Eiropas Sociālā fonda projekts Nr.9.2.6.0/17/I/001 "Ārstniecības un ārstniecības atbalsta personāla kvalifikācijas uzlabošana"

METODISKAIS MATERIĀLS

Pacientu datu aizsardzības aktuālie jautājumi

Rīga

2021.

ANOTĀCIJA

Šo metodisko materiālu izstrādāja Mācību centrs LAIPA Eiropas Sociālā fonda (turpmāk – ESF) projekta Nr.9.2.6.0/17/I/001 „Ārstniecības un ārstniecības atbalsta personāla kvalifikācijas uzlabošana" darbības programmas „Izaugsme un nodarbinātība" 9.2.6. specifiskā atbalsta mērķa „Uzlabot ārstniecības un ārstniecības atbalsta personāla kvalifikāciju" vajadzībām veiktā iepirkuma „Mācību īstenošana un izstrādāta profesionālās pilnveides izglītības programmas „Pacientu datu aizsardzības aktuālie jautājumi"" (identifikācijas Nr. VM 2020/09/ESF) ietvaros.

Metodiskais materiāls sniedz informāciju par datu apstrādes un aizsardzības teorētiskajiem pamata aspektiem, atsevišķi izdalot ārstniecības iestādēm svarīgu subjektu – personu datu apstrādes īpatnības.

Metodiskajā materiālā apskatīts Latvijas Republikas teritorijā piemērojamais personas datu apstrādes tiesiskais regulējums un tā piemērošanas praktiskie aspekti, piemēram, IT drošības pamatjautājumi personas datu apstrādē.

Metodiskais materiāls ir paredzēts ārstniecības personām un ārstniecības atbalsta personām, kuras, izpildot savus darba pienākumus, ikdienā saskaras ar personas datu apstrādi, tajā skaitā ar īpašu kategoriju – pacientu veselības un diagnožu datu apstrādi.

SATURA RĀDĪTĀJS

TEKSTĀ LIETOTIE SAĪSINĀJUMI

ĀL – Ārstniecības likums

FPDAL – Fizisko personu datu apstrādes likums

KPL – Kriminālprocesa likums

PTL – Pacientu tiesību likums

VDAR – Vispārējā datu aizsardzības regula

IT - informācijas tehnoloģijas

1. IEVADS

1950. gada 04. novembrī bija pieņemta Cilvēka tiesību un pamatbrīvību aizsardzības konvencija, kuras 8. pantā paredzētas ikviena indivīda tiesības uz savas privātās un ģimenes dzīves, dzīvokļa un korespondences neaizskaramību. Tā kā dati par personu, arī dati par personas veselību, veido ievērojamu, ja ne lielāko, personas privātās dzīves daļu, personas datu aizsardzība ir privātās dzīves neaizskaramības pamatelements.

Aizsargāt personas datus tehnoloģiju attīstības laikmetā kļūst arvien grūtāk, jo automatizēti var tikt vienlaicīgi apstrādāts lielāks personas datu un personas datu saturošu nesēju skaits un lielāks informācijas apjoms. Līdz ar datu aizsardzības līdzekļiem attīstās arī līdzekļi drošības sistēmu pārkāpšanai. Līdz ar to, svarīga kļūst izpratne par to, kas ir aizsardzības objekts un kādi ikdienas aizsardzības pasākumi veicami, lai minimizētu vai izslēgtu neaizskaramības tiesību pārkāpšanas iespēju.

Metodiskā materiāla mērķis ir konspektīvā veidā sniegt pamata informāciju par personas datu apstrādes pamata jēdzieniem, kā arī personas datu likumīgas un drošas apstrādes nodrošināšanai nepieciešamajām pamata prasībām, kuras jāizpilda ārstniecības atbalsta personām, veicot savus ikdienas darba pienākumus.

Mērķa sasniegšanai ir analizēts Latvijas Republikā spēkā esošais normatīvais regulējums personas datu aizsardzības jomā, kā arī datu aizsardzības kontekstā analizētas speciālo normatīvo aktu normas, kuras skar pacienta kā datu subjekta tiesības.

Metodiskajā materiālā ir plaši izmantotas atsauces uz normatīvajiem aktiem, kuros nostiprinātas prasības gan fizisku personu datu, gan tieši pacientu datu apstrādē un aizsardzībā, līdz ar to, lietojot šo metodisko materiālu, ir jāpārbauda normatīvo aktu aktuālā redakcija, kura ir svarīga būtības korektai izpratnei.

2. TIESISKAIS REGULĒJUMS

Ikvienam cilvēkam ir noteiktas pamata tiesības jeb cilvēktiesības, viena no kurām ir personas tiesības uz privāto un ģimenes dzīvi. Pats jēdziens „tiesības uz privāto dzīvi ” ir plašs un ietver personas tiesības uz savu privāto telpu, fizisko un garīgo integritāti, godu, cieņu, kā arī tiesības uz personas datu aizsardzību. Viss, ko ārējā pasaule uzzina par personu, ir personas dati – ziņas par pašu personu, tās ģimeni, dzīves veidu un pārējā ar personu saistītā informācija, kuras aizsardzība kļūst arvien svarīgāka tehnoloģiju straujas attīstības laikmetā.

Lai nodrošinātu vienotu pieeju personas datu apstrādei un aizsardzībai starptautiskajā un Eiropas Savienības valstu nacionālajā līmenī, Eiropas Parlaments un Padome izstrādāja normatīvos aktus ar vispārīgām obligāti ievērojamām nostādnēm fizisku personu datu apstrādei. Vēsturiski normatīvo aktu regulējums laika gaitā evolucionēja gan Eiropas līmenī, gan dalībvalstu nacionālajā līmenī.

Viens no svarīgākajiem dokumentiem ir 1995. gada 24. oktobra Eiropas Parlamenta un Padomes Direktīva 95/46/EK par personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti ES. Šis dokuments vairāk kā 20 gadus bija fizisko personu datu aizsardzību regulējošais starptautiskais normatīvais akts. Direktīva tika transponēta Latvijas Republikas normatīvajā regulējumā 2000. gada 23. martā, kad spēkā stājās „Fizisko personu datu aizsardzības likums”. Katrā no ES dalībvalstīm Direktīvā paredzētais regulējums tika ieviests ļoti atšķirīgi.

Situācija mainījās ar Eiropas Parlamenta un Padomes Regulas (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti, līdz ar to atceļot Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula, turpmāk tekstā – VDAR) izstrādi un pieņemšanu. VDAR projekts sākotnēji tika publiskots 2012. gadā, dokumenta izstrāde tika pabeigta un VDAR stājās spēkā 2016. gada maijā, bet tās piemērošana tika atlikta līdz 2018. gada 25. maijam.

VDAR ir tieši piemērojams tiesību akts, t.i. tiesību akts, kura piemērošanai ES valstī nav nepieciešama atsevišķu normu integrācija nacionālajos normatīvajos aktos, tomēr Latvijā pēc VDAR stāšanās spēkā tika pieņemts lēmums aktualizēt arī nacionālo normatīvo regulējumu.

2000. gada 20. aprīlī bija pieņemts Fizisko personu datu aizsardzības likums, kas ilgus gadus reglamentēja personas datu aizsardzības pamatjautājumus Latvijas Republikas teritorijā. Minētais likums zaudēja spēku 2018. gada 05. jūlijā, kad spēkā stājās jauns normatīvais akts – Fizisko personu datu apstrādes likums (turpmāk tekstā – FPDAL), kura normas balstās uz VDAR. Būtiski, ka FPDAL satur daudzas atsauces uz VDAR, piemēram, 1. pantā „Likumā

lietotie termini" ir norāde, ka likumā ir lietoti VDAR 4. panta noteiktie termini. Tajā pašā laikā, FPDAL reglamentē jautājumus, kurus VDAR atstāj dalībvalstu ziņā, piemēram, uzraudzības iestādes (Latvijā – Datu valsts inspekcijas) uzdevumus, statusu, pilnvaras, pārbaužu veikšanas kārtību, atsevišķus jautājumus par datu aizsardzības speciālista pienākumiem u. c. jautājumus.

Šajā metodiskajā materiālā vairumā gadījumu norāde uz VDAR nozīmē arī atsauci uz Latvijas nacionālo fizisko personu apstrādes regulējumu.

Būtiskākais jauninājums sakarā ar VDAR stāšanos spēkā ir prasība obligāti un vienmēr nodrošināt datu aizsardzību un informācijas drošību, kas nozīmē, ka nevienā uzņēmumā nekādi personas dati nedrīkst parādīties un tiks izmantoti, ja nav pilnīgi skaidrs to apstrādes mērķis, nepastāv kaut viens tiesiskais pamats un nav nodrošināti datu aizsardzības mehānismi.

Neatkarīgi no iepriekšminētajiem normatīvajiem aktiem, pastāv arī citas tiesību normas, kas regulē datu aizsardzību dažādās dzīves situācijās, tostarp, veicot datu apstrādi ārstniecības jomā, piemēram:

- Pacientu tiesību likums (pieņemts 17.12.2009.);
- Ārstniecības likums (pieņemts 12.06.1997.);
- MK noteikumi Nr. 265. „Medicīnisko dokumentu lietvedības kārtība" (pieņemti 04.04.2006.).

3. PAMATJĒDZIENI

Nosakot nepieciešamību piemērot tiesību normas personas datu aizsardzībā, jāsaprot, vai konkrētajā gadījumā notiek datu apstrāde, līdz ar to, ir jāsaprot pamatjēdzieni. Pamatjēdzieni ir definēti VDAR 4. punktā, un svarīgākie no tiem ir izskatīti zemāk.

3.1. Personas dati, t. sk. īpašu kategoriju personas dati, un datu subjekts

Atbilstoši VDAR 4. panta 1. punktā sniegtajai definīcijai, „personas dati ir jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu".

Definīciju papildina VDAR Preambulā ietvertais apsvērums (27), kas nosaka, ka šo regulu nepiemēro mirušo personu personas datiem, un VDAR 4. panta 1. punkta turpinājums. Tos apkopojot, definīcijas īsā versija var būt šāda: „personas dati ir jebkura informācija, kura attiecas uz dzīvu fizisko personu, kuru var tieši vai netieši identificēt", un ietver četrus pamatelementus:

- jebkura informācija
- attiecas uz
- identificētu vai identificējamu
- fizisku personu , kur

„jebkura informācija" ir informācija par indivīdu, kas atspoguļo objektīvu vai subjektīvu apgalvojumu, var būt patiesa vai nepatiesa, var būt nepierādīta, izteikta jebkurā formā un uz jebkura nesēja.

„attiecas uz" nozīmē, ka informācija attiecas uz konkrēto indivīdu un ir par šo indivīdu, skar tā identitāti, raksturojumu vai uzvedību, vai šo informāciju izmanto, lai noteiktu vai noskaidrotu indivīdu. Šis elements var nozīmēt, ka indivīds ir tieši norādīts informācijas kopā (piem., dati medicīnas kartiņā), vai pastāv informācija, kas identificē objektu, no kura var izsecināt ar to saistīto indivīdu (piem., saistības starp nekustamo īpašumu un tā īpašnieku).

„identificētu vai identificējamu" nozīmē, ka rīcībā esošā informācija ļauj identificēt fizisko personu tieši vai ar lielu varbūtības pakāpi. Parasti šāda informācija ir pilnībā saistīta ar konkrēto indivīdu.

„fiziskā persona" ir dzīvs indivīds jeb **„datu subjekts".** Saskaņā ar vispārējo fiziskas

personas jēdziena juridisko izpratni, fiziska persona sākas ar dzimšanu un beidzas ar nāvi. Parasti mirušu personu datu aizsargāti netiek. Izņēmums ir gadījumi, ja informācija par mirušām personām tiešā veidā attiecas uz dzīvām personām (piemēram, ģenētiski mantotas slimības) vai izņēmumi, kas noteikti normatīvajos aktos.

Atsevišķi ir izdalīta grupa „īpašu kategoriju personas dati", kas satur informāciju par rases vai etnisko piederību, politiskajiem uzskatiem, reliģisko vai filozofisko pārliecību u.c. Šāda veida datu apstrāde arī ir īpaši reglamentēta.

3.2. Datu apstrāde

Atbilstoši VDAR 4. panta 2. punktā sniegtajai definīcijai: „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".

Datu apstrādes fakta konstatācijai pietiek ar viena datu subjekta datiem, pat izdomātiem un nepatiesiem.

Datu apstrāde ārstniecības procesu kontekstā ir, piemēram, pacienta reģistrēšana pieņemšanai pie ārsta, uz ārsta nozīmētajām analīzēm, manipulācijām, procedūrām, ārstniecības gaitas fiksēšana u.c. informācijas rakstiska fiksēšana gan papīra formāta dokumentos, gan arī, saglabājot elektroniskajā formātā.

3.3. Pārzinis

Atbilstoši VDAR 4. panta 7. punktā sniegtajai definīcijai: „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; ja šādas apstrādes nolūkus un līdzekļus nosaka ar Savienības vai dalībvalsts tiesību aktiem, pārzini vai tā iecelšanas konkrētos kritērijus var paredzēt Savienības vai dalībvalsts tiesību aktos".

No norādītās definīcijas izriet, ka pārzinis ir tiesību subjekts, kas nosaka datu apstrādes mērķi, kas, savukārt, nozīmē, ka datu apstrāde nevar tikt veikta bez konkrēta, pamatota, likumīga mērķa, un datu pārzinis izvēlas datu apstrādes līdzekļus, t.i. veidu, kādā tiek apstrādāti personas dati. Pārzinis ir pilnībā atbildīgs par datu drošību (aizsardzību).

Datu apstrādi var veikt kopīgi pārziņi – divi vai vairāki pārziņi, kuri kopīgi nosaka apstrādes mērķus un veidus, skaidri un pārredzami nosakot uz sevi attiecināmos pienākumus, informējot par tiem datu subjektus un uzņemoties kopīgu atbildību par datu apstrādi (VDAR 26. pants).

Pārzinis var būt gan fiziska persona, gan juridiska persona. Svarīgi izprast, ka gadījumā, ja pārzinis ir juridiska persona, tās valdes loceklis kļūst par pārziņa pārstāvi, bet nekļūst par pārzini pats.

Piemēram: apstrādājot personas datus ārsta privātpraksē, personas datu pārzinis ir pats ārsts, jeb fiziska persona. Apstrādājot personas datus ārstniecības iestādē, kur vienā uzņēmumā ir apvienojušies vairāki uz darba līguma pamata nodarināti ārsti, personas datu pārzinis ir juridiska persona – ārstniecības iestādes īpašnieks. Savukārt, šīs iestādes amatpersona ir par personas datu apstrādi atbildīgā persona, nevis pārzinis.

3.4. Apstrādātājs (personas datu operators)

Atbilstoši VDAR 4. panta 8. punktā sniegtajai definīcijai: „Apstrādātājs ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus". Apstrādātājs darbojas pārziņa interesēs un tikai saskaņā ar pārziņa norādījumiem, turklāt bez pārziņa iepriekšējās konkrētās vai vispārējās atļaujas apstrādātājs nepiesaista citu apstrādātāju. Apstrādātāja un pārziņa attiecības noformējamas ar rakstveida līgumu (dokumentēti), kura pamatelementus regulē VDAR normas. Būtiski, ka apstrādātāja pienākums ir pēc datu apstrādes pabeigšanas datus dzēst vai nodot pārzinim, dzēšot pie apstrādātāja esošās kopijas, ja normatīvie akti neparedz datu saglabāšanu.

Piemēram: uzņēmums, kas nodrošina un uztur savā mākonī programmu pacientu pierakstam pie speciālistiem, vienlaicīgi nodrošinot informācijas apkopošanu un sagatavošanu ārstniecības iestādes pārskaitu iesniegšanai, attiecībā pret ārstniecības iestādi ir datu apstrādātājs.

3.5. Citas datu apstrādē iesaistītās personas

VDAR paredz, ka datu apstrādē var piedalīties arī citas personas, t. i.:

- ***trešā persona***, kas ir fiziska vai juridiska persona, publiskā iestāde, aģentūra vai struktūra, kura nav datu subjekts, pārzinis, apstrādātājs, un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus (VDAR 4. panta 10. punkts);

- ***saņēmējs,*** kas ir fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpauž personas datus – neatkarīgi no tā, vai tā ir trešā persona vai nav (VDAR 4. panta 9. punkts);
- ***pārziņa tieši pilnvarotās personas,*** kas ir apstrādātāji un jebkura persona, kas darbojas pārziņa vai apstrādātāja pakļautībā un kam ir piekļuve personas datiem, neapstrādā minētos datus citādi, kā vien saskaņā ar pārziņa norādījumiem, ja vien to darīt nepieprasa Savienības vai dalībvalsts tiesību akti (VDAR 29. pants). Par šādām personām var tikt uzskatīti pārziņa darbinieki, turklāt darbinieku pilnvarojums var būt iekļauts arī darba līgumā; savukārt pilnvarojuma apjoms, t.i. darbinieka tiesības piekļūt personas datiem, konkrētā amata pienākumu izpildes ietvaros realizējamās apstrādes darbības, iekļaujamas amata aprakstā un var būt papildinātas ar citiem pārziņa iekšējiem dokumentiem (darba kārtības noteikumiem, instrukcijām utt.) Par darbinieku veiktajām darbībām ir pilnībā atbildīgs pārzinis, kas neizslēdz darbinieka atbildību pārziņa priekšā.

3.6. Datu apstrādes nolūks (mērķis)

Datu apstrādes mērķis (arī nolūks, arī apstrādes darbība) ir iemesls, kādēļ datu apstrāde ir nepieciešama. Mērķi nosaka pārzinis, nosakot arī rezultātu, kas tiek panākts ar datu apstrādi, un darbības, kuras ir nepieciešams mērķa (rezultāta) sasniegšanai. Mērķa definējums var atšķirties dažādās situācijās, bet gadījumā, ja tāda nav vispār, datu apstrāde kļūst prettiesiska.

Pirms datu apstrādes uzsākšanas apstrādes mērķis jānosaka tik detalizēti, lai apstrādātāji (piemēram, reģistratūras darbinieki) no tā var izsecināt, kādas tieši apstrādes darbības viņiem ir jāveic un kādas nav. Mērķim ir jābūt tādam, kuru nevar sasniegt citādi, kā tikai apstrādājot datus.

Piemēram: apstrādājot personas datus ārstniecībā, nolūks ir uz pārzini attiecināmā pienākuma izpilde – pienākums identificēt pacientu pirms ārstēšanas uzsākšanas, kā arī pašu veselības aprūpes pakalpojumu sniegšana.

3.7. Datu apstrādes tiesiskais pamatojums, t.sk. datu subjekta piekrišana

Datu apstrādes tiesiskais pamatojums ir priekšnosacījums tiesiskai un pamatotai datu apstrādei. VDAR 6. panta 1. daļā paredzēti šādi tiesiskie pamatojumi datu apstrādei:

- datu subjekta piekrišana;

- līgumsaistību izpilde;
- likumā noteikto pienākumu izpilde;
- rīcība ārkārtas situācijās;
- deleģēto publiskās varas pienākumu izpilde;
- leģitīmā jeb tiesiskā interese.

Īpaša uzmanība jāpievērš ***datu subjekta piekrišanai***, kurai normatīvais regulējums no vienas puses nosaka stingrākas prasības, no otras puses – atstāj datu pārzinim zināmu brīvību piekrišanas saņemšanai un noformēšanai.

Atbilstoši VDAR 4. panta 11. punktā sniegtajai definīcijai, ***datu subjekta piekrišana*** ir jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu personas datu apstrādei.

Datu pārzinim jāspēj uzskatāmi parādīt (pierādīt), ka datu subjekts (pacients, klients) ir piekritis savu personas datu apstrādei, turklāt piekritis labprātīgi, apzināti un nepārprotami, līdz ar to, svarīgs kļūst piekrišanas precīzs formulējums. Saņemot piekrišanu, tai jābūt noformētai tā, lai tā būtu atšķirama no citiem jautājumiem, piemēram, ja vienā dokumentā ir norādītas vairākas datu subjekta apņemšanās, lūgums dot piekrišanu datu apstrādei norādams skaidrā, nepārprotamā veidā, kas ļauj to atšķirt no pārējiem – t.i., jāizdala kā atsevišķs punkts. Datu subjektam jābūt iespējai savu piekrišanu atsaukt, taču, jau dodot piekrišanu, datu subjekts ir jāinformē, ka piekrišanas atsaukšana nevar neietekmēt pagātnē jau veiktās darbības. Datu subjekta piekrišanai jābūt brīvai (brīvprātīgai), turklāt brīvprātīgums tiek vērtēts saistībā ar apstrādājamo datu apjomu.

Datu pārzinis ir tiesīgs noteikt piekrišanas saņemšanas formu, taču tas jādara, ievērojot visus iepriekšminētos nosacījumus.

3.8. Datu pseidonimizācija un datu anonimizācija

Pacientu personas datu apstrādes kontekstā ir svarīgi pseidonimizācijas un anonimizācijas jēdzieni, lai gan medicīnas praksē tie vairāk ir attiecināmi uz klīnisko pētījumu organizēšanu.

Personas datu ***pseidonimizācija*** ir personas datu apstrāde, ko veic tādā veidā, lai personas datus vairs nebūtu iespējams saistīt ar konkrētu datu subjektu bez papildu informācijas izmantošanas, ar noteikumu, ka šāda papildu informācija tiek turēta atsevišķi un tai piemēro

tehniskus un organizatoriskus pasākumus, lai nodrošinātu, ka personas dati netiek saistīti ar identificētu vai identificējamu fizisku personu.

Savukārt ***anonimizācija*** ir personas datu apstrāde tādā veidā, ka nekādos saprātīgos apstākļos identifikācija nav iespējama – ne dati paši par sevi, ne kopā ar kādiem citiem, tajā skaitā, publiski pieejamiem datiem, nerada iespēju identificēt konkrētu indivīdu.

4. DATU APSTRĀDES PRINCIPI

Pārzinim obligāti jāievēro datu apstrādes principi un jāspēj uzskatāmi parādīt (pierādīt) principu ievērošana (***pārskatatbildība***). Formulējums „uzskatāmi parādīt" nozīmē, ka pārzinim pašam ir jāizveido, jāuztur un jāspēj uzrādīt apliecinājumi par viņa veiktajām darbībām personas datu aizsardzības nodrošināšanai, nevis kādam citam, piemēram, uzraudzības iestādei ir jāpierāda, ka apstrāde veikta nepareizi, vai jāpamato kādi citi pieņēmumi. Uzskatāmās parādīšanas līdzekļiem pieskaitāmi pārziņa iekšējie dokumenti, kas reglamentē datu apstrādi pārziņa iestādē, detalizēti izstrādāti darbinieku amatu apraksti, apliecinājumi par periodiski veiktajām apmācībām un datu drošības pārbaudēm (auditiem).

Datu apstrādes principi ir noteikti VDAR 5. pantā un tie nosaka, ka:

- dati tiek apstrādāti godprātīgi, likumīgi un datu subjektam pārredzama veidā (***likumīgums, godprātība un pārredzamība***);
- datu apstrāde tiek veikta tikai atbilstoši datu apstrādes mērķim un ne ilgāk par tā sasniegšanu (***nolūka ierobežojums***);
- dati ir adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams apstrādes nolūkos (***datu minimizēšana***);
- dati ir precīzi un aktuāli (***precizitāte***);
- glabāti tā, ka pieļauj datu subjekta identifikāciju tikai tik ilgi, cik nepieciešams mērķa sasniegšanai (***glabāšanas ierobežojums***);
- dati tiek apstrādāti, ievērojot drošību (***integritāte un konfidencialitāte***).

4.1. Likumīgums, godprātība un pārredzamība

Apstrādes likumīgums un godprātība nozīmē, ka datu apstrādei ir noteikts mērķis un pastāv apstrādes tiesiskais pamats.

Datu apstrādes tiesiskie pamati personas datiem un īpašu kategoriju personas datiem ir dažādi.

Personas datu apstrādes tiesisko pamatu vispārējos gadījumos nosaka VDAR 6. panta 1. daļa, un cita starpā, par tādiem uzskatāma datu subjekta piekrišana, uz pārzini attiecināma juridiskā pienākuma izpilde, datu subjekta vai citas fiziskās personas vitālu interešu aizsardzība, u.c.. Savukārt īpašu kategoriju personas datu, t. sk. datu par subjekta veselību, tiesiskie pamati

ir uzskaitīti VDAR 9. panta 2. daļā, no kuriem, citu starpā, īpaši jāpiemin paša datu subjekta piekrišana, kā arī nepieciešamība apstrādāt datus medicīnas sfērā noteiktu mērķu sasniegšanai (arī ar ārstniecību nesaistītos normatīvos aktos paredzētu mērķu sasniegšanai, piemēram, ārkārtējās situācijas laikā).

Godīga un likumīga apstrāde ietver sevī arī datu subjekta informēšanu piemērotā veidā par personas datu apstrādi un tās sekām.

Ņemot vērā, ka datu apstrāde ietver sevī visu un jebkādu darbību veikšanu attiecībā uz datiem, likumīgas (tiesiskas) apstrādes princips ievērojams katrā apstrādes brīdi: datus ievācot, glabājot un dzēšot. Tātad, ja dati tika iegūti nelikumīgi, var uzskatīt, ka princips ir pārkāpts ievākšanas brīdī, un arī turpmākā dzēšana tiesiskuma trūkumu neatceļ.

Apstrādes pārredzamība nozīmē informācijas sniegšanu datu subjektam par to, ka tiek apstrādāti dati, turklāt ne tikai datus vācot, bet arī sniedzot datu subjektam informāciju datu apstrādes laikā.

Piemēram: pacienta dati tiek apstrādāti ārstēšanas procesa nodrošināšanai (likumība), tikai un vienīgi šim mērķim (godprātība), kā arī pacients ir informēts par šādu apstrādi, tās apjomu un par to, kā dati tiek apstrādāti (pārredzamība).

4.2. Nolūka ierobežojums

Šī principa realizācija nozīmē, ka dati tiek **vākti** konkrēta mērķa sasniegšanai („konkrētos, skaidros un leģitīmos nolūkos"), un turpmākā apstrāde veicama tikai ar konkrētu mērķi savietojamā veidā. Datu apstrādes nolūks (mērķis) ir noteikts starptautiskos vai nacionālos normatīvajos aktos vai pārziņa apstiprinātos iekšējos normatīvos aktos. Līdz ar to, mērķis jānosaka un jāizprot precīzi, lai varētu viennozīmīgi secināt, tieši kādi dati un cik detalizēti dati nepieciešami konkrētā mērķa sasniegšanai, kā arī, lai būtu iespējams izsecināt, kad tieši (kuru datu apstrādes procesa darbību veicot) mērķis ir sasniegts.

Piemēram: personu identificējošie dati un kontakta dati var tikt izmantoti tikai ārstēšanas nodrošināšanai, nevis reklāmas materiālu sūtīšanai par medikamentiem.

4.3. Datu minimizēšana

Dati tiek apstrādāti, pirmkārt, iegūti vai ievākti, tikai tādā apmērā, kādā tie ir nepieciešami mērķa sasniegšanai, t.i. neapstrādājot datus, kuri nav nepieciešami noteikto darbību izpildei.

Piemēram: pacientu identificējošās informācijas apjoms ir noteikts normatīvajā regulējumā un attiecīgi iestrādāts medicīnas dokumentu paraugos (medicīnas kartiņās), līdz ar to, plašākas informācijas vākšana pārkāptu minimizēšanas principu.

4.4. Precizitāte

Datu precizitāte ir obligāts priekšnoteikums noteiktā nolūka sasniegšanai, jo ir apšaubāms, ka ar neprecīziem datiem pārzinis spēs sasniegt noteikto mērķi. Datu precizitāte ietver arī datu aktualitāti, t.i. datu pareizību un atbilstību pašreizējam momentam.

Datu precizitāte attiecas uz visiem datu apstrādes elementiem, t.i. uz katru datu sastāvdaļu, kas tiek ievākti. Šis princips ļoti cieši saistīts ar datu minimizēšanas principa realizāciju, jo adekvātajā apjomā datiem ir jābūt precīziem.

Piemēram: pacientu identificējošai informācijai jābūt piefiksētai precīzi, bez kļūdām.

4.5. Glabāšanas ierobežojums

Dati tiek uzglabāti līdz mērķa sasniegšanai un pēc tā sasniegšanas tiek iznīcināti. Pieļaujama datu arhivēšana un apstrāde statistiskiem mērķiem, ievērojot noteiktas tehniskās un organizatoriskās prasības, kas noteiktas normatīvajā regulējumā.

Piemēram: dokumentu glabāšanas termiņš ir noteikts normatīvajos aktos, un pēc tā beigām dokumenti tiek iznīcināti atbildīgās personas noteiktajā kārtībā.

4.6. Integritāte un konfidencialitāte

Dati tiek apstrādāti, garantējot to drošību, tai skaitā aizsardzību pret neatļautu vai nelikumīgu apstrādi, kā arī pret nozaudēšanu, iznīcināšanu vai sabojāšanu. Integritāte un konfidencialitāte ir jānodrošina datu pārzinim, ieviešot normatīvajos aktos noteiktos tehniskos un organizatoriskos pasākumus, kā arī papildinot tos ar paša pārziņa izveidotiem, apstiprinātiem iekšējiem normatīviem aktiem.

Piemēram: pacientu kartiņas jāglabā tā, lai izslēgtu iespēju nepiederošām personām tām piekļūt (jānodrošina datu konfidencialitāte) un tā, lai kartiņās saglabātos oriģinālais saturs, kas nevarētu tikt nesankcionēti manīts.

5. DATU SUBJEKTU TIESĪBAS

5.1. Tiesības uz informāciju

Datu subjekta tiesībām tikt informētam attiecīgi atbilst pārziņa pienākums sniegt informāciju, jeb informēšanas pienākums.

Šīs datu subjekta (tostarp, pacienta) tiesības realizācija nozīmē, ka pārzinim, iegūstot personas datus, ir pienākums sniegt datu subjektam vismaz nacionālajā normatīvajā regulējumā noteiktu informācijas apjomu, turklāt normatīvajā regulējumā izšķir gadījumus, kad dati ir iegūti no paša datu subjekta un, kad dati nav iegūti no datu subjekta.

Pārziņa vietā informācijas sniegšanas pienākumu var izpildīt cita persona, kas strādā pārziņa vārdā un uzdevumā (apstrādātājs, kopīgs pārzinis), bet noteikti ir jābūt pierādījumam, ka deleģēšana ir bijusi un informēšanas pienākums ir izpildīts.

Datus iegūstot no datu subjekta, pārziņa pienākums ir sniegt vismaz šādu informāciju:

- pārziņa vai pārziņa pārstāvja identitāte un kontaktinformācija;
- datu aizsardzības speciālista kontaktinformācija, ja tas piemērojams konkrētajā gadījumā;
- apstrādes nolūki, t.i., kam paredzēti personas dati (kāpēc tie ir nepieciešami);
- personas datu saņēmēji vai saņēmēju kategorijas, ja tādi ir;
- attiecīgā gadījumā – informācija, ka pārzinis paredz nosūtīt personas datus uz trešo valsti vai starptautisku organizāciju, un šādas rīcības pamatojums;
- laika posms, cik ilgi personas dati tiks glabāti, vai, ja tas nav noteikts normatīvajā regulējumā, tad kritēriji, ko pārzinis izmanto minētā laika posma noteikšanai;
- tas, ka datu subjektam (klientam, pacientam) pastāv tiesības pieprasīt pārzinim piekļuvi datu subjekta personas datiem un to labošanu vai dzēšanu, vai apstrādes ierobežošanu attiecībā uz datu subjektu, vai tiesības iebilst pret apstrādi, kā arī tiesības uz datu pārnesamību;
- ja datu apstrādes pamatā ir datu subjekta piekrišana – tiesības un to realizācijas kārtība, kas atļauj jebkurā brīdī atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana;
- tiesības iesniegt sūdzību uzraudzības iestādei (Latvijā – Datu valsts inspekcijai);

- informācija, vai personas datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī informācija par to, vai datu subjektam ir pienākums personas datus sniegt un kādas sekas var būt gadījumos, kad šādi dati netiek sniegti;
- atsevišķajos gadījumos (ja pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana) jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

Gadījumos, kad dati nav iegūti no datu subjekta, sniedzamās informācijas klāsts ir vēl plašāks.

5.2. Datu subjekta piekļuves tiesības

Datu subjektam ir tiesības noskaidrot pie pārziņa, vai datu subjekta dati tiek apstrādāti, un, ja tiek – saņemt vismaz šādu informāciju:

- apstrādes nolūki;
- attiecīgo personas datu kategorijas;
- personas datu saņēmēji vai saņēmēju kategorijas, kam personas dati ir izpausti vai kam tos izpaudīs, jo īpaši saņēmēji trešajās valstīs vai starptautiskajās organizācijās;
- ja iespējams, paredzētais laika posms, cik ilgi personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laika posma noteikšanai;
- ka pastāv tiesības pieprasīt no pārziņa datu subjekta personas datu labošanu vai dzēšanu, vai personas datu apstrādes ierobežošanu vai tiesības iebilst pret šādu apstrādi;
- tiesības iesniegt sūdzību uzraudzības iestādei;
- visa pieejamā informācija par datu avotu, ja personas dati netiek saņemti no datu subjekta;
- ja attiecināms – ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, un jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

Pārziņa pienākums ir nodrošināt apstrādē esošo personas datu kopiju, iekasējot vai neiekasējot pamatotu samaksu par tās izgatavošanu (atbilstoši administratīvajiem izdevumiem to izgatavošanai) vai sniedzot kopiju elektroniskā formātā, ja datu subjekts to pieprasa.

5.3. Tiesības labot

Šo tiesību realizācija ir cieši saistīta ar datu precizitātes principa ievērošanu un nozīmē, ka datu subjektam ir tiesības pieprasīt, lai pārzinis bez nepamatotas kavēšanās labotu neprecīzus subjekta personas datus (VDAR 16. pants).

Svarīgi, ka atsevišķos gadījumos pārzinim nav iespējams realizēt datu precizitātes principu, pirms datu subjekts ir izmantojis šīs savas tiesības. Līdz ar ko, šīs tiesības zināmā mērā arī datu subjektam uzliek pienākumu parūpēties, lai pārzinis apstrādātu aktuālos un precīzos datu subjekta datus (piemēram, uzvārda, dzīvesvietas adreses vai kontakttelefona maiņas gadījumā).

5.4. Tiesības uz dzēšanu (tiesības „tikt aizmirstam")

Šīs datu subjekta tiesības nozīmē, ka datu subjekts ir tiesīgs pieprasīt, lai pārzinis dzēš subjekta datus (VDAR 17. panta 1. daļa ar punktiem). Tomēr, normatīvajā regulējumā ir paredzēti gadījumi, kad datu subjekts ir tiesīgs pieprasīt datu dzēšanu, kā arī noteikti gadījumi, kad šīs tiesības netiek realizētas. Visbiežāk (bet ne tikai), dati ir dzēšami šādos gadījumos:

- personas dati vairs nav nepieciešami saistībā ar nolūkiem, kādos tie tika vākti vai citādi apstrādāti;
- datu subjekts atsauc savu piekrišanu, ja datu apstrāde tika balstīta uz datu subjekta piekrišanu, un cita likumīga pamata datu apstrādei nav;
- personas dati ir apstrādāti nelikumīgi;
- personas dati ir jādzēš, lai nodrošinātu, ka tiek pildīts juridisks pienākums, kas noteikts Savienības vai dalībvalsts tiesību aktos, kuri ir piemērojami pārzinim.

Datu dzēšanas izņēmumi ir pieļaujami un viens no tiem (arī ārstniecības iestādēm piemērojamais) ir, lai izpildītu juridisku pienākumu, kas prasa veikt apstrādi, kā paredzēts Savienības vai dalībvalsts tiesību aktos, kuri piemērojami pārzinim, vai arī, lai izpildītu uzdevumu, ko pārzinis veic sabiedrības interesēs, vai saistībā ar pārzinim likumīgi piešķirto oficiālo pilnvaru īstenošanu (VDAR 17. panta 3. daļas b) punkts).

5.5. Tiesības ierobežot apstrādi

Šīs datu subjekta tiesības izpaužas, kad noteiktu apstākļu pastāvēšanas gadījumā (VDAR 18. panta 1. daļa) datu subjekts ir tiesīgs ierobežot savu datu apstrādi laikā vai apjomā. Visbiežāk (bet ne tikai), par tādiem apstākļiem uzskatāmi gadījumi, kad:

- datu subjekts apstrīd precizitāti, turklāt apstrāde tiek ierobežota tikai uz laiku (kamēr tiek pārbaudīta un, ja nepieciešams, ieviesta precizitāte – piemēram, ir mainījies personas uzvārds, un datos ir jāveic labojumi);
- apstrāde ir nelikumīga, un datu subjekts iebilst pret datu dzēšanu un pieprasa datu ierobežošanu.

5.6. Tiesības uz datu pārnesamību

Šīs tiesības nozīmē, ka datu subjekts var saņemt apstrādājamos datus par viņu no viena pārziņa un nodot tos apstrādei citam pārzinim, kas tehnisko iespēju pastāvēšanas gadījumā ir iespējams, pārziņiem tieši apmainoties ar informāciju (VDAR 20. panta 1. un 2. daļa). Turklāt pārziņa pienākums ir datu subjekta pieprasīto informāciju sniegt strukturētā, plaši izmantotā un mašīnlasāmā formātā (piemēram, plaši izmantotā elektroniskajā formātā). Tomēr normatīvajā regulējumā paredzēti tikai daži gadījumi, kad datu pārnesamības tiesības ir realizējamas. Tie ir gadījumi, ja datu apstrāde tiek veikta sakarā ar līgumisko saistību izpildi vai uz datu subjekta piekrišanas pamata (piemēram, pacients ir parakstījis piekrišanu, ka atļauj ārstniecības iestādei nosūtīt Valsts ieņēmumu dienestam informāciju par ārstniecības iestādē saņemto pakalpojumu apmaksu).

5.7. Saziņa ar datu subjektu

Pārzinim, apstrādājot informāciju un nodrošinot datu subjekta tiesību realizāciju, ir pienākums sniegt informāciju kodolīgā, pārredzamā, saprotamā un viegli pieejamā veidā, datu subjektam saprotamā valodā (VDAR 12. panta 1. daļa). Informācija sniedzama rakstiski vai elektroniski vai arī mutiski, ja ir veikta datu subjekta identificēšana.

Uz datu subjekta pieprasījumu pārzinim jāatbild bez liekas kavēšanās, bet ne vēlāk, kā viena mēneša laikā, Tomēr, ja jautājums ir sarežģīts vai pieprasījumu skaits ir liels, informācijas sniegšana var tikt pagarināta vēl uz diviem mēnešiem, par to sastādot un sniedzot datu subjektam saprotamu starpatbildi (VDAR 12. panta 3. daļa). Tātad, kopējais atbildes

sniegšanas termiņš nevar būt garāks par trīs mēnešiem, turklāt šādā gadījumā ir jābūt divām datu subjektam adresētajām atbildēm: viena ne vēlāk, kā mēneša laikā no pieprasījuma saņemšanas – par informācijas sniegšanas termiņa pagarināšanu un pagarinājuma iemesliem, bet otra – ne vēlāk kā divu nākamo mēnešu laikā, kurā sniegta atbilde uz pieprasījumu.

6. ĪPAŠO KATEGORIJU DATU APSTRĀDE

6.1. Definīcija

Īpašu kategoriju personas dati ir dati, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, ģenētiskie dati, biometriskie dati, kas izmantojami, lai veiktu fiziskas personas unikālu identifikāciju, **veselības** dati vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju.

Iepriekšējā normatīvajā regulējumā – Fizisko personu datu aizsardzības likumā, bija paredzēts tāds datu veids kā ***sensitīvie dati,*** un par tādiem tika uzskatīti personas dati, kas norāda personas rasi, etnisko izcelsmi, reliģisko, filozofisko un politisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas veselību vai seksuālo dzīvi. VDAR tekstā ir lietots termins *īpašu kategoriju personas dati,* un šis termins ietver sevī plašāku personas datu klāstu. Tomēr teorētiskajos VDAR apskatos, it īpaši angļu valodā, joprojām ir sastopams termins *sensitīvie dati* (*sensitive data – angl.*). Turpmāk tekstā tiks lietots termins „īpašu kategoriju personas dati".

Ļoti svarīgi, lai mērķis, kura sasniegšanai pārzinis apstrādā īpašu kategoriju personas datus, bez to apstrādes nebūtu sasniedzams.

6.2. Īpašu kategoriju datu apstrādes tiesiskais pamatojums

Datu apstrādes tiesiskie pamatojumi, t. i. izņēmuma situācijas, kurās īpašu kategoriju personas datu apstrāde ir atļauta, ir uzskaitīti VDAR 9.panta 2. daļā. Ir daudzi tiesiskie pamatojumi, bet svarīgākais no tiem – ***datu subjekta sniegta nepārprotama piekrišana*** (VDAR 9. panta 2. daļas a) punkts) viņa īpašu kategoriju personas datu apstrādei. Tajā pašā laikā valsts var noteikt gadījumus, kas vispārējais aizliegums apstrādāt šāda tipa datus nav atceļams ar paša subjekta izteiktu piekrišanu.

Īpašu kategoriju personas datu apstrāde ir pieļaujama arī (bet ne tikai), ja:

- apstrāde nepieciešama ***nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības tiesību jomā***, ja to nosaka konkrēti normatīvie akti vai koplīgums, kas atbilst konkrētiem normatīvajiem aktiem (VDAR 9. panta 2. daļas b) punkts);

- apstrāde tiek veikta, lai ***aizsargātu datu subjekta vai citas fiziskas personas vitālās intereses***, ja datu subjekts ir fiziski vai tiesiski ***nespējīgs*** dot savu piekrišanu (VDAR 9. panta 2. daļas c) punkts);
- apstrādi veic ***fonds, apvienība vai jebkura cita bezpeļņas struktūra***, kas to dara ar politisku, filozofisku, reliģisku vai ar arodbiedrībām saistītu mērķi un ar nosacījumu, ka apstrāde attiecas tikai uz šīs struktūras locekļiem vai bijušajiem locekļiem, vai arī uz personām, kas ar šo struktūru uztur regulārus sakarus saistībā ar tās nolūkiem, ievērojot normatīvajā regulējumā ietvertos apstrādes nosacījumus (VDAR 9. panta 2. daļas d) punkts).

7. PACIENTU TIESĪBAS UN PACIENTU PERSONAS DATU APSTRĀDE

7.1. Pacientu personas datu apstrādes nolūks

Veicot pacienta datu apstrādi, papildus VDAR un Fizisko personu datu apstrādes likuma prasībām, ir jāņem vērā arī Ārstniecības likuma un Pacientu tiesību likuma prasības, kā arī uz to pamata izdotu tiesību aktu normas.

7.2. Pacientu personas datu apstrādes tiesiskais pamats

Nosakot pacientu datu apstrādes tiesisko pamatu, jāņem vērā, ka ārstniecības iestāde apstrādā ne tikai datus par pacienta veselības stāvokli un diagnozi. Atbilstoši sniegtajai personas datu definīcijai personas dati ir „…jebkādi dati par […] personu…", līdz ar to, vārds, uzvārds, personas kods un citi pacienta identificēšanai nepieciešami dati arī ir personas dati, kaut arī nav uzskatāmi par īpašu kategoriju personas datiem.

Tātad, nosakot pacienta personas datu apstrādes tiesisko pamatu, jāņem vērā visu apstrādājamo datu kategorijas.

Pacienta personas datu, kuri nav uzskatāmi par īpašu kategoriju datiem, apstrādes tiesiskais pamatojums ir paredzēts VDAR 6. panta 1. daļas c) apakšpunktā, t.i., „lai izpildītu uz pārzini attiecināmu juridisku pienākumu".

Tiesiskā nolūka noteikšanas kontekstā svarīgi atšķirt divus jēdzienus:

- pacienta kā ***datu subjekta piekrišana*** datu apstrādei un
- ***pacienta***, kas vienlaicīgi arī ir datu subjekts, ***informēta piekrišana*** ārstēšanai.

Ņemot vērā apstrādes tiesisko pamatojumu, secināms, ka pacienta kā datu subjekta piekrišana viņa datu apstrādei nemaz nav nepieciešama. Savukārt, informēta piekrišana ārstēšanai ir pacienta izteikta piekrišana saņemt ārstēšanu, piekrišana ārstēšanā izmantojamajām metodēm (PTL 6. pants), un tai nav tiešas saistības ar pacienta personas datu apstrādi.

Savukārt īpašu kategoriju datu apstrādes tiesiskais pamatojums ir paredzēts VDAR 9. panta 2. daļas h) apakšpunktā – paredzēts, ka ir atļauta šāda veida datu apstrāde, kas nepieciešama ***profilaktiskās vai arodmedicīnas nolūkos, darbinieka darbspējas novērtēšanai,***

medicīniskas diagnozes, veselības vai sociālās aprūpes vai ārstēšanas vai veselības vai sociālās aprūpes sistēmu un pakalpojumu pārvaldības nodrošināšanas nolūkos. Būtiski, ka īpašu kategoriju personas datu apstrādei uz šī tiesiskā pamata ir noteikts īpašs tiesīgu personu (pārziņu) loks, t.i. īpašu kategoriju personas datus uz šī pamata drīkst apstrādāt:

- profesionāļi, uz kuriem – saskaņā ar ES vai dalībvalsts tiesību aktiem vai valsts kompetento iestāžu ieviestiem noteikumiem – attiecas dienesta noslēpuma ievērošanas pienākums;
- personas, kuras datus apstrādā minētā profesionāļa ***atbildībā***;
- citas personas, uz kurām arī attiecas pienākums ievērot dienesta noslēpumu saskaņā ar Savienības vai dalībvalsts tiesību vai valsts kompetento iestāžu ieviestiem noteikumiem.

Secināms, ka šis ir ārstniecības procesam un ārstniecības iestādēm piemērojamais izņēmums no vispārējā aizlieguma apstrādāt īpašu kategoriju personas datus, jo apstrādi veic profesionāļi – ārsti vai to darbinieki viņu atbildībā (ārsts ir atbildīgs par datu apstrādes principu ievērošanu), un, atbilstoši normatīvo aktu regulējumam, šīm personām jāievēro neizpaušanas pienākums.

Uz ārstniecības iestādēm ir attiecināmi arī citi normatīvajā regulējumā paredzētie datu apstrādes nolūki. Piemēram, nolūks apstrādāt personas datus (arī īpašu kategoriju personas datus – veselības datus), ja tas ir nepieciešams, lai aizsargātu datu subjekta vai citas fiziskās personas vitālās intereses, kas ir paredzēts VDAR 6. panta 1. daļas d) punktā, kas izņēmuma gadījumā ļauj ārstniecības personai gūt informāciju par pacientu no citiem avotiem – viņa draugiem, ja tie ir atveduši datu subjektu uz ārstniecības iestādi; savukārt, īpašu kategoriju personas datus uz šī pamata ļauj izmantot VDAR 9. panta 2. daļas c) punktā paredzētā līdzīgā norma, kas tomēr precizē, ka datu apstrāde ir pieļaujama uz šāda pamata, ja datu subjekts fiziski vai tiesiski nav spējīgs savu piekrišanu izteikt (piemēram, atrodas bezsamaņā, sāpju šokā vai tādā veselības stāvoklī, kad apzināta un situācijai adekvāta lēmuma pieņemšanu pacients pats nevar veikt).

Atsevišķi jāatzīmē pacienta personas datu apstrāde ārstniecības iestādes grāmatvedībā – grāmatvedībā atsevišķu dokumentu veidā, termiņā, kas atšķiras no medicīnas dokumentu uzglabāšanas termiņiem, tiek uzglabāti dokumenti, kas satur pacienta personas datus, arī īpašu kategoriju personas datus. Faktiski tas ir vēl viens apstrādes nolūks, lai izpildītu uz pārzini attiecināmu juridisku pienākumu. Ja pacients nenokārto savas maksāšanas saistības, ārstniecības iestādei ir tiesības nodot prasību parādu piedziņai, šādi apstrādājot personas datus ar nolūku aizstāvēt savas leģitīmās intereses, kā to nosaka VDAR 6. panta 1. daļas f) punkts.

Visi minētie apstrādes nolūki, uzrādot no to veikšanas tiesisko pamatojumu, attiecīgi atspoguļojami apstrādes reģistros, kuru izveidošanas nepieciešamību nosaka VDAR 30. pants.

7.3. Pacienta, arī kā datu subjekta, tiesības

Pacientu tiesību likums paredz pacienta tiesības saņemt informāciju, un šo tiesību realizācijas ietvaros pacientam ir iespēja noskaidrot vismaz šādu informāciju, daļa no kuras ir publiski pieejama (piemēram, izvietota ārstniecības iestādes mājas lapā un/vai ārstniecības iestādes telpās), daļa – rezervēta pašam pacientam.

Publiski pieejama informācija ir:

- Veselības aprūpes pakalpojumu saņemšanas iespējas;
- Veselības aprūpes pakalpojumu apmaksas kārtība.

Pacientam ir tiesības iegūt ar viņa ārstēšanas procesu saistītu informāciju, tostarp, bet ne tikai:

- Ārstējošā **ārsta vārdu, uzvārdu, amatu**, profesiju, specialitāti un kvalifikāciju;
- veselības aprūpes procesā iesaistīto **ārstniecības personu vārdu, uzvārdu, amatu**, profesiju, specialitāti un kvalifikāciju;
- informāciju par savu veselības stāvokli, t.sk. slimības diagnozi, ārstēšanas, izmeklēšanas un rehabilitācijas plānu, prognozi un sekām, kā arī slimības radītajiem funkcionēšanas ierobežojumiem un profilakses iespējām;
- pēc ārstniecības ietvaros veiktas izmeklēšanas un ķirurģiskās vai cita veida invazīvās iejaukšanās – informāciju par ārstniecības rezultātiem, par iepriekš neparedzētu iznākumu un tā iemesliem.

Jāatzīmē, ka šajā gadījumā personu vārda, uzvārda un amata, kas ir identificējošā vai identifikāciju atvieglojošā informācija, izpaušana neliecina par datu prettiesisku izmantošanu, jo šajā gadījumā ārsti un veselības aprūpes personāls, kas veic savu profesionālo darbību, nav uzskatāmi par aizsargājamajiem datu subjektiem.

Savukārt, paša pacienta dati tiek aizsargāti – tas nostiprināts normatīvajā regulējumā, kas nosaka, ka informācija, kas attiecas uz identificētu vai identificējamu pacientu, ir aizsargājama saskaņā ar fizisko personu datu aizsardzību regulējošiem normatīvajiem aktiem, un nav izpaužama pat pēc pacienta nāves. Tomēr, likumā ir paredzēti izņēmumi no vispārējās kārtības, t.i. informācija var tikt izpausta:

- pēc pacienta nāves – normatīvajos aktos īpaši paredzētajos gadījumos un noteiktajām personām (PTL 10. panta 4. daļa un 7. panta 1. daļa);
- uz pacienta rakstiskas piekrišanas pamata;
- citos šajā likumā noteiktajos gadījumos, t.i. informācijas sniegšana valsts institūcijām (Datu valsts inspekcijai, Tieslietu ministrijai, Valsts darba inspekcijai u.c.) un noteikta veida privātajām iestādēm (ārstniecības iestādēm, apdrošināšanas sabiedrībām u.c.) likumā noteikto nolūku realizācijai;
- ja pacients ir pilnvarojis citu personu realizēt viņa pacienta tiesības, piemēram, parakstot attiecīgu dokumentu vai izsniedzot notariāli apliecinātu pilnvaru šādu darbību veikšanai;
- ja pacients sava veselības stāvokļa vai vecuma dēļ pats nespēj pieņemt lēmumu par ārstniecības procesu un citiem ārstēšanas procesā svarīgiem tiesiskajiem aspektiem, un viņa vietā to dara normatīvajā regulējumā noteiktā persona (PTL 7. pants);

Pašam pacientam ir tiesības iegūt informāciju par sevi un saņemt šo informāciju apliecinošās dokumentu kopijas, norakstus, izrakstus no viņa medicīnas dokumentiem, t.i. saņemt visu viņa personas datus saturošu informāciju. Tomēr, sniedzot pacientam viņa pieprasīto informāciju, arī izsniedzot dokumentu kopijas, ārstniecības iestādei jāievēro datu apstrādes drošība, izvēloties tādu informācijas un pieprasīto dokumentu nodošanas veidu, kas neapdraud datu drošību.

No VDAR paredzētajām tiesībām, uz pacientu kā personas datu subjektu nav pilnā mērā attiecināmas tiesības datus labot, jo labojami ir tikai dati, kas attiecas uz pašu subjektu, bet pieraksti par pacienta veselības stāvokli un viņam sniegto ārstēšanu nav dzēšami to obligātajā glabāšanas laikā, lai gan diagnoze vēlāk var arī neapstiprināties.

Tiesības uz dzēšanu ir realizējamas ierobežotā apmērā un var tikt realizētas tikai pēc noteiktā datu apstrādes termiņa beigām. Tomēr pēc noteiktā dokumentu glabāšanas termiņa beigām pārziņa pienākums ir gādāt par datu iznīcināšanu.

7.4. Nepilngadīga pacienta tiesības un viņa aizbildņa tiesības saņemt informāciju

Persona juridiski iegūst neierobežotu rīcībspēju, kā arī tiesības patstāvīgi pieņemt neatkarīgus lēmumus par savu dzīvi, ar pilngadības, t. i. astoņpadsmit gadu vecuma,

sasniegšanu. Tomēr personas kā datu subjekta tiesības un loma ārstēšanas procesā ievērojami atšķiras no vispārīgās juridiskās prakses.

Pacientu tiesību likums paredz, ka četrpadsmit gadu vecums ir tā robeža, kad nepilngadīgajai personai ir tiesības piedalīties lēmumu pieņemšanā par ārstēšanas procesu, un, līdz ar to, iegūt informāciju kā datu subjektam.

Pacientu tiesību likumā ir noteikts, ka nepilngadīga pacienta (līdz 14 gadu vecumam) ārstniecība pieļaujama, ja viņa likumiskais pārstāvis par to ir informēts un devis savu piekrišanu. Likumiskais pārstāvis ir viens no vecākiem vai ar bāriņtiesas lēmumu iecelts aizbildnis, kā arī persona, kura vecāku prombūtnes laikā uz vecāku (vai viena no viņiem) izdotās pilnvaras pamata rūpējas par bērnu. Turklāt nepilngadīgam pacientam ir tiesības tikt uzklausītam un atbilstoši savam vecumam un briedumam piedalīties ar ārstniecību saistītā lēmuma pieņemšanā.

Sākot ar brīdi, kad pacients sasniedzis 14 gadu vecumu, pacients kļūst par pirmo personu, kurai jāpiekrīt ārstēšanai. Ja nepilngadīgais, 14 gadu vecs pacients, ārstēšanai nepiekrīt, bet ārsts pamatoti uzskata, ka ārstēšana ir pacienta interesēs, piekrišanu var dot likumiskais pārstāvis.

Tajā paša laikā, informāciju par nepilngadīgo pacientu kā par datu subjektu viņa likumiskais pārstāvis ir tiesīgs iegūt līdz pilngadības sasniegšanai. Svarīgi, ka informāciju par nepilngadīgu pacientu likumiskajam pārstāvim nesniedz, ja šādas informācijas izpaušana var kaitēt pacienta interesēm. Ārsts pieņemto lēmumu ieraksta pacienta medicīniskajos dokumentos un informē par to bāriņtiesu. Ir būtiski ņemt vērā, ka šādas tiesības ir piešķirtas ārstam, nevis speciālistiem, kuri sadarbojas un/vai palīdz ārstam (piemēram, medicīnas māsa, klientu un pacietu reģistrators).

7.5. Ārstniecības personu pienākums izpaust informāciju par pacientu

Normatīvajos aktos ir paredzēti atsevišķi gadījumi, kas ārstniecības iestādēm ir ne tikai tiesības, bet pat pienākums izpaust datus par pacientiem, tomēr tie ir īpaši gadījumi.

Ārstniecības iestādei ir pienākums ne vēlāk, ka 12 stundu laikā paziņot Valsts policijai, ja, sniedzot palīdzību pacientam, ārstniecības iestādei ir pamats uzskatīt, ka pacients ir cietis no vardarbības. Attiecībā uz nepilngadīgajām personām likums nosaka ārstniecības iestāžu pienākumu paziņot Valsts policijai, ja, sniedzot palīdzību nepilngadīgajam pacientam, rodas

aizdomas ne tikai par to, ka pacients cietis no pienācīgas aprūpes un uzraudzības trūkuma, bet arī no citiem bērnu tiesību pārkāpumiem (ĀL 56^1. pants). Savukārt bērna tiesības, kuras varētu būt pārkāptas, un pārkāpšanas pazīmes, kuras var tikt pamanītas ārstēšanas laikā, ir uzskaitītas Bērnu tiesību aizsardzības likumā.

Vardarbības pazīmes, kuras norādītas minētajā Ārstniecības likuma pantā ir precizētas Kriminālprocesa likuma 369. panta 2. daļā, kur uzskaitītas pazīmes, ziņojums par kurām var būt par pamatu krimināllietas ierosināšanai – tās ir: ziņojumi par traumām, slimībām vai nāves gadījumiem, kuru cēlonis varētu būt noziedzīgs nodarījums.

Pārējos gadījumos ārstniecības iestādes var sniegt informāciju, kas iegūta, pildot profesionālos pienākumus (t. i. ārstēšanas gaitā) tikai pēc procesa virzītāja rakstveida pieprasījuma (KPL 121. panta 4. daļa).

8. PERSONAS DATU AIZSARDZĪBAS PASĀKUMI

8.1. Risku pārvaldība

Atkarībā no apstrādājamajiem personas datiem, personas datu apstrādē izmantotajiem līdzekļiem (informācijas sistēmas, tradicionālie dokumenti), kā arī apstrādes procesiem, pārzinim ir jāizvērtē riski (draudi), tos raksturojošie riska faktori (apstākļi, kuru iestāšanās veicina risku) un jāveic atbilstoši pasākumi risku pārvaldīšanai: novēršanai, minimizēšanai, kontrolei.

Pie vērtējamajiem riska faktoriem pieskaitāmi tādi faktori kā apstrādājamo datu apjoms un saturs, apstrādē iesaistīto personu skaits un to reputācija, apstrādē izmantojamās metodes un līdzekļi, telpu raksturojums, kurās notiek apstrāde.

8.2. Personas datu fiziskās aizsardzības līdzekļi

Fiziskās aizsardzības līdzekļi ir pasākumu kopums, kas nodrošina datu aizsardzību no fiziskās iejaukšanās tajos, to bojāšanas vai iznīcināšanas (integritāte, drošība un konfidencialitāte).

Šādiem līdzekļiem pieskaitāmi tādi pasākumi kā apsardzes un ugunsdrošības signalizācijas uzstādīšana telpās, kur personas dati tiek apstrādāti vai arī uzglabāti, piekļuves kontroles sistēmas uzstādīšana vai citāda tehniskā piekļuves ierobežošana, norobežojošu konstrukciju uzstādīšana, ierobežojot iespēju nesankcionēti iegūt datus vai izlasīt datus no datora vai dokumenta u.c. pasākumi.

Šādi personas datu aizsardzības līdzekļi īpaši lielu nozīmi iegūst ārstniecības iestādēs, kurās personas dati tiek apstrādāti papīra formā (piemēram, pacientu kartiņas tiek aizpildītas rokrakstā) vai, kuras savā darbā mazāk izmanto informācijas tehnoloģijas.

8.3. Personas datu aizsardzība informācijas tehnoloģijās

Informācijas tehnoloģiju produktiem ir daudz priekšrocību un arī daudz trūkumu. No vienas puses, IT produktu straujā attīstība rada daudz labuma, ļaujot efektīvāk organizēt darbu, vienlaicīgi strādāt lielam personu daudzumam, apstrādāt lielākus informācijas apjomus,

pieņemt elastīgus un informētus lēmumus. Tajā pašā laikā, informācijas tehnoloģijās slēpjas pietiekami daudz draudu, ieskaitot draudus datu saglabāšanai.

Izmantojot IT risinājumus datu apstrādē un saglabāšanā, ļoti svarīgi ir ievērot IT drošības un datu aizsardzības speciālistu izstrādātos personas datu aizsardzības pasākumus. Diemžēl arī aizsargātā vidē dati pakļauti uzbrukumiem, bet tad uzbrukumus veikt ir daudz grūtāk.

Sociālā inženierija ir viens no uzbrukuma veidiem un nozīmē manipulēšanu ar cilvēku, lai tas veiktu zināmas darbības vai izpaustu konfidenciālu informāciju, tehniski nepiekļūstot informācijas sistēmai. Sociālās inženierijas paņēmieni tiek īstenoti, pamatojoties uz īpašiem atribūtiem cilvēka lēmumu pieņemšanas mehānismos. Cilvēku var iebiedēt, var veikli izmantot cilvēka ambīcijas, nogurumu, pret cilvēku vērstu psihisku spiedienu.

Pikšķerēšana (phishing) ir sociālās inženierijas veids, kurā krāpnieks mēģina krāpnieciski iegūt likumīgu lietotāju sensitīvo informāciju, imitējot uzticamas organizācijas elektroniskos komunikācijas kanālus[1].

Spožākais piemērs ir kredītiestāžu viltus mājas lapu izveidošana un lūgumu sūtīšana ienākt tajās.

Vēl viens populārs uzbrukumu veids ir ***ļaunatūra jeb kaitīgā programma***, kas ir datorvīruss *(computervirus)* jeb programma, kas patvaļīgi pievienojas citām datora programmām un to darba laikā veic dažādas nevēlamas darbības: bojā datnes, katalogus un skaitļošanas rezultātus, dzēš vai piesārņo atmiņu, kā arī citādi traucē datora darbību.

Ļaunatūras iegūšanas veidi ir dažādi, piemēram, no ļaundaru apzināti izveidotas interneta vietnes, īpaši bieži – pornogrāfiska rakstura vietnēm, sērfojot internetā, t. sk., šim mērķim izmantojot mobilo ierīci; kad tiek „uzlauztas" interneta vietnes, kurās slēpti ievietots kaitīgs kods; ievietojot nezināmas izcelsmes (piemēram, biroja ēkas gaitenī atrastas) ārējo datu nesēja ievietošana datorā.

Šeit minētie uzbrukumu veidi nav vienīgie. IT joma attīstās ļoti strauji. Daļa no produktiem tiek radīti, lai nopelnītu, sniedzot papildus ērtības programmas lietotājiem, bet daļa produktu rada reālu apdraudējumu lietotāju labklājībai.

Jāatzīmē, ka ne vienmēr datu apstrādes apdraudējuma pamatā ir ielaušanās no ārpuses. Ārējo ļaundaru ietekmēti vai pašu savtīgo vai ziņkārības motīvu vadīti, to var izdarīt arī pārziņa vai apstrādātāja darbinieki vai viņu pakļautībā strādājošās personas.

Līdz ar to, ir svarīgi ieviest datu aizsardzības noteiktās prasības, kas palīdz gan

[1]https://lv.fondoperlaterra.org/comdifference-between-phishing-and-spoofing-9#menu-2

uzbrukumu novēršanā, gan to atklāšanā. No tādiem līdzekļiem jāpiemin:

- ***auditācijas pieraksti*** – analīzei pieejami pieraksti, kuros reģistrēti dati par noteiktiem notikumiem informācijas sistēmā, to veikšanas nodrošināšana, to uzglabāšana un regulāra analīze.
- ***piekļuves kontrole***, kuras ietvaros tiek noteiktas atsevišķu lietotāju piekļuves tiesības, veicot to autentifikāciju un atbilstošu autorizāciju, minimizējot piekļuvi ieguvušo personu skaitu sistēmai, šādi nodrošinot, ka attiecīgās profesijas vai amatā esoša persona piekļūst tikai darbam nepieciešamajam datu apjomam;
- ***tiesību pārvaldības*** nodrošināšana, t.i. situācijas izveidošana, kad, mainoties personas statusam attiecībā pret datu pārzini vai apstrādājamajiem datiem, mainās (palielinās vai samazinās) šis personas tiesības piekļūt personas datiem;
- ***autentifikācijas***, t.i. personas identitātes apliecināšanas nodrošināšana piekļuvei informācijas sistēmai un tajā esošajiem datiem. Šiem mērķiem var tikt izmantoti vairāki līdzekļi, no kuriem jāpiemin paroles, piekļuves kartes, biometrijas dati.

Ir būtiski saprast arī, ka ļoti lielu apdraudējumu daļu veido drošības instrukciju ignorēšana no cilvēka – sistēmas lietotāja puses, kā arī cilvēka nepārdomāta rīcība un uzmanības nepievēršana iespējamām savas rīcības vai bezdarbības sekām.

9. INCIDENTI UN INCIDENTU PĀRVALDĪBA

9.1. Incidenta jēdziens

Jebkuram datu apstrādes dalībniekam – gan pārzinim, gan apstrādātājam – ir jāievēro vispārējie datu apstrādes principi un jāapzinās atbildība par datu apstrādes pārkāpumiem. Ir nepieciešams radīt datu apstrādes sistēmu, kura nodrošina, ka:

- dati ir pieejami tikai pilnvarotām personām (konfidencialitāte);
- dati ir pasargāti pret pilnīgiem vai daļējiem datu zudumiem (integritāte).
- dati ir pieejami tikai un vienīgi tādā apjomā, kāds nepieciešams konkrētā datu apstrādes mērķa sasniegšanai (pieejamība);

Datu apstrādes ***konfidencialitāte*** nozīmē, ka informācija ir pieejama tikai tādā apjomā, kādā nepieciešams, tikai pašam datu subjektam vai viņa pilnvarotajai personai un tikai tajā laikā, kad šīs konkrētās identificētās personas ir autorizējušās, lai iegūtu konkrēto informāciju.

Datu ***integritāte*** nozīmē, ka informācija – dati ir pilnīgi un neizmainīti jebkurā apstrādes stadijā, neatkarīgi no apstrādes veidiem.

Datu ***pieejamība*** nozīmē, ka informācija – dati tiek apstrādāti ar konkrētu mērķi, ir pieejami īstajā laikā, īstajā apmērā, īstajai personai un formulēti izmantojamā veidā.

Jebkurš notikums, kas ietekmē datu konfidencialitāti, integritāti vai pieejamību, uzskatāms par ***incidentu***. Kaut gan skaidrojošajās vārdnīcās par ”incidentu” dēvē nejaušu notikumu, gadījumu, parasti vārdam ”incidents” ir negatīva nozīme un ar to ir pieņemts apzīmēt negatīvus notikumus.

Normatīvajā regulējumā datu aizsardzības incidenta apzīmēšanai paredzēts termins ***personas datu aizsardzības pārkāpums***, kas ir „drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem” (VDAR 4. pants 12. punkts).

Acīmredzams, ka pārkāpuma konstatēšanai nemaz nav nepieciešams ļauns nolūks; tas var tikt izdarīts arī nejauši un neuzmanības dēļ, tomēr, ņemot vērā definīcijā iekļautā vārda „pārkāpums” nozīmi, var iedomāties, ka, lai notiktu pārkāpums, tomēr jānotiek noteiktai, kaut arī nejaušajai, personas rīcībai; tajā pašā laikā incidents ne vienmēr ir saistīts ar šādu darbību. Kaut arī incidenta jēdziens ir plašāks, normatīvo aktu prasības izpildei ieteicams šos divus

jēdzienus nenošķirt un katru incidentu uzskatīt par pārkāpumu.

9.2. Rīcība datu aizsardzības pārkāpuma gadījumā

Normatīvais regulējums paredz tikai noteiktu darbību veikšanu saistībā ar personas datu aizsardzības pārkāpumiem, nevis incidentiem. Tomēr, ņemot vērā jēdzienu nošķiršanas grūtības, ieteicams izmeklēt katru incidentu. Turpmāk tekstā tiks lietots termins „pārkāpums".

Katrs datu aizsardzības pārkāpums pārzinim ir jādokumentē, t.i. jāveido pārkāpumu reģistrs, kurā norāda pārkāpumu, ar to saistītos faktus, sekas un veiktās koriģējošās darbības.

Par katru notikušo pārkāpumu bez nepamatotas kavēšanās, bet ne vēlāk kā 72 stundu laikā no pārkāpuma konstatēšanas brīža, ir jāziņo uzraudzības iestādei (Datu valsts inspekcijai). Šāds paziņošanas termiņš pārzinim ir jāievēro attiecībā pret uzraudzības iestādi, bet apstrādātājam – attiecībā pret pārzini. Paziņojuma iesniegšanas termiņa nokavējums ir pieļaujams tikai pārzinim, un, iesniedzot paziņojumu ar nokavējumu, nokavējuma iemesli ir jāpamato.

Sniedzot paziņojumu par pārkāpumu, pārzinim ne tikai ir jāapraksta pārkāpuma apstākļi un sekas, bet arī jāsniedz apraksts pasākumiem, kas ir veikti vai tiks veikti, lai novērstu datu aizsardzības pārkāpumu.

Pārzinim pirms paziņošanas uzraudzības iestādei ir jāizvērtē, vai pārkāpuma rezultātā ir radīts risks fizisku personu tiesībām un brīvībām. Ja šāda riska iestāšanās ir maz ticama, paziņošanas pienākums atkrīt. Savukārt, ja fizisku personu tiesībām un brīvībām radītais risks ir augsts, tad papildus uzraudzības iestādei tiek informēti arī datu subjekti. Datu subjektus var neinformēt, ja dati ir šifrēti, pārzinis ir veicis pasākumus negatīvo seku mazināšanai, kā arī, ja subjektu informēšana prasītu nesamērīgi lielas pūles, ar nosacījumu, ja uzraudzības iestāde atzinusi, ka pastāv apstākļi, kas atceļ paziņošanas pienākumu.

9.3. Administratīvā atbildība

Atbilstoši normatīvajam regulējumam, uzraudzības iestādei ir tiesības piemērot noteiktos korektīvos līdzekļus pārzinim vai apstrādātājam, t.i.

- izteikt brīdinājumu (pirms pārkāpuma izdarīšanas),
- izteikt rājienu,
- izdot dažāda satura rīkojumus,

- ierobežot vai aizliegt datu apstrādi;
- piemērot administratīvos sodus;
- u.c.

Administratīvā soda noteikšanai ir svarīgi izvērtēt, vai pārkāpums ir tīšs vai aiz neuzmanības izdarīts. Svarīgas ir arī pārkāpuma sekas.

Normatīvajā regulējuma paredzēti sodu apmēri ir ļoti iespaidīgi un iedalīti divās grupās:

- Sods par pārziņa vai apstrādātāja pienākumu nepildīšanu (piemēram, netiek izveidots datu apstrādes reģistrs, nav iecelts datu aizsardzības speciālists u. tml.) – līdz EUR 10’000’000 vai 2% no globālā gada apgrozījuma, vadoties pēc tā, kura no summām ir lielāka;
- Sods par datu subjekta tiesību neievērošanu (piemēram, neinformēšanu, prasību ignorēšanu u. tml.) – līdz EUR 20’000’000 vai 4% no globālā gada apgrozījuma, vadoties pēc tā, kura no summām ir lielāka.

9.4. Krimināatbildība

Krimināatbildība par pārkāpumiem fizisko personu datu apstrādes jomā ir paredzēta Krimināllikuma 145. pantā. Minētajā pantā paredzētās sankcijas ir alternatīvas, t.i. paredz vairākus alternatīvos sodus, un tie var būt naudas sods, piespiedu darbs vai pat brīvības atņemšana – īslaicīga (no piecpadsmit dienām līdz trīs mēnešiem) vai uz laiku līdz pieciem gadiem, kas ir smagākais sods.

Izšķir nelikumīgas darbības ar fiziskas personas datiem, ar kurām radīts būtisks kaitējums, kas likumdevēja ieskatā ir mazāk smags noziegums, kā arī nodarījums, kas saistīts ar pārziņa un citu apstrādē iesaistīto personu ietekmēšanu, arī vardarbīgu, ar nolūku veikt nelikumīgas darbības ar personas datiem.

Būtisks kaitējums nosakāms, pamatojoties uz tiesā pārbaudītiem pierādījumiem, izvērtējot interešu apdraudējuma veidu, saturu, intereses nesēja jeb personas, pret kuru vērsts apdraudējums, īpašības un attieksmi pret konkrēto interešu apdraudējumu.

10. IZMANTOTĀS LITERATŪRAS UN AVOTU SARAKSTS

1. Eiropas parlamenta un padomes regula 2016/679 (2016. gada 27. aprīlis) 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). Pieejams: https://ej.uz/123regula
2. Eiropas parlamenta un padomes regula 2018/1725 (2018. gada 23. oktobris) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi Savienības iestādēs, struktūrās, birojos un aģentūrās un par šādu datu brīvu apriti un ar ko atceļ Regulu (EK) Nr. 45/2001 un Lēmumu Nr. 1247/2002/EK. Pieejams: https://ej.uz/ugwx
3. Cilvēka tiesību un pamatbrīvību aizsardzības konvencija. Pieejams https://ej.uz/zgcd
4. Kriminālprocesa likums. Pieejams https://ej.uz/6gss
5. Augstākās tiesas 06.11.2020. spriedums lietā Nr. SKA-41/2020. Pieejams https://ej.uz/pu1c , Kriminālprocesa likums, 121.pants, ceturtā daļa
6. Fizisko personu datu apstrādes likums. Pieejams: https://ej.uz/dati_2018
7. Pacientu tiesību likums. Pieejams: https://ej.uz/ebas
8. Ārstniecības likums. Pieejams: https://ej.uz/g5xs.
9. Administratīvās atbildības likums. Pieejams: https://ej.uz/f4r3
10. Likums "Par fizisko personu datu apstrādi kriminālprocesā un administratīvā pārkāpuma procesā". Pieejams: https://ej.uz/em8p
11. Eiropas Datu aizsardzības uzraudzītāja atzinums "Mobilā veselība – tehnoloģisko jauninājumu un datu aizsardzības saskaņošana" (2015/C 232/06). Pieejams: https://ej.uz/1fxr
12. EDAK-EDAU kopējais atzinums 1/2019 par pacientu datu apstrādi un Eiropas Komisijas pienākumiem e- veselības digitālo pakalpojumu infrastruktūrā (eHDSI). Pieejams: https://ej.uz/e6a6
13. Eiropas pacientu foruma vadlīnijas pacientiem. Pieejams: https://ej.uz/bkxu
14. Veselības datu definīcija iekārtās. Pieejams: https://ej.uz/5km2