Risinājuma apraksts

Kiberdrošība interneta pakalpojumos

1. Atsevišķos Latvijas Mobilais Telefons SIA, reģ.nr. 50003050931, juridiskā adrese Ropažu iela 6, Rīga, LV-1039 (turpmāk – LMT) sniegtajos interneta pakalpojumos (Mobilais internets (ar un bez apjoma ierobežojuma), Internets mājai, Internets privātmājai, Neierobežots internets+, Internets biznesam un Profesionālais internets (turpmāk – pakalpojums) LMT klientiem ir iekļauts kiberdrošības risinājums (turpmāk – Risinājums).

2. Pirms pakalpojuma izmantošanas uzsākšanas klientam ir pienākums iepazīties ar šo aprakstu un LMT Privātuma politiku. Šis apraksts ir pastāvīgi pieejams LMT mājaslapā un LMT klientu centros. Turpinot vai uzsākot izmantot pakalpojumu, klients apliecina, ka ir iepazinies ar šo aprakstu.

3. LMT ir Risinājuma uzturētājs un veidotājs. Risinājums tiek nodrošināts sadarbībā ar Whalebone s.r.o., izmantojot šī pakalpojuma sniedzēja izstrādāto pielāgotā *DNS Resolver* drošības risinājumu.

4. *DNS Resolver drošības* risinājums pasargā klienta iekārtu (planšeti, datoru) pret kiberapdraudējumiem interneta vidē (phishing, ransomware, spam, coin miners, worms, trojans u.c). Risinājums tiek nodrošināts tikai LMT tīklā. Risinājums nav pieejams ārpus LMT tīkla, kā arī klientam izmantojot jebkādu Wi-Fi tīklu bez pakalpojuma drošības risinājuma.

5. Risinājumā izmantotais *DNS Resolver* drošības risinājums novērš piekļuvi ļaundabīgām un bīstamām interneta vietnēm, pāradresējot klientu uz drošu informatīvo lapu ar informāciju par apdraudējumu. Informācija par šādām vietnēm tiek nemitīgi atjaunota un papildināta, balstoties uz rūpīgi izvēlētiem ārējiem avotiem par kiberapdraudējumiem.

6. Risinājums tiek uzstādīts un atjaunināts automātiski.

7. Neraugoties uz Risinājumam paredzēto plašo drošības funkcionalitāti, neviens risinājums negarantē 100% drošību pret apdraudējumu interneta vidē. Klients patstāvīgi rūpējas par jebkādiem papildu drošības pasākumiem, lai aizsargātu iekārtā izmantoto tīklu no kiberdrošības apdraudējumiem un izmantotu iekārtas tīklu atbildīgā un drošā veidā. Pakalpojumā izmantotais risinājums nepasargā klientu no nedrošām vietnēm ārpus *DNS Resolver* risinājuma, ar pakalpojuma risinājumu neaizsargāta Wi-Fi lietošanas gadījumā, kā arī no apdraudējumiem, kas rodas paša klienta neapdomātas rīcības rezultātā (informācijas nodošana krāpniekiem; piekļūšana vietnēm, ignorējot pakalpojuma risinājuma brīdinājumus u.tml.). Risinājums nepasargā iepriekš inficētas klienta iekārtas.

8. Interneta piekļuves pakalpojumu ietvaros tiek sniegta piekļuve internetam un visiem tā galapunktiem neatkarīgi no klienta izmantotās tīkla tehnoloģijas un galiekārtas ar izņēmumiem atbilstoši normatīvajos aktos noteiktajām prasībām.

9. Tehniskā palīdzība saistībā ar pakalpojumu un tajā iekļauto Risinājumu pieejama, rakstot uz info@lmt.lv.

10. Pakalpojums tiek sniegts atbilstoši Latvijas Republikā spēkā esošo tiesību aktu prasībām un LMT pakalpojumu līguma noteikumiem.

11. LMT ir tiesības jebkurā laikā pēc saviem ieskatiem pievienot vai atcelt jebkādu Risinājuma funkcionalitāti vai risinājuma izpildījumu, kā arī grozīt šo aprakstu, par to iepriekš informējot klientu un norādot vietu, kurā ir pieejama informācija un kur var iepazīties ar Risinājuma apraksta aktualizēto redakciju.

Informācija par personas datu apstrādi

12. Attiecībā uz personas datu apstrādi Risinājuma ietvaros LMT ir personas datu pārzinis, bet Whalbone s.r.o. ir apstrādātājs. LMT sniegto pakalpojumu ietvaros datus apstrādājam tikai nepieciešamajā apjomā un laika periodā, kas izriet no pakalpojuma būtības un saistošo normatīvo aktu prasībām. Lai nodrošinātu Risinājumu klientiem, var tikt apstrādāti personas pamatdati, kā arī elektronisko sakaru metadati – ar elektronisko sakaru pakalpojumu sniegšanu saistītā informācija. Tostarp – klienta pieprasītais DNS vaicājums, DNS atbilde, laika zīmogs, IP adrese. Apstrādājamo datu mērķis ir īstenot pakalpojuma izpildi, tostarp nodrošināt ar to saistīto kvalitāti, drošību un pieteikto jautājumu risināšanu, ja tādi rodas, kā arī saistošo normatīvo aktu izpildi.

13. Datu apstrādes pamats ir LMT pakalpojumu līgums un ar to saistīto normatīvo aktu īstenošana. Šāda apstrāde ir priekšnosacījums darījuma izpildei, un datu nesniegšana var daļēji vai pilnībā kavēt vai pārtraukt darījuma nodrošināšanu. Lai nodrošinātu personas datu pienācīgu aizsardzību, apstrādājot personas datus, tiek piemēroti tehniski un organizatoriski pasākumi, tostarp drošības pasākumi.

14. Klients ir informēts, ka Risinājuma nodrošināšanas ietvaros var tikt izmatoti datu saņēmēji – pakalpojumu sniedzēji, kuriem LMT var rasties nepieciešamība sniegt datus, ja tas ir funkcionāli nepieciešams Risinājuma nodrošināšanai un tehniskai uzturēšanai, tostarp nodot atsevišķus datus apstrādei trešajās valstīs ārpus Eiropas Savienības un Eiropas Ekonomiskās zonas atbilstoši ar pakalpojumu sniedzēju apstiprinātajiem datu apstrādes noteikumiem un veicot pienācīgus pasākumus, lai nodrošinātu atbilstošu fizisku personu datu aizsardzības līmeni. Piemēram, trešā valsts, kurā pakalpojuma sniedzējs atrodas, atbilstoši Eiropas Savienības Komisijas lēmumam nodrošina pietiekamu aizsardzības līmeni, pakalpojuma sniedzējs ir sniedzis atbilstošas garantijas ar saistošiem uzņēmuma noteikumiem, atbilstošām standarta datu aizsardzības klauzulām vai citos gadījumos. Statistikas un pakalpojuma uzlabošanas nolūkā klientu dati var tikt izmantoti anonimizētā formā.

15. Plašāka informācija par LMT īstenoto personas datu aizsardzību un datu subjektu tiesībām pieejama LMT Privātuma politikā, kas ir šo noteikumu neatņemama sastāvdaļa.

16. Jautājumu gadījumā par šo aprakstu vai klienta datu apstrādi lūdzam rakstīt uz info@lmt.lv; datu aizsardzības speciālists: personasdati@lmt.lv.

Rīgā, 25.03.2024.