojumi (izņemot īpašus piedāvājumus, bonusus). Komercdarbības kontekstā ir svarīgi nenovirzīties, ka primāri darbības, ko attiecībā uz klientu veic komersants, ir veiktas peļņas nolūkā. Tādējādi faktiski jebkurš zvans telemārketinga ietvaros (arī SMS, e-pasts), kura rezultātā klients kaut apdomātu iespēju vai nepieciešamību komersanta pakalpojumu izmantot, jāuztver kā potenciāls aicinājums iegādāties, pasūtīt, īrēt, darīt to atkārtoti u.tt.

Zvani par pasūtījuma statusu, problēmām pasūtījumā, piegādē vai citi tehniska rakstura zvani esošam klientam nebūs uzskatāmi par komerciālu paziņojumu, jo tie būs nepieciešami, lai izpildītu līgumu vai, piemēram, pabeigtu pasūtījumu. Savukārt zvans anonīmai personai, kur tikai tās telefona numurs ir komersanta rīcībā, reti kad būs uzskatāmi par ko citu kā mārketinga saziņu. Tāpat kā zvani esošajam klientam par to, ka komersanta tīmekļa vietnē publicēti jauni produkti. Jebkurā gadījumā, tāpat kā ar jebkuru datu apstrādi, jebkura zvana pamatojums un mērķis būtu jāvērtē individuāli, un komersantam vienmēr būtu jāspēj skaidrot un pamatot, kāpēc tas tika veikts.

Veicot komerciālu paziņojumu sūtīšanu fiziskai personai, izmantojot telefonsakarus, būtiski ir izprast arī 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).

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.

Komerciālā paziņojuma būtība un mērķis nemainās no tā, vai patiesais zvana nolūks tiek slēpts vai ir atklāti pateikts.

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.

---

[27] ISPL 9. panta ceturtā daļa

[28] Definīcijas avots: https://tezaurs.lv/komercdarb%C4%ABba

Piemērs: Zvans ar tekstu: "Labdien! Esam izveidojuši jaunu produktu kategoriju mūsu mājas lapā!" (Ir komerciāls paziņojums)

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.

Piemērs: Zvans ar tekstu: "Labdien! Jūsu pasūtījumu saņēmām, bet vēl neizrakstīsim rēķinu, jo viena ķermeņa krēma vietā esat pasūtījis piecdesmit! Vai esat pārliecināts, ka pasūtījumu sastādījāt pareizi?" (Nav komerciāls paziņojums)

Savukārt ISPL 8. panta pirmā daļa noteic, ka komerciāls paziņojums atbilst vispārējām Reklāmas likuma[29] 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.

Lai piemērotu atbilstošus normatīvos aktus komerciālu paziņojumu sūtīšanai un tādējādi apzinātos prasības šādu darbību likumīgai veikšanai, sākotnēji jāsaprot, vai tiks veikta persona datu apstrāde. Kad komersants apstrādā personas telefona numuru, pēc kura atsevišķi personu identificēt nevar, kā arī jā tā rīcībā ir vien personas elektroniskā pasta adrese, netiek veikta datu apstrāde, tādējādi ir piemērojamas vien ISPL noteiktās prasības attiecībā uz komerciāla paziņojuma sūtīšanu.

Ja komersanta rīcībā ir gan viens no iepriekš nosauktajiem papildu identifikatoriem – telefona numurs, gan papildu informācija par personu, piemēram, vārds un uzvārds un citi klienta dati, tad ir jāpiemēro gan ISPL, gan Datu regulas prasības.

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.[30] Pieejas tiesībām datiem darbiniekiem jābūt priviliģētām, atbilstoši tiešajiem darba pienākumiem. Šo personas datu vākšana, glabāšana vai izmantošana ir uzskatāma par apstrādi[31] 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[32]. 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

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

[30] Saskaņā ar Datu regulas 4. panta 1. punktu, personas dati 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.

[31] 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.

[32] ISPL 9. panta piektā daļa.

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.

4.1. FIZISKU UN JURIDISKU PERSONU NOŠĶIRŠANA UN NUMURU ĢENERĒŠANA

Ja fiziska persona jau ir devusi savu piekrišanu komerciālu zvanu saņemšanai, piemēram, ievadot savu tālruņa numuru komersanta tīmekļa vietnes jaunumu lodziņā vai veicot pasūtījumu ir izdarījusi atzīmi, ka piekrīt komerciālu zvanu saņemšanai, tad komersantam ir pamatojums jeb "piekrišana" komerciāla paziņojuma sūtīšanai. Šādā situācijā komersantam nav būtisks zvana saņēmēja statuss, jo neatkarīgi no tā, vai tālruņa numurs pieder fiziskai vai juridiskai personai, katrā nākamajā reizē zvana saņēmējam ir jādod iespēja atteikties no turpmāku zvanu saņemšanas jeb atsaukt iepriekš sniegto piekrišanu.

Tomēr, kad komersants izmanto kādu automātisko telefona numuru ģenerēšanas rīku, pirms komerciāla paziņojuma sūtīšanas ir jābūt skaidrībai par to, vai reklāmas zvana saņēmējs – anonīmā tālruņa numura īpašnieks ir fiziska vai juridiska persona. Komersantam būtu jāizveido procedūra, kurā aprakstīta kārtība, kā tiks noteikts numura īpašnieka statuss. Tālruņa numurus, kuri pieder juridiskām personām, komersants var apzvanīt bez iepriekšējas piekrišanas iegūšanas, tomēr fiziskām personām komerciālus paziņojumus aizliegts sūtīt bez to iepriekšējas piekrišanas iegūšanas.

Kā jau minēts, piekrišana nav iegūstama, zvanot automātiski ģenerētam telefona numuram, bet gan ar aktīvu personas iesaisti pēc savas vēlēšanās, piemēram, kad tas aizpilda anketu internetā, e-pastā vai reģistrējoties lietotnē.

4.2. 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, pārziņi nodod uzņēmumu rīcībā savu datubāzi ar fizisko personu datiem, un konkrētais uzņēmums kā apstrādātājs attiecīgi izmanto šo 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 pārziņa izsniegto datubāzi nedrīkst izmantot cita pārziņa interesēs, piemēram, pārdodot to citam komersantam. 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.

Komersanti kā pārziņi uzņemas atbildību par telemārketinga uzņēmumiem (apstrādātājiem) nodoto datubāžu saturu, tomēr arī apstrādātājam ir jāņem vērā Datu regulas nosacījumi, tai skaitā personas tiesības uz datu aizsardzību, tostarp, datu izmantošana veicot zvanus tikai pastāvot piekrišanai.

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"[33], 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 uzsākta personas datu apstrāde, 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. Tādējādi praksē reti kad automātisku numuru ģenerēšana un pēc tam šo numuru izmantošana komerciālu zvanu veikšanai, būs likumīga un atbilstoša ISPL prasībām.

Nereti pārziņi 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).

4.3. MĒRĶĒTU ZVANU VEIKŠANA FIZISKĀM PERSONĀM

Personas datu apstrāde, kas izriet no telemārketinga, būs likumīga tikai, ja tā būs atbilstoša Datu regulas 5. pantā noteiktajiem personas datu apstrādes principiem, tai skaitā nodrošinot, ka tiek apstrādāti tikai tādi dati, kuru apstrādei pārzinim ir Datu regulas 6. panta 1. punktam atbilstošs tiesiskais pamats.

Ievērojot to, ka personas datu ievākšana vēlāku komerciālu paziņojumu sūtīšanai tiek veikta ar nolūku īstenot darbību, kuras veikšana noteikta ISPL, arī vērtējot Datu regulas tiesiskā pamata piemērošanu, jāņem vērā ISPL noteiktais speciālais regulējums attiecībā uz komerciālu paziņojumu sūtīšanu.

Zvans tiks uzskatīts par komerciālu paziņojumu, ja uzņēmums zvana klientam un:

- reklamē produktu vai pakalpojumu,
- piedāvā atlaidi vai lojalitātes programmu,
- zvana un prasa piekrišanu, lai varētu sarunas turpinājumā vai citā zvanā izteikt komerciālus paziņojumus.

Ņemot vērā minēto, datu apstrāde (iegūšana, glabāšana, saziņa u.c.) nolūkā izmantot datus komerciāla paziņojuma sūtīšanai (zvana veikšanai), ir veicama pamatojoties uz Datu regulas 6. panta 1. punkta a) apakšpunktu jeb personas piekrišanu, un šādai piekrišanai ir jāatbilst visiem Datu regulas 7. pantā noteiktajiem nosacījumiem.

4.4. ZVANI NEPILNGADĪGĀM PERSONĀM

Normatīvais regulējums Latvijā aizliedz uzņēmuma darbiniekiem apzināti veikt zvanus personām, kuras vēl nav sasniegušas 18 gadu vecumu, ar mērķi piedāvāt preces, pakalpojumus vai komerciālu informāciju.

Reklāmas likuma 5. pants nosaka, ka ir aizliegts izmantot nepilngadīgo uzticēšanos un pieredzes trūkumu. Bērniem paredzētā reklāma nedrīkst apdraudēt bērnu tiesības un intereses, un tās veidošanā jāņem vērā bērnu uztvere un psihe.

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

Saskaņā ar Negodīgas komercprakses aizlieguma likuma 13. pantu par agresīvu komercpraksi jebkuros apstākļos uzskatāma komercprakse, ja tās īstenotājs reklāmā iekļauj tiešu bērniem adresētu aicinājumu iegādāties preci vai saņemt pakalpojumu, digitālo pakalpojumu vai digitālo saturu vai arī pierunāt vecākus vai citus pieaugušos iegādāties preci vai saņemt pakalpojumu, digitālo pakalpojumu vai digitālo saturu.

Līdz ar to zvana laikā iegūta piekrišana no nepilngadīgās personas nav juridiski spēkā esoša, un to nevar izmantot par pamatu turpmākai komerciālai saziņai vai datu apstrādei. Tikai personas likumīgais pārstāvis (vecāks, aizbildnis) var sniegt derīgu piekrišanu.

Tādējādi, ja pastāv šaubas par adresāta pilngadību, saziņa nekavējoties jāpārtrauc, līdz tiek pārbaudīta un dokumentēta saziņa ar pieaugušo vai iegūts pierādījums, ka persona tomēr ir pilngadīga.

Ja uzņēmuma rīcībā nonāk personas dati, kas attiecināmi uz bērnu, tie nedrīkst tikt izmantoti telemārketinga vajadzībām. Jebkāda šādu personas datu glabāšana, apstrāde vai nodošana trešajām pusēm būtu jāizvērtē, vai tā atbilst visiem personas datu apstrādes principiem, kā arī pēc iespējas būtu jākonsultējas ar datu aizsardzības speciālistu.

Šīs prasības būtu attiecināmas arī uz gadījumiem, kad nav skaidri zināms zvana saņēmēja vecums. Proti, ja rodas aizdomas, ka adresāts varētu būt nepilngadīgs, saziņa nekavējoties jāpārtrauc.

5. APSTRĀDES DROŠĪBA

Datu regulas 32. pantā noteikts, 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 minētā panta b) apakšpunktā noteikto 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.

5.1. 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 Uzņēmuma A rīcībā esošajiem personas datiem un tos apstrādāt. Uzņēmums B un tā darbinieki – apkopēji – ir uzskatāmi par trešo personu[34], 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.

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

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 ļaunatūrām 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 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.

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*[35] ("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. Tāpat darbiniekiem būtu jāizvairās no personas datu, paroļu un citas darba pienākumu veikšanai nepieciešamās informācijas glabāšanu uz sava darba galda, ja šī informācija nav paredzēta izmantošanai citiem nodarbinātajiem. Attiecīgi šādi pasākumi attiecas gan uz darbu ofisā, attālināto darbu, kā arī tie jāņem vērā, kad darbinieka darba galda tuvumā var atrasties klienti, telpu apkopēji, ģimenes locekļi, kā arī citas, ar konkrētajiem personas datiem nesaistītas personas.

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

[35] Ietverta ISO 27001 standartā.

minētā izvairītos, ieteicams sastādīt pārskatu, kādi personas dati ir uzņēmuma 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, tāpat kā piesaistot apstrādātāju, 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.

5.2. 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. Šai parolei nevajadzētu būt vienkāršai, visiem uzņēmumā zināmai, tāpat arī tai nevajadzētu būt veidotai pēc līdzīgiem principiem, kā tiek veidotas citas paroles organizācijā, piemēram, “Organizacija_123” u.tml.

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 pietiekami 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.

5.3. 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.

Arī veicot personas datu apstrādi "mākonī", šī pakalpojumu sniedzējs attiecībā pret pārzini (komersantu) 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 mākoņpakalpojuma 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 trešajām 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.

5.4. DATU AIZSARDZĪBA PĒC NOKLUSĒJUMA

Ņemot vērā tehnikas līmeni, īstenošanas izmaksas un apstrādes raksturu, apmēru, kontekstu un nolūkus, kā arī dažādas iespējamības un nopietnības pakāpes riskus attiecībā uz fizisku personu tiesībām un brīvībām, kurus rada apstrāde, pārzinis gan apstrādes līdzekļu noteikšanas, gan pašas apstrādes laikā īsteno atbilstošus tehniskus un organizatoriskus pasākumus, piemēram, pseidonimizāciju, kas ir paredzēti, lai efektīvi īstenotu datu aizsardzības principus, piemēram, datu minimizēšanu, un lai apstrādē integrētu vajadzīgās garantijas nolūkā izpildīt Datu regulas prasības un aizsargāt datu subjektu tiesības.

Datu aizsardzība pēc noklusējuma paredz to, ka pārzinis, ievācot, glabājot vai kā citādi apstrādājot datus, jau sākotnēji izvērtē, kādi dati nepieciešami mērķa sasniegšanai un neievāc liekas datu kategorijas, kā arī neglabā datus nepamatoti ilgu laika posmu. Pārzinis (kā arī tā darbinieki, norīkotais apstrādātājs, datu aizsardzības speciālists) spēj jebkurā brīdī paskaidrot un ir informēts par to, kāpēc datus komersants apstrādā. Ja apstrādē iesaistītās personas, kuras piekļūst personas datiem nespēj uzreiz datu subjektam vismaz vispārīgi paskaidrot, kāpēc konkrēti dati tiek apstrādāti, tad būtu vismaz jāzina persona, pie kuras nosūtīt datu subjektu. Piemēram, ja datu subjekts telefoniski ir jautājis papildu jautājumus ārpus paša pakalpojuma vai preces aprakstošās informācijas, tad apstrādātāja darbinieks var norādīt, kur meklēt vairāk informācijas vai pie kādas personas vērsties. Ērtākais veids vispārīgas informācijas nodošanai ir komersanta tīmekļa vietnē izveidota privātuma politika, kurā skaidrotas komersanta veiktās datu apstrādes.

Šī nosacījuma pamatā ir nepieciešamība datu apstrādes procesus veidot tā, lai pašam datu subjektam nebūtu jāpieliek pūles savu datu aizsardzībai, jo to jau preventīvi, cik tas ir iespējams, ir ieviesis komersants. Šī pieeja ir paredzēta, lai līdz minimumam samazinātu iespējamos pārkāpumus datu iegūšanas un apstrādes procesā un nesankcionētas piekļuves un riskus, kas varētu rasties, ja personas dati nonāk trešās personas rīcībā.

Tāpat datu aizsardzība pēc noklusējuma ir saistīta ar iekšēju drošības nosacījumu ieviešanu, veicot atbilstošus tehniskus un organizatoriskus pasākumu, lai dati tiktu apstrādāti un glabāti nepiederošām personām nepieejamā vietā un veidā. Pārzinim, savu veikto datu apstrāžu pārredzamībai būtu jāizveido iekšēji noteikumi vai vadlīnijas, kas būtu saistoši visām apstrādē iesaistītajām personām, t.sk. apstrādātāja darbiniekiem. Par šāda dokumenta esamību un tajā ietvertās informācijas īstenošanu praksē ir jāinformē saistošās personas, kā arī šī informācija ir periodiski jāatjauno, mainoties apstrāžu veidiem, drošības pasākumu tendencēm, notiekot kādam incidentam vai vienkārši, ja dokuments ilgstoši nav pārskatīts un aktualizēts.

5.5. DARBINIEKU IZGLĪTOŠANA UN APMĀCĪBAS DATU AIZSARDZĪBAS JOMĀ

Kaut arī atbildību par datu apstrādes atbilstību datu aizsardzības prasībām nes pārzinis jeb komersants un tā vadība, lai datu apstrāde noritētu droši, pienācīgs svarīgums ir jāpiešķir arī darbinieku apmācīšanai darbam ar datiem. Tas ne vien nozīmē to, kādus datus ievākt no klienta, bet arī ko darbiniekam ar tiem darīt, kad tie nonākuši viņa rīcībā pamatoti vai vēl jo vairāk - nepamatoti. Darbinieku regulāras apmācības palīdz pārzinim izvairīties no datu apstrādes incidentiem, kad nezināšanas vai neuzmanības dēļ darbinieks var nopludināt klientu datus. Tāpat arī zinošs darbinieks spēs atbildēt uz klientam radušies jautājumiem par savu datu apstrādi, ja tāda nepieciešamība būs.

Darbinieku būtu jāapmāca, kad tas uzsāk darba tiesiskās attiecības ar komersantu un ne retāk kā reizi gadā vai biežāk pēc nepieciešamības (piemēram, ieviešot jaunu pakalpojumu vai jaunu informācijas sistēmu) vai pēc kāda notikuma. Tāpat darba devējs vai datu aizsardzības speciālists var regulāri informēt darbiniekus par iekšējiem notikumiem, kuri notikuši vienreiz, bet kuriem būtu jāpievērš uzmanība, lai tādi neatkārtotos.

Piemērs: **Darbinieks nosūtījis vairākiem klientiem jaunumus e-pastā, nenoslēpjot to e-pasta adreses un tādējādi tās padarot par redzamām citiem klientiem. Izsverot notikušā iespējami radīto kaitējumu datu subjektiem, kā arī datu apjomu un iesaistīto datu subjektu apjomu, pārzinis secina, ka notikušais neapdraud datu subjektus, tādējādi nav uzskatāms par datu apstrādes incidentu. Tomēr, lai nākotnē izvairītos no šādām situācijām, pārzinis vai jebkura persona uzņēmumā, piemēram, IT speciālists vai datu aizsardzības speciālists var izsūtīt visiem darbiniekiem vispārīgu šīs situācijas aprakstu (nesaucot vārdā darbinieku un neizpaužot kādu konkrētu informāciju par notikumu) un darbības, kas jāveic katrreiz pirms e-pasta izsūtīšanas, lai šāds gadījums vairs neatkārtotos.**

Svarīgi, ka gadījumā, kad darbinieks klientu vai kolēģu personas datus izmanto privātām vai krāpnieciskām darbībām, kuras nav iekļautas uzņēmuma procesos, par šādu datu apstrādi atbildība tiks prasīta no darbinieka, ja līdz tam darba devējs būs pielicis pietiekamas pūles, lai darbiniekus izglītotu un apmācītu.

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