Madonas slimnīca	Madonas novada pašvaldības SIA "Madonas slimnīca" **PERSONAS DATU APSTRĀDES NOTEIKUMI** Dokumenta reģistrācijas Nr. 38/1.6/23	Versija 01 Apstiprināts ar Madonas novada pašvaldības SIA "Madonas slimnīca" valdes priekšsēdētājas Līgas Šernas 19.12.2023. rīkojumu Nr. /2.1/23

I VISPĀRĪGIE NOSACĪJUMI

1. Madonas novada pašvaldības SIA "Madonas slimnīca" personas datu apstrādes noteikumu (turpmāk – Noteikumi) mērķis ir:

1.1. noteikt Madonas novada pašvaldības SIA "Madonas slimnīca" (turpmāk – Organizācija) organizatorisko pasākumu un nepieciešamo tehnisko līdzekļu kopumu, kas nodrošina godprātīgu un likumīgu personas datu apstrādi un lietošanu tikai paredzētajiem mērķiem, to glabāšanas, atjaunošanas, labošanas un dzēšanas veidu, nodrošinot ikvienas fiziskas personas tiesības uz savu personas datu aizsardzību;

1.2. nodrošināt drošu un normatīvajos aktos noteiktajām prasībām atbilstošu Personas datu apstrādes aizsardzības sistēmu.

2. Noteikumi ir saistoši visiem Organizācijas darbiniekiem vai citādi ar Organizāciju saistītajām personām, kuras, veicot savus tiešos darba vai citu saistību pienākumus, nonāk saskarē ar Organizācijas rīcībā esošiem Personas datiem.

II PERSONAS DATU DROŠĪBAS PAMATNOSACĪJUMI

Organizācijas tiesības un pienākumi:

3. Par personas datu aizsardzību, personas datu drošības un drošības pilnveidošanas procesu kopumā atbild Organizācijas valde, kura pati vai ar atbilstoši norīkotu personu starpniecību kontrolē personas datu apstrādes sistēmu drošību.

4. Personas datu apstrādi Organizācijā veic tikai darbinieki, kuriem, saskaņā ar amata pienākumiem, ir tiesības Personas datus apstrādāt (turpmāk - Pilnvarotās personas),.

5. Organizācija var bez brīdinājuma ierobežot pilnvarotās personas piekļuvi Organizācijas informācijas sistēmām (turpmāk - IS) vai citā formā glabātiem personas datiem, ja pilnvarotā persona pārkāpj Organizācijas iekšējos vai ārējos normatīvos aktus.

6. Personas uzsākot darba tiesiskās attiecības (vai uz cita līguma pamata) Organizācijā iepazīstas un paraksta apliecinājumu (1.pielikums), par Noteikumu un konfidencialitātes prasību ievērošanu darbā ar Personas datiem un IS. Apliecinājumu glabā Personāla speciāliste.

7. Organizācijas pienākums ir rūpēties par personas datu aprites drošību, nodrošinot tikai pilnvaroto personu autorizētu piekļuvi personas datiem, personas datu nepieejamību neautorizētām personām, kā arī iespēju datu subjektam iepazīties ar saviem personas datiem.

8. Organizācija nosaka atbildīgos darbiniekus par noteiktiem mērķiem veiktām datu apstrādēm: atbildīgie darbinieki par IS incidentu reģistrēšanu (IT nodaļas vadītājs) un datu apstrādes reģistra vešanu (datu aizsardzības speciālists) (turpmāk – Procesa īpašnieki). Procesa īpašniekiem ir sekojoši pienākumi attiecībā uz to pārziņā nodotiem procesiem:

8.1. nodefinēt/pārskatīt atbildībā nodotās datu apstrādes mērķus (to būtiskumu, nepieciešamību);

8.2. izveidot/ pārskatīt atbildībā nodoto procesu regulējošās procedūras/ instrukcijas/ politikas/ paziņojumus;

8.3. izveidot/pārskatīt datu subjektu informēšanas mehānismus (*piemēram, datu apstrādes paziņojumus*);
8.4. izvērtēt saņemtos datu subjektu pieprasījumus (dzēst, labot, iebilst, saņemt informāciju un citi) un nodrošināt atbilžu sniegšanu uz tiem;
8.5. izvērtēt saņemtās sūdzības par Personas datu apstrādi un nodrošināt atbilžu sniegšanu uz tām;
8.6. izvērtēt un nodrošināt atbilstošu sadarbības partneru (apstrādātāju) izvēli, līguma noslēgšanu un uzraudzību;
8.7. piedalīties Personas datu drošības incidentu izvērtēšanā, risku identificēšanā, seku minimizēšanā un nākotnes pasākumu izstrādē, lai nepieļautu turpmāku risku iestāšanos, kā arī sekot šo veicamo darbu izpildei;
8.8. sekot līdzi apstākļu un normatīvo aktu izmaiņām, kas varētu ietekmēt Personas datu apstrādi attiecīgajam mērķim, un attiecīgu izmaiņu rezultātā pārbauda apstrādāto Personas datu veidu aktualitāti un adekvātumu, un, ja nepieciešams, veic apstrādē izmantojamo Personas datu veidu aktualizēšanu, lai nodrošinātu izmantojamo Personas datu atbilstību Personas datu apstrādes mērķim;
8.9. noteikt tās darbinieku kategorijas, kurām ir tiesības piekļūt tā atbildībā nodotiem Personas datiem;
8.10. sadarbībā ar citām struktūrvienībām/darbiniekiem (juristu, IS administratoru) izstrādāt atbilstošus tehniskos un organizatoriskos pasākumus tā atbildībā nodoto personas datu apstrādei, tai skaitā, apstrādātājiem nodoto personas datu apstrādei.
9. Organizācija ir tiesīga pieprasīt informāciju par pienākumu izpildi no Pilnvarotajām personām, kuras iesaistītas Personas datu apstrādē.

Pilnvarotās personas tiesības, pienākumi un atbildība:

10. Pilnvarotā persona apstrādā Personas datus, ievērojot atbilstošajos normatīvajos aktos noteikto kārtību un Noteikumu prasības.
11. Pilnvarotā persona Personas datu apstrādes laikā nodrošina, ka apstrādājamie Personas dati nav pieejami Trešajām personām.
12. Pilnvarotā persona reģistrē Personas datu nodošanas un saņemšanas faktu Organizācijas noteiktā kārtībā, izņemot ja šāda datu nodošana tiek reģistrēta ar automātiskiem līdzekļiem.
13. Pilnvarotās personas lietošanā nodotos Personas datus vai piekļuvi Personas datiem tā izmanto tikai uzdoto uzdevumu izpildes vajadzībām.
13. Pilnvarotai personai aizliegts izpaust ziņas par IS uzbūvi un konfigurāciju, fiziskās un loģiskās Personas datu aizsardzības līdzekļiem, kā arī atklāt Personas datus nepilnvarotām personām un/vai Trešajām personām, izņemot šajos Noteikumos noteiktos gadījumos. Pirms Personas datu izpaušanas nepieciešams veikt informācijas saņēmēja identificēšanu, pārliecināties par informācijas saņēmēja pilnvarojumu vai tiesībām saņemt Personas datus, šaubu gadījumā neveicot Personas datu saturošas informācijas izplatīšanu, ziņojot par nepamatotiem Personas datu saturošas informācijas pieprasījumiem Organizācijas datu aizsardzības speciālistu.
14. Pilnvarotās personas pienākums ir saglabāt un bez tiesiska pamata neizpaust Personas datus arī pēc darba tiesisko attiecību vai citu līgumattiecību izbeigšanas ar Organizāciju. Šādam pienākumam ir beztermiņa raksturs.
15. Pilnvarotās personas pienākums ir lietot Organizācijas noteiktos, kā arī, ja nepieciešams, paša izvēlētus tehniskos un organizatoriskos līdzekļus, lai aizsargātu Personas datus un novērstu to nelikumīgu iegūšanu.
16. Pilnvarotā persona atbildīga par IS un citā formātā glabātiem Personas datiem, kas nodoti viņa rīcībā, kā arī par citiem dokumentiem, kas nepieciešami darba pienākumu vai citu saistību pildīšanai.

17. Pilnvarotai personai aizliegts izmantot nelicencētu informācijas tehnoloģiju (turpmāk - IT) programmatūru tam nodotos informācijas resursos.
18. Pilnvarotā persona nedrīkst izdarīt darbības, kas būtu vērstas pret IS drošību, izmantojot neparedzētas pieslēgšanās iespējas.
19. Pilnvarotā persona nodrošina, ka pārtraucot darbu ar informācijas resursiem, kuros apstrādāti Personas dati, ja apstrāde notiek IS - Pilnvarotā persona aizver pārlūkprogrammu, savukārt, ja Personas datu apstrāde notiek, izmantojot papīra dokumentus, – Pilnvarotā persona tos novieto to glabāšanas vietā.
20. Pilnvarotai personai, ja tā nav īpaši pilnvarota uz šādām darbībām, aizliegts saņemtos Personas datus pārveidot, atsavināt, reproducēt to kopumā vai tās daļas, izmantot to citu datu apstrādes sistēmu izveidei, kā arī glabāt publiski pieejamās vietās bez uzraudzības.
21. ziņot Organizācijai, ja ir aizdomas par riskiem IS un citā veidā apstrādātiem datiem, par bojājumiem IS, par paroles iespējamu nonākšanu trešo personu rīcībā un citām situācijām, kas var radīt riskus Personas datu drošībai.
22. par prettiesisku nodarījumu Pilnvarotā persona atbild normatīvajos aktos noteiktajā kārtībā;
23. Pilnvarotai personai ir tiesības izteikt priekšlikumus Personas datu aizsardzības sistēmas uzlabošanai, pilnveidošanai un tās atbilstības nodrošināšanai normatīvajos aktos noteiktajām prasībām, par to informējot Organizācijas datu aizsardzības speciālistu.
24. Par drošības pasākumu ievērošanu atbild visi Organizācijas darbinieki, kam ir pieeja IS un citā formātā glabātiem Personas datiem.
25. Ja Organizācijai ir nepieciešams padarīt darbiniekiem vai citām personām (pakalpojuma nodrošinātājiem) pieejamu daļu no Organizācijas Personas datus saturošiem resursiem, šo pieeju vienmēr kontrolē, pie tam, padarot pieejamu iespējami minimālo Personas datu apjomu, tai skaitā, ja tas iespējams, veicot datu pseidonimizēšanu (personas identifikatoru aizklāšanu).
26. Izpaužot Personas datus Trešajām personām, Organizācija saglabā datus par Personas datu izpaušanas laiku; personu, kas nodevusi informāciju; personu, kas pieprasījusi informāciju un to saņēmusi; nodotās informācijas apjomu.
27. Tāpat Organizācija nodrošina, ka Personas datu apstrādi, tas ir, vākšanu, reģistrāciju, organizēšanu, strukturēšanu, glabāšanu, pielāgošanu, pārveidošanu, atgūšanu, aplūkošanu, izmantošanu, izpaušanu, nosūtīšanu, izplatīšanu vai citādi darot tos pieejamus, saskaņošanu, kombinēšanu, ierobežošanu, dzēšanu vai iznīcināšanu veic tikai tam Pilnvarotas personas un/vai Personas datu apstrādātājs, kā arī nodrošina iespēju noteikt tos Personas datus, kuri ir bijuši apstrādāti bez attiecīgā pilnvarojuma, kā arī apstrādes laiku un personu, kas to veikusi.
28. Darbiniekiem savā darba vietā un veicot darba pienākumus ir pēc iespējas jāsamazina Personas datu nonākšanas nepilnvarotu personu rīcībā risks, kas var rasties darbinieka rīcības dēļ: kļūda, zādzība, neuzmanība informācijas nodošanā vai nepareiza informācijas resursu lietošana.
29. Organizācijai kā darba devējam ir jāveic Organizācijas darbinieku informēšana, nodrošinot, ka Personas datu lietotāji apzinās Personas datu drošības nozīmību un iespējamos draudus tai un ir pietiekami kvalificēti, lai ievērotu un izpildītu Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (27.04.2016.) 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) (turpmāk - Regula) un Fizisko personas datu apstrādes likuma, Pacientu tiesību likuma un citu normatīvo aktu tiesību normas fizisko personu datu apstrādes un aizsardzības jomā, tajā skaitā, normatīvajiem aktiem, kas reglamentē pacientu tiesības.
30. Organizācijas darbiniekus iepazīstina ar informācijas drošības prasībām, kā arī apmāca pareizi izmantot IS pirms darbiniekam piešķir pieeju tām.

III PERSONAS DATU APSTRĀDES ORGANIZĒŠANA

Personas datu apstrādes uzsākšana jauniem mērķiem vai grozījumu veikšana esošos mērķos:

31. Organizācija pirms Personas datu apstrādes uzsākšanas jauniem mērķiem, rakstiski informē datu aizsardzības speciālistu:

31.1. nodefinē datu apstrādes mērķi;

31.2. nosaka par apstrādi atbildīgos darbiniekus;

31.3. izvērtē tiesiskos pamatus, leģitīmu interešu gadījuma izvērtē vai nav nepieciešams veikt pārziņa vai trešās personas interešu un datu subjekta interešu līdzsvarošanas testu;

31.4. to personu loku, kurai būtu nepieciešams piekļūt informācijai;

31.5. nosaka Personas datu glabāšanas termiņu;

31.6. nosaka Personas datu apstrādē izmantojamos tehniskos resursus;

31.7. nosaka Personas datu apstrādē izmantojamos tehniskos un organizatoriskos pasākumus, ja tie atšķiras no kopējiem pasākumiem;

31.8. izvērtē vai nav nepieciešams veikt novērtējumu par ietekmi uz datu aizsardzību.

32. Ja tiek veiktas izmaiņas datu apstrādē, Organizācija pārskata esošā personas datu apstrādes saturu un pēc nepieciešamības koriģē to.

33. Personas datu apstrāde tiek veikta Organizācijas telpās, Personas datu apstrādātāju telpās (saskaņā ar noslēgtu rakstveida līgumu) vai citā vietā saskaņā ar Organizācijas vajadzībām un norādījumiem.

Personas datu nodošana un saņemšana:

34. Aizliegts kopēt Personas datus saturošus failus uz ārējiem datu nesējiem, izņemot ja šādām darbībā ir saņemta tiešā vadītāja atļauja vai citas Organizācijas nozīmētas personas atļauja.

35. Personas datu pārsūtīšanu, pēc iespējas, veic šifrētā veidā. Pārsūtamās informācijas kopumu nodrošina ar aizsardzību, *piemēram, informācijas pieejai izmantojot unikālu paroli, kura pieejama tikai atsevišķām Pilnvarotām personām un/vai informācijas adresātam*.

36. Personas datus, kas fiksēti papīra formātā, Organizācija glabā slēgtā dokumentu glabātuvē, kurai nodrošināta pieeja tikai atsevišķām Pilnvarotām personām.

37. Aizliegts dokumentus vai to projektus, kuros ir fiksēti Personas dati, atstāt vietās, kur tie ir pieejami nesankcionēti un nekontrolēti Organizācijas darbiniekiem, kas nav Pilnvarotas personas, kā arī Trešajām personām, *piemēram, atstājot dokumentus nekontrolēti uz savas darba vietas galda, darba vietu pametot ("tīrā galda politika")*.

Personas datu glabāšana:

38. Elektroniski saglabātā informācija tiek glabāta atbilstoši Organizācijas noteiktajai kārtībai, ievērojot datu minimizēšanas principu, ka dati tiek glabāti tikai tikmēr kamēr ir pamatota nepieciešamība to glabāšanai.

39. Personas datus, kas iekļauti elektroniskos un papīra formāta dokumentos, glabā kopā ar attiecīgu dokumentu atbilstoši lietu nomenklatūrā noteiktajam glabāšanas laikam, kurus regulāri Organizācija pārskata, lai nodrošinātu atbilstošā un pamatotā glabāšanas termiņa noteikšanu.

40. Personas datu glabāšanas termiņi ir noteikti Organizācijas lietu nomenklatūrā un personas datu apstrādes reģistrā. Lietu nomenklatūrā un personas datu apstrādes reģistrā noteiktie dokumentu un Personas datu glabāšanas termiņi tiek pārskatīti, ne retāk kā vienu reizi gadā.

41. Izvērtējot Personas datu glabāšanas termiņus Organizācija ņem vērā šādus aspektus:

41.1. Personas dati tiek uzglabāti vismaz kamēr tie ir nepieciešami to apstrādes nolūka sasniegšanai;

41.2. Personas dati tiek uzglabāti vismaz tiesību aktos noteiktos glabāšanas termiņus;

41.3. Personas dati tiek uzglabāti vismaz tikmēr, kamēr pret Organizāciju kāds var celt juridiskas pretenzijas un/vai uzsākt tiesvedības procesus, lai nodrošinātu pierādījumu saglabāšanu;
42. Personas datus nedrīkst dzēst no dokumentiem, ja tādējādi tiek ietekmēts attiecīgā dokumenta juridiskais spēks.
43. Pēc glabāšanas termiņa beigām personas dati un/vai papīra un elektroniskie dokumenti tiek iznīcināti vai atsevišķos gadījumos nodoti valsts arhīvam. Elektronisku informāciju iznīcina tā, lai nebūtu iespējams atjaunot informācijas failus. Rakstisku (papīra) informāciju iznīcina, lai nebūtu atjaunojama tajos esošā informācija.

Personas datu dzēšana:

44. Aizliegts nodot (atsavināt) Trešajām personām IT iekārtas, ja tās satur Personas datus. Ja IS iekārtai nepieciešams garantijas remonts, pirms tās nodošanas remontā ir jānodrošina tajā esošo Konfidenciālo datu, tai skaitā, Personas datu, drošība.
45. Personas datus, kas ir kļuvuši nepilnīgi, novecojuši, nepatiesi, pretlikumīgi apstrādāti vai arī tie vairs nav nepieciešami Organizācijā noteiktajam Personas datu apstrādes mērķim, nekavējoties labo, precizē vai dzēš un par to, pēc iespējas, informē personas, kurām Organizācija iepriekš nosūtījusi apstrādātos Personas datus.
46. Izbeidzot Personas datu apstrādi un iestājoties glabāšanas termiņa beigām, Organizācija vai Pilnvarotā persona neatgriezeniski dzēš Personas datus no IS.
47. Personas datu saturoši papīra dokumenti vai to projekti pēc datu apstrādes un glabāšanas termiņa beigām tiek iznīcināti individuāli vai nodoti Organizācijai, kura dokumentu iznīcināšanu veic centralizēti.
48. Personas datu saturoši tehniskie resursi (USB, CD, HDD un citi) pēc to izmantošanas nepieciešamības beigām, tiek nodoti Organizācijas IT daļa, kura centralizēti iznīcina tehniskos resursus tā, lai nebūtu iespējama tajos uzglabātās un dzēstās informācijas atjaunošana.
49. Par datu dzēšanas īstenošanu atbild katrs Procesa īpašnieks.

Personas datu izpaušana:

50. Personas datu izpaušanu Trešajām personām Organizācija veic tikai atbilstoša tiesiskā pamata esamības gadījumā.
51. Normatīvajos aktos noteiktajos gadījumos Organizācija izpauž Personas datus publiskas personas darbiniekam, kas pirms datu saņemšanas ir identificētas. Personas datus izpauž, pamatojoties uz rakstveida iesniegumu vai vienošanos, kurā norādīts Personas datu izmantošanas mērķis, ja normatīvajos aktos nav noteikts citādi.
52. Personas datu nodošanu Trešajām personām veic normatīvajos aktos noteiktajos gadījumos, par to pārliecinoties katrā gadījumā atsevišķi. Ja citos iekšējos tiesību aktos nav noteikts savādāk, ar masu informācijas līdzekļiem vai citām trešajām personām, komunikācija notiek tikai ar Organizācijas valdes saskaņojumu.
53. Aizliegts bez attiecīga pilnvarojuma pavairot dokumentus, kuri satur Personas datus. Pavairošanas faktu fiksē IS vai persona, kuras pārraudzībā ir nodota attiecīgo datu pārraudzība.
54. Ja Personas dati tiek izpausti saņēmējam, kurš atrodas ārpus Eiropas Savienības vai Eiropas Ekonomikas zonas, Organizācija nodrošina papildus izvērtējumu, identificējot papildu *Regulā* noteiktā pamatojuma esamību *(piemēram, Personas datu saņēmēja valsts nodrošina adekvātu personas datu aizsardzības līmeni, saņēmējs sniedz adekvātas garantijas Personas datu aizsardzībai,* , tai skaitā, *'Binding Corporate Rules' esamība, ar Eiropas Komisijas apstiprinātu standarta klauzulām noslēgts sadarbības līgums, saņēmējs pievienojies rīcības kodeksam vai sertifikācijas mehānismiem, saņemta datu subjekta piekrišana, nodošana izriet no ar datu subjektu noslēgta līguma, nepieciešama tiesvedībā un citi).*

IV IS AIZSARDZĪBAS VISPĀRĪGIE NOSACĪJUMI

55. Pārzinis īsteno Personas datu obligāto tehnisko aizsardzību ar fiziskiem un loģiskiem aizsardzības līdzekļiem, nodrošinot aizsardzību pret fiziskās iedarbības radītu Personas datu apdraudējumu un aizsardzību, kuru realizē ar IT līdzekļiem. Izvēloties veidu, kā tiks uzglabāti Personas dati, ņem vērā iespēju, ka bojājumus var nodarīt uguns, plūdi, eksplozijas, tehniskie (neatbilstoša elektroenerģijas padeve u.c.) un cilvēkfaktori (tīši vai netīši bojājumi, zādzība u.c.). Ņem vērā jebkurus iespējamos draudus drošībai no līdzās esošajām telpām/ēkām/būvēm.

56. Organizācija:

56.1. nodrošina antivīrusu programmatūras uzstādīšanu, ugunsmūra konfigurēšanu, darbinieku instruēšanu, un citas nepieciešamās darbības Personas datu drošības nodrošināšanā;

56.2. nodrošina IS darbspēju, tās darbības atjaunošanu (nomaiņu), ja noticis IT bojājums vai arī IS darbība ir tikusi traucēta citu iemeslu dēļ;

56.3. nodrošina auditācijas pierakstu esamību IS, kuras tiek izmantoti Personas datu apstrādē;

56.4. nodrošina IS drošību pret drošības apdraudējumiem;

56.5. organizē IS fiziskās aizsardzības pasākumus, tai skaitā, pieeju telpām un informācijas uzglabāšanas vietām kontrolē, lai nodrošinātu, ka tām piekļūst tikai Pilnvarotas personas;

56.6. nodrošina Personas datu atjaunošanas iespēju (*piemēram, sagatavojot un uzturot IS esošās informācijas rezerves kopijas*), ja ir notikusi neautorizēta Personas datu izdzēšana vai labošana.

57. Tehniskie resursi, kas satur Personas datus (stacionārie un portatīvie datori, ārējie cietie diski), laikā, kad tie netiek lietoti, tiek glabāti slēdzamās telpās un/vai skapjos.

58. Organizācija, ja tas nepieciešams, pieļauj Pilnvarotai personai izmantot portatīvo datoru un IS attālināti. Šādā gadījumā, tehnisko nodrošinājumu veic IT daļa.

59. Bez Organizācijas vadības attiecīgi pilnvarotu personu atļaujas aizliegts pieslēgt IT jebkādas ārējās atmiņas ierīces.

60. Lietot IT, kurās ir izvietoti Personas dati, atļauts tikai Pilnvarotām personām.

61. Beidzot darbu, Pilnvarotā persona izslēdz datoru *(piemēram, izslēgšanas procedūra: Start =>Shut Down =>Ok),* bet, ja Pilnvarotā persona atstāj datoru uz īsu laiku, lieto ekrāna saudzētāju ar paroli vai bloķē pieeju datora informācijai, noslēdzot datora klaviatūru ar attiecīgas *(piemēram, Ctrl-Alt-Del vai WIN+L)* funkcijas palīdzību.

62. Datoriem, kas tiek izmantoti Personas datu apstrādē ir parole vismaz operētājsistēmas līmenī. Portatīvā datora cietajam diskam ir jābūt pilnīgi šifrētam vai tiek nodrošināti citi mehānismi, kā garantēt tajā esošo Personas datu drošību.

63. Datoros ir aizliegts izmantot nelicencētu programmatūru, kā arī instalēt jebkādu programmatūru bez Organizācijas atļaujas. Programmatūrai jābūt nodrošinātai ar visiem pieejamajiem atjauninājumiem.

64. Aizliegts pieslēgties IS, kurā tiek veikta Personas datu apstrāde, izmantojot neaizsargātu bezvadu datortīklu (Unencrypted Wireless Networks).

65. Drošības pasākumi pret ārkārtas apstākļiem tiek īstenoti saskaņā ar ugunsdrošības noteikumiem Organizācijā, kā arī normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību. Iespēju robežās, Personas datus saturoši dokumenti ir glabājami pret uguns risku aizsargātos skapjos.

66. Telpas, kurās atrodas Personas datus saturoši tehniskie resursi un dokumentācija, ir nodrošinātas ar funkcionējošu apsardzes signalizāciju, dūmu detektoriem un ugunsdzēšamo aparātu.

67. Visi šajā sadaļā uzskaitītie nosacījumi attiecas arī uz citiem IT datu nesējiem, tai skaitā, mobilajiem telefoniem, planšetēm, ja tie tiek izmantoti tiešo darba pienākumu veikšanai un satur Personas datus.

V PAROĻU VEIDOŠANAS UN GLABĀŠANAS NOSACĪJUMI

68. IT aizsardzība un Pilnvaroto personu identifikācija tiek nodrošināta ar datora paroli, kura atbilst sekojošām prasībām:

68.1. minimālais paroles garums ir 9 simboli, no kuriem viens simbols ir vismaz cipars, lielais un mazais burts;

68.2. maksimālais paroles maiņas periods nav ilgāks par 90 dienām;

68.3. paroles uzbūve ir komplicēta, to veido izmantojot burtu, ciparu un īpašo rakstzīmju kombināciju, *piemēram, !@#$%^*()+;*

69.4. veidojot paroli, tā nav vienāda ar piecām iepriekšējām parolēm;

69.5. piecu secīgi nepareizi ievadītu paroļu gadījumā, konts tiek nekavējoties bloķēts.

70. Paroli aizliegts veidot, izmantojot ar Pilnvarotu personu tieši saistītu informāciju (*piemēram, vārdus, uzvārdus, dzimšanas dienas, tālruņa numurus, mājdzīvnieku un tuvinieku vārdus u.tml.).* Parole nedrīkst saturēt garumzīmes un mīkstinājuma zīmes.

71. Pilnvarotai personai aizliegts izpaust savu paroli trešajām personām. Parole ir jāiegaumē. Rakstiskā veidā paroles atļauts glabāt tikai citiem darbiniekiem nezināmā un nepieejamā vietā.

72. Ja Pilnvarotai personai ir aizdomas, ka paroli zina Trešā persona, tai ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt IT nodaļai to izdarīt savā vietā.

73. Ja gadījumā parole ir kļuvusi zināma Trešajām personām, Pilnvarotā persona vai cita persona, kurai par to ir kļuvis zināms, nekavējoties ziņo "Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība" noteiktajā kārtībā.

74. Nodrošinot piekļuves tiesības Organizācija izsniedz Pilnvarotajai personai sākotnējo paroli, kura jānomaina pie pirmās autentifikācijas un sistēmas lietošanas.

VI E-pasta lietošana

75. Viena e-pasta sūtījuma apjoms nevar pārsniegt 25 MB. Aizliegts atkārtoti sūtīt e-pasta vēstuli, ja ir saņemts paziņojums, ka adresāts nevar saņemt sūtījumu e-pasta servera limita pārsniegšanas dēļ.

76. Esiet piesardzīgs vienmēr, kad no kādas vietnes saņemat e-pasta ziņojumu, kurā ir lūgts norādīt personas informāciju.

77. Neklikšķināt uz saitēm un nenorādiet personas informāciju, kamēr neesat pārliecinājies, ka e-pasta ziņojums ir īsts. Ja sūtītājam ir Organizācijas adrese, ziņojiet Organizācijas juristam. Organizācija nekad nelūgs norādīt personas informāciju, *piemēram, paroli*, e-pasta ziņojumā.

78. Pārbaudiet, vai e-pasta adrese atbilst sūtītāja vārdam. Pirms noklikšķināt uz kādas saites, virziet virs tās kursoru. Ja saites URL neatbilst saites aprakstam, iespējams, tiksiet novirzīts uz pikšķerēšanas vietni. Pārbaudiet ziņojumu galvenes — pārliecinieties, ka galvenē "No" vai "From" netiek rādīts nepareizs vārds, e-pasts, *piemēram, liga.serna@madonasslimnica.lv*. Aizliegts atvērt neskaidras izcelsmes e-pasta sūtījumus (*piemēram, īpatnēji temati laukā "Subject", pievienota nezināma formāta datne vai izpildāmā datne, interneta saites vēstules saturā), it īpaši, ja par bīstamo datņu veidiem saņemts brīdinājums*). Par šādiem e-pasta sūtījumiem nekavējoties jāziņo uzņēmuma IT nodaļai.

79. Aizliegts e-pasta ziņojumam pievienot izpildāmās datnes (*piemēram, *.exe, *.com, *.shs, *.vbs, *.bat).*

80. E-pasta lietotājs, regulāri nodzēšot nevajadzīgo informāciju, kontrolē, lai e-pasta sistēmā atrastos tikai aktuāla un vajadzīga informācija. Nav pieļaujama privāta rakstura un prettiesiska (*piemēram, nelikumīga licenču glabāšana).*

VII DATU SUBJEKTU PIEPRASĪJUMU APSTRĀDE

Vispārīgie Datu subjekta pieprasījumu apstrādes noteikumi:

81. Respektējot normatīvajos aktos noteiktās Datu subjektu tiesības, Organizācija pieņem rakstiskus iesniegumus no identificējamiem Datu subjektiem par Personas datu saturošas informācijas sniegšanu. Organizācija, pēc iespējas, nodrošina Datu subjektam pieejamu standartizētu Datu subjektu tiesību realizācijas pieprasījumu formu (2.pielikums), tomēr nodrošinot iespēju saņemt no Datu subjektiem pieprasījumus arī citās to izvēlētās formās.

82. Visa komunikācija ar Datu subjektu un informācijas izsniegšana Datu subjektam ir jāveic bez maksas, izņemot gadījumus, ja pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi. Šādā gadījumā Organizācija var atteikties izpildīt pieprasījumu vai pieprasīt administratīvajās izmaksās pamatotu saprātīgu maksu, kas saistīta ar informācijas sniegšanas nodrošināšanu.

83. Par pieprasījuma izpildi atbildīgais darbinieks pārbauda tās personas identitāti, par kuru Datu subjekta pieprasījums ir iesniegts. Ja personu nav iespējams identificēt, Datu subjekta pieprasījuma iesniedzējam tiek lūgts sniegt papildus informāciju, lai Datu subjektu identificētu.

Organizācijas rīcība Datu subjekta pieprasījumu piekļūt saviem datiem (jeb iegūt par sevi informāciju) gadījumos

84. Ja netiek konstatēts, ka Organizācijas rīcībā būtu attiecīgā Datu subjekta personas dati, par pieprasījuma izpildi atbildīgais darbinieks sagatavo atbildi Datu subjektam, norādot, ka Organizācija nav konstatējusi Datu subjekta datu apstrādi.

85. Par pieprasījuma izpildi atbildīgais darbinieks atlasa Organizācijas rīcībā esošos personas datus, tai skaitā pārbaudot Organizācijas datu bāzēs esošo informāciju, uz serveriem glabāto informāciju, papīra formātā esošo informāciju (*piemēram, klienta vai darbinieka lietu*) un citas informācijas glabāšanas vietas.

86. Sagatavojot Datu subjekta pieprasīto datu kopiju, Organizācija pārliecinās, ka apkopotā informācija nesatur trešo personu (citu Datu subjektu) datus. Šajā gadījumā šie dati būtu dzēšami un nebūtu izsniedzami Datus subjektam šo tiesību ietvaros.

Organizācijas rīcība Datu subjekta pieprasījumu labot savus datus gadījumā

87. Saņemot Datu subjekta pieprasījumu labot savus datus, par pieprasījuma izpildi atbildīgais darbinieks pārbauda vai pieprasījumā norādītie dati ir atšķirīgi no Organizācijas apstrādē esošiem datiem.

89. Pirms tiek izpildīts Datu subjekta pieprasījums, par pieprasījuma izpildi atbildīgais darbinieks pārbauda vai iesniegtie dati ir precizējami, tas ir, vai precizējamā informācija patiešām ir kļūdaina vai tikai, tas ir, subjekta viedoklis tas ir ka tie ir kļūdaini. Ja Organizācija nepiekrīt datu labošanas pieprasījuma pamatotībai, tā sniedz Datu subjektam atbildi, kurā norāda savus apsvērumus tam, ka dati netiks laboti.

90. Ja tiek konstatēts, ka pamatoti personas dati ir labojumi, Organizācija veic labojumus pēc iespējas īsākā laikā.

91. Ja Organizācija labo Datu subjekta personas datus, tā pārbauda vai labotos personas datus tā nav nodevusi kādai Trešajai personai un, ja tas neprasa pārmērīgas pūles, par labojumiem informē arī attiecīgus datu saņēmējus.

Organizācijas rīcība Datu subjekta pieprasījumu dzēst savus datus gadījumā

92. Ja netiek konstatēts, ka Organizācijas rīcībā būtu attiecīgā Datu subjekta personas dati, par pieprasījuma izpildi atbildīgais darbinieks sagatavo atbildi Datu subjektam, norādot, ka Organizācija nav konstatējusi Datu subjekta datu apstrādi.

93. Ja attiecīgi personas dati Organizācijā tiek apstrādāti, par pieprasījuma izpildi atbildīgais darbinieks dzēš datus tad, ja konstatē kādu no sekojošiem gadījumiem:

93.1. Pieprasījumā norādītie personas dati Organizācijai vairs nav nepieciešami nolūkiem, kādiem tie bija vākti un apstrādāti, bet izņemot gadījumus, ja šādu datu apstrādi ilgāk pieprasa veikt tiesību akti, nepieciešami arhīva vajadzībām vai Organizācijas leģitīmo interešu aizsardzībai (*piemēram, tiesvedības riskiem*);
93.2. Ja Datu subjekta attiecīgo datu apstrāde tiek veikta uz Datu subjekta piekrišanas pamata un tā tiek atsaukta;
93.3. Ja Datu subjekta attiecīgo datu apstrāde tiek veikta pamatojoties uz Organizācijas leģitīmām interesēm un Datu subjekts pamatoti iebilst šādai datu apstrādei, norādot uz būtiskiem iemesliem pārtraukt šādu apstrādi;
93.4. Ja Datu subjekta attiecīgo datu apstrāde tiek veikta tiešās tirgvedības vajadzībām, ietverot profilēšanu, ciktāl tā ir saistīta ar tiešās tirgvedības vajadzībām;
93.5. ja Datu subjekta attiecīgo datu apstrāde tiek veikta nelikumīgi;
93.6. ja dati ir jādzēš saskaņā ar spēkā esošiem un Organizācijai piemērojamiem tiesību aktiem;
93.7. Ja dati ir savākti, lai bērnam piedāvātu informācijas sabiedrības pakalpojumus.
94. Tomēr jebkurā gadījumā par pieprasījuma izpildi atbildīgais darbinieks, izvērtē vai datus nav nepieciešams saglabāt, jo šādu datu apstrādi pieprasa veikt tiesību akti, tie nepieciešami arhīva vajadzībām vai Organizācijas leģitīmo interešu aizsardzībai (*piemēram, tiesvedības riskiem*);
95. Par pieprasījuma izpildi Organizācija informē Datu subjektu.
96. Ja Organizācija dzēš Datu subjekta personas datus, tā pārbauda vai dzēstos personas datus tā nav nodevusi kādai Trešajai personai un, ja tas neprasa pārmērīgas pūles, par dzēšanas faktu informē arī attiecīgus datu saņēmējus.

Organizācijas rīcība Datu subjekta pieprasījumu ierobežot savus datus gadījumā

97. Ja netiek konstatēts, ka Organizācijas rīcībā būtu attiecīgā Datu subjekta personas dati, par pieprasījuma izpildi atbildīgais darbinieks sagatavo atbildi Datu subjektam, norādot, ka Organizācija nav konstatējusi Datu subjekta datu apstrādi.
98. Ja attiecīgi personas dati Organizācijā tiek apstrādāti, par pieprasījuma izpildi atbildīgais darbinieks ierobežo datu apstrādi sekojošos gadījumos:
98.1. Uz laiku, kamēr Organizācija pārbauda pieprasījuma pamatotību, ja tiek apstrīdēta datu precizitāte;
98.2. Uz Datu subjekta norādīto laiku, ja Datu subjekts ir iebildis datu dzēšana un tiek konstatēta nelikumīga datu apstrāde;
98.3. Uz Datu subjekta norādīto laiku, ja Organizācijai ir beigusies nepieciešamība glabāt datus, savukārt Datu subjektam tie ir nepieciešami, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
98.4. Uz laiku, kamēr tiek pārbaudīti Datu subjekta būtiskie iemesli datu apstrādes, kas pamatojas uz Organizācijas leģitīmām interesēm, pārtraukšanai.
99. Ja datu apstrāde ir ierobežota, attiecīgie personas dati netiek izmantoti citiem mērķiem, kā tikai glabāšanai, Organizācijas vai Trešās personas likumīgu prasību īstenošanai un aizstāvēšanai, dalībvalstu noteiktu svarīgu interešu dēļ vai atsevišķos gadījumos, ja Datu subjekts ir izteicis piekrišanu savu ierobežoto personas datu apstrādei.
100. Ja ierobežojums tiek atcelts, Organizācija informē Datu subjektu pirms ierobežojumu atcelšanas.
101. Ja Organizācija ir ierobežojusi Datu subjekta personas datus, tā pārbauda vai dzēstos personas datus tā nav nodevusi kādai Trešajai personai un, ja tas neprasa pārmērīgas pūles, par datu ierobežošanas faktu informē arī attiecīgus datu saņēmējus.

Organizācijas rīcība Datu subjekta pieprasījumu nodrošināt savu datu pārnesamību gadījumā

102. Ja netiek konstatēts, ka Organizācijas rīcībā būtu attiecīgā Datu subjekta personas dati, par pieprasījuma izpildi atbildīgais darbinieks sagatavo atbildi Datu subjektam, norādot, ka Organizācija nav konstatējusi Datu subjekta datu apstrādi.

103. Ja attiecīgi Personas dati Organizācijā tiek apstrādāti, par pieprasījuma izpildi atbildīgais darbinieks pārbauda vai attiecīgie dati ir pakļauti pārnesamībai, tas ir, pārbauda vai attiecīgie dati:

103.1. tiek apstrādāti uz Datu subjekta piekrišanas pamata vai pamatojoties uz līgumsaistību izpildi;

103.2. tiek apstrādāti elektroniskā vidē.

104. Ja Organizācijas rīcībā ir konstatēti dati, kuriem piemērojama pārnesamība, par pieprasījuma izpildi atbildīgais darbinieks sagatavo attiecīgos datus elektroniskā (*.xml, *.doc, *.csv) formātā un izsniedz datu subjektam vai viņa norādītai Trešajai personai.

105. Ja Datu subjekts norādījis, ka Personas dati pārsūtāmi tiešā veidā Trešajai personai, Organizācija izvērtē nosūtāmo datu apjomu un saturu un lemj par atbilstošiem drošības pasākumiem pieprasītās informācijas nosūtīšanā, informāciju kriptējot, aizsargājot ar paroli vai izmantojot citus risinājumus drošas informācijas nosūtīšanai.

106. Organizācija nodrošina, ka realizējot Datu subjekta tiesības, netiek aizskarts citas personas privātums, tai skaitā, netiek izsniegti citu Datu subjektu dati, kuru izsniegšanai nav pamatojuma.

Organizācijas rīcība Datu subjekta pieprasījuma nebūt automatizētu lēmumu subjektam izteikšanas gadījumā

107. Ja netiek konstatēts, ka Organizācijas rīcībā būtu attiecīgā Datu subjekta personas dati, par pieprasījuma izpildi atbildīgais darbinieks sagatavo atbildi Datu subjektam, norādot, ka Organizācija nav konstatējusi Datu subjekta datu apstrādi.

108. Ja attiecībā uz Datu subjektu tiek pieņemti pilnībā automatizēti lēmumi, kas attiecībā uz datu subjektu rada tiesiskās sekas vai līdzīgā veidā ietekmē Datu subjektu, Organizācija turpmāk pārtrauc automatizētu lēmumu pieņemšanu attiecībā uz Datu subjektu, izņemot sekojošus gadījumus:

108.1. Ja lēmums ir vajadzīgs, lai noslēgtu vai izpildītu līgumu starp datu subjektu un pārzini;

108.2. Ja lēmuma pieņemšanu, nosaka tiesību akti;

108.3. Ja lēmums pamatojas uz Datu subjekta piekrišanu.

109. Atteikuma gadījumā pārtraukt automatizētu lēmumu pieņemšanu, Organizācija nodrošina lēmuma manuālu (ar cilvēka līdzdalību) pārskatīšanu, izņemot ja lēmuma pieņemšana ir noteikta tiesību aktos.

IIX IS DARBĪBU NEPĀRTRAUKTĪBA

110. Personas datu apstrādei izmantotām IS datu bāzēm tiek nodrošinātas rezerves kopijas. Rezerves datu kopēšanu nodrošina IT daļa.

111. Rezerves datu kopijas tiek uzglabātas tā, lai to drošību neietekmē vieni un tie paši draudi. Rezerves datu kopijām ir jābūt pieejamām jebkurā laikā.

112. Rezerves kopēšana tiek organizēta tā, lai būtu iespējams atjaunot datus. Organizējot rezerves datu kopēšanu, tiek ņemtas vērā normatīvajos aktos noteiktās prasības.

113. Rezerves kopiju integritāte tiek pārbaudīta vismaz vienu reizi gadā.

114. Uz Organizācijas serveriem ir uzstādīts nepārtrauktās barošanas avots (UPS), kas nodrošina nepārtrauktu elektrības padevi un iespēju izmantot sistēmu vēl pēc elektroenerģijas padeves atslēgšanas.

IX DARBINIEKU APMĀCĪBA

115. Organizācija nodrošina savu darbinieku apmācību un informēšanu par datu aizsardzības pasākumiem vismaz šādos gadījumos:

115.1. veicot sākotnējo apmācību (uzsākot darba attiecības);

115.2. veicot regulāro apmācību;

115.3. neplānoto apmācību.

116. Sākotnējajā apmācībā, Organizācijas Personāla speciālists, veic šādas darbības:

116.1. iepazīstina ar šiem Noteikumiem un citiem Organizācijā saistošajiem normatīvajiem aktiem personas datu aizsardzības jomā. Ir iespēja noskatīties prezentācijas materiālu par Personas datu aizsardzību Organizācijā;

116.2. nodrošina, ka tiek parakstīts apliecinājums.

117. Regulārā apmācība notiek periodiski, bet ne retāk kā reizi gadā, kad datu aizsardzības speciālists apmāca darbiniekus – lekcijas veidā vai tiem tiek nosūtītas uzlabotas procedūras un testa jautājumi.

118. Pēc regulārās apmācības, darbiniekam ir jāizpilda tests par datu aizsardzības jautājumiem.

119. Neplānoto personas datu aizsardzības instruktāžu (prezentāciju) Organizācija organizē, ja:

119.1. darbiniekam mainās darba apstākļi vai rodas citi faktori, kas var būtiski ietekmēt personas datu apstādi;

119.2. darbinieks pārtraucis darbu uz laiku, kas ilgāks par vienu gadu.

X Nobeiguma noteikumi

120. Atzīt par spēku zaudējušiem Slimnīcas 14.12.2018. Madonas novada pašvaldības SIA "Madonas slimnīca" iekšējie personas datu aizsardzības noteikumi attiecībā uz klientu personas datu apstrādi.

121. Atzīt par spēku zaudējušiem Organizācijas 14.12.2018. Madonas novada pašvaldības SIA "Madonas slimnīca" iekšējie personas datu aizsardzības noteikumi attiecībā uz nodarbināto personas datu apstrādi.

122. Noteikumi stājas spēkā 20.12.2023.

123. Organizācijas vadība nodrošina periodisku Noteikumu un tā pielikumu pārskatīšanu atbilstoši nepieciešamībai, bet ne retāk kā reizi gadā.

APLIECINĀJUMS

Vārds, Uzvārds	
Amats	

apņemos atbilstoši normatīvo aktu un Madonas novada pašvaldības SIA "Madonas slimnīca" , vienotais reģistrācijas Nr.40003356507, turpmāk - Darba devējs, iekšējo normatīvo aktu regulējumam:

1. saglabāt un prettiesiski neizpaust amata (darba) pienākumu veikšanas laikā iegūto konfidenciālo informāciju, tai skaitā, personas datus, trešajām personām, bez darba devēja piekrišanas;
2. amata (darba) pienākumu veikšanas laikā iegūto konfidenciālo informāciju, tai skaitā, personas datus, prettiesiski neizpaust trešajām personām arī pēc darba tiesisko attiecību izbeigšanas;
3. nekavējoties informēt Darba devēju par nesankcionētu piekļuvi manā rīcībā esošajai konfidenciālajai informācijai, tai skaitā, personu datiem, kas iegūti veicot amata (darba) pienākumus pie Darba devēja;
4. pārtraucot darba (līguma) attiecības ar Darba devēju jebkādu iemeslu dēļ, nekavējoties nodot Darba devējam manā rīcībā esošo Darba devēja aprīkojumu, kas izmantots personas datu apstrādei, kā arī manā rīcībā esošo Konfidenciālo informāciju, tai skaitā, personas datus, to saturošus dokumentu oriģinālus un kopijas, kas ir saņemti darba (līguma izpildes) laikā, un kura manā rīcībā vai kura ir citādi tieši vai netieši ir manā valdījumā.

Ar šo apliecinu, ka esmu brīdināts/brīdināta, ka konfidenciālas informācijas, tai skaitā, personas datu, izpaušanas gadījumā datu subjektiem var tikt nodarīts būtisks kaitējums un darba devējam ar šādu rīcību var tikt nodarīti zaudējumi, kā arī esmu informēts, ka par šā apliecinājuma pārkāpumu varu tikt saukts/saukta pie normatīvajos aktos noteiktās atbildības (tai skaitā, administratīvās un krimināatbildības).

Ar šo apliecinu, ka esmu iepazinies/iepazinusies un man ir izskaidroti šādi Darba devēja iekšējie normatīvie akti: 01.11.2023. "Personas datu apstrādes noteikumi" un 01.11.2023. "Personas datu aizsardzības pārkāpumu atklāšanas, novēršanas un paziņošanas kārtība".

Datums: _____._____._____.

_____
/paraksts/

2.pielikums
Personas datu apstrādes noteikumi

Datu subjekta pieprasījuma veidlapa

I. INFORMĀCIJA PAR PĀRZINI	
Pārziņa nosaukums, reģistrācijas numurs:	Madonas novada pašvaldības SIA "Madonas slimnīca" 40003356507
II. INFORMĀCIJA PAR DATU SUBJEKTU	
Vārds uzvārds:	
Personas kods *(vai dzimšanas datums, ja nav personas koda)*:	
Kontaktadrese *(nav nepieciešams norādīt, ja datu subjekts pieprasījumu parakstījis ar drošu e-parakstu vai internetbanku autorizāciju):*	
Tālruņa numurs saziņai:	
E-pasta adrese saziņai:	
Papildus informācija Jūsu identifikācijai *(nav nepieciešama, ja notikusi datu subjekta klātienes identifikācija, datu subjekts pieprasījumu parakstījis ar drošu e-parakstu vai internetbanku autorizāciju):*	*[šeit norādiet datu subjekta personas apliecības vai pases numuru izdošanas datumu, izdevēja iestādi]*
III. INFORMĀCIJA PAR PĀRSTĀVI (JA PIEPRASĪJUMU IESNIEDZ CITA PERSONA DATU SUBJEKTA INTERESĒS)	
Vārds uzvārds:	
Personas kods *(vai dzimšanas datums, ja nav personas koda):*	
Kontaktadrese *(nav nepieciešams norādīt, ja datu subjekts pieprasījumu parakstījis ar drošu e-parakstu vai internetbanku autorizāciju):*	
Tālruņa numurs saziņai:	
E-pasta adrese saziņai:	
Uz kāda tiesiska pamata Jūs pārstāvat datu subjektu *(piemēram vecāks, pilnvarnieks, aizgādnis un citi)*:	
Lūdzu aprakstiet dokumentu, kas apstiprina Jūsu tiesības pārstāvēt datu subjektu un pievienojiet kopiju vai oriģinālu šim	

pieprasījumam:	
IV. VĒLAMAIS ATBILDES SAŅEMŠANAS VEIDS	
☐ **Klātienē:**	Pārziņa birojā: Rūpniecības iela 38, Madona, Madonas novads, LV 4801
☐ **Uz sekojošu e-pastu:**	
☐ **Uz sekojošu adresi:**	
☐ **izmantojot pašapkalpošanās portālu:**	
Esmu informēts, ka Pārzinis izvērtēs iepriekš norādītos saziņas kanālus un atbilstoši izsniedzamās informācijas sensitivitātei un apjomam var noteikt atšķirīgus saziņas kanālus, par ko Jūs tiksiet atsevišķi informēts.	
V. DATU SUBJEKTA PIEPRASĪJUMA BŪTĪBA	
☐ **VĒLOS PIEKĻŪT SAVIEM PERSONAS DATIEM JEB IEGŪT PAR SEVI INFORMĀCIJU**	
Lūdzu norādiet kādiem personas datiem vēlaties piekļūt?	
Lūdzu norādiet kādā statusā Jūsu personas dati varētu tikt pie mums apstrādāti *(piemēram, darbinieks, pacients, pretendents, klients, apmeklētājs un citi):*	
Ja vēlaties piekļūt foto vai video ierakstos esošiem personas datiem lūdzu norādiet papildus identificējošu informāciju par sevi *(piemēram, pievienojiet fotogrāfiju, aprakstiet savu izskatu vai apģērbu attiecīgā vietā un citi):*	
Ja vēlaties piekļūt video ierakstos esošiem personas datiem lūdzu norādiet datumu un laiku, kad Jūs varējāt būt iekļuvis video novērošanas ierakstos:	
☐ **VĒLOS SAŅEMT INFORMĀCIJU PAR SAVU PERSONAS DATU APSTRĀDI**	
Lūdzu norādiet par kādiem personas datiem vēlaties saņemt informāciju?	
Lūdzu atzīmējiet Jūs interesējošo informāciju:	☐ Apstrādes nolūki; ☐ Apstrādāto personas datu kategorijas; ☐ Personas datu saņēmēji vai saņēmēju kategorijas, kam personas dati ir izpausti vai kam tos plānots izpaust; ☐ Personas datu glabāšanas laika posms vai kritēriji laika posma noteikšanai;

	☐ Informāciju par datu subjekta tiesību izmantošanas iespējām, tai skaitā, par tiesībām uz datu labošanu, dzēšanu, datu apstrādes ierobežošanu un tiesībām iebilst; ☐ Informācija par tiesībām iesniegt sūdzību uzraudzības iestādei; ☐ Informācija par to, no kāda avota personas dati ir iegūti; ☐ Informācija par automatizētu lēmumu pieņemšanu (ja tāda ir), tajā ietverto loģiku un paredzamajām sekām.
☐ **VĒLOS LABOT SAVUS PERSONAS DATUS**	
Lūdzu norādiet kādus personas datus vēlaties labot:	
Lūdzu norādiet iemeslu personas datu labošanai:	
Lūdzu norādiet personas datus kādi tie būtu pēc labojumiem:	
☐ **VĒLOS DZĒST SAVUS PERSONAS DATUS**	
Lūdzu norādiet kādus personas datus vēlaties dzēst:	
Lūdzu norādiet iemeslu personas datu dzēšanai:	
☐ **VĒLOS IEROBEŽOT SAVU PERSONAS DATU APSTRĀDI**	
Lūdzu norādiet kādu personas datu apstrādi vēlaties ierobežot:	
Lūdzu norādiet iemeslu personas datu apstrādes ierobežošanai:	☐ apstrāde ir nelikumīga, bet es nevēlos, lai dati tiktu dzēsti, bet ierobežoti sekojošu iemeslu dēļ: _____ _____ _____ _____ _____ Ierobežojumu noteikt līdz: ___.___.20___.
	☐ apzinoties, ka Pārzinim dati varētu nebūt vairs vajadzīgi, bet man tie varētu būt nepieciešami nākotnē sekojošu iemeslu dēļ: _____ _____ _____

	_____ _____ Ierobežojumu noteikt līdz: ___.___.20___.
Papildus informējam, ka datu apstrāde tiks ierobežota automātiski sekojošos gadījumos: ▪ *ja ir apstrīdēta arī personas datu precizitāte (uz laiku, kamēr precizitāte tiek pārbaudīta);* ▪ *ja Jūs esat iebildis pret Pārziņa leģitīmo interešu nozīmīgumu un pārākumu pār savām leģitīmām interesēm (uz laiku, kamēr Pārzinis pārbauda argumentus un pārvērtē interešu līdzsvaru).*	
☐ **VĒLOS IZMANTOT TIESĪBAS UZ PERSONAS DATU PĀRNESAMĪBU**	
Lūdzu norādiet veidu kā vēlaties saņemt pārnesamībai pakļauto informāciju *(piemēram, izvietot uz Jūsu iesniegta informācijas nesēja (CD, USB), nosūtīt uz e-pastu)*:	
Ja vēlaties, lai dati tiktu pārsūtīti tieši citam pārzinim, lūdzu norādiet informāciju par saņēmēju *(nosaukums, reģistrācijas numurs, juridiskā adrese, e-pasta adrese uz kuru nosūtāma informācija):*	
Esmu informēts, ka saskaņā ar Vispārīgo datu aizsardzības regulu tiesības uz personas datu pārnesamību attiecas tikai uz tādiem personas datiem, kas attiecas uz datu subjektu, tiek apstrādāti ar automatizētiem līdzekļiem, kā arī apstrāde pamatota uz datu subjekta piekrišanu un/vai pamatota uz ar datu subjektu noslēgta līguma izpildi.	
Esmu informēts, ka Pārzinis izvērtēs iepriekš norādītos saziņas kanālus un atbilstoši izsniedzamās informācijas sensitivitātei un apjomam var noteikt atšķirīgus saziņas kanālus, par ko Jūs tiksiet atsevišķi informēts. Sākotnēji lūdzam aplūkot Pārziņa pašapkalpošanās portālos pieejamo informāciju un iespējas to iegūt un saglabāt elektroniskā formātā.	
☐ **VĒLOS IEBILST SAVU PERSONAS DATU APSTRĀDEI**	
Lūdzu norādiet kādai personas datu apstrādei vēlaties iebilst:	
Norādiet iebildumu būtību:	☐ iebilstu pret Pārziņa leģitīmo interešu (sabiedrības interešu, valsts pārvaldes uzdevumu veikšanai nepieciešamo datu apstrādes) nozīmīgumu un pārākumu pār manām leģitīmām interesēm, jo_____ _____ _____
	☐ iebilstu sava sekojoša e-pasta: _____ izmantošanu komerciālu paziņojumu saņemšanai;
	☐ iebilstu sava sekojoša tālruņa numura: _____ izmantošanu komerciālu paziņojumu saņemšanai;

	☐ iebilstu savu datu izmantošanai profilēšanai tiešās tirgvedības vajadzībām.
☐ **VĒLOS ATTEIKTIES NO SAVU DATU IZMANTOŠANAS AUTOMATIZĒTA INDIVIDUALA LĒMUMA PIEŅEMŠANĀ VAI LŪGT PĀRSKATĪT AUTOMATIZĒTU INDIVIDUĀLA LĒMUMA PIEŅEMŠANU**	
Lūdzu norādiet kādu automatizētu personas datu apstrādē nevēlaties, lai Jūsu dati tiktu izmantoti:	
Esmu informēts, ka saskaņā ar Vispārīgo datu aizsardzības regulu atteikšanās tiesības neattiecas uz tādām datu apstrādi, kura: ▪ *rada tiesiskas sekas Jums;* ▪ *ir vajadzīga, lai izpildītu līgumu starp Jums un Pārzini (šajā gadījumā Jūs varat pieprasīt manuālu lēmuma pārskatīšanu);* ▪ *ir atļauta vai uzlikta kā pienākums ar Pārzinim piemērojamiem normatīvajiem aktiem;* ▪ *pamatota ar datu subjekta pieprasījumu (šajā gadījumā Jūs varat pieprasīt manuālu lēmuma pārskatīšanu).*	
Lūdzu norādiet, kurus automatizētus lēmumus vēlaties pārskatīt:	
Lūdzu norādiet papildus argumentus, kādēļ pēc Jūsu domām, automatizēts lēmums ir neprecīzs:	
VI. PARAKSTS	
Datums:	
Paraksts:	
VII. PĀRZIŅA ZIŅAS PAR PIEPRASĪJUMA IZPILDES GAITU (iekšējai lietošanai):	
Atbildīgā Pārziņa darbinieka vārds, uzvārds:	
Veikto darbību apraksts:	
Atbildes izsūtīšanas laiks:	
Jautājuma atrisināšanas statuss:	
Paraksts:	