

Noziedzības tendences Covid-19 laikā: kam pievērst uzmanību, lai pasargātu savu uzņēmumu

2/19/2020

Reaģējot uz starptautisko Covid-19 uzliesmojumu un sabiedrībā radīto nenoteiktības sajūtu, ir novērojamas vispārējas noziedzības, tostarp krāpšanas, izspiešanas, noziedzīgi iegūtu līdzekļu legalizācijas un citu ekonomiska rakstura noziegumu pieauguma tendences. Savā būtībā tā ir racionāli sagaidāma rīcība no to personu puses, kuras arī iepriekš ir iesaistījušās prettiesiskās darbībās un centušās izmantot pastāvošās tiesiskās sistēmas un sabiedriskās kārtības vājākos posmus savās interesēs. Gluži analoga prettiesiskas rīcības stratēģija tiek īstenota arī šī brīža situācijā, kad sabiedrības uzmanība ir pievērsta citiem būtiskiem un steidzamiem jautājumiem, mazinot cilvēku piesardzību vai liekot tiem pārsteidzīgi rīkoties ārkārtējās situācijas dēļ. Arī prakse liecina, ka pieaugošie noziedzīgu nodarījumu apjomi ir tieši saistāmi ar Covid-19 radītajiem apstākļiem.

Starptautisko organizāciju novērojumi

Starptautiskās tiesībsargājošās organizācijas (t.sk. INTERPOL, *Europol*) sniedz ieskatu noziedzīgo darbību attīstības tendencēs un ir identificējušas būtiskākos prettiesiskas rīcības draudus, tostarp:

- Būtisks pieaugums draudiem, kas saistīti ar kiberdrošību, piemēram, ļaunprātīgi izveidoti domēni, ļaunprātīga programmatūra vai izpirkuma programmatūra (*ransomware*);
- Mērķtiecīgi uzbrukumi veselības un medicīnas pakalpojumu sniedzējiem un veselības aprūpei nozīmīgu preču izplatītājiem kā kritiski nozīmīgiem infrastruktūras elementiem;
- Krāpnieciska tirdzniecība un viltojumi personiskās drošības aprīkojuma un pretvīrusu medikamentu izplatīšanas jomā;
- Paaugstināta nelegālo apreibinošo vielu tirdzniecība, izmantojot sociālos tīklus, šifrētas lietotnes vai darknet tīklus;
- Personas un uzņēmumi, kas cieš no būtiska ienākumu samazinājuma, var krist par upuriem organizētās noziedzības grupējumu finansētiem aizdevējiem, kas piemēro nesamērīgi augstas aizdevuma procentu likmes.

Arī Financial Action Task Force (FATF) norāda uz dažādu noziedzīga rakstura darbību izplatību, piemēram, dažāda veida krāpniecību, līdzekļu vākšanu viltus labdarības organizāciju labā, viltus medicīniskās palīdzības vai aprīkojuma reklamēšanu, fiktīvu investēšanas iespēju piedāvājumus un pikšķerēšanas (*phishing*) metodes. Uzraugošās un tiesībsargājošās iestādes tiek aicinātas turpināt sniegt informatīvu atbalstu privātajam sektoram, skaidrojot situācijas būtiskumu un iespējamo ietekmi uz organizāciju darbību. Uzņēmumiem jāpievērš pastiprināta uzmanība Covid-19 apstākļu ietekmē radītajiem draudiem, kas saistīti ar noziedzīgi iegūtu līdzekļu legalizāciju (NILL), it īpaši vērtējot krāpšanas gadījumiem raksturīgu noziedzīgu nodarījumu iespējamību un terorisma finansēšanu (TF).

Aicinām Jūs iepazīties arī ar PwC sagatavotās Globālo Ekonomisko noziegumu un krāpniecības aptaujas rezultātiem, kas atspoguļo noziedzības globālās tendences laikā pirms ārkārtējās situācijas iestāšanās.

NILLTPFN riski

Noziedzīgi iegūtu līdzekļu legalizācijas un terorisma un proliferācijas finansēšanas novēršanas likuma (NILLTPFN likums) subjektiem šobrīd jābūt īpaši piesardzīgiem. Papildus ierastajiem riska faktoriem būtu jāvērtē ārkārtējās situācijas radītie apstākļi un to ietekme uz NILLTPFN likuma subjektu klientiem, darījumu partneriem, finanšu vai cita veida darījumiem un ieviestajām iekšējās kontroles sistēmām kā arī saistītajiem risku vadības mehānismiem.

Ārkārtējās situācijas laikā īpaša uzmanība būtu jāpievērš:

- neparastai klientu un darījumu partneru rīcībai;
- jaunu darījuma attiecību nodibināšanai (veicot padziļinātu sākotnējo izpēti un pastiprinātu turpmāko uzraudzību);
- šķietami izdevīgiem darījuma vai sadarbības nosacījumiem;
- aizdomīgiem un sarežģītiem darījumiem;
- jebkādam novirzēm no ierastās klientu rīcības - ienākumu apjomā, juridiskajos vai grāmatvedības risinājumos, izmantotajos pakalpojumos, veiktajā saimnieciskajā darbībā, kā arī neliela apjoma finanšu darījumos.

Sekojoši līdzīgi apkārtējās sociālās un ekonomiskās vides izmaiņām, arī uzņēmumiem ir nepieciešams vērtēt, kā pilnvērtīgi pielāgot uzņēmuma izmantotos risku vadības un kontroles mehānismus, kā arī nepieciešamības gadījumā lemt par jaunu iekšējās kontroles sistēmas elementu ieviešanu, lai cīnītos ar situācijas radītajiem draudiem. Izvērtējot konkrētos apstākļus un uzņēmuma darbības specifiku, būtu kritiski jāvērtē:

- uzņēmuma iekšējās kontroles sistēmas uzbūve un funkcionalitāte, tostarp pielietotās atsevišķu risku vadības metodes;
- nepieciešamība pārskatīt vai novērtēt uzņēmuma NILLTPFN vai sankciju riskus;
- uzņēmuma IT sistēmas infrastruktūra, drošības uzstādījumi un funkcionalitāte, tostarp vērtējot darbības nepārtrauktības, informācijas uzglabāšanas, datu analīzes un vadības mehānismus;
- iekšējā audita vai ārējo ekspertu veikto pārbaūžu rezultāti un nepilnību novēršanas plāna izpilde, nepieciešamības gadījumā pārskatot darba plānu un izvērtējot ieteikumu ieviešanas būtiskumu;
- uzņēmuma vadības modelis un organizatoriskā struktūra, tostarp atsevišķu funkciju tiesības, pienākumi un rīcības nosacījumi.

Atgādinām, ka savlaicīga un pārdomāta risku vadības prakse pasargās Jūs no prettiesiskas rīcības ietekmes, uzņēmuma operacionālajiem ierobežojumiem, iespējamiem juridiska vai finansiāla rakstura sarežģījumiem un ļaus nodrošināt efektīvu uzņēmuma darbību arī ārkārtējās situācijas apstākļos.