RAKSTNIECĪBAS
UN MŪZIKAS
MUZEJS

Latvijas Republikas Kultūras ministrija
Rakstniecības un mūzikas muzejs
Reģ. Nr. 90009175091
Pulka iela 8, Rīga, LV-1007
T. +371 67 216 425
E. muzejs@rmm.lv
www.rmm.lv

APSTIPRINU

28.12.2021.
Direktore Iveta Ruskule

Nr. 2021/3

Rakstniecības un mūzikas muzeja iekšējie datu aizsardzības noteikumi.

Noteikumi nosaka Rakstniecības un mūzikas muzeja personas datu apstrādi, tās kārtību, 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 – Regula)

I Izmantoto terminu skaidrojums

1.	**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, nosūtot, izplatot vai citādi darot tos pieejamus, saskaņošana vai kombinēšana, ierobežošana, dzēšana vai iznīcināšana
2.	**Apstrādātājs (datu operators)**	Fiziska vai juridiska persona, kas uz rakstveida līguma pamata veic personas datu apstrādi atbilstoši līgumā norādītajam apjomam, paredzētajiem nolūkiem un pārziņa norādījumiem;
3.	**Datu subjekts**	– fiziska persona, kuru var tieši vai netieši identificēt;
4.	**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;
5.	**Datu aizsardzības speciālists**	Pārziņa piesaistīts ārpakalpojuma sniedzējs, kas konsultē Pārziņa darbiniekus jautājumos, kas saistīti ar personas datu apstrādi, sazinās ar Uzraudzības iestādi, veic
6.	**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 barometriskajiem datiem, veselību, dzimumdzīvi vai seksuālo orientāciju;
7.	**Lietotājs**	Pārziņa darbinieks. Tekstā var tikt izmantots arī kā Darbinieks;
8.	**Pārzinis**	Rakstniecības un mūzikas muzejs – kas attiecībā uz personas datu apstrādi nosaka personas datu apstrādes nolūkus un apstrādes līdzekļus, kā arī atbild par personas datu apstrādi atbilstoši piemērojamo normatīvo aktu prasībām (var tikt lietots tekstā kā Muzejs);
9.	**Personas dati**	jebkura informācija, kas attiecas uz identificētu vai identificējamu fizisku personu; Ar datiem saprot jebkādu informāciju, kas sniedz ziņas par identificējamu fizisko personu, tai skaitā objektīva (piemēram, personas vārds, uzvārds, personas kods, adrese, tālruņa numurs) un arī subjektīva informācija (piemēram, personas psiholoģiskais raksturojums, dzīves stāsts). Tāpat ar datiem ir saprotama jebkādā formā fiksēta informācija, t.i., gan papīra formātā, gan elektroniskā veidā, t.sk. foto un video ierakstos fiksētie dati;
10.	**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.
11.	**Par personas datu apstrādi atbildīgā persona**	Rakstniecības un mūzikas muzeja direktore vai tās deleģētā persona, kuras pārziņā ir datu apstrādes process – tā koordinē, uzrauga datu apstrādi, nepieciešamības gadījumā, iesaistot datu aizsardzības speciālistu.
12.	**Par sistēmu drošību atbildīgā persona**	Muzeja iecelts darbinieks, IT speciālists, kas atbild par datu apstrādi un to aizsardzību informācijas sistēmās, e-pastos, programmās u.c.
13.	**Personas datu apstrādes 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.
14.	**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.
15.	**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;

16.	**Uzraudzības iestāde**	Datu valsts inspekcija.

II Personas datu aizsardzības pārvaldīšana

17. Par personas datu aizsardzību Muzejā atbild tā direktore. Direktore var deleģēt savu atbildību ar rīkojumu ieceļot citu darbinieku kā atbildīgo par datu aizsardzību.
18. Atbildīgo personu par Pārziņa informācijas sistēmu tehniskajiem resursiem un informācijas sistēmās apstrādājamo datu aizsardzību Muzejs nosaka ar rīkojumu.
19. Personas datu lietotājs ir atbildīgs par tā lietošanā nodoto personas datu drošību un aizsardzību, to apstrādi saskaņā ar šiem noteikumiem un ārējiem normatīviem aktiem.
20. Datu aizsardzības speciālists sniedz konsultācijas Par personas datu apstrādi atbildīgajai personai personu datu apstrādes jautājumos.

III Informācijas klasifikācija

21. Informācijas klasifikācijas līmeņi:
    i. slepena – augstākais līmenis. Šīs informācijas izpaušana vai nozagšana var radīt ievērojamus vai ilgstošus zaudējumus un nopietni kaitēt Muzeja labajai slavai. Strādājot ar šo informāciju ir jāievēro vislielākā piesardzība un šo informāciju drīkst izpaust tikai ārkārtējas nepieciešamības gadījumos.
    ii. ierobežotas pieejamības – ikdienas darbā paredzētā informācija, kas paredzēta tikai noteiktam darbinieku lokam. Šīs informācijas izpaušana vai nozagšana var radīt Muzeja iekšējas vai ārējas neērtības. Piekļuvi šai informācijai piešķir tikai pilnvarotiem darbiniekiem.
    iii. neklasificēta – informācija, kas jau sabiedrībai zināma, ko brīvi izplata vai kas pieejama visiem Muzeja darbiniekiem un citām trešajām personām. Šīs informācijas izpaušana vai nozagšana neietekmē Pārziņa darbu.
22. Dati, kas tiek izmantoti personas datu apstrādē, ir klasificējami kā ierobežotas pieejamības informācija, kurai ir tiesības piekļūt un veikt to apstrādi tikai pilnvarotiem darbiniekiem.

IV Personas datu aizsardzības organizatoriskā procedūra

23. Personas datu apstrāde Muzejā tiek veikta, ievērojot šajos noteikumos ietvertos principus un norādījumus.
24. Lai nodrošinātu darbinieku izpratni par personas datu apstrādi, Par personas datu apstrādi atbildīgā persona sadarbībā ar Datu apstrādes speciālistu organizē darbinieku apmācības ne retāk kā 2 reizes gadā, ietverot tajās arī zināšanu pārbaudes testu. Testu jākārto arī par datu aizsardzību atbildīgajām personām. Testu sagatavo Datu aizsardzības speciālists, kā arī pārbauda Darbinieku sniegtās atbildes.
25. Iepriekšējā punktā minētā testa nenokārtošanas gadījumā darbiniekam jāveic atkārota zināšanu pārbaude termiņā, kas nav garāks par 1 mēnesi. Ja arī atkārtotā

zināšanu pārbaude netiek nokārtota, darbiniekam tiek organizētas atkārtotas apmācības.

26. Par personas datu apstrādi atbildīgā persona ir atbildīga par to, lai jaunie darbinieki tiktu apmācīti par personas datu apstrādes principiem. Apmācības tiek veiktas sadarbībā ar Datu aizsardzības speciālistu.
27. Par personas datu apstrādi atbildīgā persona reizi gadā ar datu aizsardzības speciālistu organizē ieviesto tehnisko un organizatorisko pasākumu novērtējumu. (Pielikums Nr. 1). Novērtējumā sniegtās atbildes izvērtē datu aizsardzības speciālists un pauž savus ieteikumus apstrādes uzlabošanai, ja tādi nepieciešami.
28. Personas datu apstrādes drošību, kas saistīta ar informācijas sistēmām – programmām, datoriem, e-pastiem u.c. nodrošina Muzeja iecelta atbildīgā persona jeb Par sistēmu drošību atbildīgā persona, ja nepieciešams – iesaistot Datu aizsardzības speciālistu.
29. Personas datus Muzejs apstrādā saskaņā ar Personas datu apstrādes principiem un tikai gadījumos, ja personas datu apstrādei ir tiesisks pamats.
30. Personas datu apstrādes reģistru Muzejs uztur un atjauno sadarbībā ar Datu aizsardzības speciālistu.
31. Uzsākot jaunu personas datu apstrādi (kas nav uzskaitīta Personas datu apstrādes reģistrā), Muzejs konsultējas ar datu apstrādes speciālistu.
32. Publiskos pasākumos, kuros ir paredzēta filmēšana/fotografēšana, par to apmeklētājiem redzamā vietā tiek izvietota informācija, norādot Muzeja informāciju, kontaktinformāciju, mērķi ar kādu dati tiek apstrādāti.
33. Nododot personas datus apstrādei kādam, kas nav Muzeja darbinieks, Muzejs slēdz Personas datu apstrādes līgumu. Ja nepieciešams – līguma nosacījumus var saskaņot ar Datu aizsardzības speciālistu.
34. Konstatējot personas datu apstrādes pārkāpumu, Lietotājs par to nekavējoties ziņo struktūrvienības vadītājam, kas par minēto nekavējoties sagatavo rakstveida ziņojumu.
35. Par datu aizsardzību atbildīgā persona, izvērtējot 31. punktā minēto ziņojumu un citus būtiskus apstākļus, konsultējoties ar datu aizsardzības speciālistu, kvalificē to saskaņā ar II nodaļā ietverto un sagatavo rakstveida izvērtējumu par nepieciešamību ziņot par personas datu pārkāpumu Uzraudzības iestādei un datu subjektam atbilstoši Regulas 33. panta 1. daļas un 34. panta 1., 2. un 3. daļas prasībām, kuru nekavējoties iesniedz Muzeja direktorei un nosūta uz Datu aizsardzības speciālista e-pastu.
36. Par datu aizsardzību atbildīgā persona Muzeja direktores uzdevumā, pamatojoties uz šo noteikumu 35. punktā minēto izvērtējumu, konsultējoties un sadarbojoties ar Datu aizsardzības speciālistu, Regulas 33. pantā noteiktajos gadījumos sagatavo ziņojumu Uzraudzības iestādei atbilstoši Uzraudzības iestādes mājas lapā norādītajai informācijai un veidlapas paraugam par personas datu aizsardzības pārkāpuma paziņošanu, kā arī organizē un kontrolē šī paziņojuma iesniegšanu Uzraudzības iestādē tā, lai tiktu ievērots Regulas 33. panta 1. daļā noteiktais termiņš.
37. Par datu aizsardzību atbildīgā persona Muzeja direktores uzdevumā, pamatojoties uz šo noteikumu 30. punktā minēto izvērtējumu, konsultējoties un sadarbojoties ar Datu aizsardzības speciālistu, Regulas 34. pantā noteiktajos gadījumos sagatavo paziņojumu datu subjektam atbilstoši Regulas 24. panta 1. un 2. daļas prasībām.

38. Visu informāciju par iespējamu vai notikušu personas datu aizsardzības pārkāpumu, kā arī par veiktajām un plānotajām darbībām tā seku minimizēšanai Par datu aizsardzību atbildīgā persona fiksē, veicot ierakstu Personas datu aizsardzības pārkāpumu reģistrā (Pielikums Nr. 2) un nodod informāciju datu aizsardzības speciālistam.

V Tehniskie resursi, ar kuriem tiek nodrošināta personas datu apstrāde, un to aizsardzības līdzekļi pret tīšu bojāšanu un neatļautu apstrādi

39. Personas datu apstrādes nodrošināšanai Muzejs izmanto tehniskos un manuālos resursus un nodrošina tos ar aizsardzības līdzekļiem pret tīšu bojāšanu un neatļautu apstrādi saskaņā ar ārējiem normatīvajiem aktiem, Muzeja iekšējiem normatīvajiem aktiem, informācijas sistēmu drošību, ugunsdrošības pasākumu organizēšanu un ārkārtas situāciju gadījumos reglamentējošās jomās.
40. Ikvienam personas datu lietotājam ir pienākums lietot tehniskos resursus, informācijas sistēmas kā arī manuāli apstrādāt personas datus ar pienācīgu rūpību un uzmanību un tikai Muzeja noteiktajiem apstrādes mērķiem.
41. Informācijas sistēmām, serveriem, programmām, kuros ir personas dati, piekļuve ir ierobežotu personu lokam un tikai tādā apjomā, kāds nepieciešams tiešo darba pienākumu veikšanai.
42. Darba pienākuma pildīšanai nepieciešamajos gadījumos pārvietojot vai iznesot informācijas nesēju ārpus Muzeja telpām, Lietotājs veic pasākumus, kas nodrošina informācijas nesēja aizsardzību pret tīšu bojāšanu, vai neatļautu iegūšanu (piemēram – nepieļauj tā atstāšanu bez uzraudzības).
43. Ja radušās aizdomas, ka informācijas nesēja vai informācijas sistēmas piekļuves parole ir kļuvusi zināma kādam citam, Lietotājs to nekavējoties nomaina un par incidentu ziņo Par personas datu aizsardzību atbildīgajai personai.
44. Ja rodas nepieciešamība nosūtīt informāciju, kas satur personas datus uz elektronisko pastu, personas datus saglabā atsevišķā pielikumā, kurš aizsargāts ar paroli. Parole, lai pielikumu atvērtu, tiek nosūtīta atsevišķā e-pastā, vai sms.
45. Par personas datu aizsardzību atbildīgā persona uzdod Datu aizsardzības speciālistam veikt periodisku izvērtējumu par datu pārsūtījumu drošību, ja nepieciešams, piesaistot IT speciālistu.

VI Par sistēmu drošību atbildīgās personas pienākumi

46. Par informācijas resursiem atbildīgā persona:
    i. nodrošina loģiskās aizsardzības pasākumus;
    ii. nosaka kārtību, kādā informācijas sistēmas lietotājiem piešķir tiesības piekļūt informācijas resursiem un rīkoties ar tiem, un organizē šo resursu izmantošanas kontroli;
    iii. nodrošina informācijas resursu darbības atjaunošanu, ja noticis tehnisko resursu bojājums vai arī informācijas resursa darbība ir tikusi traucēta citu iemeslu dēļ;
    iv. īsteno procesu, kas regulāri pārbauda un novērtē ar informācijas resursiem saistīto pasākumu efektivitāti, lai nodrošinātu apstrādes drošību.

v. nodrošina tehnisko resursu darbspēju;
vi. nodrošina, ka tehniskie resursi (dators) novietoti atsevišķā slēdzamā telpā, kurai var piekļūt tikai pilnvaroti darbinieki;
vii. nodrošina apstrādes sistēmu un pakalpojumu pastāvīgu konfidencialitāti, integritāti, pieejamību un elastīgumu;
viii. veicot riska analīzi, nosaka ar tehniskajiem resursiem saistītus informācijas sistēmas apdraudējumus un novērtē šo apdraudējumu īstenošanās varbūtību;
ix. nodrošina fiziskās aizsardzības pasākumus, tostarp pret dabas stihijām, ugunsgrēka, plūdiem u.tml. Pasākumi pret ārkārtas apstākļiem tiek īstenoti saskaņā ar ugunsdrošības noteikumiem, kā arī vispārējām normatīvo aktu prasībām par elektroiekārtu drošu ekspluatāciju un to aizsardzību;
x. nodrošina tehnisko resursu atjaunošanu vai nomaiņu, ja tie bojāti;
xi. savlaicīgi atjauno pieejamību un piekļuvi personas datiem fiziska vai tehniska rakstura incidenta gadījumā;
xii. īsteno procesu, kas regulāri pārbauda un novērtē tehnisko pasākumu efektivitāti, lai nodrošinātu apstrādes drošību.

VII Paroles uzbūve un lietošana

47. Informācijas sistēmas aizsardzība tiek nodrošināta ar datora paroli, kurai jāatbilst šādām prasībām:
i. minimālam paroles garumam ir jābūt vismaz 8 simboli;
ii. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 60 dienām;
iii. paroles uzbūvei jābūt komplicētai, izmantojot burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+);
iv. nedrīkst atkārtot nevienu no 3 (trīs) iepriekšējām parolēm.
48. Lietotājs nedrīkst izpaust savu paroli citiem darbiniekiem vai jebkurām citām trešajām personām.
49. Lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.
50. Ja lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, darbiniekam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt.
51. Lietotājam ir aizliegts jebkādā veidā mainīt lietošanā saņemtās datortehnikas un programmatūras konfigurāciju, kā arī instalēt programmatūru uz to.

VIII Personas datu apstrādes principi

52. Lietotājs, apstrādājot personas datus, ievēro šādus principus:
5.2.1. dati tiek apstrādāti likumīgi, godprātīgi un datu subjektam pārredzamā veidā;
5.2.2. dati tiek vākti konkrētos, skaidros un leģitīmos nolūkos;
5.2.3. dati, kas vākti konkrētam mērķim, drīkst tikt apstrādāti tikai šim mērķim – ja datus nepieciešams apstrādāt citam mērķim, tad ir jāiegūst datu subjekta piekrišana;

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

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

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

5.2.7. 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;

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

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

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

IX Personas datu apstrādes tiesiskais pamats

53. Lietotājs ir tiesīgs veikt personas datu apstrādi, ja pastāv vismaz viens no turpmāk minētajiem pamatojumiem:

5.3.1. Datu subjekta piekrišana;

5.3.2. Līgumsaistību izpilde;

5.3.3. Juridiska pienākuma izpilde;

5.3.4. Datu subjekta vai citas personas vitāli svarīgas intereses;

5.3.5. Uzdevumi, ko veic sabiedrības interesēs, vai īstenojot oficiālas pilnvaras;

5.3.6. Pārziņa vai trešās personas leģitīmās intereses, sabalansējot ar datu subjekta interesēm.

54. Lietotājam ir aizliegts veikt īpašu kategoriju datu apstrādi, izņemot, ja ir piemērojams kāds no turpmāk minētajiem pamatojumiem:

5.4.1. datu subjekta piekrišana;

5.4.2. normatīvajos aktos noteikto pienākumu izpilde nodarbinātības, sociālā nodrošinājuma un sociālās aizsardzības tiesību jomā;

5.4.3.datu subjekta vai citas fiziskas personas vitāli svarīgu interešu aizsardzība, ja datu subjekts ir fiziski vai tiesiski nespējīgs dot savu piekrišanu;

5.4.4. 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;

5.4.5. apstrāde attiecas uz personas datiem, kurus datu subjekts apzināti ir publiskojis;

5.4.6. apstrāde ir vajadzīga, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;

5.4.7.apstrāde ir vajadzīga būtisku sabiedrības interešu dēļ;

5.4.8. apstrāde ir vajadzīga profilaktiskās vai arodmedicīnas nolūkos darbinieka darbspējas novērtēšanai, medicīniskas diagnozes, veselības vai sociālās aprūpes vai ārstēšanas vai veselības vai sociālās aprūpes sistēmu un pakalpojumu pārvaldības nodrošināšanas nolūkos;

5.4.9. apstrāde ir vajadzīga sabiedrības interešu dēļ sabiedrības veselības jomā;

5.4.10. apstrāde ir vajadzīga arhivēšanas nolūkos sabiedrības interesēs, zinātniskās vai vēstures pētniecības nolūkos, vai statistikas nolūkos.

55. Lietotājs sniedz datu subjektam visu nepieciešamo informāciju par datu subjekta personas datu apstrādi un nodrošina saziņu attiecībā uz apstrādi.

X Datu subjekta piekrišana

56. Gadījumos, kad dati tiek apstrādāti uz piekrišanas pamata-

5.6.1. 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.

5.6.2. Īpašu kategoriju personas datu apstrādei, lietotājs iegūst nepārprotamu datu subjekta piekrišanu.

5.6.3. 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.

5.6.4. 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.

XI Informācijas nesēju glabāšanas un iznīcināšanas kārtība

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

XII Lietotāju tiesības, pienākumi un atbildība

59. Lietotāji ar savu parakstu apliecina, ka atbild par šo noteikumu prasību ievērošanu (Pielikums Nr. 3 "Apliecinājums par Rakstniecības un mūzikas muzeja Iekšējo datu aizsardzības noteikumu" prasību ievērošanu").
60. Lietotājiem ir tiesības izmantot viņa lietošanā nodotos dokumentus, datorus un to programmatūru, kā arī lietotājam ir tiesības pieprasīt lietotāju atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi, vai arī lietotājam ir pietiekams uzskats par iespējamo draudu (apdraudējumu) esamību.
61. Lietotāju pienākums ir iepazīties ar Noteikumiem un ievērot tos ikdienas darbā.
62. Uzsākot sistēmu lietošanu, kā arī sistēmas izmaiņu gadījumā, Lietotājiem tiek organizētas mācības.

63. Lietotājs nedrīkst izpaust ziņas par Pārziņa datoru tīkla uzbūvi un konfigurāciju, telpu pieejamības parolēm, kā arī atklāt klasificēto informāciju trešajām personām.
64. Lietotājs nedrīkst atļaut piekļūt personas datiem trešajām personām, ja to nevajag tiešo darba pienākumu pildīšanai un to pilnvarojumu ir devis Pārzinis.
65. Lietotājs nedrīkst kopēt personu datu saturošus dokumentus, failus uz ārējiem datu nesējiem (USB kartēm un / vai kompaktdiskiem), ja to nevajag tiešo darba pienākumu pildīšanai un / vai to pilnvarojumu nav devis Pārzinis.
66. 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.
67. Ja Lietotājs ir saņēmis datu subjekta pieprasījumu izsniegt tam visu informāciju, kas par attiecīgo datu subjektu tiek savākta, Lietotājam ir pienākums paziņot par to Pārzinim un atbildīgajai personai.
68. Lietotājs ar Pārziņa akceptu pēc datu subjekta pieprasījuma bez nepamatotas kavēšanās labo vai papildina neprecīzus datu subjekta personas datus.
69. Lietotājam ir pienākums paziņot atbildīgajai personai par datu apstrādi un norādīt uz personas datu dzēšanu gadījumos, kad:
    6.9.1. personas dati vairs nav nepieciešami saistībā ar nolūkiem, kādos tie tika vākti vai citādi apstrādāti;
    6.9.2. datu subjekts atsauc savu piekrišanu, uz kuras pamata veikta apstrāde, un ja nav cita likumīga pamata apstrādei;
    6.9.3. 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;
    6.9.4. personas dati ir apstrādāti nelikumīgi;
    6.9.5. personas dati ir jādzēš, lai nodrošinātu, ka tiek pildīts juridisks pienākums, kas noteikts Savienības vai dalībvalsts tiesību aktos, kuri ir piemērojami pārzinim;
    6.9.6. personas dati ir savākti saistībā ar informācijas sabiedrības pakalpojumu piedāvāšanu, kā minēts Vispārīgās datu aizsardzības regulas 8. panta 1. punktā.
70. Lietotājam ir pienākums paziņot par personas datu apstrādes ierobežošanu, pastāvot šādiem kritērijiem:
    7.0.1. Ja datu subjekts apstrīd personas datu precizitāti – uz laiku, kurā pārzinis var pārbaudīt personas datu precizitāti;
    7.0.2. Ja apstrāde ir nelikumīga, un datu subjekts iebilst pret personas datu dzēšanu un tās vietā pieprasa datu izmantošanas ierobežošanu;
    7.0.3. Ja pārzinim personas dati apstrādei vairs nav vajadzīgi, taču tie ir nepieciešami datu subjektam, lai celtu, īstenotu vai aizstāvētu likumīgas prasības;
    7.0.4. 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.
    7.0.5. Lietotājam ir pienākums ziņot par datu apstrādi atbildīgajai personai vai datu aizsardzības speciālistam, ja tāds ir iecelts.

71. Lietotājs pēc pieprasījuma strukturētā, plaši izmantotā un datorraksta formātā izsniedz datu subjektam personas datus attiecībā uz sevi, kurus datu subjekts sniedzis pārziņa darbiniekam.
72. Lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī lietotājs atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.
73. Lietotājs apņemas saglabāt informācijas konfidencialitāti arī pēc darba tiesisko attiecību izbeigšanas.

PIELIKUMĀ:

1. Pielikums Nr.1 "Tehnisko un organizatorisko pasākumu novērtējuma anketa"
2. Pielikums Nr.2 "Personas datu aizsardzības pārkāpumu reģistrs"
3. Pielikums Nr. 3 Apliecinājums par Rakstniecības un mūzikas muzeja Iekšējo datu aizsardzības noteikumu" prasību ievērošanu

Pielikums Nr. 1

Rakstniecības un Mūzikas muzeja (RMM) Personas datu apstrādē ieviesto tehnisko un organizatorisko pasākumu novērtējums

Personas datu apstrādē ieviesto tehnisko un organizatorisko pasākumu novērtējums (Novērtējums) ir nepieciešams, lai, atbildot uz jautājumiem, persona varētu pati izvērtēt, vai tās ieviestie datu aizsardzības pasākumi nodrošina apstrādātajam datu apjomam atbilstošu drošības līmeni. Ja persona, veicot šo novērtējumu ir konstatējusi riskus datu apstrādei, personai ir jāveic nepieciešamie pasākumi, lai konstatētos riskus samazinātu vai novērstu.

Novērtējums tiek veikts saskaņā ar RMM personas datu apstrādes noteikumiem, vai biežāk, ja, izvērtējot situāciju ir konstatēta tāda nepieciešamība.

1.Vai ir izstrādāti personas datu apstrādes aizsardzības noteikumi?	jā ☐ nē ☐
2.Kādā kārtībā personas datu apstrādē iesaistītās personas informē par pienākumu neizpaust personas datus? Kā tiek kontrolēta šā pienākuma ievērošana?	
3.Par informācijas resursiem, tehniskajiem resursiem un personas datu aizsardzību atbildīgā persona	
4.Kādi personas datu aizsardzības pasākumi tiek piemēroti informācijas tehnoloģijām?	
5.Raksturojiet aizsardzības pasākumus, kas ir ieviesti pēc neautorizētas un prettiesiskas piekļuves personas datiem, kas ir apstrādāti automatizēti vai manuāli	
6.Vai īpašās kategorijas personas datu apstrādei ir noteikts lielāks (augstāks) datu aizsardzības līmenis? Ja atbilde ir "jā", raksturojiet noteikto aizsardzības līmeni.	jā ☐ nē ☐
7.Vai personas datu apstrādei ir sagatavoti informācijas sistēmu drošības noteikumi?	jā ☐ nē ☐
8.Vai ir noteiktas par informācijas sistēmu drošības pārvaldību un īstenošanu atbildīgās personas?	jā ☐ nē ☐
9.Vai personas datu apstrādei tiek veikta informācijas sistēmu risku analīze?	jā

	nē ☐
10.Vai Jums ir izstrādātas informācijas sistēmu piekļuves kontroles procedūras? Ja atbilde ir "jā", kā Jūs pārvaldāt informācijas sistēmu lietotāju kontus?	jā ☐ nē ☐
11.Kādas ir prasības lietotāju kontu parolēm vai citiem kontu aizsardzības rīkiem?	
12.Vai ir noteikti pienākumi informācijas sistēmu lietotājiem? Kādi?	jā ☐ nē ☐
13.Vai tiek veikta drošības apmācība personām, kas veic datu apstrādi informācijas sistēmās? Cik bieži minētā drošības apmācība tiek veikta, kāds ir tās saturs?	jā ☐ nē ☐
14.Vai Jūs pirms informācijas sistēmas nodošanas ekspluatācijā veicat drošības atbilstības pārbaudi? Ja atbilde ir "jā", norādiet pārbaudes norises kārtību	jā ☐ nē ☐
15.Vai personas datu apstrādei ir izstrādāta informācijas sistēmas uzturēšanas kārtība un procedūras?	jā ☐ nē ☐
16.Vai personas datu apstrādei ir nodrošināta informācijas sistēmas notikumu reģistrēšana un monitorēšana? Raksturojiet kārtību	jā ☐ nē ☐
17.Vai personas datu apstrādei ir nodrošināta datu rezerves kopiju veidošana un pārbaude? Raksturojiet kārtību	jā ☐ nē ☐
18.Vai personas datu apstrādei tiek izmantotas ārējas informācijas sistēmas, kas savienotas ar iestādes informācijas sistēmām? Ja atbilde ir "jā", kāda ir kārtība un nosacījumi, saskaņā ar kuriem izveido sadarbību ar citām personām?	jā ☐ nē ☐
19.Kādas tehnoloģijas un rīki tiek izmantoti, lai savienotu sistēmas?	
20.Vai personas datu apstrādē izmantotajām informācijas sistēmām var piekļūt attālināti? Ja atbilde ir "jā", kāda ir attālinātas piekļuves procedūra un nosacījumi?	jā ☐ nē ☐

21.Vai personas datu apstrādei ir noteikta kārtība ārējo atmiņas ierīču pārvaldībai un lietošanai?	jā ☐ nē ☐
22.Vai informācijas sistēmās tiek izmantota datu šifrēšana? Ja atbilde ir "jā", raksturojiet to	jā ☐ nē ☐
23.Vai pirms informācijas publiskošanas tiek izvērtēts tās konfidencialitātes līmenis un iespējamie riski?	jā ☐ nē ☐
24.Vai personas datu apstrādei ir izstrādāta incidentu pārvaldības kārtība un procedūras?	jā ☐ nē ☐
25.Vai personas datu apstrādei ir izstrādāta kārtība atklāto trūkumu novēršanai?	jā ☐ nē ☐

Pielikums Nr. 2
Rakstniecības un mūzikas muzeja iekšējie datu aizsardzības noteikumi

Personas datu aizsardzības pārkāpumu reģistrs

Nr. p. k.	**Datums un laiks, kad konstatēts iespējamais personas datu aizsardzības pārkāpums**	**Personas, kura uzzināja un informēja par personas datu aizsardzības pārkāpumu, identificējoši dati** (vārds, uzvārds, amats)	**Personas datu aizsardzības pārkāpuma apraksts**	**Ietekmēto datu veidi un apjoms**	**Vai ir ziņots Datu valsts inspekcijai** (Regulas 33. pants) **un datu subjektam/-iem** (Regulas 34.pants) (ja ir ziņots, tad datums un laiks, kad paziņots)	**Veiktie pasākumi turpmākai personas datu aizsardzības pārkāpuma atkārtošanās iespējamības novēršanai** (īss apraksts)
1.						
2.						
3.						

Pielikums Nr. 3
"Rakstniecības un mūzikas muzeja iekšējie datu aizsardzības noteikumi"

APLIECINĀJUMS
PAR RAKSTNIECĪBAS UN MŪZIKAS MUZEJA IEKŠĒJO DATU AIZSARDZĪBAS NOTEIKUMU" PRASĪBU IEVĒROŠANU

Ar šo es, zemāk parakstījies (-usies), apliecinu:

1. Esmu iepazinies(-usies) ar Rakstniecības un mūzikas muzeja iekšējiem datu aizsardzības noteikumiem" un izprotu to, kā arī apņemos ievērot šajos noteikumos ietvertās prasības.
2. Apņemos neizpaust un neizmantot ierobežotas pieejamības informāciju, kas saņemta no Pārziņa, savu vai trešo personu interesēs, kā arī apņemos ievērot Informācijas atklātības likuma un Fizisko personu datu aizsardzības likuma prasības.
3. Es piekrītu, ka pārtraucot darba (līguma) attiecības ar Pārzini jebkādu iemeslu dēļ, es nekavējoties nodošu Pārzinim man rīcībā esošo aprīkojumu, kā arī man rīcībā esošos informācijas oriģinālus un kopijas, ko esmu saņēmis(usi) darba (līguma izpildes) laikā, un kura ir manā rīcībā vai kura ir citādi tieši vai netieši manā dotībā.
4. Apņemos saglabāt informācijas konfidencialitāti arī pēc darba (līguma izpildes) tiesisko attiecību izbeigšanas.

Datums	Paraksts	Paraksta atšifrējums