

LMT grupas aizsargājamās informācijas apstrādes prasības Sadarbības partneriem

“Latvijas Mobilais Telefons” SIA un tā grupas sabiedrībām “ZetCOM” SIA un “LMT Retail & Logistics” SIA, turpmāk tekstā katrs atsevišķi un visi kopā – **LMT**, ir būtiski nodrošināt nepārtrauktu aizsargājamās informācijas (tai skaitā, personas datu) konfidencialitāti, integritāti un pieejamību.

Aizsargājamā informācija ir personas dati, komercnoslēpums, kā arī cita LMT un LMT uzticēta informācija jebkādā formā, tajā skaitā, informācijas sistēmas un papīra dokumenti, izņemot tiesiskā veidā pieejamu publisku informāciju. Aizsargājamās informācijas konfidencialitātes, integritātes vai pieejamības zudums vai samazinājums var radīt ievērojamu un ilgstošu kaitējumu LMT likumīgajām interesēm, radīt zaudējumus LMT un negatīvi ietekmēt LMT reputāciju, kā arī personas datu gadījumā var radīt riskus un/vai apdraudēt datu subjekta tiesības un brīvības.

Lai nodrošinātu labās prakses standartu rekomendāciju un Vispārīgās datu regulas Nr. 679/2016 (turpmāk – **Datu regula**) prasību izpildi, LMT ir noteikusi prasības LMT aizsargājamās informācijas, tajā skaitā personas datu, apstrādei un prasības, kādām Sadarbības partnerim ir jāatbilst, veicot aizsargājamās informācijas apstrādi (turpmāk – **Prasības**).

Šīs Prasības ir piemērojamas un attiecināmas uz ikvienu, kurš veic aizsargājamās informācijas apstrādi (turpmāk – **Sadarbības partneris**).

1. Vispārīgie noteikumi

- 1.1. Sadarbības partneris apņemas ievērot šīs Prasības, sadarbības līguma noteikumus, Latvijas Republikā piemērojamos normatīvos aktus (t. sk., Datu regulu), un nodrošināt Sadarbības partnera un tā darbības atbilstību iepriekš minētajam.
- 1.2. Sadarbības partnerim ir pienākums nodrošināt aizsargājamās informācijas aizsardzību šajās Prasībās noteiktā kārtībā. Gadījumā, ja sadarbības līgumā ir ietverta informācijas klasifikācija, Sadarbības partnerim ir pienākums nodrošināt sadarbības līgumā noteikto informācijas klasifikāciju un aizsardzību papildus šīm Prasībām. Sadarbības partneris nekavējoties informē LMT gadījumā, ja Sadarbības partneris neatbilst Prasībām vai nevar izpildīt kādu no Prasībās ietvertajiem norādījumiem.
- 1.3. Jebkādu izmaiņu gadījumā, kas ietekmē vai var ietekmēt Sadarbības partnera un tā darbības atbilstību šīm Prasībām, Sadarbības partneris nekavējoties informē LMT, pirms minētās izmaiņas tiek ieviestas Sadarbības partnera darbībā vai statusā.
- 1.4. Sadarbības partneris reizi gadā pārskata savas darbības atbilstību šīm Prasībām un sniedz LMT rakstisku novērtējumu par Sadarbības partnera un tā darbības atbilstību šīm Prasībām, vai arī par Sadarbības partnera vai tā darbības aspektiem, kas neatbilst šīm Prasībām.
- 1.5. LMT ir tiesības prasīt Sadarbības partnerim tā darbības pārskatīšanu biežāk nekā noteikts Prasību 1.4. punktā, izvērtējot aizsargājamās informācijas apstrādes raksturu un citus apstākļus, kas var ietekmēt aizsargājamās informācijas apstrādi.
- 1.6. LMT, pilnveidojot aizsargājamās informācijas apstrādi un drošības prasības, var vienpusēji veikt izmaiņas šajās Prasībās, par ko LMT paziņos Sadarbības partnerim, informējot par izmaiņām elektroniskā formā (LMT mājas lapā un/vai nosūtot paziņojumu sadarbības partnera kontaktpersonai).

2. Sadarbības partnera atbildība

- 2.1. Sadarbības partnerim ir pienākums nodrošināt un spēt uzskatāmi parādīt, ka tiktāl, cik tas attiecas uz sadarbību ar LMT, tā statuss, darbība, procesi un piemērojamie līdzekļi aizsargājamās informācijas apstrādē atbilst Latvijas Republikā piemērojamo normatīvo aktu (tai skaitā, Datu regulas), sadarbības līguma un Prasību noteikumiem. Par jebkāda veida neatbilstību prasībām Sadarbības partneris nekavējoties informē LMT.
- 2.2. Papildus šo Prasību 1.4. punkta nosacījumiem, Sadarbības partnerim ir pienākums pēc LMT pieprasījuma LMT noteiktā laika periodā sniegt LMT pieprasīto informāciju un pierādījumus par Sadarbības partnera un tā darbības atbilstību šīm Prasībām, kā arī nodrošina LMT iespēju

pašam veikt Sadarbības partnera aizsargājamās informācijas pārvaldības un apstrādes auditu/revīziju, nodrošinot iespēju LMT grupas uzņēmuma pārstāvjiem piekļūt un iepazīties ar dokumentiem, kas pamato Sadarbības partnera un tā darbības atbilstību Latvijas Republikā piemērojamo normatīvo aktu prasībām (tai skaitā, Datu regulas prasībām), šīm Prasībām un sadarbības līgumam. LMT patur tiesības, vienojoties ar Sadarbības partneri, prasīt arī neatkarīga trešās puses audīta veikšanu, lai izvērtētu Sadarbības partnera aizsargājamās informācijas pārvaldību un apstrādi.

3. Drošības prasības

3.1. Risku vadība

- 3.1.1. Sadarbības partneris ir novērtējis aizsargājamās informācijas drošības riskus uzņēmumā, kā arī veicis nepieciešamās kontroles un riska mazinošos pasākumus.
- 3.1.2. Sadarbības partneris ir dokumentējis aizsargājamās informācijas drošības risku pārraudzību savā darbībā.
- 3.1.3. Sadarbības partneris periodiski novērtē riskus, kas saistīti ar informācijas resursiem un aizsargājamās informācijas apstrādi, glabāšanu un nosūtīšanu, un spēj to pamatot ar atbilstošu dokumentāciju.

3.2. Aizsargājamās informācijas drošības noteikumi

- 3.2.1. Sadarbības partneris nodrošina, ka aizsargājamā informācija netiek izpausta un nav pieejama nevienai trešajai personai, izņemot šo Prasību 5. punkta kārtībā piesaistīto apakšpartneri tikai tā pienākumu veikšanai nepieciešamajā apjomā, kā arī nodrošina minētās informācijas aizsardzību pret nesankcionētu piekļuvi, nejaūšu iznīcināšanu vai noplūdi.
- 3.2.2. Sadarbības partneris nodrošina, ka IT sistēmām, serveriem un citām informācijas turēšanas vietām un objektiem, kur tiek apstrādāta, t.sk. glabāta, aizsargājamā informācija, un aizsargājamās informācijas saturam nepieklūst neviena persona, izņemot Sadarbības partnera un/vai šo Prasību 5. punktā noteiktā kārtībā piesaistītā apakšpartnera darbinieki, kuriem piekļuve nepieciešama tiešo pienākumu veikšanai un sadarbības līguma izpildei. Tas attiecas gan uz fizisko piekļuvi, gan loģisko piekļuvi (caur informācijas sistēmām), gan piekļuvi dokumentiem papīra formā.
- 3.2.3. Sadarbības partneris ir ieviesis un dokumentējis informācijas drošības vadības sistēmu, tai skaitā, Sadarbības partneris ir izstrādājis informācijas drošības noteikumus, kurus ir apliecinājušas Sadarbības partnera paraksttiesīgās personas un par kuriem ir informēti Sadarbības partnera un/vai šo Prasību 5. punktā noteiktā kārtībā piesaistītā apakšpartnera darbinieki, par ko Sadarbības partneris var iesniegt LMT rakstveida apliecinājuma dokumentus.
- 3.2.4. Sadarbības partneris ir noteicis un dokumentējis Sadarbības partnera personāla lomas un atbildību attiecībā uz aizsargājamās informācijas apstrādi un drošību, kā arī veic šādu dokumentu regulāru pārskatīšanu un nodrošina to atbilstību šīm Prasībām un Latvijas Republikā piemērojamo normatīvo aktu noteikumiem (tai skaitā, Datu regulas prasībām).
- 3.2.5. Sadarbības partneris ir nozīmējis vismaz vienu darbinieku, kuram ir nepieciešamā informācijas drošības pārvaldības kompetence, atbildīgu par informācijas aizsardzības nodrošināšanu Sadarbības partnera organizācijā. Sadarbības partneris informē LMT par šādas personas iecelšanu, norādot tās vārdu, uzvārdu un kontakta tālruni un e-pastu.
- 3.2.6. Sadarbības partneris ir ieviesis un dokumentējis procesu, kas nodrošina iespēju izsekot un noteikt, kurš un kad ir piekļuvis aizsargājamajai informācijai. Tas attiecas gan uz fizisko piekļuvi, gan loģisko piekļuvi (caur informācijas sistēmām), gan piekļuvi dokumentiem papīra formā.
- 3.2.7. Sadarbības partneris nodrošina aizsargājamās informācijas obligāto tehnisko aizsardzību, kuru īsteno ar fiziskiem (piekļuves kontrole, apsardze, atbilstošs temperatūras un mitruma režīms u.c.) un loģiskiem (programmatūra, paroles, šifrēšana) aizsardzības līdzekļiem.
- 3.2.8. Sadarbības partneris ir ieviesis informācijas drošības incidentu vadības procesu, kas ietverts atbilstošos iekšējos noteikumus. Sadarbības partneris nodrošina nekavējošu LMT informēšanu gadījumā, ja notiek vai rodas aizdomas, ka varētu notikt drošības incidents un/vai aizsargājamās informācijas aizsardzības pārkāpums.
- 3.2.9. Sadarbības partneris ir noteicis un kontrolē aizsargājamās informācijas pārvaldību savā uzņēmumā, kas citu starpā ietver drošības prasības aizsargājamās informācijas apstrādē.

4. Personāla vadības jautājumi

- 4.1. Sadarbības partneris ir noslēdzis rakstveida līgumus ar visiem darbiniekiem, kas var piekļūt vai apstrādāt jebkādā veidā aizsargājamo informāciju. Šajos līgumos Sadarbības partnera darbinieks ir apņēmis nodrošināt aizsargājamās informācijas konfidencialitāti, integritāti un pieejamību, kā arī neizpaust iegūto informāciju nenoteiktu laika periodu, t.i., gan darba attiecību laikā, gan pēc darba attiecību izbeigšanas.
- 4.2. Sadarbības partneru darbinieki tiek apmācīti aizsargājamās informācijas aizsardzības un drošības jautājumos, pirms darbinieks uzsāk aizsargājamās informācijas apstrādi, kā arī tiek nodrošinātas atkārtotas mācības vismaz reizi gadā. Minētās mācības ietver, cita starpā, apmācības par piekļuvi informācijas sistēmām, par informācijas izmantošanu tikai darba vajadzībām, par informācijas apstrādi, tikai balstītu uz tiesiska pamata un drošā veidā, aktuālajiem apdraudējumiem un aizsardzības metodēm, kā arī citiem jautājumiem.
- 4.3. Sadarbības partneris, veicot darbinieku atlasī amatiem, kuri veiks LMT aizsargājamo informācijas apstrādi, izvērtē arī to, vai konkrētais kandidāts var radīt drošības riskus, veicot šo apstrādi. LMT ir tiesības iegūt un Sadarbības partnerim ir pienākums sniegt LMT informāciju par saviem darbiniekiem, kuri piekļūs LMT aizsargājamai informācijai. Sadarbības partnerim ir pienākums nozīmēt kādu citu darbinieku sadarbības ietvaros ar LMT gadījumā, ja LMT rodas pamatotas šaubas par sākotnēji nozīmētās personas spēju rīkoties ar LMT aizsargājamo informāciju saskaņā ar šīm Prasībām.
- 4.4. Sadarbības partneris informē LMT par personāla izmaiņām par tiem saviem darbiniekiem, kuri strādā ar LMT aizsargājamo informāciju, kā arī nodrošina šī pienākuma izpildi arī attiecībā uz apakšpartneriem.
- 4.5. Sadarbības partneris nodrošina, ka tā darbinieki ir informēti, apzinās un ievēro šīs Prasības, Latvijas Republikā piemērojamos normatīvos aktus (tai skaitā, Datu regulu), sadarbības līguma noteikumus un Sadarbības partnera noteiktos informācijas, infrastruktūras un sistēmu izmantošanas noteikumus.

5. Apakšpartnera piesaistīšana

- 5.1. Sadarbības partnerim ir tiesības piesaistīt apakšpartneri tikai pēc LMT rakstiskas piekrišanas saņemšanas. Pirms apakšpartnera piesaistīšanas, Sadarbības partneris iesniedz LMT tā pieprasīto informāciju, kā arī apakšpartnera sniegtu apliecinājumu par atbilstību šīm Prasībām, Latvijas Republikā piemērojamo normatīvo aktu (t.sk, Datu regulas) prasībām, un citām prasībām, kas ietvertas sadarbības līgumā vai jebkurā tā pielikumā.
- 5.2. Sadarbības partneris nodrošina, ka Sadarbības partnera izvēlētais apakšpartneris atbilst un var apliecināt savu atbilstību gan Latvijas Republikā piemērojamo normatīvo aktu prasībām, tai skaitā, Datu regulas prasībām personas datu aizsardzībā, gan šīm Prasībām, kā arī var iesniegt rakstiskus pamatojošus dokumentus, kas pierāda apakšpartnera un tā darbības atbilstību minētajam.
- 5.3. Sadarbības partneris uzņemas pilnu atbildību par apakšpartneri, tā darbību un veikto personas datu apstrādi, kā arī sedz jebkāda veida LMT radušos zaudējumus šāda apakšpartnera darbības vai bezdarbības rezultātā.
- 5.4. Sadarbības partneris nodrošina apakšpartnera aizsargājamās informācijas pārvaldības un apstrādes auditu/revīziju pēc LMT pieprasījuma LMT norādītajā laika periodā, kā arī nodrošina LMT iespēju pašam veikt minētā apakšpartnera aizsargājamās informācijas pārvaldības un apstrādes auditu/revīziju, nodrošinot iespēju LMT grupas uzņēmuma pārstāvjiem piekļūt un iepazīties ar dokumentiem, kas pamato apakšpartnera un tā darbības atbilstību Latvijas Republikā piemērojamo normatīvo aktu prasībām (tai skaitā, Datu regulas prasībām), šīm Prasībām un sadarbības līgumam.