

APSTIPRINĀTS:

SIA „Izdevniecība dienas Medijf”

Vienotais reģistrācija numurs: 40003804497

Valdes loceklis

Edgars Kots

Rīgā, 2018. gada 24. maijā

**DATU AIZSARDZĪBAS POLITIKA
UZŅĒMUMĀ**

Pamatojoties uz Eiropas Parlamenta un Padomes regulu (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**, kuras mērķis ir:

- a) paredzēt noteikumus fizisku personu aizsardzībai attiecībā uz personas datu apstrādi un noteikumus personas datu brīvai aprītei;
- b) aizsargāt fizisku personu pamattiesības un pamatbrīvības un jo īpaši to tiesības uz personas datu aizsardzību,

kā arī, pamatojoties, uz to ka SIA „Izdevniecība dienas Medijf”, vienotais reģistrācija numurs: 40003804497, turpmāk tekstā – **Sabiedrība**, savā ikdienas darbā veic fiziskas personas datu apstrādi Sabiedrībai nepieciešamos apmēros,

Sabiedrība, ņemot vērā prasības, kas noteiktas normatīvajos tiesību aktos, izdod šo „*Datu aizsardzība politikā uzņēmumā*”, turpmāk tekstā – **Nolikums**, nosakot sekojošo:

1. Terminu un definīcijas

- 1.1. **Sabiedrība vai Pārzinis** – SIA „Izdevniecība dienas Medijf”, vienotais reģistrācija numurs: 40003804497;
- 1.2. **Datu subjekts** - fiziskā persona, kuru var tieši vai netieši identificēt;
- 1.3. **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, minētās personas vārdu, uzvārdu, identifikācijas numuru, atrašanās vietas datiem, tiešsaistes identifikatoru vai vienu vai vairākiem minētajai fiziskajai personai raksturīgiem fiziskās, fizioloģiskās, ģenētiskās, garīgās, ekonomiskās, kultūras vai sociālās identitātes faktoriem;
- 1.4. **Apstrāde** - jebkura ar personas Datiem vai personas Datu kopumiem veikta darbība vai darbību kopums, ko veic ar vai bez automatizētiem līdzekļiem, piemēram, vākšana, reģistrācija, organizēšana, strukturēšana, glabāšana, pielāgošana vai pārveidošana, atgūšana, aplūkošana, izmantošana, izpaušana, nosūtīt, izplatīt vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;
- 1.5. **Darbinieks** – fiziska persona, kura uz darba līguma pamata par noteiktu darba samaksu veic konkrētus darba pienākumus Sabiedrībā;
- 1.6. **Tiešais vadītājs** – Darbinieks, kurš atbilstoši noslēgtajam darba līgumam vada noteiktu Sabiedrības struktūrvienību (nodaļu/daļu). Informācija par Darbinieka atrašanos noteiktā Sabiedrības struktūrvienībā ir ietverta darba līgumā;
- 1.7. **Datu bāze** – Datu krājums, kas sakārtots sistemātiski vai metodiski un pieejams elektroniskā vai citādā veidā;

- 1.8. **Elektroniskā ierīce vai Ierīce** – Sabiedrībai piederošs vai Sabiedrības lietošanā esošs dators, telefons, planšetdators jeb tehniska sistēma, kas saskaņā ar uzdotu programmu veic automātisku Datu apstrādi un ievadizvadi, kā arī jebkura Datu apstrādes sistēmas ierīce, kas konstruktīvi atdalīta no Elektroniskajām ierīcēm, un nodrošina sistēmas ārējos sakarus vai rada papildus iespējas (piem., monitors, printeris, skeneris u.tml.);
- 1.9. **Darba stacija** – Darbinieka vieta ar nepieciešamo inventāru Sabiedrībā;
- 1.10. **Parole** — Lietotājam zināma simbolu virkne, kuras kopija atrodas Informācijas sistēmā un kuru izmanto Lietotāja identitātes pierādīšanai;
- 1.11. **Loģiskā aizsardzība** — Datu resursu aizsardzība, kuru realizē ar programmatūras līdzekļiem, identificējot informācijas sistēmas Lietotāju, pārbaudot viņa pilnvaru atbilstību attiecīgajām darbībām informācijas sistēmā, pasargājot Datus no tišas vai nejaušas maiņas vai dzēšanas vai neatļautas izmantošanas vai izplatīšanas;
- 1.12. **Uguns mūris** — programmatūras un aparatūras komplekss, kas savieno lokālo tīklu ar ārējiem tīkliem, nodrošinot lokālajā tīklā savienoto informācijas sistēmu aizsardzību;
- 1.13. **E-pasts** – ziņojumu, t.sk., Datu, bet ne tikai, sastādīšanas, nosūtīšanas un saņemšanas metode, izmantojot Elektroniskās ierīces vai perifērijas iekārtas;
- 1.14. **Datu nesējs** - jebkāda veida fizisks objekts, kas satur Datus, t.sk. zibatmiņa, CD, DVD, dokuments, u.tml.;
- 1.15. **Ārējie normatīvie akti** – Starptautiskie, kā arī Latvijas Republikas un tās pašvaldību izdotie normatīvie tiesību akti;
- 1.16. **Iekšējie normatīvie akti** – Sabiedrības darba līgumi, darba kārtības noteikumi un citi Sabiedrības izdoti normatīvie akti, kas regulē darba kārtību un pienākumus Sabiedrībā.

*Ņemot vērā, ka Nolikums izdots saistībā ar Regulu, Regula un citi Ārējie normatīvie akti satur papildus terminus un definīcijas, kas attiecas uz šo Nolikumu un tajā noteiktā jautājuma regulējumu.

2. Mērķis

Nolikuma mērķis ir noteikt Sabiedrības un tās Darbinieku uzvedības noteikumus, kas skar Datu aizsardzību attiecībā uz personu Datu Apstrādi Sabiedrībā, un, pildot darba pienākumus Sabiedrībā, kā arī paredzēt drošības noteikumus informācijas lietošanai attiecībā uz Datiem.

3. Lietošanas sfēra

- 3.1. Šis Nolikums ir saistošs Sabiedrības Darbiniekiem, kuriem ar Sabiedrību ir noslēgts darba līgums.
- 3.2. Šis Nolikums ir pieejams papīra formātā Sabiedrības personāla daļā.
- 3.3. Nolikums tiek uzskatīts par Sabiedrības darba kārtības noteikumiem attiecībā uz Regulā paredzēto jomu un jautājumiem – Nolikums ir Sabiedrības darba kārtības noteikumu neatņemama sastāvdaļa. Pamatojoties uz šajā Nolikuma punktā noteikto, Nolikuma pārkāpums tiek uzskatīts par Sabiedrības darba kārtības un līdz ar to darba līguma pārkāpumu.

4. Sabiedrībā apstrādājami Datu veidi

- 4.1. Apstrādājami personas Dati:
 - 4.1.1. Datu subjekta vārds;
 - 4.1.2. Datu subjekta uzvārds;
 - 4.1.3. Datu subjekta personas kods;
 - 4.1.4. Datu subjekta telefona numurs;
 - 4.1.5. Datu subjekta e-pasta adrese;
 - 4.1.6. Datu subjekta faktiskā un/vai deklarētā dzīves vieta;
 - 4.1.7. Datu subjekta pases dati un/vai ID dati;
 - 4.1.8. Datu subjekta audiovizuālie dati;
 - 4.1.9. Datu subjekta ģimenes stāvoklis;

4.1.10. Datu subjekta ekonomiskais stāvoklis un ieradumi (alga, abonenti, pirkumi, u.tml.).

4.2. Apstrādājami īpašu kategoriju dati (sensitīvie dati):

4.2.1. Datu subjekta veselības stāvoklis;

4.2.2. Datu subjekta dalība arodbiedrībā.

5. Datu apstrādes principi

Nolikuma mērķa sasniegšanai Datu Apstrāde Darbiniekiem ir jāveic vadoties pēc sekojošiem principiem:

- 5.1. **Likumīgums, godprātība un pārredzamība.** Sabiedrības Darbinieki ikdienas darbībā nodrošina pret Datu subjekta Datiem godprātīgu attieksmi, kā arī Dati tiek apstrādāti labā ticībā. Godprātības princips pēc būtības ietver arī visus pārējos principus, jo visi principi pamatā ir vērsti, lai realizētu Sabiedrības kā pārziņa godīgu attieksmi pret Datu subjektu, tai skaitā, bet ne tikai, informējot viņu par Datu apstrādi, neizmantojot Datus citiem nolūkiem, kādiem tie tikuši ievākti no Sabiedrības vai tās Darbinieku puses. Godprātīga attieksme izpaužas Sabiedrības un tās Darbinieku rīcībā, respektējot Datu subjekta intereses aizsargāt savu privātumu, kā arī veidnot un atvieglojot Datu subjektam tā tiesību realizēšanu, piemēram, nodrošinot vienkāršotu Datu subjekta piekļuvi informācijai par tā Datu apstrādi, droši glabājot Datu subjekta Datus, ļaujot labot neprecīzus Datu subjekta Datus un citu tiesību īstenošanu. Sabiedrība vai tās Darbinieki, veicot Datu Apstrādi, ņem vērā Datu subjektu briedumu, vecumu un citus personības aspektus un neizmanto personas trūkumus un nezināšanu, lai sasniegtu savus nolūkus. Viena no godprātības principa izpausmēm ir Datu pārredzamības principa nodrošināšana, ar to saprotot, ka Sabiedrība vai tās Darbinieki, kas nodrošina noteiktu Sabiedrības funkciju, nodrošina pilnīgu, precīzu un pārlicinošu Datu subjektu informēšanu par sagaidāmo Datu apstrādi un tās sekām, ja nav ierobežojumu šādas informācijas izpaušanai. Turklāt, lai šo principu īstenotu, Datu subjektam informācija ir jānodrošina kodolīgā, saprotamā (ņemot vērā Datu subjekta briedumu un citas īpašības, piemēram, bērni, seniori u.c.), viegli pārskatāmā un viegli pieejamā veidā. Tādējādi Datu subjekts tiks pienācīgi informēts, apzinoties savu Datu apstrādes būtību un iespējamās sekas, un šāda Datu apstrāde neradīs nepamatotu ietekmi uz Datu subjekta privātumu. Likumīga Datu apstrāde paredz, ka Sabiedrība un tās Darbinieki atbildīgi izvēlas nolūkus, kādiem Datus plāno apstrādāt, nepieļaujot tādu nolūku rašanos un īstenošanu, kuri var nepamatoti ietekmēt Datu subjekta privātumu. Par likumīgiem nolūkiem viennozīmīgi atzīstami tādi nolūki, kas ar normatīvajiem aktiem ir uzskatāmi par samērīgiem un pieļaujamiem. Otrs būtisks likumības principa aspekts ir Datu apstrādes uzsākšana tikai atbilstoša tiesiskā pamata esamības gadījumā. Pirms jebkuru Datu ievākšanas, izpaušanas trešajām personām, kā arī pirms ievākto Datu apstrādes nolūka maiņas ir jāizvērtē, vai šādi Datu apstrādei ir piemērojams kāds no Ārējos normatīvajos tiesību aktos minētajiem tiesiskiem pamatiem. Savukārt gadījumā, ja tiek apstrādāti īpašu kategoriju Dati (piemēram, dati par veselību, tautību, reliģisko pārliecību, biometriskie dati) ir jānodrošina, ka attiecīgai Datu apstrādei ir piemērojami īpašie Regulā noteiktie tiesiskie pamati šādu datu apstrādei.
- 5.2. **Nolūka ierobežojumi.** Lai ievērotu nolūka ierobežojuma principu, Sabiedrībai un tās Darbiniekiem ir kritiski jāizvērtē katras plānotās un esošās Datu apstrādes nepieciešamība. Šī principa realizācija nepieļauj Datu ievākšanu un apstrādi bezmērķīgi (bez konkrēta nolūka) jeb neesot acīmredzamai un pastāvošai nepieciešamībai šādu Datu apstrādei. Sabiedrība un tās Darbinieki neveic Datu apstrādi, nezinot kādiem nolūkiem un kad ievāktie Dati tiktu izmantoti, kā arī neievāc Datus un neuzglabā tos nekonkrētiem nākotnes nolūkiem, kuru vajadzība nav izvērtēta un realizācijas uzsākšana nav apstiprināta ar normatīvajiem aktiem, attiecīgiem Sabiedrības valdes lēmumiem vai iekšējiem normatīviem dokumentiem (piemēram, procedūrām, instrukcijām). Šis princips arī nosaka, ka svarīgi ir konstatēt Datu ievākšanas sākotnējo nolūku, un, ja Datu izmantošanas nolūks tiek mainīts un nav saderīgs ar šo sākotnējo nolūku, tad šādi Datu apstrādei ir jāpārvērtē tiesiskais pamats.
- 5.3. **Datu minimizēšana.** Šī principa īstenošanas būtība ir apstrādāt tikai attiecīgā nolūka sasniegšanai nepieciešamos datus, tādējādi samazinot apstrādāto datu apjomu. Datu minimizēšanas principa ieviešana Sabiedrības ikdienas procesos, piemēram, pārskatot esošos risinājumus un procesus, organizējot piekļuvi Datim tikai attiecīgām struktūrvienībām, kurām tas nepieciešams pienākumu izpildei, ļauj Sabiedrībai un tās Darbiniekiem identificēt Datus, kuru apstrādes nepieciešamība attiecīgu Sabiedrības produktu un pakalpojumu nodrošināšanai ir pārvērtējama, un novērst Datu pārmērīgu apstrādi. Piemērojot šo principu, Sabiedrība un tās Darbinieki apzinās, ka Datu minimizēšana nav vienreizēji veicams pasākums, bet šī principa īstenošana Datu apstrādes ciklā būtu jāveic regulāri, jo darījumu vide, normatīvo aktu prasības un apkārtējie apstākļi ir mainīgi. Datu

minimizācijas princips vienādi ir piemērojams gan tām Datu apstrādēm, ko Sabiedrība veic iekšienē, gan arī gadījumos, ja Datus ir nepieciešams nodot Datu apstrādātājiem (piemēram, samazinot nododamo Datu apmēru un/vai pseidonimizējot Datus) vai izpaužot Datus trešajām personām.

- 5.4. **Precizitāte.** Precīzi dati ir viena no Regulas pamatvērtībām, jo tikai precīzi Dati var nodrošināt godprātīgu un taisnīgu lēmumu pieņemšanu attiecībā uz Datu subjektu. Turklāt jāņem vērā, ka neprecīzi Dati atsevišķās situācijās var radīt būtiskas negatīvās sekas attiecībā uz Datu subjektu, kuras nebūs taisnīgas. Šī principa godprātīga īstenošana ir ne tikai Sabiedrības un tās Darbinieku pienākums, bet ir nepieciešama veiksmīgas pamatdarbības nodrošināšanai, līdz ar to Sabiedrība izstrādā mehānismus (piemēram, iekļaujot līgumos vai vispārējos darījumu noteikumos datu subjektam pienākumu informēt Sabiedrību par izmaiņām Datus).
- 5.5. **Glabāšanas ierobežojums.** Glabāšanas ierobežojuma principa būtība ir, Datus glabāt tikai tik ilgi, cik tas ir nepieciešams nolūka sasniegšanai, un tiklīdz nolūks ir sasniegts Dati ir jāizdzēš, vai informācijas nesēji, kuros Dati ir fiksēti, jāiznīcina. Tomēr šis princips nebūtu jāapskata virspusēji, jo, beidzoties vienam nolūkam, var rasties jauni leģitīmi nolūki, kas var pamatot nepieciešamību Datus glabāt ilgāk – arī pēc pamatnolūka izbeigšanās, piemēram, ja pakalpojuma līgums ar klientu tiek izbeigts, pamatnolūks – sniegt pakalpojumu klientam – ir sasniegts un Dati šim nolūkam vairs nebūtu nepieciešami un apstrādājami, tomēr ir pieļaujams, ka Dati tiek apstrādāti papildus nepieciešamiem nolūkiem – izpildīt normatīvo aktu prasības par attaisnojamu grāmatvedības dokumentu glabāšanu vai lai aizsargātu Sabiedrības leģitīmās intereses, ja bijušais klients vēlētos apstrīdēt darījumus vai sniegtos pakalpojumus. Gadījumos, kad mainās Datu apstrādes nolūks, ir nepieciešams pārvērtēt Datu apstrādes apjomu, kuru nepieciešams apstrādāt, lai sasniegtu jaunus nolūkus, piemēram, ieviešot mehānismus un procedūras, kas noteiktu kārtību, kādā pārskatāms veiktās Datu apstrādes apjoms nolūku maiņas gadījumā.
- 5.6. **Integritāte un konfidencialitāte.** Ievērojot to, ka mūsdienās Datu apstrāde galvenokārt notiek ar elektroniskiem Datu apstrādes līdzekļiem, šo līdzekļu izmantošana var radīt gan priekšrocības efektīvā Datu apstrādes nodrošināšanā, gan arī trūkumus jeb riskus Datu subjektu Datu apstrādei. Līdz ar to jāpievērš uzmanību tehnisko un organizatorisko risinājumu ieviešanai Sabiedrībā, lai pēc iespējas samazinātu riskus Datim, kurus rada tehnoloģiju izmantošana (piemēram, Datu nokļūšana trešo personu rīcībā, Datu nepamatota iznīcināšana).
- 5.7. **Pārskatbaidība.** Lai šo principu īstenotu, Sabiedrībai un tās Darbiniekiem jau pirms Datu apstrādes uzsākšanas un Regulas piemērošanas ir jāapsver risinājumi, kā Sabiedrība uzskatāmi demonstrēs Regulas ievērošanu, piemēram, Datu drošības nodrošināšanā, Datu subjekta tiesību realizācijas nodrošināšanā, risku novērtēšanā un novēršanā. Atbilstību demonstrēt var veicot, piemēram, šādas darbības:
 - 5.7.1. atbilstošu tehnisko un organizatorisko līdzekļu un pasākumu ieviešana (t.sk. iekšējo normatīvo aktu izstrāde, iekšējo Datu apstrādes procesu auditu veikšana, darbinieku apmācība);
 - 5.7.2. aktuālu procedūru/instrukciju attiecībā uz apstrādes darbībām uzturēšana;
 - 5.7.3. ietekmes novērtējuma veikšana (ja nepieciešams);
 - 5.7.4. Datu apstrādes reģistra ieviešana un uzturēšana (ja nepieciešams);
 - 5.7.5. Datu aizsardzības speciālista norīkošana (ja nepieciešams);
 - 5.7.6. Datu aizsardzības "pēc noklusējuma" un integrētas datu aizsardzības īstenošana, nodrošinot datu minimizēšanu, pseidonimizāciju, pārredzamību, ļaujot datu subjektam kontrolēt un pārraudzīt savu datu apstrādi, kā arī ieviešot atbilstošus drošības pasākumus;
 - 5.7.7. pievienošanās rīcības kodeksiem vai veiktās datu apstrādes sertificēšana (ja nepieciešams);
 - 5.7.8. sadarbības ar uzraudzības iestādi tās uzdevumu izpildē nodrošināšana. Pieņemtie lēmumi, attiecībā uz datu drošību tiek dokumentēti.

6. Riski

Riski, kas var radīt apstākļus nepareizai Datu Apstrādei, ir Ārējo un/vai Iekšējo normatīvo aktu pārkāpumi, kas saistās ar Datu Apstrādes kārtības neievērošanu, kā arī judikatūras izmaiņas. Tāpat Riskus var radīt Trešo personu neatļauta darbība.

7. Atbildība un uzdevumi

Katra Darbinieka uzdevums un atbildība ir, lai viņa pārziņā esošie Dati un to apmērs tiktu apstrādāti ievērojot šo Nolikumu, kā arī, ievērojot Nolikumā pieminētos principus un vadlīnijas. Katram Darbiniekam ir saistošs šis Nolikums un ar to saistīties un regulējošie normatīvie akti. Lai nodrošinātu Nolikuma, kā arī normatīvo tiesību aktu ievērošanu, neskaidribu gadījumā Darbiniekam ir pienākums vērsties pie Tiešā vadītāja atbilstoša rīkojuma saņemšanai par turpmāko.

8. Datu apstrādes noteikumi

- 8.1. Darbinieki darbojas tikai ar tiem Datiem un to apjomā, kas nepārprotami nepieciešami to darba pienākumu izpildei Sabiedrībā – iespējas apstrādāt noteiktus Datus izriet no darba attiecību regulējošajiem dokumentiem pēc būtības. Darbiniekam parastā situācijā un jebkurā brīdī ir jāspēj saprotami paskaidrot Datu un to apjomu izmantošanas/Apstrādes pamatojumu, kas savukārt ir pierādījums likumīgumam un godprātībai attiecībā uz Datu apstrādi.
- 8.2. Darbinieki apņemas Datus glabāt droši. Darbiniekiem ir saistošs „tīrā galdā” princips, proti, Dati tiek glabāti tam paredzētā Darba stacijas skapī, atvilktnē, Elektroniskajā ierīcē vai citādi (vēlams, slēgtā), kas liedz trešajām personām, t.sk., citiem Sabiedrības Darbiniekiem piekļūt Datim vai iepazīties ar tiem. Elektroniskajās ierīcēs ar Datim tiek aizsargātas ar ieejas vārdiem un parolēm, kuras nav izpaužamas trešajām personām. Dati nedrīkst nonākt brīvpieejā. Šajā nolikuma punktā noteiktais attiecas arī uz Datu Apstrādi Sabiedrības izsniegtajos E-pastos. Darbinieki ir personiski atbildīgi par Datu Apstrādes sekām personiskajās Elektroniskajās ierīcēs vai personiskajos E-pastos.
- 8.3. Lai novērstu riskus Datu izpaušanai caur ļaunprātīgām programmām, Darbinieki nedrīkst Sabiedrības Elektroniskajās ierīcēs augšupielādēt vai lejupielādēt uz Darbinieka pienākumiem neattiecināmas vai neatļautas un nesaskaņotas programmas, kā arī atslēgt Loģisko aizsardzību un Ugunsūri.
- 8.4. Darbinieki regulāri, bet ne retāk kā ik pēc 6 (sešiem) mēnešiem pārskata turētos Datus, lai izvērtētu vai to apstrādei vēl ir tiesisks pamats. Datu dzēšana, pieļaujama vienīgi saskaņojot ar tiešo vadītāju.
- 8.5. Apstrādājot Datus atbilstoši darba pienākumiem, Darbinieki apņemas ievērot principus, kas noteikti Nolikuma 5.nodaļā.
- 8.6. Veicot darba pienākumus Sabiedrībā, kas saistās ar Datu subjektu Datu ievākšanu Datu iegūšanas laikā Darbinieki Datu subjektam atbilstošā veidā sniedz visu informāciju atbilstoši Regulas 13.pantam, t.i., bet ne tikai:
 - 8.6.1. Pārziņa un attiecīgā gadījumā Pārziņa pārstāvja/Darbinieka identitāte un kontaktinformācija;
 - 8.6.2. attiecīgā gadījumā – datu aizsardzības speciālista kontaktinformācija;
 - 8.6.3. Apstrādes nolūki, kam paredzēti personas Dati, kā arī Apstrādes juridiskais pamats;
 - 8.6.4. Pārziņa vai trešās personas leģitīmās intereses, ja Apstrāde pamatojas uz Regulas 6. panta 1. punkta f) apakšpunktu („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”);
 - 8.6.5. personas Datu saņēmēji vai saņēmēju kategorijas, ja tādi ir;
 - 8.6.6. laikposms, cik ilgi personas Dati tiks glabāti, vai, ja tas nav iespējams, kritēriji, ko izmanto minētā laikposma noteikšanai;
 - 8.6.7. tas, ka pastāv tiesības pieprasīt Pārzinim piekļuvi Datu subjekta personas datiem un to labošanu vai dzēšanu, vai Apstrādes ierobežošanu attiecībā uz Datu subjektu, vai tiesības iebilst pret Apstrādi, kā arī tiesības uz Datu pārnesamību;
 - 8.6.8. ja Apstrāde pamatojas uz Regulas 6. panta 1. punkta a) apakšpunktu („datu subjekts ir devis piekrišanu savu personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem”) vai Regulas 9. panta 2. punkta a) apakšpunktu („datu subjekts ir devis nepārprotamu piekrišanu šo personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, izņemot, ja Savienības vai dalībvalsts tiesību akti paredz, ka 1. punktā¹ minēto aizliegumu datu subjekts nevar atcelt”) – tiesības jebkurā brīdī atsaukt piekrišanu, neietekmējot tādas apstrādes likumīgumu, kuras pamatā ir pirms atsaukuma sniegta piekrišana;

¹ „Ir aizliegta tādu personas datu apstrāde, kas atklāj rases vai etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dalību arod biedrībās, un ģenētisko datu, biometrisku datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju apstrāde”.

8.6.9. tiesības iesniegt sūdzību uzraudzības iestādei;

8.6.10. informācija, vai personas Datu sniegšana ir noteikta saskaņā ar likumu vai līgumu, vai tā ir priekšnosacījums, lai līgumu noslēgtu, kā arī informācija par to, vai Datu subjektam ir pienākums personas Datus sniegt un kādas sekas var būt gadījumos, kad šādi Dati netiek sniegti;

8.6.11. tas, ka pastāv automatizēta lēmumu pieņemšana, tostarp profilēšana, kas minēta Regulas 22. panta 1. („Datu subjektam ir tiesības nebūt tāda lēmuma subjektam, kura pamatā ir tikai automatizēta apstrāde, tostarp profilēšana, kas attiecībā uz datu subjektu rada tiesiskās sekas vai kas līdzīgā veidā ievērojami ietekmē datu subjektu”) un 4. Punktā („Šā panta 2. punktā² minētos lēmumus nepamato ar īpašām personas datu kategorijām, kuras minētas 9. panta 1. punktā³, izņemot, ja tiek piemērots 9. panta 2. punkta a)⁴ vai g)⁵ apakšpunkts un tiek nodrošināti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un legītīmās intereses”), un – vismaz minētajos gadījumos – jēgpilna informācija par tajā ietverto loģiku, kā arī šādas apstrādes nozīmīgumu un paredzamajām sekām attiecībā uz datu subjektu.

8.7. Atbilstoši Regulas noteikumiem, saglabājas atvieglojumi Datu Apstrādei žurnālistikas vajadzībām (tostarp akadēmiskās, mākslinieciskās vai literārās izpausmes vajadzībām), ievērojot līdzsvaru starp tiesībām uz personas Datu aizsardzību un tiesībām uz vārda un informācijas brīvību. Ievērojot šajā Nolikuma punktā noteikto, Darbinieki, atbilstoši savam amata aprakstam apņemas, nodalīt Datu apstrādes nolūkus uz kuriem attiecas pieminēto atvieglojumi, un kuros gadījumos Datu apstrādei nepieciešams ievērot „Fizisko personu datu aizsardzības likuma” 7.⁶, 8.⁷, 9.⁸, 11.⁹ un 21.pantā¹⁰ noteiktās prasības.

8.8. Tiešais vadītājs rūpējas, lai viņa pārraudzītajā nodaļā tiktu ievērots Nolikums, kā arī sniedz priekšlikumus un rekomendācijas, lai pildītu Nolikuma mērķi pārraudzītajā struktūrvienībā.

² „Šā panta 1. punktu nepiemēro, ja lēmums:

a) ir vajadzīgs, lai noslēgtu vai izpildītu līgumu starp datu subjektu un datu pārzini;
b) ir atļauts saskaņā ar Savienības vai dalībvalsts tiesību aktiem, kuri ir piemērojami pārzinim un kuros ir arī noteikti atbilstīgi pasākumi, ar ko aizsargā datu subjekta tiesības un brīvības, un legītīmās intereses; vai pamatojas uz datu subjekta nepārprotamu piekrišanu;
c) pamatojas uz datu subjekta nepārprotamu piekrišanu.”

³ „Ir aizliegta tādu personas datu apstrāde, kas attiecas uz etnisko piederību, politiskos uzskatus, reliģisko vai filozofisko pārliecību vai dabību ar robežlīnībām, un ģenētisko datu, biometrisku datu, lai veiktu fiziskas personas unikālu identifikāciju, veselības datu vai datu par fiziskas personas dzimumdzīvi vai seksuālo orientāciju apstrāde.”

⁴ „datu subjekts ir devis nepārprotamu piekrišanu šo personas datu apstrādei vienam vai vairākiem konkrētiem nolūkiem, izņemot, ja Savienības vai dalībvalsts tiesību akti paredz, ka 1. punktā minēto aizliegumu datu subjekts nevar atteikt.”

⁵ „apstrāde ir vajadzīga būtisku sabiedrības interešu dēļ, pamatojoties uz Savienības vai dalībvalsts tiesību aktiem, kas ir samērīgas izvirzītajam mērķim, ievēro tiesību uz datu aizsardzību būtību un paredz piemērotus un konkrētus pasākumus datu subjekta pamattiesību un interešu aizsardzībai.”

⁶ „7.pants. Personas datu apstrāde ir atļauta tikai tad, ja likumā nav noteikts citādi un ja ir vismaz viens no šādiem nosacījumiem:

1) ir datu subjekta piekrišana;
2) datu apstrāde ir lietota datu subjekta līgumattiecībām vai, ievērojot datu subjekta līgumu, datu apstrāde nepieciešama, lai noslēgtu attiecīgu līgumu;
3) datu apstrāde nepieciešama pārzinim likumā noteikto pienākumu veikšanai;
4) datu apstrāde nepieciešama, lai aizsargātu datu subjekta vitāli svarīgas intereses, tajā skaitā dzīvību un veselību;
5) datu apstrāde nepieciešama, lai nodrošinātu sabiedrības interešu ieviešanu vai realizētu publiskās varas uzdevumus, kuru veikšanai personas dati ir nodoti pārzinim vai pārrādīti trešajai personai;
6) datu apstrāde ir nepieciešama, lai, ievērojot datu subjekta pamattiesības un brīvības, realizētu pārzīņa vai tās trešās personas likumiskās intereses, kurai personas dati atklā.”

⁷ „8.pants. (1) Jēgdot personas datus no datu subjekta, pārzinim ir pienākums sniegt datu subjektam šādu informāciju, ja vien tā jau nav datu subjekta rīcībā:

1) pārzīņa nosaukums vai vārds un uzvārds, kā arī adrese;
2) paredzētais personas datu apstrādes mērķis.
(2) Pēc datu subjekta pieprasījuma pārzinim ir pienākums sniegt arī šādu informāciju:
1) iespējamie personas datu saņēmēji;
2) datu subjekta tiesības piekļūt saviem personas datiem un izdarīt tajos labojumus;
3) vai atbildes sniegšana ir obligāta vai brīvprātīga, kā arī iespējamās sekas par atbildes nesniegšanu;
4) personas datu apstrādes tiesiskais pamats.
(3) Šā panta pirmā daļa netiek piemērota, ja likums ļauj veikt personas datu apstrādi, neatklājot tās mērķi.”

⁸ „9.pants. (1) Ja personas dati nav iegūti no datu subjekta, pārzinim ir pienākums, ievēcot vai pirmo reizi izpaužot šādus personas datus trešajām personām, sniegt datu subjektam šādu informāciju:

1) pārzīņa nosaukums vai vārds un uzvārds, kā arī adrese;
2) paredzētais personas datu apstrādes mērķis.
(2) (Izslēgta ar 06.02.2014. likumu)
(3) Šā panta pirmā daļa netiek piemērota, ja:
1) personas datu apstrādi paredz cits likums;
2) apstrādājot personas datus ziņātniski, vēsturiski vai statistiskiem pētījumiem, nacionālā dokumentārā mantojuma veidošanai vai oficiālās publikācijas nodrošināšanai, datu subjekta informēšana prasā nesamērīgas pūles vai ir neiespējama.”

⁹ „11.pants. Sensitīvo personas datu apstrāde ir aizliegta, izņemot gadījumus, kad:

1) datu subjekts ir devis rakstveida piekrišanu savu sensitīvo datu apstrādei;
2) speciāla personas datu apstrāde, neprasot datu subjekta piekrišanu, ir paredzēta normatīvajos aktos, kas regulē darba tiesiskās attiecības, un šie normatīvie akti garantē personas datu aizsardzību;
3) personas datu apstrāde ir nepieciešama, lai aizsargātu datu subjekta vai citas personas dzīvību un veselību, un datu subjekts tiesiski vai fiziski nav spējīgs dot savu piekrišanu;
4) personas datu apstrāde ir nepieciešama, lai sasniegtu likumīgas nekomerciālas sabiedrisko organizāciju un to apvienību mērķus, ja šī datu apstrāde ir saistīta tikai ar šo organizāciju vai to apvienību biedriem un personas dati netiek nodoti trešajām personām;
5) personas datu apstrāde ir nepieciešama ārstniecības vajadzībām, veselības aprūpes pakalpojumu sniegšanai vai to administrēšanai un zāļu un medicīnisko ierīču izplatīšanai vai to administrēšanai;
6) apstrāde attiecas uz tādiem personas datiem, kuri ir nepieciešami fiziskās vai juridiskās personas tiesību vai likumisko interešu aizsardzībai tiesā;
7) personas datu apstrāde ir nepieciešama sociālās palīdzības sniegšanai un to veic sociālās palīdzības pakalpojumu sniedzējs;
8) personas datu apstrāde ir nepieciešama nacionālā dokumentārā mantojuma veidošanai, un to veic Latvijas Nacionālais arhīvs un akreditēts privātais arhīvs;
9) personas datu apstrāde ir nepieciešama statistiskiem pētījumiem, ko veic Centrālā statistikas pārvalde;
10) apstrāde attiecas uz tādiem personas datiem, kurus datu subjekts pats ir publicējis;
11) personas datu apstrāde ir nepieciešama, pildot valsts pārvaldes funkcijas vai veidojot likumā noteiktās valsts informācijas sistēmas;
12) personas datu apstrāde nepieciešama fiziskās vai juridiskās personas tiesību vai likumisko interešu aizsardzībai, pieprasot atbilstību saskaņā ar apdrošināšanas līgumu;
13) atbilstoši Pacientu tiesību likumam pētījumā izmanto medicīniskajos dokumentos fiksētos pacienta datus.”

¹⁰ „21.pants. Pirms personas datu apstrādes uzsākšanas pārzinis reģistrē personas datu apstrādi Datu valsts inspekcijā vai norīko fizisko personu — datu aizsardzības speciālistu —, ja pārzinis:

1) paredz personas datus nodot valstij, kas nav Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalsts;
2) paredz personas datus apstrādāt, sniedzot finanšu vai apdrošināšanas pakalpojumus, veicot izlozes vai loterijas, tirgus vai sabiedriskā viedokļa pētījumus, personāla atlasī vai personāla novērtēšanu kā komercdarbības veidu, sniedzot parādu atgūšanas pakalpojumus un kredītinformācijas apstrādes pakalpojumus kā komercdarbības veidu;
3) veic sensitīvo personas datu apstrādi, izņemot gadījumus, kad minēto datu apstrādi veic grāmatvedības, personāla uzskaites (darba tiesisko attiecību) mērķiem vai to veic reliģiskās organizācijas;
4) apstrādā personas datus attiecībā uz noziedzīgiem nodarījumiem, sodāmību un sodiem administratīvo pārkāpumu lietās;
5) veic videonovērošanu, saglabājot personas datus;
6) veic ģenētisko datu apstrādi.”

9. Noslēguma informācija

- 9.1. Uz Nolikuma pamata var tikt izdoti citi Iekšējie normatīvie aktu, kas precizēs Nolikuma piemērošanu un/vai tajā noteikto Mērķu ievērošanu.
- 9.2. Tiešais vadītājs, katrā noteiktajā struktūrvienībā nepieciešamības gadījumā, ir pilnvarots veikt auditu, lai apzinātu tā pārraudzītajā struktūrvienībā izmantoto Datu apjomu, mērķi, utt.
- 9.3. Gadījumā, ja mainās judikatūra vai tiek grozīti Ārējie normatīvie tiesību akti, kas ietekmē Nolikuma saturu, Nolikums nezaudē spēku – līdz Nolikuma jaunās redakcijas izdošanas tiek piemērota vispārpieņemtā prakse nozarē, lai ievēroto normatīvos tiesību aktus.

Pielikumā: Saraksts ar Darbinieku apstiprinājumiem par iepazīšanos ar Noteikumiem.

A. Svāzi