21.05.2018.

Nr.17

NVO JURISTA PADOMS

Datu aizsardzības nozīme nevalstiskajās organizācijās

Riski, kas rodas, vācot un uzglabājot personas datus, nav tikai teorētisks jautājums un nav attiecināms tikai uz biznesa un valsts sektoriem, bet arī nevalstisko sektoru. Nevalstiskās organizācijas, kuras nav pietiekami uzmanīgas, vai ir nolaidīgas datu apkopošanā, izmanto un glabā personu datus, ne tikai rada riskus personām, kuru datus tās apstrādā, bet var radīt arī organizācijas reputāciju graujošs riskus, saņemt naudas sodu, kā arī zaudēt ziedotāju un citu atbalstītāju uzticību. Daudzu nevalstisko organizāciju rīcībā esošie dati ietver arī sensitīvus datus par to ziedotājiem, atbalstītājiem, darbiniekiem un brīvprātīgajiem, attiecīgās mērķa grupas pārstāvjiem, par kuriem var būt interese arī personām un iestādēm, kurus vada ļaunprātīgi un savtīgi mērķi. Tādēļ jebkuriem datiem ir nepieciešama aizsardzība, jo negatīvās sekas saistībā ar datu zaudējumiem, to ļaunprātīgu izmantošanu vai zādzību būs attiecināmas uz indivīdiem un nevalstiskajām organizācijām, kuri ir tieši saistīti ar šo datu drošības nodrošināšanu.

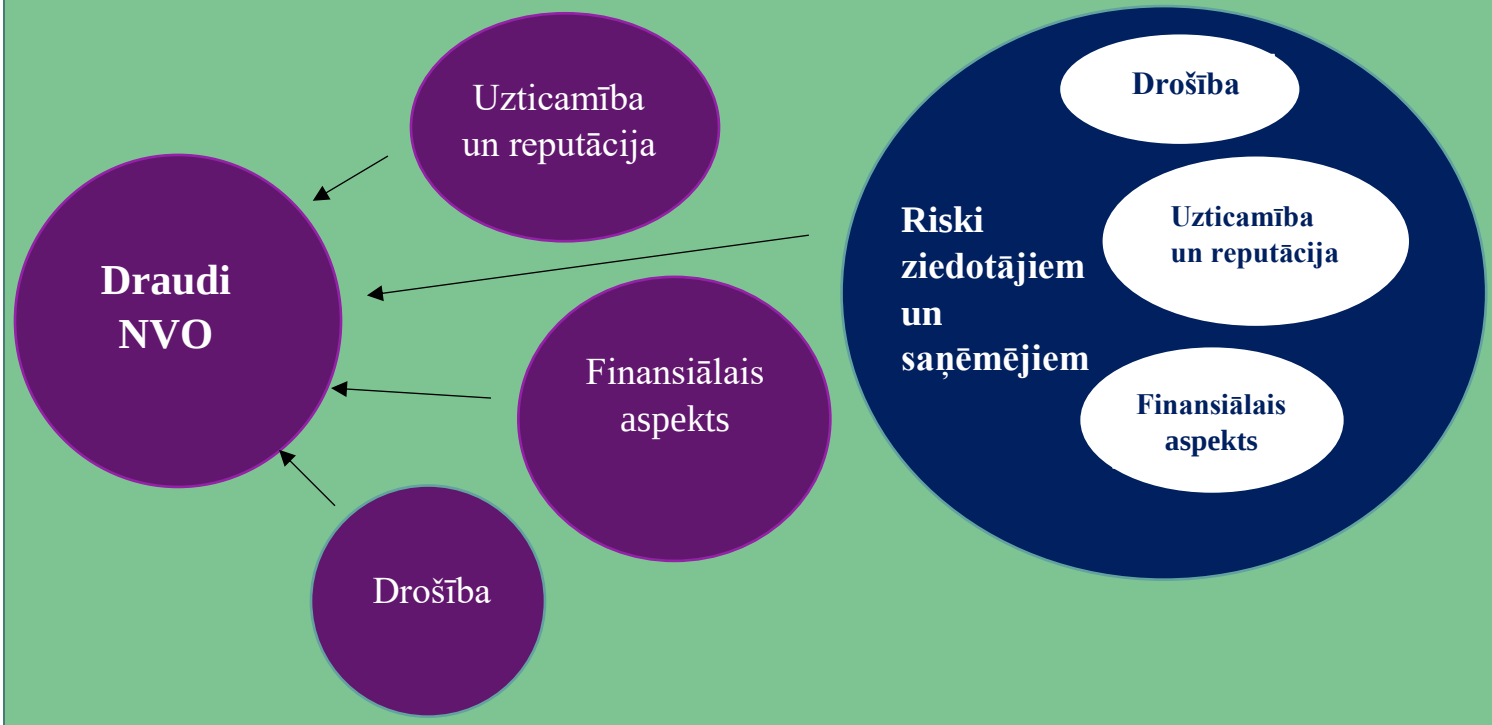
Datu aizsardzības tiesību aktu pamatprincipu interpretācija pilsoniskās sabiedrības organizācijām

Datu aizsardzības princips	Konkrēti piemēri attiecīgajam principam
Godīga un likumīga apstrāde Personas dati ir jāapstrādā godīgi, likumīgi un pārredzamā veidā	Jāprasa personas piekrišana viņa datu izmantošanai (piemēram, vārds, vecums un adrese), dalīšanās ar trešajām personām vai izmantošanai turpmākajā komunikācijā. NVO var nākties arī atklāt datus trešajai personai, ja tām ir juridisks pienākums to darīt (piemēram, valsts iestādēm, finansētājiem).
Mērķa ierobežojums Personas dati ir jāapkopo precīziem, skaidriem un likumīgiem mērķiem, un tos nedrīkst apstrādāt tādā veidā, kas neatbilst šīm prasībām.	Ir jāpaskaidro indivīdam, kāpēc ir nepieciešams viņa dzimšanas datums (piemēram, lai noskaidrotu demogrāfisko stāvokli), un šie dati nedrīkst tikt izmantoti neatbilstošiem nolūkiem (piemēram, pārdodot tos citai iestādei).
Datu minimizēšana Personas datiem jābūt adekvātiem, atbilstošiem un ierobežotiem ņemot vērā to, kam šie dati ir nepieciešami – kādam mērķim tie tiek apstrādāti.	Nevajadzētu prasīt indivīdam uzrādīt kontaktinformāciju pasākuma reģistrācijas lapā, kas publiski pieejam ikvienam dalībniekam.
Precizitāte Personas datiem jābūt precīziem un, ja nepieciešams, tie jāatjaunina.	Regulāri jālūdz personām atjaunināt savus personas datus un dot viņiem iespēju izlabot nepareizus datus.
Uzglabāšanas ierobežojumi Personas dati jāuzglabā tādā formā, kas ļauj identificēt datus ne ilgāk, kā tas ir	Vajadzētu anonimizēt vai pseidonimizēt datus, tiklīdz tos vairs nav nepieciešams uzglabāt. Piemēram, ja dati par iepriekšējiem

nepieciešams nolūkiem, kuriem tie tika ievākti.	ziedojumiem tiek turēti ilgāki par periodu, kas ir nepieciešams finanšu pārskatu un revīzijas veikšanai, ir jāapsver datu identificējošo elementu likvidēšana vai datu kopas pseidonimizēšana.
Drošība Personas dati jāapstrādā tā, lai nodrošinātu to drošību, izmantojot atbilstošas tehniskas un organizatoriskas darbības.	Jānodrošina, ka datu uzglabāšanas un apstrādes sistēmas izmanto jaunāko programmatūru un maksājumu vietnes garantē šifrētus darījumus.
Pārredzamība un atbildība Tas, kurš pārvalda organizācijas datus, ir atbildīgs par to, lai tiktu ievērota un demonstrēta attiecīga datu aizsardzības principu ievērošana.	Būtu nepieciešams iecelt datu aizsardzības inspektoru vai uzticēt šo atbildību kādai konkrētai personai organizācijas iekšienē, un būtu nepieciešams nodrošināt to, ka atbildīgā persona publicē informāciju, kā iegūtie un apstrādātie dati tiks aizsargāti.

Datu aizsardzības standartu neievērošanas risks[1]

Shēmā redzams, kādi riski draud NVO, datu aizsardzības standartu neievērošanas gadījumā, kā arī kādu iespaidu tas var atstāt uz ziedotājiem.



Informāciju sagatavoja:
Biedrība „Latvijas Pilsoniskā alianse”
Rīga, 2018

[1] http://ecnl.org/wp-content/uploads/2018/01/Data-Protection-Standards-for-CSOs.pdf