

Latvijas Mākslas akadēmijas Iekšējie datu aizsardzības noteikumi.

Noteikumi nosaka Latvijas Mākslas akadēmijas personas datu apstrādi un aizsardzību atbilstoši Eiropas Parlamenta un Padomes regulai 2016/679 par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti (Turpmāk – Vispārīgā datu aizsardzības regula).

1. Izmantoto terminu skaidrojums

- 1.1. Datu subjekts** – fiziska persona, kuru var tieši vai netieši identificēt;
- 1.2. 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;
- 1.3. Personas dati** – jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu;
- 1.4. Īpašu kategoriju personas dati** – personas dati, kas norāda personas rasi vai etnisko izcelsmi, politiskos uzskatus, reliģisko vai filozofisko pārliecību, dalību arodbiedrībās, kā arī sniedz informāciju par personas ģenētiskajiem un biometriskajiem datiem, veselību, dzimumdzīvi vai seksuālo orientāciju;
- 1.5. 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 darīt tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana;
- 1.6. Apstrādes ierobežošana** – uzglabātu personas datu iezīmēšana ar mērķi ierobežot to apstrādi nākotnē;
- 1.7. Pārzinis** – Latvijas Mākslas akadēmija;
- 1.8. Pārziņa personas datu apstrādes lietotājs** – pārziņa darbinieks vai uz ārpakalpojuma līguma pamata nodarbināta persona pārziņa uzdevumā;
- 1.9. Apstrādātājs (personas datu operators)** – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura pārziņa vārdā apstrādā personas datus;
- 1.10. Pārstāvis** – fiziska vai juridiska persona, kura veic uzņēmējdarbību Savienībā un kuru pārzinis vai apstrādātājs ir iecēlis rakstiski un kura pārstāv pārzini vai apstrādātāju saistībā ar to attiecīgajiem pienākumiem;
- 1.11. 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. Publiskas iestādes, kas var saņemt personas datus saistībā ar konkrētu izmeklēšanu, saskaņā ar Savienības vai dalībvalsts tiesību aktiem, netiek uzskatītas par saņēmējiem;

1.12. Trešā persona – fiziska vai juridiska persona, publiska iestāde, aģentūra vai cita struktūra, kura nav datu subjekts, pārzinis, apstrādātājs un personas, kuras pārziņa vai apstrādātāja tiešā pakļautībā ir pilnvarotas apstrādāt personas datus;

1.13. 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.

2. Vispārīgie jautājumi

2.1. Personas datu apstrāde tiek veikta Pārziņa telpās, kas atrodas šādās adresēs – 1)Rīgā, Kalpaka bulvārī 13, 2)Rīgā, Avotu ielā 36, 3) Rēzeknē, Baznīcas ielā 34A.

2.2. Noteikumi ir saistoši visiem LMA darbiniekiem un studējošiem kā arī citām juridiskām vai fiziskām personām, ja līgumā starp LMA un šīm citām juridiskām vai fiziskām personām ir atsauce uz šiem Noteikumiem vai LMA iekšējiem normatīviem aktiem un tiek ir attiecināmi uz visiem personas datiem, kas attiecas uz identificētu vai identificējamu fizisko personu.

3. Informācijas klasifikācija

3.1. Informācijas klasifikācijas līmeņi:

3.1.1.slepena – augstākais līmenis. Šīs informācijas izpaušana vai nozagšana var radīt ievērojamus vai ilgstošus zaudējumus un nopietni kaitēt Pārziņa labajai slavai. Strādājot ar šo informāciju ir jāievēro vislielāko piesardzību un šo informāciju drīkst izpaust tikai ārkārtējas nepieciešamības gadījumos.

3.1.2.ierobežotas pieejamības – ikdienas darbā paredzētā informācija, kas paredzēta tikai noteiktam darbinieku lokam. Šīs informācijas izpaušana vai nozagšana var radīt Pārzinim iekšējas vai ārējas neērtības. Piekļuvi šai informācijai piešķir tikai pilnvarotiem darbiniekiem.

3.1.3.neklasificēta – informācija, kas jau sabiedrībai zināma, ko brīvi izplata vai kas pieejama visiem Pārziņa darbiniekiem un citām trešajām personām. Šīs informācijas izpaušana vai nozagšana neietekmē Pārziņa darbu.

3.2. Dati, kas tiek izmantoti personas datu apstrādē, ir klasificējami kā ierobežotas pieejamības informācija, kurai ir tiesības piekļūt un veikt to apstrādi tikai pilnvarotiem darbiniekiem.

4. Tehniskie resursi, ar kuriem tiek nodrošināta personas datu apstrāde

4.1. Lietotājs datu apstrādi veic manuāli (papīra formā), pilnībā vai daļēji ar automatizētiem līdzekļiem (elektroniski) vai jaukti abos veidos.

4.2. Personas datu apstrādi veicot manuāli, tiek izmantots rakstāmpapīrs, mapes, slēdzami vai vaļēji plaukti u.c.

4.3. Personas datu apstrādi veicot pilnībā vai daļēji ar automatizētiem līdzekļiem (elektroniski), tiek izmantoti šādi tehniskie resursi:

4.3.1.Datori (galda, portatīvie, planšetdatori);

4.3.2.Serveri;

4.3.3. Datorprogrammas – tajā skaitā operētājsistēma MS Windows.

4.4. Tehnisko resursu lietošanas nosacījumi ir noteikti Informācijas sistēmu lietošanas noteikumos.

5. Paroles uzbūve un lietošana

5.1. Informācijas sistēmas aizsardzība tiek nodrošināta ar datora paroli, kurai jāatbilst šādām prasībām:

5.1.1. minimālam paroles garumam ir jābūt vismaz 8 simboli;

5.1.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 60 dienām;

5.1.3. paroles uzbūvei jābūt komplicētai, izmantojot burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#\$%^*()_+);

5.1.4. nedrīkst atkārtot nevienu no 3 (trīs) iepriekšējām parolēm.

5.2. Lietotājs nedrīkst izpaust savu paroli citiem darbiniekiem vai jebkurām citām trešajām personām.

5.3. Lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.

5.4. Ja lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, darbiniekam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt.

6. Personas datu apstrādes principi

6.1. Lietotājs, apstrādājot personas datus ievēro šādus principus:

7.1.2. dati tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā;

7.1.3. dati tiek vākti konkrētos, skaidros un leģitīmos nolūkos;

7.1.4. dati, kas vākti konkrētam mērķim, drīkst tikt apstrādāti tikai šim mērķim – ja datus nepieciešams apstrādāt citam mērķim, tad ir jāiegūst datu subjekta piekrišana;

7.1.5. dati ir adekvāti, atbilstīgi un ietver tikai to, kas nepieciešams to apstrādes nolūkos;

7.1.6. dati ir precīzi un, ja vajadzīgs, tos atjauno;

7.1.7. dati tiek glabāti veidā, kas pieļauj datu subjektu identifikāciju, ne ilgāk kā nepieciešams nolūkiem, kādos attiecīgos personas datus apstrādā;

7.1.8. dati tiek apstrādāti tādā veidā, lai tiktu nodrošināta atbilstoša personas datu drošība, tostarp aizsardzība pret neatļautu vai nelikumīgu apstrādi un pret nejaušu nozaudēšanu, iznīcināšanu vai sabojāšanu, izmantojot atbilstošus tehniskos vai organizatoriskos pasākumus;

7.1.9. datus apstrādā tikai tās personas, kurām tas ir nepieciešams tiešo pienākumu veikšanai;

7.1.10. dati pēc darba dienas beigām ir novietojami tā, lai tie nebūtu brīvi pieejami citām personām;

7.1.11. datus apstrādā, īstenojot atbilstošus tehniskos un organizatoriskos pasākumus, tostarp noteiktos gadījumos pseidonimizāciju un šifrēšanu.

8. Personas datu apstrādes tiesiskais pamats

- 8.1. Lietotājs ir tiesīgs veikt personas datu apstrādi, ja pastāv vismaz viens no turpmāk minētajiem pamatojumiem:
 - 8.1.1. Datu subjekta piekrišana;
 - 8.1.2. Līgumsaistību izpilde;
 - 8.1.3. Juridiska pienākuma izpilde;
 - 8.1.4. Datu subjekta vai citas personas vitāli svarīgas intereses;
 - 8.1.5. Uzdevumi, ko veic sabiedrības interesēs, vai īstenojot oficiālas pilnvaras;
 - 8.1.6. Pārziņa vai trešās personas legītīmās intereses, sabalansējot ar datu subjekta interesēm.
- 8.2. Lietotājam ir aizliegts veikt īpašu kategoriju datu apstrādi, izņemot, ja ir piemērojams kāds no turpmāk minētajiem pamatojumiem:
 - 8.2.1. datu subjekta piekrišana;
 - 8.2.2. normatīvajos aktos noteikto pienākumu izpilde nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības tiesību jomā;
 - 8.2.3. datu subjekta vai citas fiziskas personas vitāli svarīgu interešu aizsardzība, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu;
 - 8.2.4. apstrāde ir nepieciešama fondam, apvienībai vai jebkurai citai bezpeļņas struktūrai, kas to dara ar politisku, filozofisku, reliģisku vai ar arodbiedrībām saistītu mērķi, par saviem biedriem;
 - 8.2.5. apstrāde attiecas uz personas datiem, kurus datu subjekts apzināti ir publiskojis;
 - 8.2.6. apstrāde ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
 - 8.2.7. apstrāde ir vajadzīga būtisku sabiedrības interešu dēļ;
 - 8.2.8. apstrāde ir vajadzīga profilaktiskās vai arodmedicīnas nolūkos darbinieka darbības novērtēšanai, medicīniskas diagnozes, veselības vai sociālās aprūpes vai ārstēšanas vai veselības vai sociālās aprūpes sistēmu un pakalpojumu pārvaldības nodrošināšanas nolūkos;
 - 8.2.9. apstrāde ir vajadzīga sabiedrības interešu dēļ sabiedrības veselības jomā;
 - 8.2.10. apstrāde ir vajadzīga arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos.
- 8.3. Lietotājs sniedz datu subjektam visu nepieciešamo informāciju par datu subjekta personas datu apstrādi un nodrošina saziņu attiecībā uz apstrādi.

9. Datu subjekta piekrišana

- 9.1. Lietotājs datu subjekta piekrišanu iegūst kā skaidri apstiprinošu darbību, kas nozīmē brīvi sniegtu, konkrētu, apzinātu un viennozīmīgu norādi par datu subjekta piekrišanu ar viņu saistīto personas datu apstrādei, piemēram, ar rakstisku, tostarp elektronisku, vai mutisku paziņojumu.
- 9.2. Īpašu kategoriju personas datu apstrādei, lietotājs iegūst nepārprotamu datu subjekta piekrišanu.
- 9.3. Ja apstrāde pamatojas uz piekrišanu, pārzinim vai viņa pilnvarotam darbiniekam, proti, lietotājam ir jāspēj uzskatāmi parādīt, ka datu subjekts ir piekritis savu personas datu apstrādei.

- 9.4. Lietotājs informē datu subjektu pirms datu apstrādes par tiesībām atsaukt savu piekrišanu jebkurā laikā un to, ka piekrišanas atsaukums neietekmē apstrādes likumību, kas pamatojas uz piekrišanu pirms atsaukuma.

10. Rīcība personas datu aizsardzības pārkāpumu un incidentu gadījumos

- 10.1. Lietotājam ir pienākums nekavējoties, ne vēlāk kā 48 stundu laikā no brīža, kad pārkāpums kļuvis zināms, paziņot atbildīgajai personai par jebkuru personas datu apstrādes pārkāpumu vai incidentu, tostarp:
- 10.1.1. ja konstatēts jebkāda veida apdraudējums tehniskajiem resursiem (elektroenerģijas padeves pārtraukums, šķidrums vai svešķermeņu iekļūšana, bojājumi fiziska trieciena, uguns iedarbības vai plūdu rezultātā u.c.);
 - 10.1.2. ja konstatēts jebkāda veida apdraudējums informācijas resursiem (trešajām personām kļuvusi zināma pieejas parole, konstatēta nesankcionēta piekļuve, konstatēti darbības pārtraukumi u.c.).

11. Informācijas nesēju glabāšanas un iznīcināšanas kārtība

- 11.1. Informācijas nesēju glabāšanas un iznīcināšanas kārtību nosaka saskaņā ar Arhīvu likumu un uz tā pamata izdotajiem Ministru kabineta noteikumiem.
- 11.2. Pēc glabāšanas termiņa beigām papīra formā esošie dokumenti tiek iznīcināti, izmantojot papīra smalcināšanas iekārtu, bet elektroniskie dokumenti – neatgriezeniski dzēsti, izmantojot attiecīgu programmatūru.

12. Lietotāju tiesības, pienākumi un atbildība

- 12.1. Lietotāji ar savu parakstu apliecina, ka atbild par šo noteikumu prasību ievērošanu (Pielikums "Apliecinājums par Latvijas Mākslas akadēmijas Iekšējo datu aizsardzības noteikumu" prasību ievērošanu").
- 12.2. Lietotāju pienākums ir iepazīties ar Noteikumiem un ievērot tos ikdienas darbā.
- 12.3. Lietotājs nedrīkst atļaut piekļūt personas datiem citām personām, ja to nevajag tiešo darba pienākumu pildīšanai un to pilnvarojumu ir devis Pārzinis.
- 12.4. Lietotājs nedrīkst kopēt personu datu saturošus dokumentus, failus uz ārējiem datu nesējiem (disketēm, USB kartēm un / vai kompaktdiskiem), ja to nevajag tiešo darba pienākumu pildīšanai un / vai to pilnvarojumu nav devis Pārzinis.
- 12.5. Beidzot darbu lietotājam ir pienākums personu datu saturošus dokumentus novietot aizslēdzamos skapjos un pilnīgi izslēgt datoru, bet, ja lietotājs atstāj datoru uz pietiekošu īsu laiku, tad lietotājam ir jālieto ekrāna saudzētājs ar paroli. Atstājot darba telpu aizslēgt durvis, darba dienas beigās pievienot telpu apsardzei.
- 12.6. Lietotāju pienākums, saskaņojot ar atbildīgo personu, ir pēc datu subjekta pieprasījuma mēneša laikā no pieprasījuma iesniegšanas dienas, bez maksas sniegt tam visu informāciju, kas savākta par atbilstošo datu subjektu.
- 12.7. Lietotājs pēc atbildīgās personas pieprasījuma bez nepamatotas kavēšanās labo vai papildina neprecīzus datu subjekta personas datus.
- 12.8. Lietotājam ir pienākums paziņot atbildīgajai personai par datu apstrādi un norādīt uz personas datu dzēšanu gadījumos, kad:

- 12.8.1. personas dati vairs nav nepieciešami saistībā ar nolūkiem, kādos tie tika vākti vai citādi apstrādāti;
- 12.8.2. datu subjekts atsauc savu piekrišanu, uz kuras pamata veikta apstrāde, un ja nav cita likumīga pamata apstrādei;
- 12.8.3. datu subjekts iebilst pret apstrādi saskaņā ar Vispārīgās datu aizsardzības regulas 21. panta 1. punktu, un apstrādei nav nekāda svarīgāka leģitīma pamata, vai arī datu subjekts iebilst pret apstrādi saskaņā ar regulas 21. panta 2. punktu;
- 12.8.4. personas dati ir apstrādāti nelikumīgi;
- 12.8.5. personas dati ir jādzēš, lai nodrošinātu, ka tiek pildīts juridisks pienākums, kas noteikts Savienības vai dalībvalsts tiesību aktos, kuri ir piemērojami pārzinim;
- 12.8.6. personas dati ir savākti saistībā ar informācijas sabiedrības pakalpojumu piedāvāšanu, kā minēts Vispārīgās datu aizsardzības regulas 8. panta 1. punktā.
- 12.9. Lietotājam ir pienākums paziņot par personas datu apstrādes ierobežošanu, pastāvot šādiem kritērijiem:
 - 12.9.1. Ja datu subjekts apstrīd personas datu precizitāti – uz laiku, kurā pārzinis var pārbaudīt personas datu precizitāti;
 - 12.9.2. Ja apstrāde ir nelikumīga, un datu subjekts iebilst pret personas datu dzēšanu un tās vietā pieprasa datu izmantošanas ierobežošanu;
 - 12.9.3. Ja pārzinim personas dati apstrādei vairs nav vajadzīgi, taču tie ir nepieciešami datu subjektam, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
 - 12.9.4. Ja datu subjekts ir iebildis pret apstrādi saskaņā ar Vispārīgās datu aizsardzības regulas 21. panta 1. punktu, kamēr nav pārbaudīts, vai pārziņa leģitīmie iemesli nav svarīgāki par datu subjekta leģitīmajiem iemesliem.
- 12.10. Lietotājam ir pienākums ziņot par datu apstrādi atbildīgajai personai vai datu aizsardzības speciālistam, ja tāds ir iecelts.
- 12.11. Lietotājs pēc pieprasījuma strukturētā, plaši izmantotā un mašīnlasāmā formātā izsniedz datu subjektam personas datus attiecībā uz sevi, kurus datu subjekts sniedzis pārziņa darbiniekam.
- 12.12. Lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī lietotājs atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.
- 12.13. Lietotājs apņemas saglabāt informācijas konfidencialitāti arī pēc darba tiesisko attiecību izbeigšanas.

