VECUMNIEKU NOVADA DOME
Rīgas iela 29, Vecumnieki, Vecumnieku pagasts, Vecumnieku novads, LV-3933
Tālr. 63976100, fakss 63960524, e-pasts *vecumnieki@vecumnieki.lv*

APSTIPRINĀTS
Vecumnieku novada Domes
23.10.2019. sēdē
(prot.Nr. 15, 2.§)

IEKŠĒJIE NOTEIKUMI
Vecumnieku novada Vecumnieku pagastā

2019.gada 23.oktobrī Nr.1-9/2019/18

Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi

Izdoti pamatojoties uz Valsts pārvaldes iekārtas likuma 72.panta pirmās daļas 2.punktu, 73.panta pirmās daļas 4.punktu, likuma „Par pašvaldībām" 41.panta pirmās daļas 2.punktu

1. Vispārīgie noteikumi

1.1. Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi (turpmāk – Noteikumi) nosaka kārtību, kā Vecumnieku novada pašvaldība, tās iestādes, struktūrvienības un kapitālsabiedrības veic personas datu apstrādi, nodrošina personas datu drošību un aizsardzību, kā arī nosaka citus pamatprincipus datu aizsardzības nodrošināšanai.

1.2. Noteikumu mērķis ir nodrošināt personas datu godīgu un likumīgu apstrādi, nodrošinot, ka iegūtie personas dati tiks izmantoti noteiktā nolūka sasniegšanai.

1.3. Personas datu apstrādes nolūkus, līdzekļus un to izmantošanu nosaka Vecumnieku novada pašvaldība (turpmāk – pārzinis).

1.4. Pārzinis veic personas datu apstrādi, lai nodrošinātu pārzinim ar likumu „Par pašvaldībām" un citiem piemērojamiem normatīvajiem aktiem uzlikto uzdevumu un funkciju izpildi.

1.5. Pārzinis nosaka, ka tiek pieprasīti tikai tādi dati, kas nepieciešami noteiktā nolūka sasniegšanai, kā arī apstrādājot datus, ieskaitot: datu vākšanu, reģistrēšanu, organizēšanu, izmantošanu, ievadīšanu, glabāšanu, strukturēšanu, pielāgošanu, pārveidošanu, atgūšanu, izpaušanu, aplūkošanu, nodošanu, iznīcināšanu vai dzēšanu (turpmāk – personas datu apstrāde), nodrošina informācijas resursu un informācijas sistēmu drošību atbilstoši normatīvo aktu noteiktajai kārtībai.

1.6. Noteikumi ir saistoši visiem pašvaldības darbiniekiem un amatpersonām, kas apstrādā personas datus un kam dotas tiesības lietot datorsistēmas noteiktā kārtībā un apjomā, kā arī darbiniekiem, kam pastāv iespēja piekļūt personas datiem (turpmāk – pilnvarotā persona).

1.7. Noteikumi attiecas uz visiem personas datiem, kas attiecas uz identificētu vai identificējamu fizisko personu (turpmāk – datu subjekts).

1.8. Personas datu apstrādi pārziņa uzdevumā veic tā izveidotās pašvaldības kapitālsabiedrības, pašvaldības iestādes un struktūrvienības, kas, pamatojoties uz pārziņa noteikto personas datu apstrādes nolūku, izstrādāt savu iekšējo personas datu apstrādes kārtību.

1.9. Par pārziņa personas datu aizsardzību atbilstoši kompetencei atbild pašvaldības izpilddirektors.
1.10. Kapitālsabiedrības valdes loceklis, iestādes direktors (vadītājs) un struktūrvienības vadītājs (turpmāk – vadība) atbild par personas datu apstrādi savās pakļautībā esošajā iestādē, struktūrvienībā un kapitālsabiedrībā.
1.11. Noteikumi attiecas uz visu veidu personas datu apstrādi, neatkarīgi no tā, kādā formā un/vai vidē datu subjekts sniedz personas datus (piemēram, klātienē, mutiski vai papīra formātā, attālināti, telefoniski vai izmantojot e-pastu, sociālā tīkla kontu) un kādās informācijas sistēmās vai papīra formā tie tiek apstrādāti.
1.12. Personas datu apstrāde tiek veikta pārziņa telpās, gan ārpus tām, kā arī pārziņa iestāžu, kapitālsabiedrības un struktūrvienību telpās un vietās, kur tiek nodrošināta datu apstrāde. Personas datu apstrāde tiek veikta manuāli (papīra veidā) un arī elektroniski, izmantojot informācijas sistēmas un trešo personu izstrādātās programmas.
1.13. Noteikumos izmantotie termini un jēdzieni, kas ir saistīti ar personas datu aizsardzību, ciktāl tie nav definēti atšķirīgi, atbilst tiem terminiem un jēdzieniem, kas norādīti Eiropas Parlamenta un Padomes Regulā (ES) 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) (turpmāk – Regula), Fizisko personas datu apstrādes likumā un citos attiecībā uz personas datu apstrādi piemērojamos normatīvos aktos.
1.14. Lietotie termini:
1.14.1. *Personas dati* – jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu (datu subjektu). Ar datiem saprot jebkādu informāciju, kas sniedz ziņas par identificējamu fizisko personu, tai skaitā objektīva (piemēram, personas vārds, uzvārds, personas kods, adrese, tālruņa numurs) un arī subjektīva informācija (piemēram, personas psiholoģiskais raksturojums, personas atrašanās riska grupā). Tāpat ar datiem ir saprotama jebkādā formā fiksēta informācija, t.i., gan papīra formātā, gan elektroniskā veidā, t.sk. foto un video ierakstos fiksētie dati;
1.14.2. *Datu subjekts* – fiziska persona, kuru var tieši vai netieši identificēt;
1.14.3. *Personas datu apstrāde* – jebkuras ar personas datiem veiktas darbības, ieskaitot datu vākšanu, reģistrēšanu, ievākšanu, glabāšanu, sakārtošanu, pārveidošanu, izmantošanu, nodošanu, pārraidīšanu un izpaušanu, bloķēšanu vai dzēšanu;
1.14.4. *Pārzinis* – Vecumnieku novada pašvaldība, kas attiecībā uz personas datu apstrādi nosaka personas datu apstrādes nolūkus un apstrādes līdzekļus, kā arī atbild par personas datu apstrādi atbilstoši piemērojamo normatīvo aktu prasībām;
1.14.5. *Apstrādātājs* – uz rakstveida līguma pamata veic personas datu apstrādi atbilstoši līgumā norādītajam apjomam, paredzētajiem nolūkiem un pārziņa norādījumiem;
1.14.6. *Personas datu aizsardzības pārkāpums* – pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem;
1.14.7. *Īpašu kategoriju dati* – dati, kas sniedz informāciju par datu subjektu rasi vai etnisko piederību, politiskiem uzskatiem, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībā, kā arī ģenētiskie dati, biometriskie dati (ja tie tiek izmantoti ar nolūku veikt fiziskās personas unikālu identifikāciju), veselības dati vai dati par fiziskās personas dzimumdzīvi vai seksuālo orientāciju.

2. Personas datu aizsardzības organizēšana

2.1. Personas datu aizsardzību pārzinis nodrošina, ievērojot Regulā un šajos Noteikumos noteiktās personas datu apstrādes prasības, kā arī citos iekšējos normatīvajos aktos un

rīkojumos, ierobežotas pieejamības informācijas aizsardzību, apriti, dokumentu pārvaldību un informācijas sistēmu drošību reglamentējošās jomās.

2.2. Datu aizsardzības speciālists ir pārziņa iekšējais uzraugs, kas informē un konsultē pārzini par datu aizsardzības prasībām, uzrauga Regulas prasību un citu normatīvo aktu ievērošanu, sniedz padomus, sadarbojas ar Datu valsts inspekciju, un ir kontaktpersona jautājumos, kas saistīti ar personas datu apstrādi, it īpaši datu subjektam īstenojot savas tiesības.

2.3. Datu aizsardzības speciālists ir darbinieks, kuram ir profesionālās zināšanas un pieredze personas datu apstrādē.

2.4. Datu aizsardzības speciālists darbojas pārziņa interesēs, bet saglabā savu neatkarību un neitralitāti, norādot pārzinim par neatbilstībām un pārkāpumiem personas datu apstrādē.

2.5. Pārzinis nedrīkst ietekmēt datu aizsardzības speciālistu, piemērot sankcijas par negatīvu vērtējumu par pārziņa veikto personas datu apstrādi.

2.6. Pārzinis un pilnvarotās personas atbalsta datu aizsardzības speciālistu Regulā noteikto uzdevumu izpildē, nodrošinot piekļuvi personas datiem un apstrādes darbībām tādā apjomā, lai datu aizsardzības speciālists varētu veikt Regulā ietvertos uzdevumus.

2.7. Pārzinis ieceļ datu aizsardzības speciālistu, kurš veic šādus uzdevumus:

2.7.1. Organizēt, kontrolēt un uzraudzīt veikto personas datu apstrādes atbilstību likuma prasībām pārziņa iestādēs, struktūrvienībās un kapitālsabiedrībās;

2.7.2. Piedalīties personas datu drošības stratēģijas izveidē un īstenošanā;

2.7.3. Sniegt konsultatīvu un organizatorisku atbalstu pārziņa drošības risku identificēšanā, analīzē un pasākumu ieviešanā risku mazināšanai un novēršanai personas datu aizsardzībā;

2.7.4. Izstrādāt priekšlikumus drošības pasākumu pilnveidošanai datu aizsardzības jomā;

2.7.5. Sniegt atbalstu iekšējo normatīvo aktu un citu iekšēju dokumentu projektu izstrādē, kas atbilstoši normatīvajiem aktiem nepieciešami iestādei kā personas datu pārzinim, veicot personas datu apstrādi;

2.7.6. Informēt un konsultēt pārzini, apstrādātāju un/vai pilnvaroto personu, kuri veic personas datu apstrādi, par viņu pienākumiem saskaņā ar Regulu un citiem Eiropas Savienības vai dalībvalstu normatīvajiem aktiem par datu aizsardzību;

2.7.7. Uzraudzīt, vai tiek ievērota Regula;

2.7.8. Konsultēt, apmācīt pilnvarotās personas jautājumos, kas saistīti ar datu aizsardzības drošības pasākumiem;

2.7.9. Veikt personas datu apstrādes darbību reģistra uzturēšanu, kurā tiek norādīta Regulā noteiktā informācija;

2.7.10. U.c.

3. Personas datu aizsardzības kvalifikācija

3.1. Apstrādājamo personas datu aizsardzību pārzinis kvalificē atbilstoši konfidencialitātei, kā arī vērtības (kritiskuma) pakāpes saskaņā ar ārējiem normatīvajiem aktiem un apstiprinātu ierobežotas pieejamības informācijas sarakstu.

3.2. Personas datus iedala atbilstoši to pieejamībai un tiem piešķir vērtības (kritiskuma) pakāpi atkarībā no kaitējuma, kas varētu tikt nodarīts pārziņa autonomo funkciju izpildei, ja nav nodrošināta personas datu aizsardzība (personas datus apstrādā tā, lai piekļuve tiem ir tikai pilnvarotajai personai ar atbilstošām pilnvarām), integritāte (personas datus saglabā pilnīgi un neizmainīti, neatkarīgi no apstrādes metodēm) un pieejamība (pilnvarotā persona tikai ar atbilstošām pilnvarām var piekļūt nepieciešamajiem personas datiem un apstrādāt tos noteiktā laikā un vietā).

3.3. Personas datus pēc to pieejamības klasificē atbilstoši Informācijas atklātības likuma prasībām – vispārpieejami un ierobežotas pieejamības dati. Uz ierobežotas pieejamības informāciju attiecināmi attiecīgie normatīvajos aktos noteiktie ierobežojumi.

3.4. Personas datus pēc vērtības (kritiskuma) pakāpes klasificē kā:

3.4.1. Augsta riska personas dati, kuru integritātes vai pieejamības traucējumu rezultātā pārzinim īslaicīgi vai ilgstoši nevarēs īstenot kādu no saviem uzdevumiem un/vai var radīt būtiskas negatīvas sekas datu subjektam;

3.4.2. Vidēja riska personas dati, kuru integritātes vai pieejamības traucējumu rezultātā pārzinim īslaicīgi vai ilgstoši pazemināsies uzdevumu īstenošanas efektivitāte un/vai datu subjektam varētu radīt negatīvas sekas;

3.4.3. Zema riska personas dati, kuru integritātes vai pieejamības traucējumi būtiski neietekmē pārziņa autonomo funkciju īstenošanu un/vai datu subjekta tiesības un brīvības netiek aizskartas.

4. Personas datu apstrādes principi

4.1. Pilnvarotajām personām, veicot apstrādes, jānodrošina šādu principu ieviešana:

4.1.1. Personas dati tiek apstrādāti likumīgi un godprātīgi, tas ir, atbilstoši piemērojamajiem normatīvajiem aktiem;

4.1.2. Personas dati tiek vākti tikai pārziņa definēto apstrādes nolūku sasniegšanai;

4.1.3. Personas dati ir adekvāti, atbilstoši un ietver tikai to informāciju, kas nepieciešama pārziņa definēto apstrādes nolūku sasniegšanai (datu minimizēšana);

4.1.4. Personas dati ir precīzi un, ja vajadzīgs, atjaunināti (pilnvarotajai personai ir jāveic savi pienākumi tā, lai nodrošinātu, ka neprecīzi personas dati tiek dzēsti vai laboti (precizēti), ciktāl tas nav pretrunā ar dokumentācijas vēstures veidošanas nepieciešamību);

4.1.5. Personas dati tiek glabāti veidā, kas nodrošina datu subjekta identifikāciju;

4.1.6. Personas dati tiek glabāti tikai tik ilgi, cik nepieciešams pārziņa definēto apstrādes nolūku sasniegšanai (glabāšanas ierobežojums);

4.1.7. Personas dati tiek apstrādāti veidā, kas ļauj saglabāt personas datu drošību pārziņa noteiktajā līmenī, nodrošinot aizsardzību pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos un organizatoriskos pasākumus (integritāte un konfidencialitāte) (piemēram, pārsūtot personas datus citiem apstrādātājiem pa e-pastu ieteicams aizsargāt pārsūtāmo datu saturu ar paroli, nepieciešamības gadījumā pilnvarotajai personai ieteicams konsultēties ar vadītāju vai tehnisko resursu turētāju (informācijas sistēmas uzturētāju));

4.1.8. Personas dati netiek pārsūtīti uz citām organizācijām, iestādēm vai ārvalstīm bez drošas adekvātas aizsardzības.

4.2. Ņemot vērā augstāk minētos aprakstītos principus, pilnvarotajai personai ir tiesības ieteikt korekcijas pārziņa veiktajās apstrādēs, kā arī izteikt priekšlikumus apstrāžu uzlabošanai.

5. Personas datu apstrādes posmi

5.1. Pārzinis veic personas datu apstrādi šādos posmos:

5.1.1. Personas datu iegūšana vai sagatavošana;

5.1.2. Personas datu lietošana;

5.1.3. Personas datu arhivēšana (ilgstoša glabāšana), t.sk., sagatavošana arhivēšanai;

5.1.4. Personas datu dzēšana.

5.2. Katrā no personas datu apstrādes posmiem katrai pilnvarotajai personai jāpiemēro šajos Noteikumos noteiktie personas datu apstrādes principi, ņemot vērā konkrētās personas datu apstrādes specifiskos datus, nolūku un citus aspektus.

6. Personas datu apstrādes veicēji

6.1. Par informācijas sistēmu tehniskajiem resursiem un informācijas sistēmās apstrādātajiem personas datiem un to aizsardzību atbildīgās personas nosaka attiecīgās informācijas sistēmas iekšējos datu apstrādes sistēmas aizsardzības vai lietošanas noteikumos.

6.2. Šo Noteikumu 6.1.apakšpunktā norādīto atbildīgo personu tiesības, pienākumi un atbildība ir noteikta informācijas sistēmu drošību reglamentējošajos iekšējos normatīvajos aktos, rīkojumos un pilnvarotās personas amata aprakstā.

6.3. Par personas datu saturošu stacionāro vai pārnēsājamo elektronisko informācijas nesēju, kā arī manuālo informācijas nesēju, piemēram, papīra dokumenti, personu lietas (turpmāk – informācijas nesējs), izņemot informācijas sistēmu serverus un resursus, kuros glabā personas datus, atbilstoši kompetencei ir atbildīga pilnvarotā persona, kurai attiecīgais informācijas nesējs ar personas datiem ir izsniegts (nodots).

6.4. Atbilstoši ieņemamajam amatam attiecīgās apstrādes veic un arī atbild par attiecīgās apstrādes atbilstību piemērojamie normatīviem aktiem atsevišķas pilnvarotās personas.

6.5. Pilnvarotā persona nodrošina vai piedalās attiecīgās apstrādes nodrošināšanā, kā arī savas kompetences un pilnvarojuma ietvaros atbild par pareizu un piemērojamiem normatīviem aktiem atbilstošu apstrādi.

6.6. Datu apstrādi savas kompetences ietvaros, balstoties uz Noteikumiem un citiem piemērojamajiem normatīvajiem aktiem, var veikt citas personas, šādos gadījumos veiktā personas datu apstrāde jāsaskaņo ar pilnvaroto personu.

6.7. Pārzinis ir tiesīgs uzlikt pilnvarotajai personai plašākas tiesības un pienākumus personas datu apstrādē, kā arī veikt citas darbības, kuras uzskata par nepieciešamu, lai tiktu nodrošināta piemērojamo normatīvo aktu prasību izpilde personas datu aizsardzības jomā.

6.8. Personas datu apstrādes veikšanai pārzinis var piesaistīt apstrādātāju, noslēdzot rakstveida līgumu un nodrošinot, ka attiecīgais apstrādātājs uzņemas atbildību par apstrādājamo datu drošību, konfidencialitāti un attiecīgās apstrādes atbilstību noteiktajam nolūkam piemērojamo normatīvo aktu prasībām.

6.9. Pilnvarotās personas tiesības, pienākumi un atbildības:

6.9.1. Pilnvarotajai personai ir tiesības veikt pārziņa rīcībā esošos personas datu apstrādi tikai pildot darba pienākumus saskaņā ar amata aprakstu un vadības norādījumiem;

6.9.2. Pilnvarotajai personai ir tiesības izmantot viņam pieejamos pārziņa informācijas apstrādes resursus (datori, programmnodrošinājums, elektronisko sakaru pakalpojumi u.c.) tikai darba uzdevumu izpildes vajadzībām;

6.9.3. Saskaņā ar Regulas 13.panta 1. un 2.punktu, lai nodrošinātu godprātīgu un pārredzamu personas datu apstrādi, pilnvarotā persona datu iegūšanas laikā datu subjektam saprotamā un viegli uztveramā veidā (bez pieprasījuma) sniedz informāciju par tā personas datu apstrādi;

6.9.4. Pilnvarotā persona informācijas sistēmās reģistrējas tikai ar piešķirto unikālo lietotājvārdu un paroli, kā arī ievēro kārtību, kas noteikta informācijas sistēmu drošību reglamentējošajos iekšējos normatīvajos aktos;

6.9.5. Datu apstrādi lieto konkrētajiem mērķiem ar paredzēto programmatūru vai informācijas sistēmu;

6.9.6. Pilnvarotās personas pienākums ir bez tiesiska pamata neizpaust personas datus arī pēc darba tiesisko attiecību vai citu saistību izbeigšanas ar pārzini;

6.9.7. Pilnvarotajai personai ir pienākums lietot nepieciešamos tehniskos un organizatoriskos līdzekļus, lai aizsargātu personas datus un novērtētu to pretlikumīgu apstrādi;

6.9.8. Pilnvarotā persona atbilstoši savai kompetencei nodrošina, lai viņam nodotie vai pieejamie personas dati nebūtu pieejami personām, kas nav pilnvarotas un tiesīgas

apstrādāt personas datus (piemēram, neatstāt neaizslēgtas telpas, kur atrodas informācijas nesēji, durvis, neatstāt informācijas nesējus bez uzraudzības ārpus personas datu apstrādes telpām u.tml.);

6.9.9. Izejot no personas datu apstrādes telpām, pilnvarotās personas pienākums ir aizslēgt telpu ieejas durvis (ja telpās nepaliek cita pilnvarotā persona), kā arī personālo datoru (darbstaciju), kurā apstrādā personas datus, tādā stāvoklī, lai darbu ar to varēti atsākt tikai pēc personas datu lietotāja autentifikācijas un autorizācijas;

6.9.10. Pilnvarotās personas nedrīkst pieprasīt un uzkrāt pārlieku daudz personas datus, ja vien tam nav tiesiska pamata;

6.9.11. Pilnvarotā persona nedrīkst izmantot no interneta vai cita datortīkla iegūtu programmatūru;

6.9.12. Pilnvarotā persona nedrīkst veikt nesankcionētas darbības ar datortīklu un datortīkla tehniku;

6.9.13. Pilnvarotā persona nedrīkst veikt nesankcionētas darbības interneta tīklā, iekštīklā vai lokālajā datortīklā pret citiem šo tīklu lietotājiem;

6.9.14. Beidzot darbu, pilnvarotā persona izslēdz datoru, bet, ja pilnvarotā persona atstāj datoru uz īsu laiku, jālieto ekrānsaudzētājs ar paroli. Beidzot darbu ar datu apstrādes programmu, tā obligāti jāaizver;

6.9.15. Pilnvarotā persona ir atbildīga par visām darbībām, kas veiktas, izmantojot viņam piešķirtās tiesības informācijas resursu lietošanai. Ja pilnvarotā persona konstatē, ka viņa tiesības izmantojis kāds cits, par to nekavējoties ziņo tiešajam vadītājam un datu aizsardzības speciālistam vienlaicīgi;

6.9.16. Pilnvarotās personas pienākums ir pēc datu subjekta rakstiska pieprasījuma, sniegt tam visu informāciju, kas savākta par atbilstošo datu subjektu, normatīvos aktos noteiktajā kārtībā;

6.9.17. Regulāri izdzēst darbam nevajadzīgos elektroniskā pasta sūtījumus;

6.9.18. Pilnvarotā persona tam uzticētos apstrādājamos personas datus drīkst izpaust citai personai pēc tam, kad ir pārliecinājies, ka attiecīgā persona saskaņā ar iekšējiem normatīvajiem aktiem ir tiesīga apstrādāt šos personas datus (piemēram, ar struktūrvienības rakstisku pieprasījumu, norādot apstrādes nolūku un tiesisko pamatu, amata aprakstu);

6.9.19. Informāciju, kas nepieciešama pieejai informācijas resursam (parole, identifikators u.c.) ir aizliegts izpaust, un pilnvarotā persona ir personīgi atbildīga par tās konfidencialitāti;

6.9.20. Pilnvarotajai personai aizliegts sūtīt „ķēdes vēstules" – elektroniskā pasta veidā, kas satur personas datus, vai pārsūtīt personas datus citiem adresātiem;

6.9.21. Pilnvarotajai personai ir aizliegts izpaust ziņas par informācijas resursiem, t.sk., bet ne tikai datortīklu, uzbūvi, konfigurāciju un aizsardzības līdzekļiem trešajām personām;

6.9.22. Pilnvarotajai personai ir aizliegts viņam pieejamos personas datus pārveidot, kopēt, izplatīt jebkādā citā formā, kamēr tas nav nepieciešams darba uzdevumu izpildei izmantot tos citu apstrādes sistēmu izveidei, kā arī glabāt publiski pieejamās vietās;

6.9.23. Pilnvarotā persona ir atbildīga par dokumentiem, to kopijām, neatkarīgi no informācijas nesēja, un datortehniku, kas nodoti pilnvarotās personas rīcībā darba pienākumu veikšanai;

6.9.24. Pilnvarotā persona pilnībā atbild par viņa rīcībā esošās informācijas (neattiecas uz datubāzēm, kas glabājas uz atsevišķa servera, centrālās datu bāzes) drošību;

6.9.25. Pilnvarotā persona atbild, lai slēdzama darba galda atvilktne, skapis vai seifs, kurā pilnvarotā persona uzglabā informācijas nesēju, pilnvarotās personas prombūtnē būtu aizslēgts;
6.9.26. Pilnvarotā persona atbild, lai pārvietojot (iznesot) informācijas nesēju ārpus personas datu apstrādes telpām, tiktu nodrošināta tā nepārtraukta aizsardzība;
6.9.27. Pilnvarotajai personai ir tiesības un pienākums pieprasīt atbalstu gadījumā, ja datoram vai programmatūrai ir radušies traucējumi vai arī pilnvarotajai personai ir pietiekams uzskats par iespējamo draudu (apdraudējumu) esamību;
6.9.28. Sistēmu administratori vai personas, kas pilda šos pienākumus ir atbildīgi par informācijas resursu izmantošanu (sniegšanu), viņiem uzticēto personas datu aizsardzību kā arī par tehnisko resursu darbību, kas ir viņa rīcībā;
6.9.29. Pilnvarotā persona nepārtrauc pretvīrusa programmas atjaunināšanas procesu;
6.9.30. Pilnvarotā persona portatīvajā datorā, kurš tiek lietots ārpus darba telpām, glabā tikai to informāciju, kas nepieciešama noteiktajā laikā, noteikto darba pienākumu veikšanai.

6.10. Par prettiesiskām darbībām ar personas datiem pilnvaroto personu sauc pie disciplinārās, civiltiesiskās, administratīvās un/vai kriminālās atbildības.

7. Drošības prasības

7.1. Personas datu apstrāde ir atļauta tikai, tad, ja normatīvajos aktos nav noteikts citādi un ja ir vismaz viens no šādiem nosacījumiem:
7.1.1. Saņemta personas datu subjekta piekrišana;
7.1.2. Datu apstrāde izriet no datu subjekta līgumsaistībām vai, ievērojot datu subjekta lūgumu, datu apstrāde nepieciešama, lai noslēgtu attiecīgu līgumu;
7.1.3. Datu apstrāde nepieciešama pārziņa noteikto juridisko pienākumu veikšanai;
7.1.4. Datu apstrāde nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas personas vitālas intereses;
7.1.5. Datu apstrāde nepieciešama, lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot likumīgi piešķirtās oficiālas pilnvaras;
7.1.6. Datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un pamatbrīvības, realizētu pārziņa vai tās trešās personas likumiskās intereses, kurai personas dati atklāti.

7.2. Vadība nodrošina tehnisko un organizatorisko prasību veikšanu, piemērojot atbilstošos fiziskos un loģiskos aizsardzības līdzekļus atbilstoši vadības līdzekļiem un ņemot vērā konkrētās personas datu apstrādes vietas, telpas un apjomus, lai aizsargātu personas datus un personas datu apdraudējumus.

7.3. Sistēmu administrators nodrošina tehnisko resursu darbības uzturēšanu un to tehnisko apkopi.

7.4. Sistēmu administrators veic risku analīzi izmantotajām informācijas sistēmām, kā arī nepieciešamības gadījumā sagatavo plānus, instrukcijas tehnisko resursu pieejamības nodrošināšanai.

7.5. Pārzinis nodrošina pilnvaroto personu apmācību par personas datu aizsardzības pamatprincipiem. Atbildīgā persona par personāla uzskaiti nodrošina pilnvaroto personu, t.sk. jaunpieņemtu pilnvaroto personu iepazīstināšanu ar šiem Noteikumiem un šo Noteikumu pieejamību.

7.6. Personas datu apstrāde tiek nodrošināta ar tehniskajiem resursiem: stacionārajām darbstacijām, portatīvo vai personālo datoru, serveriem, citām iekārtām un programmatūrām pēc vajadzības.

7.7. Lai pasargātu tehniskos resursus un informāciju no ārkārtas apstākļiem (ugunsgrēks, plūdi, u.tml.) ietekmes, tiek īstenoti drošības pasākumus atbilstoši ugunsdrošības noteikumiem, kā

arī vispārējām normatīvo aktu prasībām elektroiekārtu drošai ekspluatācijai un to aizsardzībai.

7.8. Vadība ievieš pasākumus, lai tiktu kontrolēta personu ienākšana un atrašanās telpās, kur tiek veikta personas datu apstrāde.

7.9. Telpas, kurās atrodas serveri un resursdatori ar personas datiem, ir aprīkotas ar ugunsdrošības automatizētiem sensoriem un signalizāciju. Šajās telpās vai tiešā to tuvumā ir novietoti ugunsdzēsības aparāti.

7.10. Datortehnikai un programmatūrai, ar kuru tiek veikta apstrāde, uzstādīšanu un administrēšanu nodrošina sistēmu administrators, kurš nodrošina tehnisko resursu funkcionēšanu un tehnisko resursu atjaunošanu, ja to darbība tiek traucēta vai nav iespējama.

7.11. Lai aizsargātu personas datus, kuri glabājas elektroniskā veidā, vadība nodrošina datu rezerves kopiju glabāšanu ģeogrāfiski citā vietā, nevis sākotnējā datu apstrādes vietā. Rezerves kopiju veidošanu nodrošina sistēmu administrators.

7.12. Datu rezerves kopijas tiek gatavotas atbilstoši vadības noteiktai procedūrai.

7.13. Piekļuve un darbs datorizētās informācijas sistēmās tiek nodrošināts pēc autentifikācijas veikšanas saskaņā ar sistēmu drošības politiku. Piekļūt datorizētās informācijas sistēmām un strādāt ar personas datiem atļauts tikai atbilstoši pilnvarotām un autentificētām personām.

7.14. Informācijas sistēmas personas datu apstrādes loģisko drošību vadības resursu administrators kopā ar informācijas tehnoloģiju drošības pārvaldnieku, organizējot drošības iestatījumus tā, lai iespējamie riski tiktu novērti pirms to iestāšanās.

7.15. Uz datora ir jābūt uzstādītam ekrāna saudzētajam ar aktivizācijas paroli. Tam ir automātiski jāaktivizējas, ja piecu minūšu laikā pilnvarotā persona nav veikusi nekādas darbības.

7.16. Aizliegts jebkāda nešifrēta bezvadu datortīkla izmantošana (Unencrypted Wireless Networks).

7.17. Personas dati jāglabā, ievērojot vispārīgās datu glabāšanas un drošības prasības, tai skaitā ar tehniskajiem un organizatoriskajiem līdzekļiem jānodrošina, ka personas datus nevar sagrozīt, bojāt un tiem nepiekļūst nepilnvarotas personas.

7.18. Izmantojot informācijas sistēmas resursus, pilnvarotai personai ir nekavējoties jāziņo sistēmas administratoram šādos gadījumos:

7.18.1. Saņemot neskaidras izcelsmes elektroniskā pasta sūtījumus (piemēram, nepazīstami korespondenti, īpatnēji norādīti vēstuļu temati);

7.18.2. Ja radušās aizdomas, ka dators inficēts ar vīrusu.

8. Informācijas sistēmas paroles uzbūve un lietošana

8.1. Informācijas sistēmas aizsardzība tiek nodrošināta ar datora paroli operētājsistēmas (MS Windows) līmenī.

8.2. Parole (MS Windows līmenī) atbilst sekojošām prasībām:

8.2.1. Minimālās paroles garums ne mazāk kā astoņi simboli;

8.2.2. Paroles maiņas periods 6 mēneši;

8.2.3. Paroles uzbūve ir komplicēta, kas sastāv no burtu, ciparu un īpašo rakstzīmju kombinācijas;

8.2.4. Parole nedrīkst atkārtoties.

8.3. Paroli aizliegts veidot, izmantojot ar pilnvarotu personu saistītu informāciju (piemēram, vārdus, uzvārdus, dzimšanas dienas, tālruņa numurus, mājdzīvnieku un tuvinieku vārdus u.tml.).

8.4. Pilnvarotai personai aizliegts izpaust savu paroli.

8.5. Ja pilnvarotai personai ir aizdomas, ka paroli zina trešā persona, tai ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt.

8.6. Paroli nav atļauts sūtīt pa elektronisko pasta adresi, vai kā citādi darīt zināmu trešajām personām.

8.7. Aizliegts izmantot automatizētas pieslēgšanās programmatūru.
8.8. Pilnvarotajai personai parole ir jāiegaumē, rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā skapī vai vietā, kur tai nepiekļūst trešās personas.
8.9. Pilnvarotā persona ir atbildīga par visām darbībām, kas veiktas, lietojot viņa identifikatorus.
8.10. Gadījumā, ja ir aizdomas, ka identifikatoru un paroli izmanto (vai mēģinājusi izmantot) cita persona, par to nekavējoties jāinformē tiešo vadītāju un datu aizsardzības speciālistu.
8.11. Tiešais vadītājs organizē nekavējoties paroles un identifikatoru anulēšanu pēc pilnvarotās personas saņemtā ziņojuma par paroles vai identifikatora nozaudēšanu vai nokļūšanu trešās personas rīcībā. Ja paroles vai identifikatora maiņa pilnvarotās personas rīcības dēļ notiek trīs reizes gada laikā tiešajam vadītājs par to ziņo vadībai, kura lemj par tālāko rīcību.
8.12. Tiešais vadītājs informē sistēmu administratoru par pilnvarotās personas atlaišanu vai atstādināšanu, kam ir pieejas tiesības informācijas resursiem un kvalificētai informācijai. Pēc informācijas saņemšanas sistēmu administrators anulē pilnvarotās personas paroles un identifikatorus un nodrošina pilnvarotās personas darbstacijas dzēšanu.

9. Datu aizsardzība lietojot datu failus un elektronisko pastu

9.1. Vadība ir tiesīga kontrolēt un ierobežot resursu un saziņas līdzekļu izmantošanu, lai nodrošinātu tīkla drošību atbilstoši apdraudējumiem un samazinātu personas datu apdraudējumu.
9.2. Vadībai nav tiesības:
  9.2.1. Saņemt automātiskas kopijas no visām saņemtajām un nosūtītajām pilnvarotās personas elektroniskā pasta vēstulēm;
  9.2.2. Saglabāt informāciju par visām darbībām, ko pilnvarotā persona veic ar datoru, izņemot, ja ir nepieciešams nodrošināt augsta līmeņa drošības aizsardzību (lēmumu par šādu aizsardzību pieņem Domes priekšsēdētājs);
  9.2.3. Bez pamatota iemesla pārbaudīt un kontrolēt pilnvarotas personas telefona sarakstus.
9.3. Sistēmu administrators nav tiesīgs apstrādāt personas datus, izmantojot piekļuves tiesības vietnēm un informāciju sistēmām (t.sk. saņemt informāciju) bez pilnvarotās personas piekrišanas, izņemot:
  9.3.1. Ja ir konstatēts datu aizsardzības pārkāpums un minētā informācija ir nepieciešama, lai noskaidrotu vainīgo personu;
  9.3.2. Ja tas nepieciešams, lai novērtētu sistēmas darbības traucējumus, ja fiksēts apdraudējums personas datos.
9.4. Sistēmu administrators piecu darba dienu laikā neatgriezeniski dzēš atlaistās vai atstādinātās pilnvarotās personas elektroniskā pasta kontu, kā arī citus dokumentus, kuriem piekļuve ir bijusi tikai attiecīgajām pilnvarotajām personām, ja vien šī informācija nav nepieciešama turpmākajam darbam (statistikas pārskatiem, utt.).
9.5. Datu failiem, kuri tiek glabāti uz serveriem, ir profesionāls raksturs un tiem brīvi var piekļūt tikai pilnvarotās personas.
9.6. Pilnvarotās personas pieejas tiesību paroles ir konfidenciālas un nevar tikt nodotas citām personām (t.sk. vadītājiem vai darba devējam plašākā nozīmē). Ja pilnvarotā persona ir prombūtnē un tā rīcībā esošā informācija ir nepieciešama, lai izpildītu noteiktās funkcijas vai uzdevumus, vadība var pieprasīt sistēmu administratoram nodrošināt pieeju datnēm attiecīgā pilnvarotās personas darbstacijā un servera mapēs.
9.7. Pilnvarotā persona drīkst izmantot elektroniskos sakaru līdzekļus (e-pastu), tomēr ir jāapzinās, ka, izmantojot elektroniskos saziņas līdzekļus, apstrādātājs nespēj kontrolēt interneta drošības, pieejamības un darbības aspektus no trešo personu prettiesiskajām darbībām, līdz ar ko pilnvarotajai personai ir jāveic šādus personas datu aizsardzības pasākumus gadījumos, kad personas dati tiek sūtīti pa e-pastu:

9.7.1. Ja pilnvarotā persona nosūta e-pastu ar personas datu saturošo informāciju datu subjektam pēc datu subjekta lūguma, pilnvarotā persona e-pastam klāt pievieno šādu atrunu:

9.7.1.1. *Šī vēstule un jebkuri tās pielikumi satur konfidenciālu informāciju, kura ir paredzēta tikai vēstulē minētajam adresātam. Ja Jūs neesiet šīs vēstules adresāts, Jūs nedrīkstiet tajā iekļauto informāciju izmantot, pavairot, izplatīt, pārsūtīt, atklāt iekļauto informāciju citām personām, atskaitot vēstules adresātu. Ja esiet saņēmis šo vēstuli kļūdas rezultātā, lūdzam nekavējoties sazināties ar sūtītāju un izdzēst šo vēstuli, kā arī visus šīs vēstules pielikumus. Par neautorizētas personas datu apstrādi (t.sk. personas datu glabāšanu), persona var tikt saukta pie atbilstības normatīvajos aktos noteiktajam.*

9.7.2. Ja pilnvarotajai personai ir nepieciešams nosūtīt e-pastu ar personas datu saturošu informāciju citai pilnvarotajai personai, personas datu saturošu informāciju (ja iespējams) saglabāt datu failā, kuram ir uzstādīta atvēršanas parole, kuras garums ir vismaz 8 simboli. Šīs paroles izpaušana nedrīkst izpaust e-pastu, bet būtu jāizmanto alternatīvs veids, piemēram, tālrunis vai tml.

9.8. Pilnvarotā persona var veikt personas datu apstrādi uz datortehnikas (t.sk. datoriem, mobilajām ierīcēm), kas ir viņa personīgā rīcībā, tikai un vienīgi, ja šāda nepieciešamība ir saskaņota ar tiešo vadītāju un personas datu saturoša informācija tiek glabāta datu failos, kam ir uzstādīta atvēršanas parole, kuras garums ir vismaz astoņi simboli (mobilajām ierīcēm nepieciešama automātiskā ekrāna bloķēšana, tas nozīme, ka pirms katras lietošanas ierīce ir jāatslēdz vai nu ar pirkstu nospiedumu vai paroli (piemēram, ciparu kombinācija vai figūra)).

10. Personu rīcība apdraudējuma gadījumos

10.1. Par jebkuru datu apstrādes apdraudējumu personas datu apstrādē iesaistītajai personai, kas to konstatējusi nekavējoties jāziņo vadībai, tai skaitā gadījumos:

10.1.1. Ja konstatēts jebkāda veida apdraudējums tehniskajiem resursiem (elektroenerģijas padeves pārtraukums, šķidrumu vai svešķermeņu iekļūšana, bojājumi fiziska trieciena, uguns iedarbības vai plūdu rezultātā u.c.);

10.1.2. Ja konstatēts jebkādā veida apdraudējums informācijas resursiem (trešajām personām kļuvuši zināmas pieejas paroles, konstatēta nesankcionēta piekļuve, konkrēti darbības pārtraukumi u.c.);

10.1.3. Ja konstatēts jebkāda veida apdraudējums personas datiem papīra formātā (pārāk augsts mitrums telpās, metāla skapja vai telpu durvju slēdzenes nefunkcionēšana, signalizācijas nefunkcionēšana, trešo personu piekļūšana dokumentiem u.c.).

10.2. Apdraudējuma gadījumā personas datu apstrādē iesaistītajai personai savu iespēju un pilnvaru ietvaros ir pienākums nodrošināt informācijas sistēmas drošību līdz vadības ierašanās brīdim.

10.3. Gadījumos, kad tiek konstatēta prettiesiska personas datu nokļūšana trešo personu rīcībā (datu noplūde), personas datu apstrādē iesaistītajai personai nekavējoties jāinformē vadību.

11. Personas datu aizsardzības pārkāpuma konstatēšana un ziņošana par pārkāpumu

11.1. Personas datu aizsardzības pārkāpums (turpmāk – Incidents) ir drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem. Incidenta piemēri:

11.1.1. Ierīce ir nozaudēta vai nozagta;

11.1.2. Documents ir nozaudēts vai atstāts brīvi pieejamā vietā;

11.1.3. Pasts (papīra formātā) ir nozaudēts vai piegādāts atvērts;

11.1.4. Urķēšana;

11.1.5. Ļaunprogrammatūras;

11.1.6. Pikšķerēšana;

11.1.7. Nepareiza personas datu iznīcināšana papīra formātā;
11.1.8. Nepārdomāta publikācija;
11.1.9. Izpausti personas dati citam/nepareizajam datu subjektam;
11.1.10. Personas dati nosūtīti nepareizajam adresātam;
11.1.11. Verbāla nesankcionēta personas datu izpaušana;
11.1.12. U.tml.

11.2. Konstatējot faktu vai apstākļus, kas varētu liecināt par Incidentu, pilnvarotajai personai ir pienākums ziņot tiešajam vadītājam.

11.3. Tiešais vadītājs, saņemot informāciju no pilnvarotās personas, iepazīstas ar konstatētajiem faktiem un apstākļiem, ievāc papildus nepieciešamo informāciju, un gatavo ziņojumu par datu apstrādes incidentu (5.pielikums), iesniedz vadībai. Ziņojumā par datu apstrādes incidentu tiek atspoguļoti konstatētie fakti un tiek secināts – vai ir noticis Incidents. Ziņojumā par datu apstrādes incidentu jānorāda tā sastādīšanas datums un laiks.

11.4. Vadība saņemot ziņojumu par datu apstrādes incidentu, nodrošina tā tūlītēju iesniegšanu pārzinim, kurš konsultējoties ar datu aizsardzības speciālistu lemj par nepieciešamību informēt Datu valsts inspekciju un Incidentā skartos datu subjektus.

11.5. Ja Incidents nav noticis, tiešais vadītājs informē vadību par papildus aizsardzības pasākumiem, ja tādus nepieciešams un iespējams veikt, lai nākotnē izvairītos no notikumiem, kas varētu radīt Incidentu.

11.6. Ja Incidents ir noticis pārzinis bez nepamatotas kavēšanās un, ja iespējams, ne vēlāk kā 72 stundu laikā no brīža, kad pārkāpums tam kļuvis zināms, paziņo par Incidentu Datu valsts inspekcijai, iesniedzot paziņojumu par personas datu aizsardzības pārkāpumu (3.pielikums). Minētais paziņojums par personas datu aizsardzības pārkāpumu nosūtāms pa e-pastu, lietojot drošu elektronisko parakstu. Ja paziņošana Datu valsts inspekcijai nav notikusi 72 stundu laikā, paziņojumam pievieno kavēšanās iemeslus.

11.7. Datu aizsardzības speciālists dokumentē visus personas datu aizsardzības pārkāpumus, norādot faktus, kas saistīti ar Incidentu, tā sekas un veiktās koriģējošās darbības. Minētā dokumentācija ļauj Datu valsts inspekcijai pārbaudīt normatīvo aktu ievērošanu.

11.8. Pārzinim ir pienākums informēt datu subjektu par Incidentu, kā arī sastādīt nosūtīt ziņojumu (4.pielikums) par Incidentu datu subjektam, ja konstatēts, ka Incidents radījis augstu risku (apdraudējumu) datu subjekta tiesībām un brīvībām.

11.9. Noteikumu 11.8.apakšpunktā norādītājs ziņojums datu subjektam nav jānosūta, ja:

11.9.1. Pārzinis ir īstenojis atbilstošus tehniskos un organizatoriskos aizsardzības pasākumus un minētie pasākumi ir piemēroti tiem personas datiem, ko skāris Incidents, jo īpaši tādi pasākumi, kas personas datus padara nesaprotamus personām, kurām nav pilnvaru piekļūt datiem (piemēram, šifrēšana);

11.9.2. Pārzinis ir veicis turpmākus pasākumus, ar ko nodrošina, lai, visticamāk, vairs nevarētu iestāties Incidentā konstatētais augstais risks attiecībā uz datu subjektu tiesībām un brīvībām;

11.9.3. Ziņojuma nosūtīšana prasītu nesamērīgi lielas pūles. Šādā gadījumā individuāla ziņojuma vietā datu subjektam izmanto publisku saziņu vai līdzīgu pasākumu, ar ko datu subjekts tiek informēts vienlīdz efektīvā veidā.

11.10. Ja pārzinis vēl nav ziņojis datu subjektam par Incidentu, Datu valsts inspekcija, var pieprasīt pārzinim paziņot datu subjektam vai var nolemt, ka ir izpildīti visi nosacījumi un attiecīgais paziņojums nav jāsniedz.

11.11. Ja ir pamats uzskatīt, ka Incidents noticis normatīvo aktu pārkāpuma rezultātā, vadība ziņo par Incidentu Datu valsts inspekcijai un CERT.LV (informācijas tehnoloģiju drošības incidentu novēršanas institūcijai).

11.12. Konstatējot drošības Incidentu informācijas sistēmās, tai skaitā serveros un resursdatoros, kuros apstrādā personas datus, pilnvarotā persona ievēro informācijas sistēmu drošības reglamentējošos iekšējos normatīvos aktu prasības.

12. Personas datu apstrādes izmaiņu identificēšana un reģistrēšana

12.1. Tiešais vadītājs atbilstoši kompetencei nodrošina, lai informācija par identificētajām vai plānotajām izmaiņām personas datu apstrādē tiktu iesniegta datu aizsardzības speciālistam, identificējot vai plānojot izmaiņas, kas attiecas uz personas datu apstrādes nolūkiem, personas datu apstrādes tiesisko pamatu, datu subjekta kategorijām personas datu veidiem, personas datu saņēmēju kategorijām, personas datu apstrādes veidiem, personas datu apstrādes vietām, personas datu veidiem, kurus nodos citām valstīm, kas nav Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstis, kā arī informācijas resursu vai tehnisko resursu turētājiem un atbildīgajiem par informācijas sistēmu drošību, par ko iepriekš nav veikts novērtējums par ietekmi uz personas datu aizsardzību.

12.2. Par izmaiņu identificēšanu personas datu apstrādē un informācijas sniegšanu datu aizsardzības speciālistam par identificētajām, tai skaitā plānotajām izmaiņām datu apstrādes nolūkos vai uzsākot jaunu, iepriekš nereģistrētu datu apstrādi, atbildīgā persona ir tiešais vadītājs.

12.3. Tiešais vadītājs veic šādus uzdevumus:

12.3.1. Sistemātiski un plānveidīgi organizē un veic pasākumus, kas nodrošina informācijas iegūšanu par izmaiņām personas datu apstrādē, tai skaitā par plānotajām izmaiņām (piemēram, iztaujā pilnvarotās personas, personīgi seko informācijai par iespējamām plānotajām vai notikušajām izmaiņām);

12.3.2. Identificējot izmaiņas personas datu apstrādē vai saņemot informāciju par plānotajām izmaiņām, kas iepriekš nav fiksētas personas datu apstrādes darbību reģistrā, 15 dienu laikā sagatavo informāciju tālākai iesniegšanai datu aizsardzības speciālistam (6.pielikums);

12.3.3. Nodrošina, lai ne vēlāk kā līdz 30.martam, 30.jūnijam, 30.septembrim un 30.decembrim datu aizsardzības speciālistam tiktu iesniegta aktuālā informācija par identificētajām, tai skaitā plānotajām, izmaiņām personas datu apstrāde.

12.4. Datu aizsardzības speciālists, saņemot informāciju par identificētajām vai plānotajām izmaiņām personas datu apstrādē:

12.4.1. Apkopo saņemto informāciju, pārbauda, vai personas datu apstrādes darbību reģistrā jau nav reģistrēta tāda veida informācija par identificēto vai plānoto personas datu apstrādi, kā arī izvērtē attiecīgo apstrādes darbību risku, ņemot vērā apstrādes raksturu, apjomu, kontekstu un nolūku;

12.4.2. Nosaka identificēto vai plānoto personas datu apstrādes izmaiņu atbilstību normatīvajiem aktiem, kas reglamentē personas datu apstrādes aizsardzības obligātās tehniskās un organizatoriskās prasības, kā arī informācijas sistēmu drošības reglamentējošiem iekšējiem normatīvajiem aktiem, ja personas datu apstrādi veic personas datu apstrādes sistēmās;

12.4.3. Glabā dokumentu kopijas par izmaiņu izdarīšanu personas datu apstrādē;

12.4.4. Informē atbildīgo personu, kurš sniedzis informāciju par identificētajām vai plānotajām izmaiņām personas datu apstrādē, par lēmumu par izmaiņu veikšanu personas datu apstrādes darbību reģistrā, kā arī nepieciešamības gadījumā sniedz rekomendācijas identificēto risku mazināšanai.

13. Personas datu apstrādes darbību reģistrs un novērtējums par ietekmi uz datu aizsardzību

13.1. Saskaņā ar Regulas 30.pantu pārzinis izveido un regulāri aktualizē (vismaz vienu reizi 12 mēnešos) personas datu apstrādes darbību reģistru.

13.2. Pirms pārzinis uzsāk jaunu apstrāžu veikšanu tiek sastādīts novērtējums par ietekmi uz datu aizsardzību saskaņā ar Regulas 35.pantu.

13.3. Pārzinis regulāri aktualizē (vismaz vienu reizi 12 mēnešos) novērtējumu par ietekmi uz datu aizsardzību, it īpaši:

13.3.1. Noticis Incidents (neatkarīgi no tā, vai pārzinis par to ziņojis datu subjektam vai Datu valsts inspekcijai);
13.3.2. Tiek veiktas vai plānots veikt nozīmīgas izmaiņas datubāzēs (par nozīmīgām izmaiņām uzskatāmas tādas, kas ietekmē apstrāžu pamatojumu, nolūku, datu apjomu, veidu, struktūru, kopējo drošību un datu nodošanas kārtību ārpus ES vai EEZ dalībvalstīm);
13.3.3. Tiek apvienotas datubāzes/personas datu apstrādes;
13.3.4. Tiek izveidotas jaunas datubāzes/personas datu apstrādes;
13.3.5. Tiek ieviestas jaunas datu apstrādes tehnoloģijas vai metodes.

14. Personas datu izpaušanas kārtība trešajām personām

14.1. Personas datus bez datu subjekta atļaujas nedrīkst izpaust trešajām personām, izņemot, ja datu izpaušanu nosaka normatīvie akti.
14.2. Personas dati tiek izpausti tikai tām valsts un pašvaldības amatpersonā, kuras pirms datu izpaušanas ir identificētas, pamatojoties uz rakstveida iesniegumu vai vienošanos, norādot datu izmantošanas mērķi. Personas datu pieprasījumā norāda informāciju, kas ļauj identificēt datu pieprasītāju un datu subjektu, kā arī pieprasāmo personas datu apjoms (aizliegts izpaust datus pa tālruni un trešo personu klātbūtnē).
14.3. Pirms personas datu izpaušanas vai nodošanas citām personām (tai skaitā citiem darbiniekiem) jāpārliecinās, vai tam ir tiesisks pamats un likumīgs mērķis.
14.4. Personas datu pieprasījumu izskata viena mēneša laikā no pieprasījuma saņemšanas dienas un noteiktā kārtībā sniedz pieprasīto informāciju vai pamatotu rakstveida atteikumu.

15. Datu subjekta pieprasījumu izpildes kārtība

15.1. Saņemot datu subjekta jautājumus, iesniegumus vai citus pieprasījumus, jāaicina attiecīgo datu subjektu iepazīties ar Vecumnieku novada Domes 2019.gada 28.augusta iekšējiem noteikumiem Nr.1-9/2019/16 „Vecumnieku novada pašvaldības personas datu apstrādes privātuma politika" (turpmāk – Privātuma politika).
15.2. Saņemot datu subjekta mutvārdu pieprasījumu, jāinformē datu subjekts, ka informācija par personas datiem tiek izpausta pienācīgi identificētām personām un tikai par pienācīgi identificētām personām, līdz ar to, mutvārdos sniegtā datu subjekta informācija var nebūt pietiekama personas datu izpaušanai.
15.3. Izskatot datu subjekta pieprasījumu jāizvērtē:
15.3.1. Vai pieprasījumā datu subjekts ir pienācīgi (attiecīgos apstākļos – nesajaucami ar citām fiziskām personām) identificēts;
15.3.2. Vai ir identificējams datu subjekts, par kuru tiek pieprasīta informācija (ja tiek prasīts izsniegt, iepazīties, koriģēt vai veikt citas darbības ar konkrētajiem personas datiem);
15.3.3. Vai ir saglabāti attiecīgie personas dati un tie nav dzēsti;
15.3.4. Vai nav aizliegts sniegt pieprasīto informāciju datu subjektam (jāņem vērā, ka pārzinis var netikt uzskatīts par juridisko informācijas resursu turētāju valsts nozīmes informācijas sistēmās (piemēram, Valts izglītības informācijas sistēma, Iedzīvotāju reģistrs u.c.) un pārzinim ir pieeja tikai daļai datu, kas šajās informācijas sistēmās ir saglabāti);
15.3.5. Vai pieprasījumu var veikt, ieguldot tā izpildē saprātīgas pūles (tas ir, pieprasītie dati atrodas automatizētās sistēmās (elektroniskā formā) vai personas datu apkopojums, kas sakārtots pēc kartotēkas/ katalogu principa, vai pieprasījums aptver samērīgu laika posmu, vai pieprasījums pēc būtības vērsts pārziņa darbības ievērojamai traucēšanai).
15.4. Ja konstatējama viena vai vairākas negatīvas atbildes uz Noteikumu 15.3.apakšpunktā norādītajiem jautājumiem, ir pamats nesniegt atbildi datu subjektam pēc būtības, bet norādīt uz trūkumiem, kas jānovērš, ja tas ir iespējams (piemēram, jāprecizē meklējamais datu subjekts, attiecīgi dati ir dzēsti u.tml.), un datu subjektam jāsniedz atkārtots pieprasījums. Ja

vairāk netiek glabāti pieprasītie personas dati, tad tiek informēts datu pieprasītājs, ka rīcībā nav attiecīgā informācijas.

15.5. Saskaņā ar Regulas 15.-22.pantu datu subjektam realizējot savas tiesības un iesniedzot attiecīgu pieprasījumu, informāciju atbilstoši šo Noteikumu 7.pielikumam sagatavo un datu subjektam pēc tā pieprasījuma sniedz attiecīgās pilnvarotās personas vai, gadījumos, kad šādu pieprasījumu iesniegusi pilnvarotā persona, - pilnvarotās personas tiešais vadītājs.

15.6. Ja datu subjekts pieprasa dzēst visus vai daļu par viņu uzkrātajiem personas datiem pilnvarotā persona izvērtē, vai attiecīgais pieprasījums atbilst Regulas 17.panta norādītajiem kritērijiem:

15.6.1. Personas dati vairs nav nepieciešami to nolūku sasniegšanai, kādiem attiecīgie personas dati tika vākti vai citādi apstrādāti;

15.6.2. Datu subjekts atsauc savu piekrišanu, ja datu apstrāde tika veikta uz piekrišanas pamata (Regulas 6.panta 1.punkta a)apakšpunkts), un nav piemērojams nekāds cits likumīgs personas datu apstrādes pamats (piemēram, Regulas 6.panta 1.punkta f)apakšpunkts);

15.6.3. Datu subjekts iebilst pret attiecīgo personas datu izmantošanu automatizēta individuāla lēmuma pieņemšanai attiecībā uz viņu un attiecīgo personas datu apstrādei nav piemērojams cits likumīgs personas datu apstrādes pamats;

15.6.4. Personas dati ir apstrādāti nelikumīgi;

15.6.5. Personas dati ir jādzēš, lai nodrošinātu attiecībā uz pārzini piemērojamo normatīvo aktu prasības;

15.6.6. Vai personas dati ir savākti saistībā ar informācijas sabiedrības pakalpojumu piedāvāšanu, kā minēts Regulas 8.pants 1.punktā.

15.7. Ja attiecīgais pieprasījums atbilst vismaz vienam Noteikumu 15.6.apakšpunktā uzskaitītajiem kritērijiem, pilnvarotā persona nodrošina attiecīgo datu subjekta personas datu vai to daļu dzēšanu.

15.8. Ja pārzinis ir publiskojis personas datus, kuri jādzēš atbilstoši 15.6.apakšpunktam, pilnvarotā persona, ņemot vērā pieejamo tehnoloģiju un tās piemērošanas izmaksas, veic saprātīgus pasākumus, tostarp tehniskus pasākumus, lai informētu pārziņus, kas veic personas datu apstrādi, ka datu subjekts ir pieprasījis, lai minētie pārziņi dzēstu visas saites uz minētajiem personas datiem un to atveidojumiem.

15.9. Saskaņā ar Regulas 16.pantu, 17.panta 1.punktu, 18.pantu un ievērojot Regulas 19.panta prasības, pēc datu subjekta pieprasījuma veikto personas datu labošanas, precizēšanu, to apstrādes ierobežošanas vai dzēšanas, iestāde vai kapitālsabiedrība, kura ir veikusi attiecīgās izmaiņas personas datu apstrādē, vadība nodrošina nepilnību vai pārkāpumu novēršanu un informācijas sniegšanu datu subjektam mēneša laikā atbilstoši šo Noteikumu 8.pielikumam un trešajai personai, kas iepriekš ir saņēmusi minētos datus, - atbilstoši šo Noteikumu 2.pielikumam par personas datu papildināšanu, precizēšanu, apstrādes ierobežošanu vai dzēšanu.

15.10. Lai nodrošinātu pilnīgas informācijas pārskatu par pieprasījumu iesniegšanas personas datu apstrādi, pilnvarotā persona, sagatavojot informāciju datu subjektam par personas datu apstrādi un personas datiem, ja nepieciešams, pieprasa informāciju par personas datu apstrādi un personas datiem arī no citām iestādēm un kapitālsabiedrībām.

15.11. Visi datu subjekta iesniegtie iesniegumi vai pieprasījumi, t.sk., arī mutiski informācijas pieprasījumi, tiek pieņemti un reģistrēti atbilstoši apstiprinātajai dokumentu aprites kārtībai.

15.12. Atbilde datu subjektam jānoformē atbilstoši normatīvajos aktos noteiktajai kārtībai, jāreģistrē un jānosūta datu subjektam atbilstoši apstiprinātajai dokumentu aprites kārtībai.

16. Personas datu glabāšanas termiņi un dzēšana

16.1. Personas datu glabāšana ir viens no personas datu apstrādes veidiem, kad apstrādājamie personas dati tiek saglabāti atkārtotai un vairākkārtējai lietošanai.

16.2. Personas datu glabāšanas termiņš konkrētās apstrādes ietvaros ir atkarīgs no attiecīgai apstrādei noteiktajiem apstrādes nolūkiem.
16.3. Personas datu glabāšanas termiņi attiecīgajām apstrādēm ir noteikti iekšējos vai ārējos normatīvajos aktos (piemēram, lietu nomenklatūra).
16.4. Pēc tam, kad ir notecējis attiecīgās apstrādes ietvaros saglabāto personas datu glabāšanas termiņš un nav piemērojami citi pamatojumi attiecīgo personas datu apstrādē, pilnvarotajai personai ir jānodrošina personas datu dzēšana, par to sastādot attiecīgo dokumentu, vai jānodod attiecīgais dokuments glabāšanā valsts arhīvam saskaņā ar Arhīvu likuma prasībām.

17. Informācijas nesēju glabāšana, iznīcināšana un aizsardzības pasākumi pret ārkārtas apstākļiem

17.1. Informācijas nesēju glabāšanu, iznīcināšanu un aizsardzības pasākumus pret ārkārtas apstākļiem (piemēram, ugunsgrēku, plūdiem) organizē saskaņā ar ārējiem normatīvajiem aktiem un iekšējiem normatīvajiem aktiem un rīkojumiem, ierobežotas pieejamības informācijas aizsardzību, apriti un dokumentu pārvaldību, informācijas sistēmas drošību, ugunsdrošības pasākumu organizēšanu un rīcību ārkārtu situāciju gadījumos reglamentējošās jomās.
17.2. Atkarībā no iespējamo zaudējumu apjoma vadība nodrošina pietiekamu serveru un serveru telpu aizsardzību pret fiziskiem apdraudējumiem, nepieciešamības gadījumā ierīkojot apsardzes un ugunsdzēsības signalizāciju, automātiskās ugunsdzēšanas sistēmu u.tml.
17.3. Personas datu apstrādes telpās vai to tuvumā ir novietoti ugunsdzēsības aparāti (pulvera vai ogļskābās gāzes).
17.4. Nepiederošas personas, t.sk. ārējie pakalpojumu sniedzēji serveru telpās drīkst uzturēties tikai pilnvarotu personu pavadībā.
17.5. Vadība nodrošina, ka visas informācijas sistēmas tiek ekspluatētas ierobežotas pieejamības, slēdzamās telpās, kuru fiziskā aizsardzība nodrošina tikai pilnvarotu personu piekļuvi, vai nodrošina serveru fizisko aizsardzību, lai tos nevarētu izslēgt, pārvietot, bojāt un nesankcionēti mainīt to konfigurāciju. Serveru telpas izvieto ēkas vietās, kurās ir mazāka apdraudējuma īstenošanās iespējamība.
17.6. Informācijas nesēju glabāšana un iznīcināšana notiek saskaņā ar normatīvo aktu prasībām un izdotajiem iekšējiem normatīvajiem aktiem.
17.7. Papīra dokumenti tiek uzglabāti atbilstoši noteikumiem iekārtotā arhīva telpā vai attiecīgajā zonālā valsts arhīva telpās, saskaņā ar lietu nomenklatūru.
17.8. Elektronisko dokumentus arhivē uz pilnvaroto personu datoriem vai serveriem, kā arī nodoti zonālā valsts arhīva telpās, saskaņā ar lietu nomenklatūru.
17.9. Pēc glabāšanas termiņa beigām dokumenti papīra formā tiek sagriezti ar dokumentu smalcinātāju, bet automatizētiem – neatgriezeniski dzēsti.
17.10. Par datu glabāšanu un iznīcināšanu ir atbildīga atbildīgā persona par arhīvu.
17.11. Jautājumos, kas saistīti ar elektronisko datu glabāšanu un iznīcināšanu serveros vai pilnvaroto personu datoros, atbildīgā persona par arhīvu sadarbojas ar sistēmu administratoru un datora lietotāju.

18. Noteikumu pārskatīšana un aktualizācija

18.1. Pārzinis nodrošina regulāru (vienu reizi 12 mēnešos) īstenotās personas datu apstrādes un aizsardzības prakses, analīzi, attiecīgi koriģējot normatīvo aktu vai noslēgto līgumu noteikumus.
18.2. Pārzinim ir pienākums pārskatīt īstenoto personas datu apstrādes un aizsardzības praksi, ja:
18.2.1. Noticis Incidents, par kuru pārzinis ziņojis datu subjektam un Datu valsts inspekcijai;
18.2.2. Tiek veiktas vai plānotas veikt nozīmīgas izmaiņas datubāzē (par nozīmīgām izmaiņām uzskatāmas tādas, kas ietekmē apstrāžu pamatojumu, nolūku, datu apjomu, veidu, struktūru, kopējo drošību un datu nodošanas kārtību ārpus ES vai EEZ dalībvalstīm);

18.2.3. Tiek apvienotas datubāzes/personas datu apstrādes;
18.2.4. Tiek izveidotas jaunas datubāzes/personas datu apstrādes;
18.2.5. Tiek ieviestas jaunas datu apstrādes tehnoloģijas vai metodes.

18.3. Nodrošinot personas datu apstrādes un aizsardzības prakses pārskatīšanu, pārzinim ir jādokumentē veiktā izvērtēšana (arī gadījumos, kad netiek veiktas nekādas izmaiņas un esošā kārtība atzīstama par piemērotu turpmākajai darbībai) un izmaiņas, norādot:
18.3.1. Kādas izmaiņas ir veiktas;
18.3.2. Vai un kā attiecīgās izmaiņas ietekmē datu subjekta tiesības un brīvības;
18.3.3. Ja veiktās izmaiņas negatīvi ietekmē datu subjekta tiesības un brīvības, jānorāda pamatojums attiecīgo izmaiņu veikšanai, kā arī veiktie pasākumi, līdz līdzsvarotu datu subjektu tiesību un brīvību ierobežojumu vai riskus.

19. Citi noteikumi

19.1. Pilnvarotā persona aizpilda apliecinājumu (1.pielikums) par apņemšanos saglabāt un nelikumīgi neizpaust personas datus, kā arī saņem normatīvajos aktos noteikto informāciju par savu datu apstrādi. Parakstīto apliecinājumu pilnvarotās personas tiešais vadītājs nodod glabāšanai atbildīgajai personai par personāla uzskaiti. Par pilnvarotās personas informēšanu un apliecinājuma parakstīšanu un nodošanu atbildīgajai personai par personāla uzskaiti ir atbildīgs tiešais vadītājs.
19.2. Noteikumi stājas spēkā ar to apstiprināšanas brīdi.
19.3. Notikumu oriģināls glabājas pie pārziņa.
19.4. Noteikumu kopijas atrodas pārziņa struktūrvienībās, iestādēs un kapitālsabiedrībās.

Vecumnieku novada pašvaldības Domes priekšsēdētāja vietā –
Domes priekšsēdētāja vietnieks *J.Kovals*

1.pielikums
Vecumnieku novada Domes 2019.gada 23.oktobra
iekšējiem noteikumiem Nr.1-9/2019/18
„Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi"

APLIECINĀJUMS

Es, _____
(vārds, uzvārds, personas kods)

apņemos:

1. apstrādāt, saglabāt un nelikumīgi neizpaust personas datus, kas man kļūst zināmi un būs pieejami, pildot amata pienākumus;
2. ziņot par prettiesiskiem mēģinājumiem iegūt no manis personas datus saturošu informāciju, kā arī man zināmiem datu aizsardzības pārkāpumiem;
3. pārtraucot darba līguma un/vai citas tiesiskās attiecības ar pārzini jebkādu iemeslu dēļ, es nekavējoties nodošu pārzinim man rīcībā esošo aprīkojumu, kā arī man rīcībā esošos informācijas orģinālus un kopijas, ko esmu saņēmis(-usi) darba (līguma izpildes) laikā, un kura ir manā rīcībā vai kura ir citādi tieši vai netieši manā rīcībā;
4. saglabāt informācijas konfidencialitāti arī pēc darba līguma un/vai jebkādu citu tiesisku attiecību izbeigšanas.

Ar šo apliecinu, ka esmu brīdināts(-a), ka personas datu izpaušanas gadījumā varu tikt saukts(-a) pie normatīvajos aktos noteiktās atbildības un uzņemos atbildību par savas darbības rezultātā pieļautajām kļūdām un radītajiem zaudējumiem saistībā ar dalību personas datu apstrādē.

Ar šo apliecinu, ka esmu iepazinies(-usies) un man ir skaidri Vecumnieku novada Domes 2019.gada 23.oktobra iekšējie noteikumi Nr.1-9/2019/18 „Vecumnieku novada domes pašvaldības personas datu aizsardzības noteikumi", kā arī apņemos ievērot šajos noteikumos ietvertās prasības.

20___.gada ___._____ _____ _____
(vārds, uzvārds) *(paraksts)*

2.pielikums
Vecumnieku novada Domes 2019.gada 23.oktobra
iekšējiem noteikumiem Nr.1-9/2019/18
„Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi”

PARAUGS

VECUMNIEKU NOVADA DOME
Reģ. Nr. 90009115957, Rīgas iela 29, Vecumnieki, Vecumnieku pagasts, Vecumnieku novads, LV-3933
Tālr. 63976100, fakss 63960524, e-pasts vecumnieki@vecumnieki.lv

Vecumnieku novada Vecumnieku pagastā

_____ Nr. _____
(datums)

_____
(vārds, uzvārds)

_____
(adrese)

Par personas datu labošanu

Saskaņā 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 un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (turpmāk – Regula) 19.pantu informējam, ka Vecumnieku novada dome 20____.gada ____._____ vēstulē Nr._____ Jums sniedza informāciju par _____ *(Norāda konkrēta datu subjekta datus (vārds, uzvārds, personas kods un citu informāciju), ja tie minēti iepriekš sniegtajā informācijā, un neprecīzo, kļūdaino informāciju, kas tiek iepriekš sniegta trešajai personai)*

Pēc datu subjekta pieprasījuma Jums iepriekš sniegtā informācijā ir veiktas izmaiņas attiecībā uz _____
(Norāda, kas konkrēti tiek veikts, - papildināti, precizēti, laboti personas dati, ierobežota apstrāde u.c.; trešajām personām precizēto, laboto informāciju sniedz, ja konkrētajā brīdī joprojām nav zudis trešās personas datu apstrādes tiesiskais pamats un mērķis)

Izpilddirektors *(paraksts)* _____
(vārds, uzvārds)

Dok. izstrādātāja
Uzvārds
Tālruņa numurs
E-pasts

3.pielikums
Vecumnieku novada Domes 2019.gada 23.oktobra
iekšējiem noteikumiem Nr.1-9/2019/18
„Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi”

Paziņojums par personas datu aizsardzības pārkāpumu

Iesnieguma veids	Sākotnējais iesniegums

1. Informācija par pārzini

1.1. Kontaktinformācija

Pārziņa nosaukums	
Reģistrācijas Nr.	
Juridiskā adrese	
Iesniedzējs	☐ pilnvarotā persona ☐ paraksttiesīgā persona
Iesniedzējs (vārds, uzvārds)	
Atbildīgā kontaktpersona (vārds, uzvārds)	
Atbildīgās personas amats	
Elektroniskā pasta adrese	
Tālruņa numurs	

2. Laika grafiks

Pārkāpuma konstatēšanas datums	
Iemesls novēlotai paziņošanai par pārkāpumu	

3. Informācija par pārkāpumu

Konfidencialitāte (nesankcionēta izpaušana vai nesankcionēta piekļuve)	☐
Integritāte (notikušas izmaiņas)	☐
Pieejamība (dati ir zaudēti vai iznīcināti)	☐

Pārkāpuma raksturs:	
ierīce ir nozaudēta vai nozagta;	☐
dokuments ir nozaudēts vai atstāts brīvi pieejamā vietā;	☐
pasts (papīra formātā) ir nozaudēts vai piegādāts atvērts;	☐
urķēšana;	☐
ļaunprogrammatūra;	☐
pikšķerēšana;	☐
nepareiza personas datu iznīcināšana papīra formātā;	☐
E-atkritumi (personas dati atrodas novecojošā ierīcē);	☐
nepārdomāta publikācija;	☐
izpausti personas dati citam/nepareizajam datu subjektam;	☐
personas dati nosūtīti nepareizajam adresātam;	☐
verbāla nesankcionēta personas datu izpaušana;	☐
cits	☐
„Cits" pārkāpuma raksturs (apraksts)	
Pārkāpuma cēlonis:	
iekšēja neapzināta ļaunprātīga rīcība (iekšējās politikas pārkāpums);	☐
iekšēja ļaunprātīga rīcība;	☐
ārēja neļaunprātīga rīcība;	☐
ārēja ļaunprātīga rīcība;	☐
cits	☐
„Cits" pārkāpuma cēlonis (apraksts)	

4. Par apdraudēto datu kategoriju

Aptuvenais personas datu ierakstu skaits, kurus skar pārkāpums	

4.1. Vispārējie dati:

datu subjekta identitāte (vārds, uzvārds,	☐

dzimšanas datums);	
nacionālais identifikācijas numurs;	
kontaktinformācija;	
identificējošie dati;	
oficiālie dokumenti;	
atrašanās vietas dati;	
informācija par kriminālsodāmību un/vai nodarījumiem	

4.2. Īpašās datu kategorijas:

dati, kas atklāj rasi vai etnisko piederību;	
politiskie uzskati;	
reliģiskie vai filozofiskie uzskati;	
dalība arodbiedrībā;	
dati par seksuālo dzīvi;	
veselības dati;	
ģenētiskie dati;	
biometriskie dati;	
nav vēl zināms;	
cits	

„Cits" apraksts	

5. Informācija par datu subjektiem:

nodarbinātie;	
lietotāji;	
abonētāji;	
studenti;	
militārais personāls;	
klients (pašreizējie un potenciālie);	
pacienti;	
nepilngadīgie;	
neaizsargātas personas;	
vēl nav zināms;	
cits	

Detalizēts iesaistīto datu subjektu apraksts	

Aptuvenais personu skaits, uz kurām attiecas pārkāpums	

6. Par pasākumiem, kas ieviesti pirms pārkāpuma

7. Sekas

7.1. Konfidencialitātes pārkāpums:

plašāka izpaušana, kā nepieciešama mērķa sasniegšanai, vai kādai piekrituši datu subjekti;	☐
apstrādātie dati var būt saistīti ar datu subjekta citu informāciju;	☐
dati var tikt izmantoti citiem mērķiem un/vai negodprātīgā veidā;	☐
cits	☐

„Cits" konfidencialitātes pārkāpuma seku apraksts	

7.2. Integritātes pārkāpums:

dati ir/var būt modificēti un tiek izmantoti, kaut arī tie vairs nav derīgi;	☐
dati ir/var būt modificēti citos derīgos datos un izmantoti citiem mērķiem;	☐
cits	☐

„Cits" integritātes pārkāpuma seku apraksts	

7.3. Pieejamības pārkāpums:

būtiska pakalpojuma sniegšanas iespējas zudums ietekmētajiem datu subjektiem;	☐
būtiska pakalpojuma sniegšanas iespējas maiņa ietekmētajiem datu subjektiem;	☐
cits	☐

„Cits" pieejamības pārkāpuma seku apraksts	

7.4. Fiziski, materiāli vai nemateriāli kaitējums vai būtiskas sekas datu subjektiem:

potenciālās ietekmes uz datu subjektu apraksts zaudēta kontrole pār saviem personas datiem;	☐
ierobežotas personas tiesības;	☐
diskriminācija;	☐
identitātes zādzība;	☐
krāpšana;	☐
finansiālais zaudējums;	☐
neatļauta pseidonimizācijas atcelšana;	☐
kaitējums reputācijai;	☐
personas datu, ko aizsargā dienesta noslēpums, konfidencialitātes zaudēšana;	☐
cits	☐

„Cits" potenciālās ietekmes uz datu subjektu apraksts	

Iespējamo datu pārkāpuma ietekmes seku datu subjektam novērtējums:

nenozīmīgs;	☐
maznozīmīgs;	☐
nozīmīgs;	☐
ļoti nozīmīgs	☐

8. Veicamās darbības

8.1. Paziņošana datu subjektam

Datu subjekta informēšana:

jā;	☐
nē, bet informēts;	☐
nē, netiks informēts;	☐
nav zināms	☐

Iemesls, kāpēc datu subjekts netiks informēts par datu pārkāpumu:

kontrolieris ir ieviesis atbilstošus tehniskos un organizatoriskās prasības un piemērojis personas datu pārkāpuma skartajiem personas datiem, it īpaši tiem, kuri ir neaizsargāti, brīvi pieejami citām neautorizētām personām;	☐
kontrolieris ir veicis atbilstošas darbības, kas nodrošina, ka datu subjekta tiesības un brīvība turpmāk nematerializēsies;	☐

tas ietvertu nesamērīgus pūliņus, lai katru datu subjektu informētu individuāli;	
Informācija nav nepieciešama	
Datu subjektam sniegtās informācijas saturs pievienots pielikumā	
Informācija nav nepieciešama	

8.2. Pārziņa veiktie pasākumi pārkāpuma ietekmes mazināšanai

Apraksts pasākumus, ko pārzinis veicis, lai mazinātu pārkāpuma ietekmi	

8.3. Pārrobežu un citi paziņojumi

Vai šis paziņojums ir sagatavots kā pārrobežu paziņojums, kas nosūtīts vadošajai uzraudzības iestādei?	
ES valsts saraksts, uz kurām attiecas datu pārkāpums (jānorāda valsts kods, piemēram: EN, FR u.tml.)	

4.pielikums
Vecumnieku novada Domes 2019.gada 23.oktobra
iekšējiem noteikumiem Nr.1-9/2019/18
„Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi”

PARAUGS

VECUMNIEKU NOVADA DOME
Reģ. Nr. 90009115957, Rīgas iela 29, Vecumnieki, Vecumnieku pagasts, Vecumnieku novads, LV-3933
Tālr. 63976100, fakss 63960524, e-pasts vecumnieki@vecumnieki.lv

Vecumnieku novada Vecumnieku pagastā

_____ Nr. _____
(datums)

_____
(vārds, uzvārds)

_____
(adrese)

Par personas datu aizsardzības pārkāpumu

Diemžēl esam spiesti paziņot, ka mūsu veiktajā personas datu apstrādē ir noticis personas datu aizsardzības pārkāpums (turpmāk – incidents), kas skar Jūsu personas datus. Saskaņā ar likumā noteikto esam iesnieguši Datu valsts inspekcijā paziņojumu par personas datu aizsardzības pārkāpumu. Šobrīd tiek veikts darbs, lai mazinātu incidenta negatīvo ietekmi uz personas datiem. Incidents visticamāk iestājies šādu notikumu rezultātā:

_____
(notikuma apraksts)

Incidenta rezultātā negatīvai ietekmei pakļauti/skarti šādi personas dati/personas datu kategoriju/veids:

_____
(personas datu veidi/kategoriju saraksts: vārds, uzvārds, tālruņa numurs, adrese, u.tml.)

Mūsuprāt attiecībā uz Jums incidents var radīt šādas sekas:

_____
(reālo potenciālo negatīvo seku apraksts)

Lai mazinātu incidenta kaitīgās sekas, iesakām nekavējoties:

_____
(ieteicamās darbības – paroles maiņa, u.tml.)

Lai nodrošinātu, ka šādi vai līdzīgi incidenti neatkārtotos, Vecumnieku novada pašvaldība (turpmāk – Pašvaldība) nodrošinās:

_____
(veikto/plānoto aizsardzību pasākumu apraksts, nav pienākuma norādīt konfidenciālu vai pārzinim būtisku informāciju, ja vien tas nav būtiski datu subjekta pārliecināšanai)

Lai iegūtu papildu informāciju par incidentu aicinām sazināties ar Pašvaldības atbildīgo personu datu aizsardzības jautājumos – datu aizsardzības speciālistu _____.
(vārds, uzvārds, tālruņa numurs, e-pasts)

Pašvaldība no savas puses atvainojas par radītajām neērtībām, kā arī apņemas veikt visus iespējamos pasākumus minētā incidenta radīto seku mazināšanai un situācijas risinājuma panākšanai pārrunu ceļā.

Izpilddirektors *(paraksts)* _____
(vārds, uzvārds)

Dok. izstrādātāja
Uzvārds
Tālruņa numurs
E-pasts

5.pielikums
Vecumnieku novada Domes 2019.gada 23.oktobra
iekšējiem noteikumiem Nr.1-9/2019/18
„Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi”

Ziņojums par datu apstrādes incidentu

Darbinieka informācija:

Vārds, uzvārds	
Amats	
Elektroniskā pasta adrese	
Tālruņa numurs	

Laika grafiks:

Pārkāpuma konstatēšanas datums un laiks: 20___.gada ___._____ plkst. ___:___

Iemesls novēlotai paziņošanai par datu pārkāpumu *(ja piemērojam)*	

Incidenta raksturs:

- ☐ Nozagta vai nozaudēta ierīce
- ☐ Nozaudēts dokuments vai atstāts brīvi pieejamā vietā
- ☐ Pasts (papīra formātā) ir nozaudēts vai piegādāts atvērts
- ☐ Urķēšanas (hacker) uzbrukums, nesankcionēta piekļuve e-pastiem/datnēm
- ☐ Pikšķerēšana (ar viltu iegūti dati, parole (-es)/mēģinājums izkrāpt datus)
- ☐ Nepareiza personu datu izmantošana papīra formātā
- ☐ E-atkritumi (personas dati atrodas novecojušā ierīcē)
- ☐ Nepārdomāta publikācija
- ☐ Izpausti personas dati citam/nepareizajam datu subjektam
- ☐ Personas dati nosūtīti nepareizam adresātam
- ☐ Verbāla nesankcionēta personas datu izpaušana
- ☐ Cits

„Cits” incidenta raksturs	

Incidenta apmērs:

Aptuvenais datu ierakstu un/vai ietekmēto datu subjektu skaits	

Incidentā skartie dati:

- ☐ Datu subjekta identitāte (vārds, uzvārds, dzimšanas datums)
- ☐ Nacionālais identifikācijas numurs
- ☐ Personas kods
- ☐ Kontaktinformācija (tālruņa numurs, e-pasts, adrese)
- ☐ Identificējoši dati (fotoattēls, videonovērošanas ieraksts, īpašas pazīmes, u.tml.)
- ☐ Ekonomiskie un finanšu dati (maksājumi, norēķinu informācija)
- ☐ Atrašanās vietas dati (videonovērošanas ieraksti, GPS informācija)

- ☐ Informācija par krimināLsodāmību un/vai nodarījumiem
- ☐ Dati, kas atklāj rasi un etnisko piederību
- ☐ Politiskie uzskati
- ☐ Reliģiskie vai filozofiskie uzskati
- ☐ Dalība arodbiedrībā
- ☐ Dati par seksuālo dzīvi
- ☐ Veselības dati (slimības vēsture, diagnoze, veiktās manipulācijas)
- ☐ Ģenētiskie dati
- ☐ Biometriskie dati
- ☐ Cits

„Cits" apraksts	

Ietekmētās datu subjekta kategorijas:

- ☐ Nodarbinātie
- ☐ Lietotāji
- ☐ Nepilngadīgie
- ☐ Klients (pašreizējie un potenciālie)
- ☐ Pacienti
- ☐ Neaizsargātas personas
- ☐ Vēl nav zināms
- ☐ Cits

„Cits" apraksts	
Detalizēts ietekmēto datu subjektu apraksts	
Darbinieka paskaidrojums un incidenta apraksts brīvā formā, t.sk. veiktie pasākumi incidenta ietekmes mazināšanai	

_____ _____

(datums) *(paraksts)*

6.pielikums
Vecumnieku novada Domes 2019.gada 23.oktobra
iekšējiem noteikumiem Nr.1-9/2019/18
„Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi"

Par _____ apstrādātajiem fizisko personu datiem
(iestādes, kapitālsabiedrības, nodaļas nosaukums)

Aizpildot tabulu par attiecīgajā iestādēs, kapitālsabiedrības, nodaļas apstrādātajiem fiziskās personas datiem, vēlams norādīt vismaz šādu informāciju (tabula var tikt precizēta izdodot rīkojumu par datu apstrādi).

1.	Datu subjekta kategorija (darbinieki, klienti, semināru apmeklētāji utt.)	
2.	Datu kategorijas – precīzi jānorāda, tieši kādi (piemēram: vārds, uzvārds, tālruņa numurs, vecums, personas kods utt.)	
3.	Ar datiem veicamās darbības (vākšana, glabāšana, sistematizēšana – elektroniski, papīra formā, publiskošana u.c.)	
4.	Datu apstrādes juridiskais pamatojums (likuma pants/ līgumsaistības/ personas piekrišana u.c.)	
5.	Datu apstrādes nolūks	
6.	Kur un cik ilgi dati tiek glabāti	
7.	Kādā veidā tiek organizēta personas piekrišanas izteikšana datu apstrādei un glabāšanai (vai piekrišana izteikta rakstveidā)	
8.	Kādā veidā (ar fiziskiem vai programmatūras līdzekļiem) tiek nodrošināta datu aizsardzība	
9.	Kas šos datus apstrādā (amats)	
10.	Kam ir piekļuve datiem un cik lielā apjomā	
11.	Kādos gadījumos personas datus izsniedz trešajām personām	
12.	Kādā veidā notiek personas datu aktualizēšana un cik bieži	
13.	Kādā veidā dati tiek iznīcināti	
14.	Personas tiesības piekļūt saviem personas datiem un izdarīt tajos labojumus	
15.	Cita nozīmīga informācija (ja nepieciešams)	

7.pielikums
Vecumnieku novada Domes 2019.gada 23.oktobra
iekšējiem noteikumiem Nr.1-9/2019/18
„Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi”

PARAUGS

VECUMNIEKU NOVADA DOME
Reģ. Nr. 90009115957, Rīgas iela 29, Vecumnieki, Vecumnieku pagasts, Vecumnieku novads, LV-3933
Tālr. 63976100, fakss 63960524, e-pasts vecumnieki@vecumnieki.lv

Vecumnieku novada Vecumnieku pagastā

_____ Nr. _____
(datums)

_____
(vārds, uzvārds)

_____
(adrese)

Par informācijas sniegšanu

Vecumnieku novada dome (turpmāk – Pašvaldība) ir izskatījusi *(Adresāta vārds, uzvārds, personas kods, iesnieguma datums, numurs un tā satura izklāsts)* un sniedz šādu informāciju.

Saskaņā 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 un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (turpmāk – Regula) 15.pantu *(Atsauci uz konkrēto Regulas pantu un normatīvajiem aktiem norāda atkarībā no tā, kādu informāciju fiziskā persona ir pieprasījusi konkrētajā gadījumā)* informējam, ka Pašvaldība apstrādā Jūsu personas datus, lai nodrošinātu normatīvajos aktos noteikto pienākumu izpildi, sabiedrības interešu un īstenotu pilnvaru realizāciju, pamatojoties uz Regulas 6.panta 1.punkta c) un e)apakšpunktu, likuma „Par pašvaldībām” 15.pantā noteikto autonomo funkciju nodrošināšanai, Sociālo pakalpojumu un sociālās palīdzības likumā un citos normatīvajos aktos noteikto pienākumu un uzdevumu veikšanai.

(Turpmāk sadaļas aizpilda atkarībā no tā, kādu informāciju fiziskā persona ir pieprasījusi konkrētajā gadījumā)

Pašvaldības kā personas datu apstrādes pārziņa rīcībā ir šādu Jūsu personas datus saturoša informācija:
(Norāda visu informāciju par Pašvaldībā apstrādātajiem datu subjekta personas datiem, izmantojot personas datu apstrādes darbību reģistrā norādītās datu kategorijas)

- Datu subjekta tiesības piekļūt saviem personas datiem:

(Pēc šāda datu subjekta pieprasījuma sagatavo datu subjekta apstrādāto datu (nevis dokumentu) kopijas, piemēram, izdruku ar datu subjekta datiem no sistēmas vai aprakstot datu kopumu šajā atbildē)

- Personas datu saņēmēji vai saņēmēju kategorijas, kam personas dati ir izpausti vai kam tie varētu tikt izpausti (iespējamie datu saņēmēji):

(Norāda, kad, kam, kāda informācija sniegta par noteiktu laika posmu (ja ir fiksēts), datu saņēmēju kategorijas vai iespējamos datu saņēmējus atbilstoši personas datu apstrādes darbību reģistram; aizliegts iekļaut informāciju par valsts institūcijām, kuras ir kriminālprocesa virzītāji, operatīvās darbības subjekti, vai citām institūcijām, par kuriem saskaņā ar normatīvajiem aktiem ir aizliegts šādas ziņas izpaust)

- Paredzamais laikposms, cik ilgi personas dati tiks glabāti, vai, ja nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai:

(Norāda lietu nomenklatūrā noteikto glabāšanas termiņu attiecīgajam datu apstrādes veidam/klasifikācijai)

- Datu subjekta personas datu labošana vai dzēšana, vai personas datu apstrādes ierobežošanu vai tiesības iebilst pret šādu apstrādi:

(Ņemot vērā datu subjekta pieprasījumā norādīto argumentāciju. Ja rodas šaubas par pieprasījuma pamatotību, ir tiesības prasīt datu subjektam iesniegt papildu pieprasījumus par datu labošanas nepieciešamību)

- Personas datu ieguves avots, ja dati nav iegūti no datu subjekta:

(Piemēram, darba devēja sniegtā informācija, citas pašvaldības sniegtā informācija u.c., izmantojot deklarācijas, pārskatus, paziņojumus, iesniegumus, ziņojumus, izziņas, čekus, maksājuma uzdevumus, pārbaužu aktus, līgumus, lēmumus un nolēmumus, atzinumus, personas mutiski sniegto informāciju, plašsaziņu līdzekļos iegūto informāciju, vienotās pašvaldības informācijas sistēmas un pieejamo informāciju integrētajos valsts datu reģistros)

- Automatizētās apstrādes sistēmās izmantotās apstrādes metodes:

(Aizpilda, ja attiecībā uz datu subjektu Pašvaldībā ir pieņemti vai var tikt pieņemti individuāli automatizēti lēmumi)

Izpilddirektors *(paraksts)* _____
(vārds, uzvārds)

Dok. izstrādātāja
Uzvārds
Tālruņa numurs
E-pasts

8.pielikums
Vecumnieku novada Domes 2019.gada 23.oktobra
iekšējiem noteikumiem Nr.1-9/2019/18
„Vecumnieku novada pašvaldības personas datu aizsardzības noteikumi"

PARAUGS

VECUMNIEKU NOVADA DOME
Reģ. Nr. 90009115957, Rīgas iela 29, Vecumnieki, Vecumnieku pagasts, Vecumnieku novads, LV-3933
Tālr. 63976100, fakss 63960524, e-pasts *vecumnieki@vecumnieki.lv*

Vecumnieku novada Vecumnieku pagastā

_____ Nr. _____
(datums)

_____
(vārds, uzvārds)

_____
(adrese)

Par informācijas sniegšanu

Vecumnieku novada dome (turpmāk – Pašvaldība) ir izskatījusi *(Adresāta vārds, uzvārds, personas kods, iesnieguma datums, numurs un tā satura izklāsts)* un sniedz šādu informāciju.

Saskaņā 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 un ar ko atceļ Direktīvu 95/46/EK (Vispārīgā datu aizsardzības regula) (turpmāk – Regula) 16.-18.pantu *(Izvēlas atsauci uz atbilstošu Regulas 3.iedaļas pantu atkarībā no tā, ko tieši datu subjekts ir pieprasījis – datu labošanu, dzēšanu vai apstrādes ierobežošanu)* informējam, ka Pašvaldība apstrādā Jūsu personas datus, lai _____ *(Piemēram, lai gādātu par veselības aprūpes pieejamību, organizētu Pašvaldības iedzīvotāju komunālos pakalpojumus, nodrošinātu sociālo palīdzību u.tml.)*, izpildot uz Pašvaldību attiecināmu juridisku pienākumu, pamatojoties uz Regulas 6.panta 1.punkta c)apakšpunktu, *(Ieteicams iekļaut arī citus normatīvos aktus, kas reglamentā attiecīgo Pašvaldības darbības jomu)*

Pašvaldība pēc Jūsu sniegtās informācijas par nepieciešamību veikt Jūsu personas datu _____, ir veikusi šādas darbības:
(Norāda, kas konkrēti tika veikts, precizēti, laboti personas dati u.c.: trešajām personām, kurām iepriekš sniegti neprecīzi dati, sniedz informāciju tikai tad, ja nav zudis trešās personas datu apstrādes tiesiskais pamats un nolūks)

Izpilddirektors *(paraksts)* _____
(vārds, uzvārds)

Dok. izstrādātāja
Uzvārds
Tālruņa numurs
E-pasts