Rīgā 2020.gada 9.decembrī

VSIA „Latvijas Radio" Valdes

Lēmums Nr. 2-28/A1-7

Par VSIA „Latvijas Radio" iekšējo normatīvo aktu apstiprināšanu

VSIA „Latvijas Radio" valde, pamatojoties uz Elektronisko plašsaziņas līdzekļu likuma 65.panta pirmo daļu, Publiskas personas kapitāla daļu un kapitālsabiedrību pārvaldības likuma 80.pantu, VSIA „Latvijas Radio" Statūtu 8., 10.punktu, **nolemj**:

1. Apstiprināt Vispārīgo personas datu apstrādes un aizsardzības procedūru.

Pielikumā: *Vispārīgā personas datu apstrādes un aizsardzības procedūra uz 8 lpp.*

2. Apstiprināt Darbinieku personas datu apstrādes politiku.

Pielikumā: *Darbinieku personas datu apstrādes politika uz 12 lpp.*

3. Apstiprināt Personas datu aizsardzības pārkāpumu izmeklēšanas kārtību.

Pielikumā: *Personas datu aizsardzības pārkāpumu izmeklēšanas kārtība uz 14 lpp.*

Valdes priekšsēdētāja U.Klapkalne

Valdes locekle M.Tukiša

Valdes locekle S. Dika-Bokmeldere

e-pasts: struktūrdaļu vadītāji

APSTIPRINĀTS
ar 09.12.2020. valdes lēmumu Nr.2-28/A1-7

DARBINIEKU PERSONAS DATU APSTRĀDES POLITIKA

1. Politikā lietotie termini

Darbinieku personas datu apstrādes politikā (Politika) lietoto terminu definīcijas izriet no 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 tekstā – Regula, 4.panta:

1.1. **Personas dati** - jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu (Datu subjekts); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, tajā skaitā, bet ne tikai, personas vārdu, uzvārdu, personas kodu, dzimšanas datiem, dzīvesvietas adresi, darba vietu, tālruņa numuru, ģimenes stāvokli, e-pasta adresi, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.
1.2. **Īpašo personas datu kategorijas personas dati** - Personas dati, kas atklāj rasi vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, kā arī, ģenētiskie dati, biometriskie dati, lai veiktu fiziskas personas unikālu identifikāciju, veselības dati vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju.
1.3. **Personas datu apstrāde** - jebkuras ar Personas datiem vai Personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, pielāgošanu, sakārtošanu, pārveidošanu, izmantošanu, aplūkošanu, nodošanu, pārraidīšanu, izpaušanu, nosūtīšanu, izplatīšanu, saskaņošanu, ierobežošanu, bloķēšanu, dzēšanu vai iznīcināšanu. (Politika tiek piemērota jebkāda veida personas datu apstrādei – manuālai un datorizētai).
1.4. **Datu subjekts** - fiziskā persona, kuru var tieši vai netieši identificēt un kuras Personas dati tiek apstrādāti.
1.5. **Datu subjekta piekrišana** - jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz Datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu Personas datu apstrādei.
1.6. **Uzņēmums (Darba devējs)** – Valsts sabiedrība ar ierobežotu atbildību "Latvijas Radio", reģistrācijas numurs 40003080614, juridiskā adrese: Doma laukums 8, Rīga, LV-1505, e-pasta adrese: radio@latvijasradio.lv, tīmekļa vietne: www.latvijasradio.lsm.lv.
1.7. **Pārzinis** – Regulas izpratnē Uzņēmums ir pārzinis par Darbinieku Personas datiem, kurus Uzņēmums apstrādā šajā Politikā vai Datu apstrādes reģistrā norādītajiem mērķiem.
1.8. **Apstrādātājs** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura Pārziņa vārdā apstrādā Personas datus.

1.9. **Personas datu saņēmējs** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpaužPersonas datus – neatkarīgi no tā, vai tā ir trešā persona vai nav. Tomēr publiskas iestādes, kas var saņemt Personas datus saistībā ar konkrētu izmeklēšanu saskaņā ar Eiropas savienības vai dalībvalsts tiesību aktiem, netiek uzskatītas par saņēmējiem; minēto datu apstrāde, ko veic minētās publiskās iestādes, atbilst piemērojamiem datu aizsardzības noteikumiem saskaņā ar apstrādes nolūkiem.
1.10. **Trešā persona** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav Datu subjekts, Pārzinis, Apstrādātājs un personas, kuras Pārziņa vai Apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt Personas datus.
1.11. **Darbinieks** – persona, kura ar Uzņēmumu slēdz vai ir noslēgusi darba līgumu vai saskaņā ar citu civiltiesisku līgumu veic vai varētu veikt pienākumus, kuras Personas dati var tikt apstrādāti un kurai ir jāievēro šajā Politikā minētie Personas datu apstrādes nosacījumi.
1.12. **Datu aizsardzības speciālists** - Persona Uzņēmumā, kas ir sasniedzama izmantojot e-pasta adresi: datuaizsardziba@latvijaradio.lv, un kuram ir šādi uzdevumi: informēt un konsultēt Uzņēmumu, tā darbiniekus, uzraudzīt vai tiek ievērotas normatīvo aktu prasības attiecībā uz Personas datu aizsardzību, pēc pieprasījuma sniegt padomus par nepieciešamību sagatavot novērtējumu par ietekmi uz datu aizsardzību, sadarboties ar uzraudzības iestādi un būt par kontaktpunktu jautājumos, kas saistīti ar datu apstrādi (Regulas 37.pantā noteiktajā kārtībā iecelts datu aizsardzības speciālists, un kuram ir Regulas 39.pantā noteiktie uzdevumi).
1.13. **Žurnālistika** - Personas datu apstrāde, kuru veic, lai īstenotu tiesības uz vārda un informācijas brīvību, ievērojot personas tiesības uz privāto dzīvi, un netiek skartas tādas datu subjekta intereses, kurām nepieciešama aizsardzība un kuras ir svarīgākas par sabiedrības interesēm, attiecīgā datu apstrāde ir veikta ar mērķi publicēt informāciju, kas skar sabiedrības intereses un Regulas prasību ievērošana nav savietojama vai liedz īstenot tiesības uz vārda un informācijas brīvību.

2. Politikas mērķis un uzdevumi

2.1. Lai nodrošinātu godprātīgu, likumīgu un pārredzamu Darbinieku Personas datu apstrādi, Uzņēmums ir izstrādājis Politiku ar mērķi nodrošināt Uzņēmuma saimniecisko darbību, tiesiskās intereses un normatīvo aktu ievērošanu.
2.2. Politikas uzdevums ir nodrošināt Personas datu apstrādi Darbiniekiem pārredzamā un saprotamā veidā, izskaidrojot Uzņēmuma veiktās darbības ar Darbinieku Personas datiem, sniedzot informāciju par datu apstrādes nolūku, juridisko pamatu, informējot Darbiniekus par viņu tiesībām un pienākumiem saistībā ar viņu Personas datu apstrādi u.tml.

3. Darbinieku Personas datu apstrādes nolūki (mērķi)

3.1. Lai realizētu Darba devēja pienākumus un īstenotu Darba devēja vai Darbinieka konkrētas tiesības nodarbinātības, sociālā nodrošinājuma, sociālās aizsardzības tiesību jomā, kā arī nodrošinātu Darba devēja saimniecisko darbību, tiesiskās intereses un normatīvo aktu ievērošanu, Uzņēmumam kā Darba devējam ir nepieciešams apstrādāt Darbinieku Personas datus.

3.2. Darbinieku personas dati Uzņēmumā galvenokārt tiek izmantoti līgumattiecību nodibināšanai (piemēram, darba līguma vai cita civiltiesiska līguma noslēgšanai), to grozīšanai un no attiecīgā noslēgtā līguma izrietošo saistību izpildes nodrošināšanai un novērtēšanai. Līdz ar to Uzņēmums kā Darba devējs Darbinieku personas datus apstrādā šādiem nolūkiem (mērķiem):

3.2.1. **līgumattiecību nodibināšanai.** Darbinieku personas dati tiek apstrādāti pamatojoties uz Regulas 6.panta 1.punkta b) un c) apakšpunktu, kā arī Regulas 9.panta 2.punkta b) apakšpunktu. Personas datu apstrāde ir nepieciešama pasākumu veikšanai pirms attiecīgā līguma noslēgšanas ar Darbinieku (piemēram, Darbinieka identificēšanai personu apliecinošs dokuments un tā dati darba līguma sagatavošanai, obligātās veselības pārbaudes veikšanai, pieņemot darbā darbinieku, u.tml.), kā arī lai izpildītu uz Darba devēju attiecināmus juridiskus pienākumus (piemēram, prasību ziņot Valsts ieņēmumu dienestam par jauna Darbinieka pieņemšanu darbā) un atsevišķos gadījumos personas datu apstrādes tiesiskais pamats var būt Regulas 6.panta 1.punkta f) apakšpunkts, tas ir, lai Uzņēmums nodrošinātos ar pierādījumiem un spētu aizstāvēt savas tiesiskās intereses:

3.2.1.1. Darbinieka Personas datu apstrādi veic Darba devēja pilnvaroti darbinieki, kuri ir iesaistīti attiecīgā līguma projekta sagatavošanā. Normatīvajos aktos noteiktajos gadījumos un apmērā personas dati tiek nodoti arī Valsts ieņēmumu dienestam, Valsts arhīvam, kapitāla daļu turētājam un citām institūcijām. Atsevišķos gadījumos informācija var tikt nodota citām kontrolējošām institūcijām, piemēram, Valsts darba inspekcijai, Datu valsts inspekcijai u.tml. Personas datus nodot saņēmējiem ārpus Eiropas Savienības vai Eiropas ekonomiskās zonas valstīm, pārliecinoties, ka Eiropas Savienības iedzīvotāju personas datu apstrādē arī trešajās valstīs tiks piemērots līdzvērtīgs fizisko personu datu aizsardzības līmenis – datu apstrāde būs likumīga un samērīga, dati būs drošībā, tiks ievērotas datu subjekta tiesības kontrolēt savus datus;

3.2.1.2.Personas dati tiek glabāti normatīvajos aktos noteikto laika periodu;

3.2.1.3.Darbinieka Personas datu apstrāde ir nepieciešama, lai tiktu noslēgts attiecīgais līgums (piemēram, darba līgums vai cits civiltiesisks līgums) ar Darbinieku, kā arī lai Darba devējs varētu izpildīt pienākumus, kas tam ir noteikti ar spēkā esošajiem normatīvajiem aktiem;

3.2.1.4.ja Personas dati 3.2.1.apakšpunktā paredzētajam mērķim netiek sniegti, ar potenciālo Darbinieku nav iespējams noslēgt darba līgumu vai citu civiltiesisko līgumu;

3.2.2. **personālsastāva dokumentu uzskaitei un uzturēšanai**, lai uzglabātu svarīgu informāciju par Darbinieka darba izpildi, atalgojumu, apmācībām un uzvedību. Darbinieku personas dati tiek apstrādāti, pamatojoties uz Regulas 6.panta 1.punkta b) apakšpunktu un c) apakšpunktu. Apstrāde ir vajadzīga ar Darbinieku noslēgtā līguma izpildei, ka arī lai izpildītu uz Pārzini attiecināmus juridiskus pienākumus, tajā skaitā, lai izpildītu prasības, ko nosaka darba drošību reglamentējošie normatīvie akti. Atsevišķos gadījumos personas datu apstrādes tiesiskais pamats var būt Regulas 6.panta 1.punkta f) apakšpunkts, tas ir, lai Uzņēmums nodrošinātos ar pierādījumiem un spētu aizstāvēt savas tiesiskās intereses. Saskaņā ar Regulas 9.panta 2.punkta b) apakšpunktu apstrādes mērķis ir, lai izpildītu uz Uzņēmumu attiecināmus pienākumus nodarbinātības jomā, piemēram, izmeklētu nelaimes gadījumus darbā. Par Uzņēmuma leģitīmajām interesēm ir atzīstamas arī Darba devēja

tiesības veikt uzskaiti par Darbinieka darba izpildes kvalitāti un kvantitāti, darbalaika ievērošanu un kvalifikācijas celšanas apmācībām:

3.2.2.1. Darbinieka Personas datu apstrādi veic Uzņēmuma pilnvaroti darbinieki (personāla, grāmatvedības darbinieki, juristi, IT speciālisti, struktūrdaļu vadītāji u.c. darbinieki, kuru kompetencē ir darbs ar Personas datiem), kā arī normatīvajos aktos noteiktajos gadījumos un apmērā dati var tikt nodoti institūcijām, kurām datu nodošanu paredz normatīvie akti;

3.2.2.2. Darbinieka Personas dati tiek glabāti, normatīvajos aktos noteikto laika periodu. Vienlaicīgi, Uzņēmums paskaidro, ka informācija, kas raksturo Darbinieka darba izpildes aspektus, tiek glabāta visu darba tiesisko attiecību laiku;

3.2.2.3. Darbinieka personas datu apstrāde ir nepieciešama, lai varētu izpildīt saistības, kas izriet no attiecīgā darba līguma vai civiltiesiskā līguma ar Darbinieku, lai Darbinieks varētu veikt savus ikdienas darba pienākumu, kā arī lai Uzņēmums varētu izpildīt pienākumus, kas noteikti ar spēkā esošajiem normatīvajiem aktiem (aprēķināt un izmaksāt Darbiniekam darba samaksu). Ja Personas dati šajā apakšpunktā paredzētajam mērķim netiek sniegti vai apstrādāti, nav iespējams izpildīt normatīvo aktu prasības, kas izriet no attiecīgā darba līguma vai civiltiesiskā līguma saistības, un realizēt tiesības;

3.2.3. **grāmatvedības vajadzībām**. Darbinieku Personas dati tiek apstrādāti, pamatojoties uz Regulas 6.panta 1.punkta b) apakšpunktu un c) apakšpunktu. Personas datu apstrāde ir nepieciešama noslēgtā darba līguma un/vai cita civiltiesiskā līguma izpildei, kā arī lai izpildītu uz Uzņēmumu attiecināmu juridisku pienākumu (piemēram, darba samaksas nodrošināšana). Atsevišķos gadījumos personas datu apstrādes tiesiskais pamats var būt Regulas 6.panta 1.punkta f) apakšpunkts, tas ir, lai Uzņēmums nodrošinātos ar pierādījumiem un spētu aizstāvēt savas tiesiskās intereses:

3.2.3.1. Darbinieka Personas datu apstrādi veic Uzņēmuma pilnvaroti darbinieki (grāmatvedības darbinieki, Personālu daļas darbinieki, juristi, u.c. darbinieki, kuru kompetencē ir darbs ar Personas datiem) un normatīvajos aktos noteiktajos gadījumos un apmērā dati var tiek nodoti Valsts ieņēmumu dienestam u.c. iestādēm, kurām datu nodošanu paredz normatīvie akti. Personas datus var nodot saņēmējiem ārpus Eiropas Savienības vai Eiropas ekonomiskās zonas valstīm, pārliecinoties, ka Eiropas Savienības iedzīvotāju personas datu apstrādē arī trešajās valstīs tiks piemērots līdzvērtīgs fizisko personu datu aizsardzības līmenis – datu apstrāde būs likumīga un samērīga, dati būs drošībā, tiks ievērotas datu subjekta tiesības kontrolēt savus datus;

3.2.3.2. Personas dati tiek glabāti, normatīvajos aktos noteikto laika periodu;

3.2.3.3. Darbinieka Personas datu apstrāde ir nepieciešama, lai varētu izpildīt saistības, kas izriet no attiecīgā darba līguma un/vai cita civiltiesiska līguma ar Darbinieku, un/vai lai izpildītu normatīvo aktu prasības (piemēram, aprēķinātu un izmaksātu darbiniekiem darba algas, kompensētu izdevumus, analizējot Darbinieka veiktās telefona sarunas uzskaites vai iztērēto transportlīdzekļa degvielas limitu, veiktu aprēķinu par Darbinieka pārtērēto un atmaksai paredzēto naudas summu u.tml.). Ja Personas dati šajā apakšpunktā paredzētajam mērķim netiek sniegti, nav iespējams izpildīt normatīvo aktu prasības (veikt grāmatvedības uzskaiti) un/vai izpildīt no attiecīgā darba līguma vai cita civiltiesiskā līguma izrietošās saistības;

3.2.4. **līgumattiecību izpildei**, pildot ikdienas darba pienākumus, Darbinieka personas dati var tikt apstrādāti, lai Darba devējs varētu realizēt Darba devēja pienākumus, īstenotu Darba

devēja vai Darbinieka konkrētas tiesības nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības jomā, kā arī nodrošinātu savu saimniecisko darbību, uz Darba devēju attiecināmus juridiskus pienākumus vai lai aizsargātu savas un/vai trešo personu leģitīmās intereses, pamatojoties uz Regulas 6.panta 1.punkta b), c) un f) apakšpunktu un Regulas 9.panta 2.punkta b) apakšpunktu:

3.2.4.1. Šāda apstrāde var būt nepieciešama, piemēram, lai organizētu un nodrošinātu Uzņēmuma ikdienas darbu, lai nodrošinātu Darbinieku un citu personu profesionālo apmācību vai kvalifikācijas paaugstināšanu, lai nodrošinātu Darbinieku ar naktsmītni komandējuma laikā, vai lai Darbiniekam varētu sagatavot pilnvarojumu pārstāvēt Uzņēmumu, vai norādīt kā kontaktpersonu līgumos, vizītkartēs, e-pasta sūtījumos, piešķirtu pieejas tiesības (piemēram, lietotājvārdu un paroli) sadarbības partneru datu bāzēm vai sistēmām, ja tas nepieciešams darba pienākumu izpildei, informācijas nodošanai pakalpojumu sniedzējiem, lai nodrošinātu darba aizsardzības un drošības prasību izpildi u.c.;

3.2.4.2. Darbinieku darba telefonu, e-pastu, interneta un ierīču lietojums ikdienā netiek monitorēts, tomēr Darbiniekiem jāapzinās, ka Darba devējs kā Pārzinis to var veikt, ja Pārzinim rodas aizdomas par Darbinieka neētisku vai prettiesisku rīcību. Ievērojot minēto, Darbiniekam ir jāizvairās šajās ierīcēs apstrādāt privātu vai kādu citu informāciju, ko tas nevēlas, ka tā var nonākt Darba devēja rīcībā, tāpat Darbiniekam ir jāizvairās šajās ierīcēs un iekārtās apstrādāt citu personu privātu informāciju, kas nav nepieciešama, lai Darbinieks varētu pildīt savus amata pienākumus. Lai arī Pārzinis kā Darba devējs respektē žurnālistikas profesionālās darbības standartus (piemēram, informācijas avota aizsardzība), Darbiniekam ir jāatzīst, ka nolūkā veikt preventīvus pasākumus, lai nodrošinātos pret kiberuzbrukumiem, Darba devējam ir nepieciešams piekļūt un/vai veikt ierīču lietojuma monitoringu. Piemēram, lai novērstu iespēju instalēt ļaunatūras vai lai samazinātu riskus, kas var būt saistīti ar hakeru uzbrukumiem Pārziņa infrastruktūrai;

3.2.4.3. Personas dati var tikt nodoti pilnvarotiem Uzņēmuma darbiniekiem un sadarbības partneriem, klientiem, tiesībsargājošajām institūcijām, medicīniskās palīdzības vienībām, Valsts Ugunsdzēsības un glābšanas dienestam, apdrošināšanas kompānijai un citām fiziskām un juridiskām personām, ja šāda apstrāde izriet no normatīvo aktu prasībām vai ir nepieciešama saistībā ar Darbinieka veicamajiem pienākumiem, un bez datu nodošanas secināms, ka Darbinieks faktiski nevarēs veikt savus amata pienākumus vai arī Uzņēmumam būs pamatotas šaubas par pienākumu izpildes efektivitāti, kā arī Personas datu nodošana ir nepieciešama, lai nodrošinātu Uzņēmuma un trešo personu leģitīmās intereses;

3.2.4.4. Personas datus nav paredzēts nodot saņēmējiem ārpus Eiropas Savienības vai Eiropas ekonomiskās zonas valstīm. Tomēr atsevišķos gadījumos šāda nepieciešamība var rasties, piemēram, lai nodotu Darbinieka kontaktinformāciju sadarbības partnerim, kas atrodas ārpus Eiropas Savienības vai Eiropas ekonomiskās zonas valstīm, lai nodrošinātu Darbinieku ar naktsmītni komandējuma laikā valstī, kas nav Eiropas Savienības vai Eiropas ekonomiskās zonas dalībvalsts, ievērojot Vispārīgās datu aizsardzības regulas 49.panta nosacījumus;

3.2.4.5. apakšpunktā 3.2.4. minētajiem nolūkiem apstrādātie Personas dati var tikt glabāti, kamēr pastāv vismaz viens no šādiem kritērijiem:

3.2.4.5.1. kamēr ir spēkā un/vai tiek pilnībā izpildītas saistības, kas izriet no attiecīgā darba līgumu vai cita atbilstoša līguma;

3.2.4.5.2. kamēr pastāv iespēja, ka Pārzinim būs nepieciešams pierādīt savu saistību pienācīgu izpildi (atbilstoši vispārējo saistību tiesību noilguma termiņam – 10 gadi);

3.2.4.5.3. kamēr Pārzinim pastāv normatīvajos aktos noteikts pienākums glabāt attiecīgos datus (piemēram, likums par Grāmatvedību, Arhīvu likums un tiem pakārtotie normatīvie akti);

3.2.4.5.4. ja personas dati tiek apstrādāti, lai nodrošinātu Pārziņa vai trešās personas tiesiskās intereses, Personas dati var tikt glabāti līdz konkrētās tiesiskās intereses pilnīgai realizācijai;

3.2.4.6. Ja Personas dati šajā 3.2.4. apakšpunktā paredzētajam mērķim netiek sniegti, nav iespējams izpildīt normatīvo aktu prasības un no attiecīgā darba līguma vai civiltiesiskā līguma izrietošās saistības, kā arī Darbiniekam nav iespējams veikt viņa darba pienākumus (atsevišķos gadījumos - Darbinieks nevar izpildīt savas amata aprakstā minētās saistības), bet Darba devējam nav iespējams realizēt Darbinieka tiesības nodarbinātības (darba), sociālā nodrošinājuma vai sociālās aizsardzības tiesību jomā. Šādā gadījumā Darba līgums vai cits civiltiesisks līgums var tikt izbeigts.

3.3. Datu apstrāde saistībā ar priekšrocību izmantošanu:

3.3.1. Darbiniekiem, kuriem ir nepilngadīgi bērni vai citos priekšrocību gadījumos (grūtniecība, sievietes pēcdzemdību periodā, invaliditāte u.c.), normatīvajos aktos ir noteiktas atsevišķas papildu garantijas un priekšrocības tiesības. Ja Darbinieks vēlas izmantot šīs papildu garantijas vai priekšrocības tiesības (piemēram, apgādājamo gadījumā papildu atvaļinājumi vai brīvdienas, priekšrocības kā asins donoram u.tml.), Darbiniekam ir pienākums iesniegt attiecīgu iesniegumu ar pamatojumu un uzrādīt attiecīgo faktu apliecinošus dokumentus Uzņēmuma pilnvarotiem Darbiniekiem (personāla, grāmatvedības darbiniekiem u.c. darbiniekiem, kuru kompetencē ir darbs ar Personas datiem). Tāpat, ja Uzņēmums veic veselības apdrošināšanas polises iegādi Darbiniekiem, tad, ja Darbinieks nevēlas šīs priekšrocības izmantot, viņam ir pienākums par to informēt Uzņēmumu;

3.3.2. punktā 3.3.1. minētie personas dati tiek apstrādāti, pamatojoties uz Regulas 6.panta pirmā punkta a) apakšpunktu un apstrāde ir nepieciešama, lai Darbinieks varētu izmantot tiesības, kuras viņam piešķirtas jeb pienākas. Gadījumā, ja Darbinieks ir iesniedzis informāciju priekšrocību saņemšanai, tad Uzņēmums uzsāks Personas datu apstrādi, papildu pamatojoties uz Regulas 6.panta 1.punkta c) apakšpunktu, kas ir Uzņēmuma pienākumu izpilde normatīvajos aktos noteiktajos gadījumos (attiecībā uz papildu atvaļinājumiem vai papildu priekšrocības kā donoram), Regulas 6.panta 1.punkta f) apakšpunkta un nosacījumiem (papildu priekšrocības, kas tiek piešķirtas pēc darba devēja iniciatīvas, piemēram, veselības apdrošināšana), Regulas 6.panta 2.punkta b) apakšpunktu - līgumsaistību izpilde ar datu subjektu, kā arī lai nodrošinātos ar pierādījumiem, ka Pārzinis ir sniedzis Darbiniekam priekšrocības, kas tam pienākas saskaņā ar normatīvajiem aktiem;

3.3.3. Personas datu apstrādi veic Uzņēmuma pilnvaroti darbinieki (personāla, grāmatvedības darbinieki u.c. darbinieki, kuru kompetencē ir darbs ar Personas datiem). Personas datus nav paredzēts nodot saņēmējiem ārpus Eiropas Savienības vai Eiropas ekonomiskās zonas valstīm;

3.3.4. Personas dati šajā punktā minētajam mērķim tiek glabāti līdz brīdim, kad Darbinieks atsauc savu piekrišanu Personas datu apstrādei, bet ne ilgāk kā normatīvajos aktos noteiktajos termiņos. Informācija, kas piekrišanas rezultātā tikusi apstrādāta citiem mērķiem (piemēram, grāmatvedības vajadzībām, normatīvo aktu izpilde nodarbinātības jomā) tiks glabāta saskaņā ar normatīvajos aktos noteiktajiem glabāšanas laikposma noteikumiem šiem mērķiem un piekrišanas atsaukšana to neietekmēs;
3.3.5. Personas datu sniegšana ir priekšnosacījums, lai Darbinieks varētu izmantot savas tiesības un saņemt priekšrocības. Ja informācija netiek sniegta, Pārzinis nevar nodrošināt Darbinieka tiesību realizāciju. Savukārt, ja darbinieks vairs nevēlas izmantot normatīvajos aktos vai Uzņēmuma iekšējos noteikumos paredzētās priekšrocības tiesības, Darbinieks ar attiecīgu iesniegumu vēršas pie Uzņēmuma vadības.
3.4. Personas datu apstrāde korporatīvās informācijas atspoguļošanai iekšējā tīklā, Pārziņa administrētajā tīmekļa vietnē, plašsaziņas līdzekļos un sociālajos tīklos ar mērķi popularizēt un veicināt Pārziņa un tā pārstāvēto zīmolu atpazīstamību un nodrošināt kolektīva saliedētību, kā arī lai nodrošinātu ikdienas darba organizēšanu, darbinieku informēšanu un operatīvu savstarpēju komunikāciju (informācija par jaunajiem darbiniekiem, telefoni (Uzņēmuma pārziņā), rīkojumi).
3.4.1. Personām ar noteiktu kategoriju amatiem (it sevišķi, ētera personībām) ir jārēķinās, ka tām pildot amata pienākumus, tās ir atzīstamas par publiskām personām un to tiesības uz privātās dzīves neaizskaramību ir daudz ierobežotākas, vienlaicīgi, Pārzinis uzsver, ka tas respektē un ļauj darbiniekiem, kuri, pildot amata pienākumus, ir atzīstami par publiskām personām, pašām izvēlēties informācijas apjomu, ko tās vēlas sniegt sabiedrībai. Ievērojot minēto, sabiedrības informēšanas nolūkos, kā arī ar mērķi popularizēt Pārziņa tēlu un atpazīstamību, Pārziņa informatīvie materiāli, fotogrāfijas un videoieraksti, saistībā ar Pārziņa darbību var tikt ievietoti dažādos masu plašsaziņas līdzekļos un Pārziņa administrētajās tīmekļa vietnēs (piemēram, www.latvijasradio.lv, www.lsm.lv) un Pārziņa administrētos sociālajos tīklos (piemēram, facebook.com, twitter.com, youtube.com), kā arī saglabāti Pārziņa arhīvā. Tāpat, Pārzinis var rīkot dažādus iekšējos pasākumus, lai saliedētu kolektīvu, kur šādu pasākumu laikā var tikt fotografēts vai filmēts un šie materiāli saglabāti Pārziņa arhīvā, atspoguļoti Pārziņa administrētajās tīmekļa vietnēs vai sociālo tīklu profilos. Atsevišķos gadījumos šie materiāli var saturēt arī Pārziņa, darbinieku personas datus - fotogrāfijas, to kontaktinformāciju, videomateriālus, notikumu aprakstus u.tml.
3.4.2. Punkta 3.4.1.minētajos gadījumos personas datu apstrāde tiek veikta, pamatojoties uz Regulas 6.panta 1.punkta f) apakšpunktu (apstrāde ir vajadzīga pārziņa vai trešās personas leģitīmo interešu ievērošanai), t.i., Pārzinim ir leģitīma interese atspoguļot tā organizētos pasākumus vai pasākumus, kuros tas piedalās, plašsaziņas līdzekļos un Pārziņa administrētajā tīmekļa vietnēs un sociālajos tīkos, tādējādi nodrošinot Pārziņa atpazīstamību.
3.4.3. Uzņēmums, izvēloties kādu informāciju publicēt plašsaziņas līdzekļos, Pārziņa administrētajā tīmekļa vietnēs un sociālajos tīklos, vienmēr cenšas nodrošināt, ka ar pieejamiem materiāliem netiek aizskartas Darbinieku kā Datu subjektu tiesības un brīvības un Uzņēmums respektē Darbinieka tiesības uz privātās dzīves neaizskaramību. Vienlaicīgi Pārzinis apzinās, ka tam, iespējams, nav zināmi visi fakti un apstākļi par iespējamo ietekmi, tāpēc lai nodrošinātu godprātīgu datu apstrādi, jebkuram Darbiniekam ir iespēja sazināties un tiesības iebilst pret viņa personas datu atspoguļošanu Pārziņa administrētajā tīmekļa vietnēs vai sociālajos tīklos, informējot par to Juridiskās daļas vadītāju un/vai Datu aizsardzības speciālistu.

3.4.4. Personas datu saņēmēji var būt Uzņēmuma pilnvaroti darbinieki, attiecīgo plašsaziņas līdzekļu, tīmekļa vai sociālo tīklu lietotāji, apstrādātāji, tiesībsargājošās un uzraugošās institūcijas. Ja attiecīgajai trešajai personai personas dati jānodod noslēgtā pakalpojuma līguma ietvaros, lai veiktu kādu līguma izpildei nepieciešamu funkciju (piemēram, pakalpojumu sniedzējam, lai veiktu foto uzņemšanas un/vai video filmēšanas darbus).
3.4.5. Personas dati tiek glabāti pastāvīgi, veicot pieejamās informācijas periodisku pārskatīšanu.
3.4.6. Attiecībā uz Personas datiem, kas apstrādāti elektroniskajā vidē, Uzņēmums informē, ka tā izvēlētie sadarbības partneri (facebook.com, twitter.com, youtube.com u.tml.) ir atzīstami par uzņēmumiem, kas darbojas ārpus Eiropas savienības un Eiropas Ekonomiskās zonas dalībvalstīm, tāpēc Uzņēmums aicina iepazīties ar šo uzņēmumu privātuma politikām vai vērsties atsevišķi pie Uzņēmuma ar lūgumu sniegt papildu informāciju par sadarbības nosacījumiem.
3.5. **Uzņēmuma vieglajiem transportlīdzekļiem ir uzstādītas GPS (globālās izsekošanas sistēmas).** Sistēma tiek izmantota, pamatojoties uz Regulas 6.panta 1.punkta f) apakšpunktu, lai monitorētu transportlīdzekļa lietošanas efektivitāti un nodrošinātos ar pierādījumiem prettiesiskas izmantošanas gadījumā, tāpat attiecīgā informācija tiek izmantota, lai nodrošinātu korektu grāmatvedības uzskaiti. GPS uzkrāto datu monitorings var tikt izmantots, ja Uzņēmumam rodas aizdomas par Darbinieka prettiesisku rīcību, tai skaitā darba pienākumu nepildīšanu vai nepienācīgu izpildi, rīcību, kas ir pretrunā Uzņēmuma iekšējiem rīkojumiem un procedūrām, kā arī ceļu satiksmes noteikumu izmeklēšanas pārkāpumu gadījumos.
3.5.1. Informācija, kas iegūta veicot GPS uzkrāto datu monitoringu, var tikt nodota Uzņēmuma pilnvarotiem darbiniekiem, apstrādātājiem, kā arī tiesībsargājošajām, kontrolējošām un uzraugošajām iestādēm.
3.5.2. GPS uzkrāto datu monitoringa rezultātā iegūtā informācija, ar nolūku veikt korektu grāmatvedības uzskaiti, tiek glabāta vismaz 5 gadus kā grāmatvedības ierakstu attaisnojuma dokumentācija.
3.5.3. Gadījumos, ja attiecīgo informāciju var izmantot likumiskās intereses realizācijai, piemēram, disciplinārlietai, tad termiņš var tikt pagarināt līdz likumiskās intereses realizācijai vai līdz galējā tiesas sprieduma spēkā stāšanās brīdim un gadu pēc izpildes, ja attiecīgā informācija ir izmantojama, lai aizstāvētu Uzņēmuma vai trešās personas tiesiskās intereses.
3.5.4. Darbinieks apzinās, ka, ja viņš izmanto Uzņēmuma transportlīdzekli personīgām vajadzībām, monitoringa rezultātā viņa personas dati var tikt apstrādāti, un šajā gadījumā nepastāv Darbinieka tiesības uz privātumu. Attiecīgi Darbiniekam vajadzētu izvairīties izmantot Uzņēmuma transportlīdzekli, gadījumā, kad tā izmantošana var atklāt privātu informāciju, kuru Darbinieks nevēlas atklāt Uzņēmumam.
3.6. Uzņēmumā tiek veikta **videonovērošana**. Videonovērošana tiek veikta ar mērķi novērst vai atklāt noziedzīgus nodarījumus saistībā ar personu un/vai īpašuma aizsardzību, Pārziņa vai trešās personas tiesisko interešu aizsardzību un personu vitāli svarīgu interešu, tajā skaitā, dzīvības un veselības aizsardzību.
3.6.1. Videonovērošana tiek veikta, pamatojoties uz Regulas 6.panta 1.punkta d) un f) apakšpunktu, t.i., Personas datu apstrāde ir vajadzīga, lai aizsargātu Datu subjekta vai citas fiziskas personas vitāli svarīgas intereses (piemēram, personas datu apstrāde ir vajadzīga personas dzīvības un veselības aizsardzībai, kas ir saistīti ar noziedzīgu

nodarījumu novēršanu un/vai atklāšanu); Pārziņa un trešo personu leģitīmo interešu nodrošināšanai (piemēram, lai novērstu vai atklātu noziedzīgus nodarījumus saistībā ar īpašuma aizsardzību, nodrošinātos ar pierādījumiem strīdus gadījumos). Par Pārziņa leģitīmo interesi ir atzīstama arī tāda interese, kas ir uzraudzīt vai darbinieks ievēro iekšējās instrukcijas vai procedūras, vai, lai izskatītu kādu sūdzību, kas saistīta ar amata pienākumu izpildi/neizpildi. Tāpat, videoieraksti var tikt izmantoti, lai izmeklētu, piemēram, nelaimes gadījumu darbā (balstoties uz Regulas 9. panta 2.punkta b) apakšpunktu, tas ir, apstrāde ir vajadzīga, lai realizētu pārziņa vai datu subjekta konkrētās tiesības nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības tiesību jomā, ciktāl to pieļauj Eiropas savienības vai Latvijas tiesību akti) vai, balstoties uz Regulas 9.panta 2.punkta f) apakšpunktu, ja apstrāde ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgās prasības (piemēram, strīdus gadījumā par nodarīto kaitējumu apmēru) vai kādu sūdzību par amata pienākumu neizpildes apstākļiem, t.sk. darba laika neievērošanu u.tml. Vienlaicīgi, Pārzinis informē, ka šāda uzraudzība šādiem mērķim nav patstāvīga, bet tiks veikta tikai tad, ja būs kāds priekšnoteikums, kad videoierakstu vajadzētu izmantot, piemēram, par priekšnoteikumu ir atzīstama saņemta sūdzība vai nelaimes gadījums darbā.

3.6.2. Darbiniekam ieejot/nokļūstot Uzņēmuma telpās vai tās teritorijā, kurā tiek veikta videonovērošana, var tikt apstrādāti Darbinieka videoattēls un laiks, kad Darbinieks ir apmeklējis telpas un/vai teritoriju. Videonovērošana netiek veikta teritorijās, kur Darbinieks sagaida paaugstinātu privātumu, atpūtas zonās, ģērbtuvēs u.tml. Videonovērošanas kameru ieraksta zonas ir koncentrētas uz Uzņēmuma ēkas ieeju/izeju, gaiteņiem un teritoriju (piemēram, pārvietojamām studijām), kā arī, uz transportlīdzekļiem, to kustību un plūsmu Uzņēmuma teritorijā.

3.6.3. Videonovērošanai un to ierakstiem piekļūst un tie var tikt izpausti Uzņēmuma pilnvarotiem darbiniekiem, atbilstoši savos darba pienākumos noteiktajam apjomam, apstrādātājiem (apsardzes pakalpojumu sniedzējiem), juridisko pakalpojumu sniedzēji, Valsts Ugunsdzēsības un glābšanas dienestam, kā arī tiesībsargājošajām (t.sk. tiesai), kontrolējošajām un uzraugošajām institūcijām.

3.6.4. Videonovērošanas ieraksti tiks glabāti periodu, kas nepārsniedz 30 dienas, ja vien attiecīgajā videoierakstā netiks atspoguļota iespējami prettiesiska rīcība vai rīcība, kas, iespējami, palīdzēs Uzņēmumam vai trešajām personām nodrošināt to tiesiskās intereses. Šajā gadījumā, attiecīgais videoieraksts var tikt izgūts un saglabāts līdz tiesiskās intereses nodrošināšanas brīdim.

3.7. **Darbinieku caurlaižu karšu lietošana,** lai novērstu vai atklātu noziedzīgus nodarījumus saistībā ar personu un/vai īpašuma aizsardzību, Pārziņa vai trešās personas tiesisko interešu aizsardzību un personu vitāli svarīgu interešu, tajā skaitā, dzīvības un veselības aizsardzību. Darbiniekiem tiek izsniegtas speciālas formas pastāvīgās caurlaides (turpmāk – Preses karte), kas ir derīga piecus gadus. Preses karti, uzrādot un aktivizējot ar to elektroniskās ieejas kontroles sistēmu, ir derīga ienākšanai Objektā jebkurā diennakts laikā. Darbinieka Preses karte vienlaikus ir arī Uzņēmuma darbinieka apliecība un tā ir lietojama darba laikā, Darbiniekam piestiprinot to pie apģērba. Preses karte un tās turētājs – melna lenta ar Uzņēmuma logo.

3.7.1. Lietojot Preses karti Pārziņa objektā, tiek uzkrāta informācija par tās lietojumu, atspoguļojot iekļūšanas un izkļūšanas laiku ēkā un atsevišķās ēkas daļās, pamatojoties uz Regulas 6.panta 1.punkta e) un f) apakšpunktu, t.i., personas datu apstrāde ir vajadzīga, lai nodrošinātu sabiedrības interešu nodrošināšanu, atbilstoši Nacionāla drošības likuma

nosacījumiem; Pārziņa un trešo personu leģitīmo interešu nodrošināšanai (piemēram, lai novērstu vai atklātu noziedzīgus nodarījumus saistībā ar īpašuma aizsardzību, nodrošinātos ar pierādījumiem strīdus gadījumos).
3.7.2. Informācijai par Preses kartes lietojuma vēsturi var piekļūt Uzņēmuma pilnvarotie darbinieki, atbilstoši savos darba pienākumos noteiktajam apjomam, apstrādātājiem (apsardzes pakalpojumu sniedzējiem) ar mērķi nodrošināt kontrolētu darbinieku un viesu kustību Uzņēmuma ēkā.
3.7.3. Caurlaižu režīma darbības ietvaros apstrādātie dati tiks glabāti periodu, kas nepārsniedz 3 gadus, ja vien attiecīgie dati, iespējami, būs nepieciešami, lai palīdzētu Uzņēmumam vai trešajām personām nodrošināt to tiesiskās intereses. Šajā gadījumā, attiecīgie dati var tikt izgūti un saglabāti līdz tiesiskās intereses nodrošināšanas brīdim.
3.8. Gadījumā, ja Darbinieks vēlas kandidēt uz kādu no Uzņēmuma vakantajiem amatiem, tad Darbinieka kā vakantā kandidāta personas dati tiek apstrādāti tā, kā tas ir norādīts Pārziņa publiskajā privātuma politikā, kas ir pieejama tīmekļa www.latvijasradio.lv vai Pārziņa Personāla daļā.
3.9. Darbinieku personas dati var tikt apstrādāti arī citiem Uzņēmuma iekšējos dokumentos norādītajiem mērķiem par kuriem Darbinieks tiek informēts atsevišķi, bet jebkurā gadījumā Pārzinis raudzīsies, lai jebkurā turpmākā apstrāde Jums kā darbiniekam būtu prognozējama un sagaidāma.

4. Darbinieka tiesības saistībā ar viņa personas datu apstrādi

4.1. Uzņēmums apņemas Darbinieku personas datus apstrādāt godprātīgi, likumīgi un Darbiniekam pārredzamā veidā, konkrētiem, skaidriem un leģitīmiem nolūkiem. Darbiniekam ir jāvēršas pie Uzņēmuma Personāla daļas vadītāja vai Datu aizsardzības speciālista, izmantojot Uzņēmuma kontaktinformāciju.
4.2. Darbiniekam ir tiesības un pienākums saņemt informāciju par to, kādi Personas dati par Darbinieku ir Uzņēmuma rīcībā, kādiem nolūkiem Uzņēmums apstrādā šos Personas datus, Personas datu saņēmēju kategorijas (personas, kam Personas dati ir izpausti vai kam tos paredzēts izpaust), informāciju par laikposmu, cik ilgi Personas dati tiks glabāti, vai kritēriji, ko izmanto minētā laikposma noteikšanai, kā arī informācija par datu avotu, ja Personas dati netiek vākti no Datu subjekta. Gadījumā, ja Darbiniekam ir papildu jautājumi par šajā Politikā norādītajām Personas datu apstrādes aspektiem, lūdzu vērsieties pie Uzņēmuma Personāla daļas vadītāja vai Datu aizsardzības speciālista.
4.3. Darbiniekam ir tiesības prasīt savu Personas datu labošanu, ja Darbinieks uzskata, ka Uzņēmuma rīcībā esošā informācija ir novecojusi, neprecīza vai nepareiza.
4.4. Darbiniekam ir tiesības prasīt savu Personas datu dzēšanu, vai iebilst pret apstrādi, ja Darbinieks uzskata, ka Personas dati ir apstrādāti nelikumīgi, tie vairs nav nepieciešami saistībā ar nolūkiem, kādos tie tika vākti vai citādi apstrādāti. Darbinieka Personas dati netiks dzēsti, ja Personas datu apstrāde ir nepieciešama:
4.4.1. lai Uzņēmums aizsargātu Darbinieka vai citas personas vitāli svarīgas intereses, tajā skaitā, dzīvību un veselību;
4.4.2. lai Uzņēmums aizsargātu savu vai trešās personas īpašumu;
4.4.3. lai Uzņēmums izpildītu juridisku pienākumu, kas prasa veikt apstrādi;
4.4.4. lai Uzņēmums izpildītu uzdevumu, ko veic sabiedrības interesēs vai saistībā ar Pārzinim likumīgi piešķirto oficiālo pilnvaru īstenošanu;

4.4.5. arhivēšanas nolūkos, atbilstoši Latvijā spēkā esošajiem normatīvajiem aktiem, kas regulē arhīvu veidošanu;
4.4.6. lai Uzņēmums vai trešā persona celtu, īstenotu vai aizstāvētu likumīgas prasības/tiesiskās intereses.
4.5. Darbiniekam ir tiesības jebkurā brīdī atsaukt savu piekrišanu gadījumos, kad personas datu apstrādes tiesiskais pamats ir bijusi darbinieka piekrišana. Tomēr tas neietekmē apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana, tajā skaitā, gadījumos, ja tas ir izmantojis Darbinieka priekšrocības saskaņā ar šajā Politikā norādīto, ja vien uz attiecīgo datu apstrādi jau nav attiecināmi citi nosacījumi (piemēram, grāmatvedības normatīvo aktu prasības par dokumentu glabāšanas termiņu ievērošanu).
4.6. Darbiniekam ir tiesības prasīt, lai Uzņēmums ierobežotu apstrādi, ja ir viens no šādiem apstākļiem:
4.6.1. Datu subjekts apstrīd Personas datu precizitāti – uz laiku, kurā Pārzinis var pārbaudīt personas datu precizitāti;
4.6.2. apstrāde ir nelikumīga, un Datu subjekts iebilst pret Personas datu dzēšanu un tās vietā pieprasa datu izmantošanas ierobežošanu;
4.6.3. Pārzinim Personas dati apstrādei vairs nav vajadzīgi, taču tie ir nepieciešami Datu subjektam, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
4.6.4. lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
4.6.5. Datu subjekts ir iebildis pret apstrādi saskaņā ar Regulas 21.panta 1.punktu, kamēr nav pārbaudīts, vai Pārziņa leģitīmie iemesli nav svarīgāki par Datu subjekta leģitīmajiem iemesliem.
4.7. Darbiniekam ir tiesības uz datu pārnesamību Regulas 20.pantā paredzētajos gadījumos.
4.8. Darbiniekam ir tiesības iesniegt sūdzību Datu valsts inspekcijai, ja Darbinieks uzskata, ka Uzņēmums viņa Personas datus apstrādājis prettiesiski; Vienlaicīgi Uzņēmums aicina vispirms vērsties pie Uzņēmuma, lai rastu operatīvu risinājumu, ja Darbinieka tiesības uz Personas datu aizsardzību ir pārkāptas.
4.9. Pēc atbilstoša Darbinieka pieprasījuma, Uzņēmums nodrošina apstrādē esošo Personas datu kopiju. Ja Darbinieks pieprasījumu iesniedz elektroniskā formā un ja vien Darbinieks nepieprasa citādi, informāciju sniedz plaši izmantotā elektroniskā formātā. Ja Darbinieka pieprasījumi ir acīmredzami nepamatoti vai pārmērīgi, jo īpaši to regulāras atkārtošanās dēļ, Uzņēmums var pieprasīt saprātīgu maksu, ņemot vērā administratīvās izmaksas, kas saistītas ar informācijas vai saziņas nodrošināšanu vai pieprasītās darbības veikšanu, vai arī atteikties izpildīt pieprasījumu.
4.10. Darbinieka tiesības saņemt šīs Politikas 4.9.punktā minēto kopiju nedrīkst nelabvēlīgi ietekmēt citu personu tiesības un brīvības (piemēram, izsniegtajā kopijā tiks dzēsti vai retušēti citu personu Personas dati).
4.11. Ja Uzņēmumam rodas nepieciešamība Darbinieku personas datus turpmāk apstrādāt citā nolūkā, kas nav nolūks, kādā Personas dati tika vākti, Uzņēmums pirms minētās turpmākās Personas datu apstrādes informē Darbiniekus par jauno Personas datu apstrādes mērķi, tiesisko pamatu, attiecīgajām Personas datu kategorijām, iespējamajām Personas datu saņēmēju kategorijām un citu informāciju, ko saskaņā ar Regulu Uzņēmumam ir pienākums sniegt. Informāciju Pārzinis sniedz mutiski, papīra formā vai nosūta uz attiecīgo Darbinieka e-pasta adresi vai citādā veidā dara zināmu attiecīgajam Darbiniekam vai Darbiniekiem citā piemērotā veidā. Minētā informācija var tikt iekļauta

atsevišķā instrukcijā, rīkojumā, ar Darbinieku noslēgtajā līgumā vai kā pielikums tam, vai kādā citā Uzņēmuma dokumentā.

5. Nobeiguma nosacījumi

5.1. Politika tiek pārskatīta, ja mainās Darbinieku Personas datu apstrādes nosacījumi vai tiesību aktu prasības, kā arī nepieciešamības gadījumā tā tiek atjaunota un Darbinieki tiek iepazīstināti ar atjaunoto Politiku.

5.2. Darbinieki un citas atbildīgās personas, kas ir pilnvarotas vai kuru darba pienākumos ietilpst apstrādāt Darbinieku personas datus, ievēro konfidencialitātes principu attiecībā uz Personas datu apstrādi un aizsardzību, kā arī neizpauž citām personām Darbinieku Personas datus vai citu ar šiem datiem saistītu informāciju, ko viņi uzzināja savu darba pienākumu pildīšanas laikā, izņemot gadījumus, kad šāda informācija ir publiski pieejama saskaņā ar tiesību aktu prasībām. Pienākums sargāt un neizpaust šajā punktā norādīto informāciju ir spēkā arī pārejot uz citu darba amatu, izbeidzoties darba līguma vai cita izbeidzot cita civiltiesiska līguma attiecības.

5.3. Darbiniekiem ir aizliegts apstrādāt (vākt, saņemt, uzzināt, u.tml.) citu kolēģu Personas datus, ja viņi nav pilnvaroti to darīt vai to darba pienākumos neietilpst šādas informācijas apstrāde.

5.4. Darbinieki tiek iepazīstināti ar iekšējiem normatīvajiem dokumentiem, kas regulē Personu datu apstrādes noteikumus, saskaņā ar Darba un iekšējās kārtības noteikumu punktu 1.14.5 „Darbiniekiem, kuri ikdienā strādā ar datoru, uzsākot darbu, ir jāatver iekšējā mājas lapa un jāiepazīstas ar jaunāko informāciju (rīkojumi, valdes lēmumi, paziņojumi u.c.). Ja informācija ir ievietota iekšējā mājas lapā, uzskatāms, ka darbinieks ar šo informāciju ir iepazīstināts".

5.5. Darbiniekiem jāievēro Politikā noteiktās saistības un savā darbā jāievēro tajā noteiktie Personas datu apstrādes principi.

5.6. Šī Politika ir atzīstama par Uzņēmuma kā Darba devēja iekšējās darba kārtības noteikumu būtisku sastāvdaļu un Politikā noteikto saistību pārkāpums uzskatāms par rupju darba kārtības noteikumu pārkāpumu, par kuru tiek piemērotas Darba likumā noteiktās sankcijas vai sekas (t.sk. var tikt izbeigts noslēgtais Darba līgums vai cits civiltiesiskais līgums).

APSTIPRINĀTS
ar 09.12.2020. valdes lēmumu Nr.2-28/A1-7

Personas datu aizsardzības pārkāpumu izmeklēšanas kārtība

1.Mērķis

Šī Personas datu aizsardzības pārkāpumu izmeklēšanas kārtība (turpmāk tekstā – Kārtība) nosaka galvenās pamatprasības attiecībā uz tādu incidentu, kas ir novedis pie VSIA "Latvijas Radio", vienotais reģ. Nr.40003080614 (turpmāk tekstā – Uzņēmums), kontrolējamo un/vai apstrādājamo personas datu aizsardzības pārkāpuma identificēšanas, izvērtēšanas, pārvaldīšanas un administrēšanas, lai nodrošinātu personas datu aizsardzības pārkāpumu izmeklēšanas pārskatāmību, paaugstinātu personu datu apstrādes drošību un mazinātu jebkādas iespējamās nelabvēlīgās sekas Uzņēmumam un datu subjektiem.

2.Atsauces uz dokumentiem

2.1. Eiropas Parlamenta un Padomes Regula (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 tekstā - Regula);
2.2. Fizisko personu datu apstrādes likums (turpmāk tekstā - Datu likums);
2.3. citi Latvijas Republikā spēkā esošie saistošie tiesību akti, kas reglamentē šajā Kārtībā noteikto.

3. Lietotie termini

3.1. Šīs Kārtības izpratnē ar personas datu aizsardzības pārkāpumu var tikt saprastas arī **aizdomas** par personas datu aizsardzības pārkāpumu līdz brīdim, kamēr šajā Kārtībā noteiktajā veidā nav konstatēts, ka datu aizsardzības pārkāpums nav noticis.
3.2. Šajā Kārtībā lietoto terminu definīcijas izriet no Regulas 4. panta:
3.2.1. **Personas dati** - jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu (Datu subjekts); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, tajā skaitā, bet ne tikai, personas vārdu, uzvārdu, personas kodu, dzimšanas datiem, dzīvesvietas adresi, darba vietu, tālruņa numuru, ģimenes stāvokli, e-pasta adresi, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.
3.2.2. **Īpašo personas datu kategorijas personas dati** - Personas dati, kas atklāj rasi vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, kā arī, ģenētiskie dati, biometriskie dati, lai veiktu fiziskas personas unikālu identifikāciju, veselības dati vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju.
3.2.3. **Personas datu apstrāde** - jebkuras ar Personas datiem vai Personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, pielāgošanu, sakārtošanu, pārveidošanu, izmantošanu, aplūkošanu, nodošanu, pārraidīšanu, izpaušanu, nosūtīšanu, izplatīšanu, saskaņošanu, ierobežošanu, bloķēšanu, dzēšanu vai iznīcināšanu. (Politika tiek piemērota jebkāda veida personas datu apstrādei – manuālai un datorizētai).
3.2.4. **Datu subjekts** - fiziskā persona, kuru var tieši vai netieši identificēt un kuras Personas dati tiek apstrādāti.
3.2.5. **Datu subjekta piekrišana** - jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz Datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu Personas datu apstrādei.

3.2.6. **Uzņēmums (Darba devējs)** – Valsts sabiedrība ar ierobežotu atbildību "Latvijas Radio", reģistrācijas numurs 40003080614, juridiskā adrese: Doma laukums 8, Rīga, LV-1505, e-pasta adrese: radio@latvijasradio.lv, tīmekļa vietne: www.latvijasradio.lv.
3.2.7. **Pārzinis** - Regulas izpratnē Uzņēmums ir tādu fizisko personu Personas datu apstrādes pārzinis, kuriem Uzņēmums viens pats vai kopīgi ar citiem nosaka Personas datu apstrādes nolūkus (mērķus) un līdzekļus.
3.2.8. **Apstrādātājs** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura Pārziņa vārdā apstrādā Personas datus.
3.2.9. **Personas datu saņēmējs** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpaužPersonas datus – neatkarīgi no tā, vai tā ir trešā persona vai nav. Tomēr publiskas iestādes, kas var saņemt Personas datus saistībā ar konkrētu izmeklēšanu saskaņā ar Eiropas savienības vai dalībvalsts tiesību aktiem, netiek uzskatītas par saņēmējiem; minēto datu apstrāde, ko veic minētās publiskās iestādes, atbilst piemērojamiem datu aizsardzības noteikumiem saskaņā ar apstrādes nolūkiem.
3.2.10. **Trešā persona** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav Datu subjekts, Pārzinis, Apstrādātājs un personas, kuras Pārziņa vai Apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt Personas datus.
3.2.11. **Personas datu aizsardzības pārkāpums** - drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto Personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.
3.2.12. **Uzraudzības iestāde Latvijā** - Datu valsts inspekcija.
3.2.13. **Darbinieks** – persona, kura ar Uzņēmumu slēdz vai ir noslēgusi darba līgumu vai saskaņā ar citu civiltiesisku līgumu veic vai varētu veikt pienākumus, kuras Personas dati var tikt apstrādāti un kurai ir jāievēro šajā Kārtībā minētie Personas datu apstrādes nosacījumi.
3.2.14. **Atbildīgais par datu aizsardzību** - Uzņēmuma atbilstoši pilnvarots Darbinieks, kura pienākums ir organizēt un nodrošināt iespējamo Personas datu aizsardzības pārkāpumu izmeklēšanu, pārvaldību un dokumentēšanu, atbilstoši fizisku Personu datu aizsardzību regulējošo normatīvo aktu prasībām. Ja vien ar valdes rīkojumu nav noteikts savādāk, Administratīvais direktors - Juridiskās daļas vadītājs.
3.2.15. **Datu aizsardzības speciālists** - Persona Uzņēmumā, kas ir sasniedzama izmantojot e-pasta adresi: datuaizsardziba@latvijaradio.lv, un kuram ir šādi uzdevumi: informēt un konsultēt Uzņēmumu, tā darbiniekus, uzraudzīt vai tiek ievērotas normatīvo aktu prasības attiecībā uz Personas datu aizsardzību, pēc pieprasījuma sniegt padomus par nepieciešamību sagatavot novērtējumu par ietekmi uz datu aizsardzību, sadarboties ar uzraudzības iestādi un būt par kontaktpunktu jautājumos, kas saistīti ar datu apstrādi (Regulas 37.pantā noteiktajā kārtībā iecelts datu aizsardzības speciālists, un kuram ir Regulas 39.pantā noteiktie uzdevumi).

4.Darbības joma un lietotāji (atbildīgie darbinieki)

4.1. Šī Kārtība attiecas uz Uzņēmumu un tās struktūrvienībām, kas apstrādā fizisko Personu datus, lai nodrošinātu Uzņēmuma saimniecisko darbību, tiesiskās intereses un Latvijas Republikā spēkā esošo saistošo tiesību aktu prasību ievērošanu.
4.2. Ja Uzņēmums darbojas kā datu Pārzinis attiecībā uz Personas datiem, uz ko attiecas pārkāpums, tad pārkāpums tiek risināts, pamatojoties uz šīs Kārtības noteikumiem.
4.3. Ja Uzņēmums darbojas kā datu Apstrādātājs, Atbildīgais par datu aizsardzību bez liekas kavēšanās papildus informē par pārkāpumu attiecīgo datu pārzini, kura vārdā Uzņēmums veic Personas datu apstrādi, un sniedz pamatotu palīdzību datu Pārziņa pienākumu izpildē, ņemot vērā ar datu pārzini noslēgto datu apstrādes līgumu un normatīvo aktu prasības.
4.4. Šī Kārtība attiecas uz visiem Personas datiem, ko Uzņēmums saņem vai rada jebkādā formā.
4.5. Šīs Kārtības lietotāji ir visi Uzņēmuma darbinieki, kas darbojas Uzņēmuma vārdā un veic fizisko Personu datu apstrādi. Darbinieki tiek iepazīstināti ar iekšējiem normatīvajiem dokumentiem, kas regulē personu datu apstrādes noteikumus, saskaņā ar Darba un iekšējās kārtības noteikumu

1.14.5 punktu „Darbiniekiem, kuri ikdienā strādā ar datoru, uzsākot darbu, ir jāatver iekšējā mājas lapa un jāiepazīstas ar jaunāko informāciju (rīkojumi, valdes lēmumi, paziņojumi u.c.). Ja informācija ir ievietota iekšējā mājas lapā, uzskatāms, ka darbinieks ar šo informāciju ir iepazīstināts".
4.6. Ar šo Kārtību tiek iepazīstinātas arī citas personas, kas nav Darbinieki, bet kuri tomēr Uzņēmumā veic Personas datu apstrādi, kā arī šo Darbinieku tiešie vadītāji, piemēram, Apstrādātāju kontaktpersonas.

5. Aizdomas par Personas datu aizsardzības pārkāpumu

5.1. Katram Darbiniekam ir pienākums nekavējoties ziņot par jebkādām aizdomām par Personas datu aizsardzības pārkāpumu kādā no tālāk norādītajiem veidiem:
5.1.1.informējot par aizdomām savu tiešo vadītāju;
5.1.2. aizpildot paziņojuma veidlapu (1. pielikums) Uzņēmuma iekštīklā;
5.1.3. informējot Atbildīgo par datu aizsardzību e-pastā (datuaizsardziba@latvijasradio.lv), personīgi vai pa telefonu (+371 67206711).
5.2. Par faktu, ka ir noticis iespējamais datu aizsardzības pārkāpums, var liecināt šādas situācijas (uzskaitījums nav izsmeļošs):
5.2.1. nepareizajam adresātam nosūtīts e-pasta sūtījums;
5.2.2. informācijas izpaušana telefonsarunas laikā personai, kas nav viennozīmīgi identificēta un ir radušās aizdomas, ka informācija ir izpausta personai, kas nebija pilnvarota to saņemt;
5.2.3. kompromitētas pieejas tiesības (parole kļuvusi zināma nepilnvarotām personām, t.sk. gadījumos, ja ir *"uzlauzti"* personīgie profili un šis fakts var ietekmēt Uzņēmuma informācijas un tehniskos resursus, piemēram, mobilos telefonus, u.tml.);
5.2.4. datu (dokumentu papīra formā vai tādu iekārtu, kurās dati ir saglabāti) nozaudēšana (t.sk. aizmiršana) vai zādzība;
5.2.5. aizdomas par Uzņēmuma iekšējo normatīvo aktu pārkāpumu (informāciju tehnoloģiju (turpmāk tekstā – IT) drošības jomā, klientu apkalpošanas jomā u.tml.);
5.2.6. neatbilstoša piekļuves kontrole, kas ļauj nesankcionēti izmantot Personas datus;
5.2.7. mēģinājums iegūt nesankcionētu piekļuvi datorsistēmām (piemēram, hakeru darbība);
5.2.8. nesankcionēta (nejauša vai apzināta) ierakstu pārveidošana vai dzēšana;
5.2.9. vīrusu vai tamlīdzīgi uzbrukumi IT sistēmai;
5.2.10. fiziskās drošības pārkāpumi (piemēram, durvju vai logu uzlaušana telpā vai dokumentu glabāšanas skapī, kur atrodas Personas dati);
5.2.11. neaizsargātu Personas datu atstāšana vietās, kur tie pieejami personām, kuras nav pilnvarotas tiem piekļūt (dokumentu atstāšana bez uzraudzības klientiem vai nepilnvarotiem darbiniekiem pieejamās vietās, personālā datora atstāšana bez uzraudzības ar aktivizētu lietotāja kontu un bez bloķētas pieejas).

6. Pārkāpuma sākotnējais novērtējums

6.1. Saņemot jebkādu informāciju par iespējamu Personas datu aizsardzības pārkāpumu, Atbildīgajam par datu aizsardzību ir pienākums šādu informāciju pārbaudīt un veikt situācijas sākotnējo novērtējumu, pamatojoties uz 1.pielikumā norādīto informāciju un/vai sākotnējo informāciju, kas saņemta no ziņotāja. Izvērtējuma rezultātā Atbildīgais par datu aizsardzību pieņem kādu no norādītajiem lēmumiem:
6.1.1. konstatē, ka nav noticis datu aizsardzības pārkāpums Regulas izpratnē un, ja nepieciešams, informē citus atbildīgos Darbiniekus (piemēram gadījumā, ja pārkāpums ir noticis, bet tas nav Personas datu aizsardzības pārkāpums). Saņemto informāciju fiksē Personas datu aizsardzības pārkāpuma uzskaites žurnālā;
6.1.2. apstiprina aizdomas, ka ir noticis Personas datu aizsardzības pārkāpums vai ir pamatotas aizdomas, ka varētu būt noticis Personas datu aizsardzības pārkāpums un fiksē nepieciešamo informāciju

Personas datu aizsardzības pārkāpumu uzskaites žurnālā, kā arī informē par to Datu aizsardzības speciālistu.

6.2. Ievērojot pieejamo informāciju par iespējamo Personas datu aizsardzības pārkāpumu, Atbildīgais par datu aizsardzību var pats izmeklēt Personas datu aizsardzības pārkāpumu vai izveidot Drošības pārkāpuma izmeklēšanas komisiju (turpmāk tekstā – Komisija).

6.3. Vērtējot nepieciešamību izveidot Komisiju, Atbildīgais par datu aizsardzību ņem vērā *(uzskaitījums nav izsmeļošs)*:

6.3.1. ziņas par Personas datu aizsardzības pārkāpumā iesaistītajām IT sistēmām un datu bāzēm, to raksturu;

6.3.2. cik liels datu apjoms varētu būt kompromitēts Personas datu aizsardzības pārkāpumā un cik Datu subjekti varētu būt skarti;

6.3.3. kāds ir kompromitēto Personas datu raksturs (piemēram, vai ir skarti Īpašo personas datu kategorijas personas dati);

6.3.4. vai skarti Personas dati, ko var izmantot identitātes krāpniecībai vai finanšu krāpniecībai;

6.3.5. vai skarti Personas dati, kas attiecas uz neaizsargātām personām (veci cilvēki, bērni, invalīdi);

6.3.6. vai skarti detalizēti personu profili (piemēram, informācija par darba veikumu, darba algu vai personīgo dzīvi), Personas datu nozaudēšanas/nesankcionētas piekļuves gadījumā;

6.3.7. vai Personas datu zaudējums radīs negatīvas sekas Uzņēmumam vai Trešo personu darbībai, ņemot vērā Personas datu aizsardzības pārkāpuma raksturu.

6.4. Ja Atbildīgajam par datu aizsardzību rodas aizdomas, ka varētu būt noticis otrā vai trešā līmeņa pārkāpums (2. pielikums), Atbildīgais par datu aizsardzību par notikušo informē Uzņēmuma valdi nevilcinoties, t.i., cik ātri vien iespējams.

6.5. Atbildīgais par datu aizsardzību nodrošina, ka pēc informācijas saņemšanas par iespējamu Personas datu aizsardzības pārkāpumu un visu pārkāpuma izmeklēšanas laiku, Datu aizsardzības speciālists tiek iesaistīts (sniegta nekavējoša informācija, noskaidrots tā viedoklis) iespējamā Personas datu aizsardzības pārkāpuma izmeklēšanā un seku likvidācijas pasākumu noteikšanā.

7. Drošības pārkāpuma izmeklēšanas komisijas izveidošana

7.1. Ņemot vērā sākotnējā novērtējuma rezultātus, Atbildīgais par datu aizsardzību izvērtē nepieciešamību izveidot Komisiju. Katram atsevišķam pārkāpumam tiek izveidota atsevišķa Komisija, vadoties no pārkāpuma veida un iespējamās ietekmes.

7.2. Lai nodrošinātu ātru un precīzu Datu aizsardzības pārkāpuma izmeklēšanas norisi, Atbildīgais par datu aizsardzību Komisijas sastāvā var iekļaut darbiniekus no:

7.2.1. Juridiskās daļas;

7.2.2. Informācijas tehnoloģijas daļas;

7.2.3. Komunikācijas un multimediju daļas;

7.2.4. attiecīgās daļas vadītāju, kurš ir atbildīgs par konkrēto datu apstrādi (piemēram, Personāla daļa, Finanšu daļa);

7.2.5. Tehnoloģiju direktoru;

7.2.6. jebkuru citu darbinieku, kura dalību Atbildīgais par datu aizsardzību uzskata par nepieciešamu;

7.2.7. par attiecīgo jomu atbildīgo valdes loceklis;

7.2.8. Komisijas sastāvā kā patstāvīgo dalībnieku iekļauj Datu aizsardzības speciālistu.

7.3. Atbildīgais par datu aizsardzību dalībai Komisijā var nozīmēt konkrētus paša izraudzītus Darbiniekus, vai lūgt attiecīgo struktūrvienību vadītājiem nekavējoties nozīmēt atbilstošāko Darbinieku.

7.4. Pēc 7.3.punktā minētā pieprasījuma par pārstāvja piedalīšanos saņemšanas, attiecīgās struktūrvienības vadītājam ne vēlāk kā vienas stundas laikā jānodrošina atbilstoša darbinieka piedalīšanās Komisijā, informējot par attiecīgo pārstāvi Atbildīgo par datu aizsardzību.

7.5. Atbildīgais par datu aizsardzību pats var vadīt Komisijas darbu vai, ievērojot pārkāpuma veidu, nozīmēt citu Komisijas dalībnieku par Komisijas vadītāju.

8. Pārkāpuma izmeklēšana

8.1. Ja Uzņēmums darbojas kā Apstrādātājs, Komisijas vadītājs vērtē nepieciešamību ziņot Pārzinim.
8.2. Komisijas vadītājs var piesaistīt neatkarīgos konsultantus un ekspertus palīdzības sniegšanai izmeklēšanā un/vai pārkāpuma seku novēršanas procesā.
8.3. Komisijas vadītājs var prasīt Apstrādātāja pārstāvja piedalīšanos pārkāpuma izmeklēšanas, pārvaldīšanas un seku novēršanas procesā.
8.3. Novērtējot Datu aizsardzības pārkāpuma izraisīto risku, jāizskata potenciālās negatīvās sekas Datu subjektiem, tai skaitā novērtējot, cik liela ir iespējamība, ka negatīvās sekas materializēsies un cik nopietnas varētu būt sekas materializēšanās gadījumā. Pārkāpuma smaguma un riska novērtēšanas kritēriji ir norādīti 2. pielikumā.
8.4. Atbildīgais par datu aizsardzību vai Komisija ne vēlāk kā 48 stundu laikā no pārkāpuma atklāšanas brīža sagatavo ziņojumu, kurā iekļauj vismaz šādu informāciju:
8.4.1. pārkāpuma datumu un laiku (ilgstoša pārkāpuma gadījumā – laika posmu);
8.4.2. pārkāpuma iespējamo cēloni;
8.4.3. apraksta Personas datu aizsardzības pārkāpuma raksturu, tostarp, ja iespējams, skartās Datu subjektu kategorijas un aptuveno skaitu;
8.4.4. apraksta Personas datu aizsardzības pārkāpuma iespējamās sekas;
8.4.5. apraksta pasākumus, kas jau ir veikti risku mazināšanai un ko vēl plāno veikt.
8.5. Pēc izmeklēšanas pabeigšanas ziņojumu papildina ar ziņām par izmeklēšanas rezultātu un seku likvidēšanas rezultātu.
8.6. Konstatējot faktiski notikušu Personas datu aizsardzības pārkāpumu, Atbildīgais par datu aizsardzību, vai Komisija ne vēlāk kā 48 stundu laikā no pārkāpuma atklāšanas brīža lemj vai konstatētais Personas datu aizsardzības pārkāpums varētu radīt risku Datu subjekta tiesībām un brīvībām un vai ir nepieciešams:
8.6.1. paziņot par pārkāpumu Uzraudzības iestādei, iesniedzot par to attiecīgu ziņojumu atbilstoši Kārtības 9.punkta noteikumiem;
8.6.2. paziņot par to Datu subjektiem, kuru tiesības un brīvības ir/var tikt aizskartas Personas datu aizsardzības pārkāpuma rezultātā un attiecīgais pārkāpums var radīt augstu risku tā tiesībām un brīvībām, atbilstoši Kārtības 9.punkta noteikumiem.
8.7. Vidēja līmeņa un augsta līmeņa pārkāpuma gadījumā Atbildīgais par datu aizsardzību vai Komisijas vadītājs, konsultējoties ar Datu aizsardzības speciālistu, novērtē:
8.7.1. kādas darbības jāveic, lai samazinātu turpmāko pārkāpumu risku un mazinātu to ietekmi;
8.7.2. vai jāuzlabo Uzņēmuma iekšējās politikas vai ziņošanas kārtība, lai palielinātu reaģēšanas uz pārkāpumu efektivitāti;
8.7.3. vai drošības kontrolē ir vājie punkti, kas jāpastiprina;
8.7.4. vai Darbinieki un pakalpojumu lietotāji zina par saviem pienākumiem informācijas drošības jomā un vai tie ir atbilstoši apmācīti;
8.7.5. vai ir nepieciešama papildu izmeklēšana, lai samazinātu riskus, un kādi resursi tam varētu būt nepieciešami.

9. Ziņošanas kārtība un seku likvidācijas kārtība

9.1. Ja par pārkāpumu nepieciešams paziņot Uzraudzības iestādei, paziņojums nosūtāms ne vēlāk kā 72 stundu laikā no brīža, kad par pārkāpumu kļuvis zināms. Uzraudzības iestādei paziņo, izmantojot Uzraudzības iestādes sagatavotu paziņojuma formu vai paziņojuma veidlapu (3.pielikums).
Ja paziņojums tiek sūtīts vēlāk kā 72 stundu laikā no pārkāpuma atklāšanas brīža, paziņojumā jānorāda arī kavēšanās iemesli.
9.2. Datu subjekti jāinformē bez liekas kavēšanās gadījumos, kad pastāv pamatotas aizdomas, ka Personas datu aizsardzības pārkāpums var radīt augstu risku datu subjektu tiesībām un brīvībām. Atbildīgais par datu aizsardzību vai Komisijas vadītājs pieņem lēmumu par Datu subjektu informēšanai izmantojamo saziņas metodi. Gadījumā, ja Personas datu aizsardzības pārkāpums ir skāris noteiktus

un sasniedzamus Datu subjektus, tiem tiek sūtīts e-pasts ar paziņojumu skaidrā, vienkāršā valodā norādot vismaz šādu informāciju:
9.2.1. informāciju par Personas datu aizsardzība pārkāpuma raksturu;
9.2.2. kontaktinformāciju papildu informācijas iegūšanai;
9.2.3. apraksta Personas datu aizsardzības pārkāpuma iespējamās sekas;
9.2.4. apraksta pasākumus, ko Pārzinis veicis vai ierosinājis veikt, lai novērstu Personas datu aizsardzības pārkāpumu, un pasākumus, lai mazinātu pārkāpuma iespējamās nelabvēlīgās sekas.
9.3. Ziņojuma teksts Uzraudzības iestādei un paziņojuma teksts Datu subjektam iesniedzams Uzņēmuma valdei apstiprināšanai un tālākai virzīšanai ne vēlāk kā 56 stundu laikā pēc Personas datu aizsardzības pārkāpuma atklāšanas.
9.4. Ja vien ar atsevišķu rīkojumu nav noteikts citādāk, Atbildīgais par datu aizsardzību vai Komisijas vadītājs ir atbildīgs par 8.7.punktā minētā novērtējuma rezultātā konstatēto pasākumu izpildes gaitas kontroli.
9.5. Atbildīgais par datu aizsardzību, gadījumos, kad ir notikuši pārkāpumi, reizi trijos mēnešos iesniedz ziņojumu Uzņēmuma valdei, norādot statistikas informāciju par saņemto ziņojumu skaitu, faktiski konstatētajiem pārkāpumiem, informāciju par to, kāda veida pārkāpumi ir konstatēti, pārkāpuma līmeņiem un darbībām, kas veiktas vai ierosinātas veikt, lai turpmāk novērstu pārkāpumus vai mazinātu to skaitu.

1.pielikums
pie Personas datu aizsardzības pārkāpumu
izmeklēšanas kārtība

Pieteikums personas datu aizsardzības pārkāpuma reģistrēšanai

Uzņēmuma nosaukums
reģistrācijas Nr.
adrese

Ziņojuma datums
Ziņotājs (*vārds, uzvārds, amats*):
Telefona numurs:
E-pasta adrese:

Informācija par pārzini
Nosaukums
reģistrācijas Nr.

Personas datu aizsardzības pārkāpuma laiks un datums:

konstatēšanas datums un laiks:

notikuma datums un laiks
(ilgstošam pārkāpumam- sākuma un beigu datums un laiks)

Incidents

1. Kāda veida personas datu aizsardzības pārkāpums ir noticis (*atzīmēt attiecīgo*):
   - nozaudēta vai zagta ierīce, datu nesējs vai dokumenta kopija;
   - nozaudēta vai neautorizēti atvērta vēstule, vai dokuments (*atstāts brīvi pieejamā vietā*);
   - pasts (papīra formātā) ir nozaudēts vai piegādāts atvērts;
   - sistēmas uzlaušana, ļaunprogrammatūra un/vai pikšķerēšana (phishing);
   - netīši iznīcināti personas dati, t.sk. nepareiza personas datu iznīcināšana papīra formātā;
   - personas dati nepilnīgi izdzēsti no datu nesēja, t.sk. e-atkritumi (*personas dati atrodas novecojušā ierīcē*);
   - netīši publicēti personas dati (*nepārdomāta publikācija*);
   - izpausti personas dati citam/nepareizam datu subjektam;
   - verbāla nesankcionēta personas datu izpaušana;
   - klientu portālā pieejami citas personas dati;
   - personas dati nosūtīti/nodoti nepareizajam adresātam/personai;
   - cits: _____

2. Pārkāpuma cēlonis:
   - iekšēja neapzināta rīcība (*iekšējās politikas pārkāpums*);
   - iekšēja ļaunprātīga rīcība;
   - ārēja drauda ietekme (hakeru darbība, izvēlēto apstrādātāju tehnisko un organizatorisko pasākumu pārkāpums);
   - cits_____.

3. Lūdzu, aprakstiet situāciju, kas izraisīja aizdomas par personas datu aizsardzības pārkāpumu:

4. Cik cilvēku ir ietekmēti ar šo pārkāpumu:
   a) Minimums:
   b) Maksimums:

5. Norādiet personu loku, kuru datus skāris pārkāpums (*atzīmēt attiecīgo*):
   - darbinieki;
   - klienti/ iespējamie klienti;
   - sadarbības partneru darbinieki (*piemēram, kontaktinformācija*);
   - citas personas: _____.

6. Datu aizsardzības pārkāpuma veids (*atzīmēt attiecīgo*):
   - datu apskate vai neatļauta piekļuve (*piemēram, datu nosūtīšana trešajai personai*);
   - datu kopēšana;
   - modificēšana vai kļūdainu datu norādīšana;
   - dzēšana vai iznīcināšana;
   - zādzība vai nozaudēšana;
   - nav vēl zināms.

7. Uz kādiem datiem pārkāpums ir attiecināms (*atzīmēt attiecīgo*):
   - datu subjektu identitāte (*personu vārdi, uzvārdi, dzimšanas datums*);
   - identifikācijas numurs (*personas kods*);
   - kontaktinformācija (*piemēram, tālruņa Nr., e-pastu adreses*);
   - piekļuvju vai identificēšanas informācija (*piemēram, lietotājvārds, parole, konta numurs*);
   - ekonomiskie un finanšu dati (*piemēram, bankas konta numurs*);
   - sakaru pakalpojumu noslodzes dati (*piemēram, dati par atrašanās vietu, saziņas numuri*);
   - oficiālie dokumenti (*personu apliecinošu un citu personas datu saturošu dokumentu kopijas*);
   - īpašu kategoriju personas dati (piemēram, tautība, ticība, piederība arodbiedrībai);
   - informācijas par krimināLsodāmību un/vai nodarījumiem, vai uzliktajiem drošības pasākumiem;
   - Citi dati: _____.

Darbības, kas veiktas pēc personas datu aizsardzības pārkāpuma konstatēšanas *(lūdzu norādiet)*:

_____

(paraksts, atšifrējums, datums)

2. pielikums
pie Personas datu aizsardzības pārkāpumu
izmeklēšanas kārtība

Personas datu aizsardzības pārkāpuma smagums

un riska novērtējums

Lai noteiktu pārkāpuma līmeni, Atbildīgajam par datu aizsardzību (vai Komisijai) jānovērtē ar Personas datu aizsardzības pārkāpumu saistīto faktu kopums, tai skaitā, bet ne tikai, iespējamās sekas, šādu seku iestāšanās iespējamība, iesaistīto datu subjektu un personas datu ierakstu skaits un citas būtiskas ziņas par pārkāpumu.

I Informācija par pārkāpumu un tā smagumu:

Uzsākts aizpildīt: __.___._____	*Pabeigts aizpildīt:* ___.___.____
1. **Novērtējot Pārkāpuma smagumu, jāņem vērā šādi fakti:**	*Zemāk norādiet atbildes uz jautājumiem*
Ziņas par drošības pārkāpumā iesaistītajām IT sistēmām, iekārtām, ierīcēm, ierakstiem;	
ziņas par skarto informāciju (personas datiem):	
kāds ir informācijas raksturs (fakts)?	
cik liels datu apjoms ir skarts? Informācija par rezerves kopijām un to veidošanas kārtību?	
vai informācija ir unikāla? Vai tās zaudējums radīs negatīvas sekas Uzņēmumam vai trešo personu darbībai, pētniecībai, finanšu un tiesiskajiem apstākļiem, atbildībai vai reputācijai?	
cik datu subjekti ir skarti?	
vai un cik lielam saņēmēju lokam dati varētu būt kļuvuši prettiesiski pieejami?	
Vai uzņēmums ir atzīstams par pārzini? (*šajā gadījumā var neaizpildīt šīs veidlapas sadaļu Riska novērtējums)*	

vai Uzņēmums darbojas kā apstrādātājs? Ja jā - ko paredz līgumattiecības ar Pārzini? (*šajā gadījumā var neaizpildīt šīs veidlapas sadaļu Riska novērtējums, ja vien to neparedz savstarpējais līgums ar Pārzini).*	
kāds ir datu sensitivitātes raksturs? Vai kādi no skartajiem datiem uzskatāmi par augsta riska datiem (kritēriji norādīti zemāk)?	
• personas dati, kas attiecināmi uz Īpašo personas datu kategorijas datiem (tai skaitā veselības datiem);	
• informācija, ko var izmantot identitātes krāpniecībai, piemēram, personīgais bankas konts un cita finanšu informācija, kā arī nacionālie identifikācijas līdzekļi, piemēram, identifikācijas dokumenta numurs, personas kods, pasu un vīzu kopijas;	
• personas informācija, kas attiecas uz neaizsargātiem pieaugušajiem vai bērniem;	
• detalizēti personu profili, tai skaitā informācija par darba veikumu, darba algu vai personīgo dzīvi, kas var radīt nozīmīgu kaitējumu vai nodarīt postu šai personai atklāšanas gadījumā;	
• drošības informācija, kas var kompromitēt personu drošību atklāšanas gadījumā, piemēram, atrašanās vietas dati, biometriskie dati, ja tiek tiek izmantoti identifikācijai.	

II. Riska novērtējums

Novērtējot riskus Datu subjektiem, jāizskata šādi jautājumi: Kāda veida personas dati ir skarti? Kādas ir potenciālās negatīvās sekas personām? Cik nopietnas vai būtiskas ir šīs sekas? Cik liela ir iespējamība, ka tās iestāsies? Papildus apskatāmi riski **Uzņēmumam, kas ietver sekojošus jautājumus:** stratēģiskās un operatīvās sekas; atbilstības un tiesiskās saistība; finansiālās sekas; sekas reputācijai; pakalpojumu līmeņu nepārtrauktība.

Pārkāpuma līmeņa noteikšana - izvēlaties vienu aprakstu, kas visvairāk atbilst faktiskajai situācijai un norādiet pamatojumu. Ja iespējams, pamatojumā iekļaujiet paskaidrojumu kāpēc netika izvēlēts augstāks riska līmenis?

! Gadījumā, ja par atbilstošo tiek uzskatīts 2. vai 3. riska līmenis obligāti sagatavojams paziņojums Datu Valsts Inspekcijai, ievērojot Kārtībā noteikto.

1. līmenis. Vietēja / zema līmeņa Pārkāpums.

- Nenozīmīgs pakalpojumu sniegšanas traucējums; nav nopietnu draudu dzīvībai/veselībai, īpašumam vai personu tiesībām un brīvībām; nav draudu Uzņēmuma tēlam/reputācijai.
- Drošības pārkāpuma sekas, datu nozaudēšanu vai nepieejamību var risināt parasto darbības procedūru ietvaros.
- Sekas datu subjektiem: īslaicīgi nepieejami, aizkavēti vai palēninâti pakalpojumi, īslaicīga nespēja pildīt darba uzdevumus (Uzņēmuma darbiniekiem) un nav konstatējamu seku nedz datu subjekta tiesībām un brīvībām, ne Uzņēmumam.
- Ja uzņēmums darbojas kā apstrādātājs, Atbildīgais par datu aizsardzību / Komisijas vadītājs lemj, vai jāziņo pārzinim (izvērtē, ko paredz attiecīgais līgums ar pārzini).
- **Kopumā nav riska vai pastāv zems risks datu subjektu un Uzņēmuma interesēm, tiesībām un brīvībām jeb risks ir operatīvi (72 h laikā pēc atklāšanās) novēršams)**

! Ja vien nav operatīvi novērsti riski datu subjekta tiesībām un brīvībām, gadījumos, kad ir skarti augsta riska dati (skatīt Pielikuma sadaļā I), par atbilstošu tiks uzskatīts kāds cits riska līmenis

2. līmenis. Vidēji kritisks stāvoklis / vidēja līmeņa Pārkāpums. • Uzņēmuma pamatpakalpojuma funkcionēšanas traucējums; iespējami draudi dzīvībai/veselībai, īpašumam vai personu tiesībām un brīvībām nenozīmīgā līmenī. Draudi Uzņēmuma tēlam/reputācijai. • Ierobežošanai un novēršanai nepieciešama citu personāla locekļu palīdzība Uzņēmuma ietvaros vai neatkarīgu speciālistu atbalsta palīdzība. • Sekas datu subjektiem: viņu personas datu integritātes zaudējums, ilgstoša pakalpojumu nepieejamība. • Skartie personas dati ietver Augsta riska personas datus (kā norādīts šī Pielikuma sadaļā I), bet tie neveido pilnu informācijas loku jeb bez papildus informācijas iegūšanas, tiek nav izmantojami (piemēram pseidonimizēti dati). • Par Pārkāpumu jāziņo Uzņēmuma augstākajai vadībai un uzraudzības iestādei, jāvērtē, vai nepieciešams ziņot datu subjektiem (Ja uzņēmums darbojas kā apstrādātājs, jāvērtē, kam paredzēts ziņot atbilstoši līgumattiecībām ar pārzini). • Atbildīgais par datu aizsardzību / Komisijas vadītājs lemj, kam vēl jāsniedz palīdzība vai jāzina par pārkāpumu • **Kopumā vidējs risks datu subjektu un/vai Uzņēmuma interesēm, tiesībām un brīvībām**.	

3. līmenis. Liela mēroga kritisks stāvoklis / augsta līmeņa Pārkāpums.

- Uzņēmuma pamatpakalpojuma funkcionēšanas traucējumi ar iespējamu ilgtermiņa kaitējumu. Nozīmīgi draudi personu dzīvībai/veselībai, īpašumam, tiesībām un brīvībām. Iesaistīts ievērojams skaits skarto datu subjektu. Nozīmīgi draudi Uzņēmuma tēlam/reputācijai.
- Var būt iesaistītas datu apstrādes sistēmas, kas var būt vitāli svarīgas Uzņēmumam, sistēmisks traucējums. Ļoti iespējams, ka tā zaudējums radīs negatīvas finansiālas vai tiesiskas sekas, ietekme uz Uzņēmuma reputāciju.
- Pārkāpuma ierobežošana un novēršana prasa nozīmīgus Uzņēmuma resursus, kas pārsniedz parastās darba kārtības ietvarus.
- Skartie personas dati ietver nozīmīgu Augsta riska personas datu apjomu (kā norādīts šī Pielikuma sadaļā I).
- Sekas datu subjektiem: īpašu kategoriju personas datu konfidencialitātes zaudējums, krāpniecības / identitātes zādzības risks, personas datu, tai skaitā Augsta riska datu nesankcionēta atklāšana nezināmam skaitam trešo personu, pakalpojumu nepieejamība ilgtermiņā. Kompromitētos datus var izmantot apstrādei, kas varētu radīt augstu risku datu subjektu tiesībām un brīvībām, piemēram ierobežojot tā iespējas darba tirgū, var ietekmēt tā reputāciju vai labklājību.
- Par Pārkāpumu nekavējoties jāziņo Uzņēmuma augstākajai vadībai, uzraudzības iestādei un datu subjektiem (Ja uzņēmums darbojas kā apstrādātājs, jāvērtē, kam paredzēts ziņot atbilstoši līguma attiecības ar pārzini)
- Ja tā ir, Atbildīgais par datu aizsardzību / Komisijas vadītājs lemj par to, kam vēl jāsniedz palīdzība vai kas vēl ir jāinformē par pārkāpumu.
- **Kopumā augsts risks datu subjektu un Uzņēmuma tiesībām un brīvībām**.

Datu aizsardzības speciālista komentāri, ja ir: _____

_____

_____

_____

_____

3.pielikums
pie Personas datu aizsardzības pārkāpumu
izmeklēšanas kārtība

PAZIŅOJUMA FORMA UZRAUDZĪBAS IESTĀDEI

[GGGG.MM.DD]

No kā: [Uzņēmums], [Uzņēmuma reģistrācijas Nr.]

[Adrese]

[Kontaktinformācija]

Kam: [Uzraudzības iestāde]

[Adrese]

Informējam, [uzņēmuma nosaukums] ir noticis personas datu apstrādes aizsardzības pārkāpums (Personas datu pārkāpums). Ziņas par personas datu pārkāpumu ir norādītas turpmākajā tabulā.

1. **Personas datu pārkāpuma datums un laiks:** [GGGG.MM.DD hh:mm vai laika periods]
2. **Personas datu pārkāpuma raksturs:**
3. **Personas datu pārkāpuma iespējamie iemesli (cēloņi):**
4. **Iesaistītās personas datu kategorijas un dokumenti:**
5. **Personas datu pārkāpuma iespējamās sekas:**
6. **Personas datu pārkāpuma risināšanai un iespējamā kaitējuma mazināšanai veiktie pasākumi:**

Kontaktinformācija:

tālr.:_____

e-pasta adrese: _____

Atbildīgais par datu aizsardzību

_____
(Vārds, uzvārds)

APSTIPRINĀTS
ar 09.12.2020. valdes lēmumu Nr.2-28/A1-7

VISPĀRĪGĀ PERSONAS DATU APSTRĀDES UN AIZSARDZĪBAS PROCEDŪRA

1. Mērķis

Šī Vispārīgā personas datu apstrādes un aizsardzības procedūra (turpmāk tekstā – Procedūra) nosaka vispārējo personas datu apstrādes un aizsardzības kārtību valsts sabiedrības ar ierobežotu atbildību "Latvijas Radio", vienotais reģ. Nr. 40003080614, turpmāk tekstā - Uzņēmums, kas ir jāievēro, lai Uzņēmums nodrošinātu godprātīgu, likumīgu un pārredzamu fizisko personu personas datu apstrādi un aizsardzību.

2. Darbības joma un lietotāji (atbildīgie darbinieki)

2.1. Šī Procedūra attiecas uz Uzņēmumu, kas apstrādā fizisko personu datus, lai nodrošinātu Uzņēmuma pamatdarbību, tiesiskās intereses un Latvijas Republikā spēkā esošo saistošo tiesību aktu prasību ievērošanu.
2.2. Šajā Procedūrā izklāstīti pamatprincipi, saskaņā ar kuriem Uzņēmums apstrādā tādu fizisko personu kā, piemēram, klientu, apmeklētāju, klausītāju, darījumu partneru kontaktpersonu un citu fizisko personu personas datus, kā arī norāda Uzņēmuma darbinieku pienākumus un tiesības, apstrādājot fizisko personu personas datus.
2.3. Šīs Procedūras lietotāji ir visi Uzņēmuma darbinieki un sadarbības partneri, kas darbojas Uzņēmuma vārdā un veic fizisko personu datu apstrādi.

3. Atsauces uz dokumentiem

3.1. Eiropas Parlamenta un Padomes Regula (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 tekstā - Regula).
3.2. Fizisko personas datu apstrādes likums (turpmāk tekstā - Datu likums).
3.3. Citi Latvijas republikā spēkā esošie saistošie tiesību akti, kas reglamentē šajā Procedūrā noteikto, tajā skaitā, speciālie normatīvie akti.

4. Lietotie termini

Šajā Procedūrā lietoto terminu definīcijas izriet no Regulas 4. panta un, tas ir:
4.1. **Personas dati** - jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu (Datu subjekts); identificējama fiziska persona ir tāda, kuru var tieši vai netieši identificēt, jo īpaši atsaucoties uz identifikatoru, piemēram, tajā skaitā, bet ne tikai, personas vārdu, uzvārdu, personas kodu, dzimšanas datiem, dzīvesvietas adresi, darba vietu, tālruņa numuru, ģimenes stāvokli, e-pasta adresi, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem.
4.2. **Īpašo personas datu kategorijas personas dati** - Personas dati, kas atklāj rasi vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arodbiedrībās, kā arī, ģenētiskie dati, biometriskie dati, lai veiktu fiziskas personas unikālu identifikāciju, veselības dati vai dati par fiziskas personas dzimumdzīvi vai seksuālo orientāciju.

4.3. **Personas datu apstrāde** - jebkuras ar Personas datiem vai Personas datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, ieskaitot datu vākšanu, reģistrēšanu, ievadīšanu, glabāšanu, pielāgošanu, sakārtošanu, pārveidošanu, izmantošanu, aplūkošanu, nodošanu, pārraidīšanu, izpaušanu, nosūtīšanu, izplatīšanu, saskaņošanu, ierobežošanu, bloķēšanu, dzēšanu vai iznīcināšanu. (Politika tiek piemērota jebkāda veida Personas datu apstrādei – manuālai un datorizētai).
4.4. **Datu subjekts** - fiziskā persona, kuru var tieši vai netieši identificēt un kuras Personas dati tiek apstrādāti.
4.5. **Datu subjekta piekrišana** - jebkura brīvi sniegta, konkrēta, apzināta un viennozīmīga norāde uz Datu subjekta vēlmēm, ar kuru viņš paziņojuma vai skaidri apstiprinošas darbības veidā sniedz piekrišanu savu Personas datu apstrādei.
4.6. **Uzņēmums** – Valsts sabiedrība ar ierobežotu atbildību "Latvijas Radio", reģistrācijas numurs 40003080614, juridiskā adrese: Doma laukums 8, Rīga, LV-1505, e-pasta adrese: radio@latvijasradio.lv, tīmekļa vietne: www.latvijasradio.lv.
4.7. **Pārzinis** - Regulas izpratnē Uzņēmums ir tādu fizisko personu Personas datu apstrādes pārzinis, kuriem Uzņēmums viens pats vai kopīgi ar citiem nosaka Personas datu apstrādes nolūkus (mērķus) un līdzekļus.
4.8. **Apstrādātājs** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura Pārziņa vārdā apstrādā Personas datus.
4.9. **Personas datu saņēmējs** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kurai izpauž Personas datus – neatkarīgi no tā, vai tā ir trešā persona vai nav. Tomēr publiskas iestādes, kas var saņemt Personas datus saistībā ar konkrētu izmeklēšanu saskaņā ar Eiropas savienības vai dalībvalsts tiesību aktiem, netiek uzskatītas par saņēmējiem; minēto datu apstrāde, ko veic minētās publiskās iestādes, atbilst piemērojamiem datu aizsardzības noteikumiem saskaņā ar apstrādes nolūkiem.
4.10. **Trešā persona** - fiziska vai juridiska persona, publiska iestāde, aģentūra vai struktūra, kura nav Datu subjekts, Pārzinis, Apstrādātājs un personas, kuras Pārziņa vai Apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt Personas datus.
4.11. **Personas datu aizsardzības pārkāpums** - drošības pārkāpums, kura rezultātā notiek nejauša vai nelikumīga nosūtīto, uzglabāto vai citādi apstrādāto Personas datu iznīcināšana, nozaudēšana, pārveidošana, neatļauta izpaušana vai piekļuve tiem.
4.12. **Uzraudzības iestāde Latvijā** - Datu valsts inspekcija.
4.13. **Datu apstrādes reģistrs** - dokuments, kurā tiek reģistrētas Pārziņa pakļautībā veiktās Personas datu apstrādes darbības.
4.14. **Darbinieks** – persona, kura ar Uzņēmumu slēdz vai ir noslēgusi darba līgumu vai saskaņā ar citu civiltiesisku līgumu veic vai varētu veikt pienākumus, kuras Personas dati var tikt apstrādāti un kurai ir jāievēro šajā Procedūrā minētie Personas datu apstrādes nosacījumi.
4.15. **Atbildīgais par datu aizsardzību** - Uzņēmuma atbilstoši pilnvarots Darbinieks, kura pienākums ir organizēt un nodrošināt iespējamo Personas datu aizsardzības pārkāpumu izmeklēšanu, pārvaldību un dokumentēšanu, atbilstoši fizisku Personu datu aizsardzību regulējošo normatīvo aktu prasībām. Ja vien ar valdes rīkojumu nav noteikts savādāk, Administratīvais direktors - Juridiskās daļas vadītājs
4.16. **Datu aizsardzības speciālists** - Persona Uzņēmumā, kas ir sasniedzama, izmantojot e-pasta adresi: datuaizsardziba@latvijaradio.lv, un kuram ir šādi uzdevumi: informēt un konsultēt Uzņēmumu, tā darbiniekus, uzraudzīt vai tiek ievērotas normatīvo aktu prasības attiecībā uz Personas datu aizsardzību, pēc pieprasījuma sniegt padomus par nepieciešamību sagatavot

novērtējumu par ietekmi uz datu aizsardzību, sadarboties ar uzraudzības iestādi un būt par kontaktpunktu jautājumos, kas saistīti ar datu apstrādi (Regulas 37.pantā noteiktajā kārtībā iecelts datu aizsardzības speciālists, un kuram ir Regulas 39.pantā noteiktie uzdevumi).

4.17. **Žurnālistika** - Personas datu apstrāde, kuru veic, lai īstenotu tiesības uz vārda un informācijas brīvību, ievērojot personas tiesības uz privāto dzīvi, un netiek skartas tādas datu subjekta intereses, kurām nepieciešama aizsardzība un kuras ir svarīgākas par sabiedrības interesēm, attiecīgā datu apstrāde ir veikta ar mērķi publicēt informāciju, kas skar sabiedrības intereses un Regulas prasību ievērošana nav savietojama vai liedz īstenot tiesības uz vārda un informācijas brīvību.

5. Personas datu apstrādes noteikumi

5.1. Personas datus drīkst apstrādāt tikai Uzņēmuma iekšējos dokumentos paredzētajos gadījumos un kārtībā.

5.2. Pirms Personas datu apstrādes uzsākšanas, jebkurš Darbinieks, t.i., atbildīgā persona, kuras pārraudzībā tiek plānota (vai ir) Personas datu apstrāde vai kura ir iniciējusi jaunu Personas datu apstrādi, sagatavo datu apstrādes reģistru (1. pielikums „Datu apstrādes reģistrs").

5.3. Katrs darbinieks ir atzīstams par atbildīgo personu, ja konkrētais datu apstrādes mērķis izriet no konkrētā darbinieka amata apraksta.

5.4. Plānojot Personas datu apstrādi un sagatavojot Datu apstrādes reģistru, atbildīgai personai, jānodrošina, ka tiek ievēroti Personas datu apstrādes labas prakses principi, kas cita starpā ietver:

5.4.1. godprātīga un likumīga Personas datu apstrāde, Datu subjektam pārredzamā veidā;

5.4.2. Personas datu apstrādi tikai atbilstoši paredzētajam mērķim un tam nepieciešamajā apjomā;

5.4.3. tādu Personas datu glabāšanas veidu, kas datu subjektu ļauj identificēt attiecīgā laikposmā, kurš nepārsniedz paredzētajam datu apstrādes mērķim noteikto laikposmu;

5.4.4. Personas datu pareizību un to savlaicīgu atjaunošanu, labošanu vai dzēšanu, ja Personas dati ir nepilnīgi vai neprecīzi saskaņā ar Personas datu apstrādes mērķi;

5.4.5. apstrādi tādā veidā, lai tiktu nodrošināta atbilstoša Personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot un norādot atbilstošus tehniskos vai organizatoriskos pasākumus.

5.5. Tiek uzskatīts, ka Personas dati Uzņēmumā tiek apstrādāti likumīgi, ja ir vismaz viens no šādiem nosacījumiem (tiesiskais pamats datu apstrādei):

5.5.1. **ir Datu subjekta piekrišana**. Šis tiesiskais pamats Personas datu apstrādei izmantojams tikai tajā gadījumā, ja Datu subjekts ir brīvs savā izvēlē un nav saskatāma nekāda veida saikne ar citām tiesībām vai pienākumiem, ko šī piekrišana uzliek Datu subjektam. Bez tam, izvēloties šo tiesisko pamatu Personas datu apstrādei, jāņem vērā apstāklis, ka Datu subjekts ir (būs) tiesisks atsaukt savu piekrišanu jebkurā brīdī, kas, savukārt, nozīmē, ka atsaukuma gadījumā Uzņēmuma mērķis, kas izrietēja no konkrētās datu apstrādes, netiek ietekmēts un Uzņēmuma tiesiskās intereses netiks aizskartas;

5.5.2. datu apstrāde izriet no **Datu subjekta līgumsaistībām** vai, ievērojot Datu subjekta lūgumu, datu apstrāde nepieciešama, **lai noslēgtu attiecīgu līgumu**. Šis tiesiskais pamats datu apstrādei izmantojams, ja ir paredzēts slēgt līgumu ar Datu subjektu un attiecīgā Personas datu apstrāde tieši izriet no līgumsaistību izpildes. Gadījumā, ja ir vēlme apstrādāt papildu datu kategorijas, kas neizriet no nepieciešamības izpildīt līgumu, nepieciešams izvērtēt cita tiesiskā pamata esamību Personas datu apstrādei;

5.5.3. datu apstrāde nepieciešama Uzņēmumam **likumā noteikto pienākumu veikšanai**. Šis tiesiskais pamats Personas datu apstrādei izmantojams, ja Latvijas Republikas spēkā esošais

normatīvais akts tieši nosaka datu apstrādes apjomu un kārtību. Gadījumā, ja ārējā normatīvajā aktā ir norādīts tikai sasniedzamais rezultāts, nepieciešams izvērtēt cita tiesiskā pamata esamību Personas datu apstrādei;

5.5.4. datu apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas fiziskas **personas vitālas intereses**;

5.5.5. datu apstrāde ir vajadzīga, **lai izpildītu uzdevumu, ko veic sabiedrības interesēs vai īstenojot Pārzinim piešķirtās oficiālās pilnvaras**. Uz Personas datu apstrādi žurnālistikas vajadzībām, ievērojot šajā procedūrā norādīto žurnālistikas definīciju, attiecināms šis tiesiskais pamats datu apstrādei;

5.5.6. datu apstrāde ir vajadzīga **Pārziņa vai trešās personas leģitīmo interešu ievērošanai,** izņemot, ja Datu subjekta intereses vai pamattiesības un pamatbrīvības, kurām nepieciešama Personas datu aizsardzība, ir svarīgākas par šādām interesēm, jo īpaši, ja datu subjekts ir bērns. Izmantojot šo tiesisko pamatu Personas datu apstrādei, nepieciešams detalizēti definēt un izskaidrot kāda ir Uzņēmuma vai trešās personas leģitīmā interese un veicot šo datu apstrādi Datu subjekta intereses vai pamattiesības un pamatbrīvības ierobežojums ir samērojams ar Uzņēmuma vai trešās personas interesēm.

5.6. Gadījumā, ja plānotā Personas datu apstrādes mērķis ietver īpašo Personas datu apstrādi, atbildīgā persona saskaņo šādu datu apstrādi ar Administratīvo direktoru - Juridiskās daļas vadītāju un/vai Datu aizsardzības speciālistu.

5.7. Ja Personas datu apstrādes veids (jo īpaši, izmantojot jaunās tehnoloģijas un ņemot vērā apstrādes raksturu, apjomu, kontekstu, un nolūkus) varētu radīt augstu risku fizisku personu tiesībām un brīvībām, Pārziņa atbildīgais darbinieks, papildu Datu apstrādes reģistra aizpildīšanai, sadarbojoties ar Administratīvo direktoru - Juridiskās daļas vadītāju, obligāti sagatavo Personas datu apstrādes ietekmes novērtējumu. Šaubu gadījumā par nepieciešamību sagatavot Personas datu apstrādes ietekmes novērtējumu, saņemams Datu aizsardzības speciālista padoms.

5.8. Atbildīgās personas pienākums ir uzturēt Datu apstrādes reģistrus par savā pārraudzībā esošajām datu apstrādēm un regulāri atjaunot tajā esošo informāciju, it sevišķi, veicot izmaiņas esošā Personas datu apstrādes procesā, Datu apstrādes reģistrs atjaunojams un izmaiņas saskaņojamas ar Datu aizsardzības speciālistu, ne vēlāk kā dienā, kad tiek uzsākta apstrāde, kas bija par pamatu izmaiņu veikšanai.

5.9. Pēc iepazīšanās ar Datu apstrādes reģistru, tā grozījumiem, Datu aizsardzības speciālists var dot papildu uzdevumus, ko nepieciešams ieviest attiecībā uz plānoto Personas datu apstrādi vai pieprasīt papildu informāciju.

5.10. Uzņēmuma darbiniekam, kas veic Personas datu apstrādi kopā ar atbildīgo personu par konkrēto datu apstrādi, ir jācenšas savākt vismazāko iespējamo Personas datu apjomu un jānodrošina, lai apstrādājamie Personas dati neietvertu lielāku apjomu vai netiktu apstrādāti ilgāk, nekā tas ir nepieciešams mērķa sasniegšanai. Atbildīgajai personai ir jānodrošina, ka faktiskā Personas datu apstrāde ir atbilstoša Datu apstrādes reģistrā norādītajai informācijai.

5.11. Datu apstrādes mērķim ir jābūt konkrēti izvirzītam un noteiktam Datu apstrādes reģistrā vai citos Uzņēmuma valdes apstiprinātajos dokumentos. Personas dati ir jāapstrādā tikai tādam nolūkam (mērķim), kādā tie sākotnēji tika savākti. Gadījumā, ja ir nepieciešams apstrādāt savāktos Personas datus citam mērķim (nolūkam), atbildīgajam darbiniekam ir jāinformē Administratīvo direktoru - Juridiskās daļas vadītāju un jāveic pasākumi, lai nodrošinātu Datu subjekta tiesību realizāciju (būt informētam par jauno datu apstrādes mērķi, tiesisko pamatu u.tml.). Jebkurā šādā paziņojumā jāiekļauj sākotnējais mērķis, kuram dati tika vākti, kā arī jaunais vai papildu mērķis(-

i). Paziņojumā jāietver arī mērķa (-u) izmaiņu iemesls. Atbildīgais darbinieks ir atbildīgs par šī punkta noteikumu ievērošanu.

5.12. Uzņēmuma darbiniekam, kas veic Personas datu apstrādi kopā ar atbildīgo personu, ir jānodrošina, lai Personas dati vienmēr būtu precīzi, aktuāli un atbilstoši vākšanas mērķim. Tādēļ uzsākot Personas datu apstrādi vai veicot grozījumus esošajā Personas datu apstrādē, atbildīgajai personai, sazinoties ar Administratīvo direktoru - Juridiskās daļas vadītāju, nepieciešams ieviest procedūru kādā tiek nodrošināta tās rīcībā esošo Persona datu apstrāde, labošana, glabāšana, dzēšana, apstrādes ierobežošana, u.tml. Nepilnīgi, novecojuši, nepatiesi, pretlikumīgi apstrādāti dati vai dati, kuri vairs nav nepieciešami vākšanas mērķim, ir attiecīgi jāizlabo vai jāizdzēš. Par to ir jāpaziņo arī trešajām personām, kas iepriekš saņēmušas novecojušos vai nepatiesos Personas datus.

5.13. Iegūstot Personas datus no Datu subjekta, Apstrādātājam ir jāpaziņo Datu apstrādes reģistrā iekļautā informācija, izņemot informācija par tehniskajām un organizatoriskajām prasībām, kas ieviestas ar mērķi nodrošināt datu drošību, ja vien tā jau nav Datu subjekta rīcībā. Ja darbiniekam rodas šaubas par Personas datu apstrādes atbilstību (pamatojumu, mērķi un apjomu utt.), Personas datu izpaušanas likumību vai citiem jautājumiem, kas attiecas uz Personas datu apstrādi, par to jāziņo Datu aizsardzības speciālistam.

6. Sadarbība ar Apstrādātāju

6.1 Katru reizi, kad ir nepieciešams Personas datu apstrādē izmantot Apstrādātāju, lai apstrādātu Personas datus savā vārdā, Uzņēmumam ir jānodrošina, ka šis Apstrādātājs nodrošinās Personas datu drošības tehniskos un organizatoriskos pasākumus, lai aizsargātu Personas datus, kas atbilst attiecīgajiem riskiem.

6.2. Atbildīgajai personai, organizējot līguma noslēgšanu ar Apstrādātāju, to noslēdzot, ir jānodrošina sekojošu būtisko prasību izpilde:

6.2.1. ka tas nodrošinās tādu pašu vai līdzvērtīgu datu aizsardzības līmeni kā Uzņēmums. Gadījumā, ja Apstrādātājs nevar nodrošināt, tad ar šādu Apstrādātāju ir jāpārtrauc sadarbība vai līgums nevar tikt noslēgts;

6.2.2. jāapstrādā Personas dati Pārziņa uzdevumā, lai izpildītu līgumsaistības pret Uzņēmumu vai pēc Uzņēmuma norādījumiem, nevis citiem mērķiem (nolūkiem);

6.2.3. skaidri jānorāda Apstrādātāja pienākumi un atbildība, kas, cita starpā ietver Personas datu apstrādes dzīvesciklu.

6.3. Uzņēmuma darbiniekiem ir aizliegts, bez iepriekšējas Uzņēmuma valdes informēšanas un attiecīgu dokumentu sakārtošanas (procesu ieviešanas), nosūtīt/nodot Personas datus ārpus Eiropas Savienības un Eiropas Ekonomiskās zonas (EEZ) robežām. Jo pirms Personas datu nodošanas, ir jāizmanto atbilstošas drošības garantijas, tostarp Eiropas Savienības prasību par datu nodošanu līguma parakstīšana, un, ja nepieciešams, ir jāsaņem atļauja no attiecīgās uzraudzības iestādes. Tikai pēc Uzņēmuma valdes saskaņojuma saņemšanas, Uzņēmuma darbinieks ir tiesīgs nosūtīt/nodot Personas datus ārpus Eiropas Savienības un Eiropas Ekonomiskās zonas (EEZ) robežām, ievērojot Uzņēmuma valdes norādījumus par nodošanas veidu un apjomu.

7. Kārtība kādā tiek reaģēts uz Datu subjekta pieprasījumiem

7.1. Jebkuram darbiniekam, saņemot Datu subjekta pieprasījumu piekļūt saviem Personas datiem un ja tas pārsniedz ikdienas amata pienākumu izpildi, ir pienākums lūgt šādu pieprasījumu fiksēt rakstveidā un nodot to Administratīvajam direktoram - Juridiskās daļas vadītājam atbildes sagatavošanai. Gadījumā, ja Datu subjekts atsakās rakstīt rakstveida iesniegumu, jebkura

darbinieka pienākums ir ziņot par šādu situāciju Administratīvajam direktoram - Juridiskās daļas vadītājam. Administratīvais direktors - Juridiskās daļas vadītājs, izvērtējot situācijas apstākļus, ziņo par to Datu aizsardzības speciālistam.
7.2. Ja Datu subjekts pieprasa labot, grozīt vai iznīcināt Datu subjekta Personas datus, saņemt datu kopiju vai ierobežot datu apstrādi, jānodrošina, ka šie Datu subjekta pieprasījumi tiek apstrādāti saprātīgā termiņā, bet ne vēlāk kā 30 dienu laikā no Datu subjekta pieprasījuma saņemšanas dienas, izņemot, ja attiecīgie Personas dati tiek apstrādāti žurnālistikas vajadzībām. Uzņēmuma Sekretariātam jāreģistrē pieprasījumi un jāuztur reģistrācijas žurnāls par tiem. Jebkura atbilde uz Datu subjekta pieprasījumu saskaņojama ar Datu aizsardzības speciālistu.

8. Nobeiguma noteikumi

8.1. Konkrēta veida Personas datu apstrādes noteikumi (datu apstrādes tehniskās un organizatoriskās prasības) tiek papildinātas un precizētas vai grozītas atsevišķos Uzņēmuma dokumentos konkrēto Personas datu veidiem un apstrādes mērķiem. Pretrunu gadījumā starp šo Procedūru un īpašajiem noteikumiem par attiecībā uz konkrēta veida datu apstrādes noteikumiem, priekšroka dodama īpašajiem noteikumiem.
8.2. Darbinieki tiek iepazīstināti ar iekšējiem normatīvajiem dokumentiem, kas regulē Personu datu apstrādes noteikumus, saskaņā ar Darba un iekšējās kārtības noteikumu punktu 1.14.5 „Darbiniekiem, kuri ikdienā strādā ar datoru, uzsākot darbu, ir jāatver iekšējā mājas lapa un jāiepazīstas ar jaunāko informāciju (rīkojumi, valdes lēmumi, paziņojumi u.c.). Ja informācija ir ievietota iekšējā mājas lapā, uzskatāms, ka darbinieks ar šo informāciju ir iepazīstināts".
8.3. Ja rodas pretrunas starp šo Procedūru un Latvijas Republikā spēkā esošajiem saistošajiem tiesību aktiem, noteicošais ir pēdējais.
8.4. Administratīvajam direktoram - Juridiskās daļas vadītājam ne retāk kā reizi gadā jāpārbauda un, ja ir nepieciešams, ir jāatjaunina šī Procedūra.

1. pielikums
pie Vispārīgās personas datu apstrādes un aizsardzības procedūras

DATU APSTRĀDES REĢISTRS

Nr.		
1.	Pārziņa nosaukums un reģistrācijas numurs), adrese un tālruņa numurs	_____, Reģ. Nr. _____, juridiskā adrese:_____
2.	Pieprasītais Pakalpojums (Personas datu apstrādes mērķis)	
3.	Personas datu apstrādes tiesiskais pamats: a) Datu subjekta piekrišana; b) Lai izpildītu līgumu ar datu subjektu; c) Lai izpildītu likumu; d) lai aizsargātu vitālās intereses e) Lai nodrošinātu Organizācijas leģitīmās interese; f) ...	
4.	Personas datu Apstrādātājs	
4.1.	Apstrādātāja piesaistītie Apstrādātāji, ja ir	
5.	Personas datu veidi:	
6.	Datu subjektu kategorijas	

Nr.		
7.	Personas datu saņēmēju kategorijas	
8.	Paredzētais Personas datu apstrādes veids	Jaukti: elektroniski un manuāli (papīra formā).
9.	Plānotais Personas datu iegūšanas veids	
10.	Personas datu apstrādes vieta;	
11.	Laikposms, cik ilgi Personas dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai	
12.	Apraksts kādā veidā datu subjektam tiks paziņots par viņa tiesībām (pieprasīt piekļuvi, iepazīties ar Personas datiem, saņemt kopiju, pieprasīt labot, dzēst u.tml.)	Informācija iekļauta Privātuma politikā.
13.	Tehniskie un organizatoriskie pasākumi, kas nodrošina Personas datu aizsardzību	