Grupi Poliitika – Turvalisus ja Privaatsus

1 EESMÄRK

Telia Company poliitika “Turvalisus ja Privaatsus” eesmärk on toetada meie missiooni – panustada ühiskonna arengusse, et Eesti oleks parem paik nii elamiseks kui töötamiseks – kaitstes Telia kliente, töötajaid, aktsionäre ja ühiskondi kus me tegutseme, turvalisuse ja privaatsuse rikkumiste eest.

Telia, kui seadusega reguleeritud elutähtsa teenuse pakkuja, käsitleb turvalisuse ja privaatsuse riske strateegiliste äririskidena. Meie riigipõhise tegevusmudeli raames rakendame riskipõhist lähenemist, mis tähendab, et kontrollmeetmed on alati proportsionaalsed vastava riskiga. See tagab, et investeerimisotsused arvestavad riskitaluvust ja vastavat küpsustaset, kooskõlas meie ettevõtte riskijuhtimise poliitikaga.

Viimane versioon sellest grupipoliitikast on avaldatud veebilehel www.teliacompany.com.

2 PÕHIMÕTTED

Turvalisuse- ja privaatsuse kultuuri edendamine on Telia Company üks olulisemaid prioriteete. Meie põhimõtted on loodud selleks, et turvalisus ja privaatsus oleksid kogu Telia Company tegevuses läbivalt rakendatud, näidates meie pühendumust nende valdkondade kõrgeimal tasemel järgimisele.

See pühendumus hõlmab juhtimist, tuvastamist, avastamist, kaitset, reageerimist ja taastamist võimaldavaid võimekusi, mis on vajalikud meie varade kaitsmiseks. Nende elementide lõimimise kaudu püüame pakkuda tooteid ja teenuseid, mis on vastupidavad turva- ja privaatsusohtudele.

Et vältida liigset rahalist ja halduskoormust ettevõtetele, põhineb nende põhimõtete ja sellele järgnevate turva- ja privaatsusnõuete rakendamine riskidel ning vastab järelevalvelistele, seadusandlikele, kliendi- ja riikliku julgeoleku nõuetele.

Isikuandmete liigid, mida Telia Company füüsiliste isikute kohta kogub, samuti kogumise aeg ja töötlemise viis, võivad olla täiendavalt reguleeritud konkreetsete teenuste raames ja vastavate teenuste lepingutingimustes või kohalikus seadusandluses.

2.1 TURVALISUSE PÕHIMÕTTED

Järgmised turvapõhimõtted tuleb rakendada selle grupipoliitika alla kuuluvate tegevuste puhul:

- **Põhimõte 1:** Telia Companys on loodud grupi turvaorganisatsioon, millel on määratletud rollid ja vastutusvaldkonnad ning mida pidevalt täiustatakse, et juhtida ettevõtte lähenemist turvariskidele. Eelkõige:
    - Toetada riigi üksusi, et tagada ärile vastav ja turvariskipõhine mõtteviis, mis on kooskõlas riskitaluvusega;
    - Arendada, teavitada ja jõustada autoriteetne turvadokumentatsioon;
    - Tagada juhtimine, järelevalve, nõustamine ja kriitiline hindamine operatiivsetele turvariskide otsustele;
    - Teha koostööd privaatsusvaldkonnaga, et tagada terviklikud andmekaitsemeetmed, vastavus kehtivatele seadustele ning kaitse rikkumiste ja ohtude eest;
    - Tagada turvalisuse kaasamine personalipraktikatesse;
    - Edendada turvalisuse ja privaatsuse teadlikkust ning koolitusi;
    - Juhtida kindlustusteenuste pakkumist määratletud turvariskide katteks.
- **Põhimõte 2:** Rakendatakse turvanõuded ja -protsessid, mis võimaldavad turvariskide tuvastamist. See hõlmab muu hulgas:
    - Missioonikriitilised (MC), ärikriitilised (BC) ja standardkriitilised (SC) varad on tuvastatud, klassifitseeritud, loogiliselt märgistatud inventaris ja kaitstud vastavalt kriitilisusele;
    - Turvariskid on tuvastatud, hallatud ja prioriseeritud vastavalt vara kriitilisusele;
    - Haavatavused on tuvastatud ja maandatud vastavalt nende riskitasemele;
    - Äritegevused ja -protsessid on kooskõlas turvaprotsessidega.
- **Põhimõte 3:** Rakendatakse turvaprotsessid ja -nõuded, mis võimaldavad kaitset kahjulike turvaintsidentide eest, vastavalt tuvastatud riskidele. Eelkõige:
    - Füüsilise ja loogilise identiteedihalduse, autentimise ja juurdepääsukontrolli meetmed on rakendatud;
    - Võrgu- ja infosüsteemide turvanõuded on rakendatud;
    - Andmed ja teave, sealhulgas isikuandmed, on säilitatud ja kaitstud vastavalt klassifikatsioonile, sõltumata nende staatusest;
    - Füüsilise turvalisuse nõuded on rakendatud vastavalt riskitasemele;
    - Operatiivsed turvaprotsessid, mis tagavad pideva seire, on järgitud;
    - Turvalise arenduse praktikad on integreeritud arendusprotsessidesse;
    - Tegevuskerksuse nõuded on arvesse võetud ja testitud, et kaitsta varasid kahjulike olukordade eest.

- **Põhimõte 4:** Rakendatakse turvaseire nõuded ja protsessid, et tuvastada ja analüüsida võimalikke turvarünnakuid ja rikkumisi.
- **Põhimõte 5:** Rakendatakse turvanõuded ja -protsessid, mis võimaldavad turvaintsidentidele asjakohaselt reageerida ja taastuda, et suurendada tegevuskerksust. Eelkõige:
    - Turvaintsidentide reageerimise ja taastamise protsessid on rakendatud ja neid testitakse perioodiliselt;
    - Turvalisus on integreeritud ärikatkestuse, katastroofitaaste ja kriisijuhtimise nõuetesse.

2.2 Privaatsuse põhimõtted

Käesoleva poliitika alusel läbi viidavatele tegevustele kohalduvad järgmised põhimõtted:

- **Põhimõte 1:** Telia Company privaatsust juhitakse ja hallatakse nii, et täidetakse õiguslikud, lepingulised ja ärinõuded ning olemas on asjakohased ja piisavad organisatsioonilised ressursid, protsessid ja töövahendid, et tagada selle poliitika nõuetekohane rakendamine. Privaatsusriskide hindamine toimub regulaarselt ja nende riskide leevendamiseks töötatakse välja strateegiad.
- **Põhimõte 2:** Isikuandmeid töödeldakse õiglaselt ja seaduslikult määratletud õiguslikel alustel õiguspäraste äri-, töö- ja tegevuseesmärkide saavutamiseks kõigis tegevustes, sealhulgas isikuandmete edastamisel kolmandatesse riikidesse. Töödeldakse ainult neid isikuandmeid, mis on asjakohased ja mitte ülemäärased seoses eesmärgiga, milleks need koguti. Erilist tähelepanu pööratakse sideandmete, eriliigiliste andmete, laste isikuandmete ja muude haavatavate rühmade andmete töötlemisele.
- **Põhimõte 3:** Töötajatele, klientidele ja teistele isikutele antakse läbipaistev ja mõtestatud teave nende isikuandmete töötlemise kohta. Selgitatakse õiguslikke aluseid ja töötlemise eesmärke, milleks isikuandmeid töödeldakse ning isikutele antakse kasutajasõbralikud võimalused oma õiguste kasutamiseks, sealhulgas juurdepääsuõigus, parandamisõigus, kustutamisõigus, nõusolek ja töötlemisele vastuväite esitamine. Läbipaistvuse tagamiseks tehakse asjakohased privaatsusteated avalikult kättesaadavaks.
- **Põhimõte 4:** Isikuandmed hoitakse täpsed ja ajakohased. Isikuandmeid ei säilitata kauem, kui on seaduslikult nõutud või vajalik iga õiguspärase eesmärgi saavutamiseks, milleks andmeid töödeldakse. Kui isikuandmed ei ole enam vajalikud selle eesmärgi täitmiseks, mis õigustas nende algset töötlemist ja puudub muu seaduslik eesmärk, siis isikuandmed kustutatakse või anonüümitakse.
- **Põhimõte 5:** avaldame ametiasutustele isikuandmeid seadusega nõutud ulatuses või kliendi nõusolekul ja vastavalt eelnevalt kindlaks määratud juhistele.

- **Põhimõte 6:** Käesoleva poliitika mõjusid tuvastatakse ja käsitletakse kogu organisatsioonis ning privaatsusnõuded ja tehnilised ning organisatsioonilised kaitsemeetmed on integreeritud meie toodete, teenuste, protsesside, IT ja infrastruktuuri kujundamisse arenduse varases staadiumis, hõlmates kogu elutsüklit (lõimitud ja vaikimisi andmekaitse). Andmekaitse ja privaatsusnõuete täitmist tagatakse regulaarsete vastavuskontrollide ja sisekontrolli süsteemi toimimisega. Kõigi võimalike isikuandmete rikkumiste korral järgitakse määratletud uurimis- ja teavitusprotsessi. Kui seadus nõuab, siis teatakse isikuandmete rikkumistest õigeaegselt järelevalveasutustele ja mõjutatud isikutele.
- **Põhimõte 7:** Iga Telia Company töötaja läbib kohustusliku andmekaitse koolituse ja muud tema tööülesannetega soetud koolitused ning austab seadusega või lepingutega ette nähtud konfidentsiaalsuskohustust.

2.3 TURVALISUSE JA PRIVAATSUSEGA SEOTUD KOLMANDA OSAPOOLE RISKIPÕHIMÕTTED

- **Põhimõte 1:** Kolmandate osapoolte riskijuhtimise programmile ja poliitikale kohaldatakse järgmisi turva- ja privaatsusnõudeid.
- **Printsiip 2:** Kolmandate osapoolte turva- ja privaatsusriskid tuvastatakse ja hallatakse vastavalt Telia Company Ettevõtte Riskijuhtimise Poliitikale.
- **Printsiip 3:** Lõimitud ja vaikimisi turvalisus ja andmekaitse on sisse viidud tarneahelasse, sealhulgas privaatsuse ja turvalisusega seotud aspektid, mis puudutavad iga ettevõtte ja selle tarnijate või teenusepakkujate vahelisi suhteid.
- **Põhimõte 4:** Turva- ja privaatsusnõuded rakendatakse vastavalt tuvastatud riskidele tarneahelas (st riskipõhine lähenemine).
- **Põhimõte 5:** Tarnijatelt nõutakse, et nad vastaksid selle grupipoliitika nõuetele, et vältida Telia Company poolt kogutud isikuandmete kaotsiminekut, vargust, loata avalikustamist või sobimatut kasutamist. Tarnijatelt oodatakse, et nad töötleksid selliseid andmeid õiglaselt ja seaduslikult kõigis tegevustes, sealhulgas siis, kui andmeid töödeldakse väljaspool riiki, kus need koguti või saadi.

Need Telia Company põhimõtted kehtivad ulatuses, mis ei lähe vastuollu kohalike seadusandlusega. Käesoleva grupipoliitika põhimõtetega on seotud grupi juhised ja standardid, mis sisaldavad täpsemaid nõudeid.

3. ROLLID JA VASTUTUS

Käesolev poliitika kehtib Telia Company AB-le ja tema tütarettevõtetele ning sidusettevõtmistele nii nagu nende enda siduv poliitika kõigile juhatuse liikmetele, juhtidele ja töötajatele. Täiendavalt püüdleb Telia Company selle poole, et soodustada ja kehtestada käesoleva poliitika põhimõtted ja eesmärgid ka teistes ettevõtetes, mis ei ole Telia Company kontrolli all, aga mille üle on oluline mõju.

Kõik Telia Company juhatuse liikmed, kes alluvad vahetult Telia Company juhatuse esimehele, vastutavad selle eest, et käesolev Telia Company poliitika on nõuetekohaselt teavitatud ja rakendatud ning et nende vastutusvaldkonna töötajad oleks antud poliitikaga tuttavad ning järgiks seda.

Iga riigi tegevjuht on vastutav, et kõik ettevõtted sõltumata nende geograafilisest asukohast kehtestaksid ja täidaksid seda poliitikat.

4. POLIITIKA RIKKUMINE

Telia Company töötaja, kes kahtlustab vastutustundliku äri juhendi või käesoleva poliitika rikkumist, on kohustatud teavitama sellest oma otsest juhti, juhi juhti, personalijuhti, eetika- ja vastavuskoordinaatorit või kasutama teavitamisliini Speak-Up Line. Teavitamisliin on leitav Telia Company veebilehelt.

Telia Company keelab sõnaselgelt igasuguse kättemaksu teavitamisliini kasutanud inimestele. Konkreetsed nõuded on leitavad kontserni sisemise raporteerimise ja kättemaksu vältimise juhendist.

Käesoleva Telia Company kontserni poliitika rikkumised võivad tuua kaasa distsiplinaarmenetluse, mis võib viia töösuhte lõpetamiseni.

5. SIHTGRUPP

See grupipoliitika kehtib Telia Company AB-le, selle tütarettevõtetele ja sidusettevõtetele kui nende enda siduv poliitika. Lisaks töötab Telia Company selle nimel, et võtta kasutusele poliitika turvapõhimõtted kõigis teistes tegevustes, milles Telia Company omab osalust. Grupipoliitika kehtib ka kõigile kolmandate osapoolte teenusepakkujatele, kes töötavad lepingu alusel mõne eespool nimetatud üksuse heaks.

6. ERANDID

Kui kontserni poliitika suhtes soovitakse teha erandit, siis eskaleerib riigi tegevjuht või Grupi funktsioonide juht selle küsimuse kontserni peajuristile ja vastava poliitika omanikule. Kui erandiks antakse nõusolek, siis selle osas tehakse eraldi otsus.

Konkreetse tütarettevõtte jaoks kohandatud vastavasisuline poliitika peab olema kooskõlas käesoleva kontserni poliitikaga, arvestades samas asjakohaste äritegevuste, kohalike seaduste, kohalike asjaolude ja keelega.

7. KONTSERNI JUHTIMISRAAMISTIK

Kontserni poliitika moodustab osa kontserni juhtimisraamistikust, mis hõlmab muu hulgas:

a) Vastutustundliku äri juhendit, eesmärki ja väärtuseid, strateegiat, kontserni poliitikaid ja juhendeid kontserni juhatuse esimehele kinnitatuna kontserni nõukogu poolt;

b) kontserni juhatuse esimehe otsuseid, kontserni juhatuse esimehe kinnitatud otsustuskorda, tegevjuhi või vastutava kontserni funktsiooni juhi poolt kinnitatud kontserni juhendeid, ja

c) kontserni funktsiooni juhi vastutusalas välja töötatud suuniseid, parimaid tavasid, protsessikirjeldusi, malle või töökordasid.

8. VIITED

Selle poliitika väljatöötamisel kasutatud viited hõlmasid, kuid ei piirdunud, riiklike julgeoleku nõuetega, üldtunnustatud turvapraktikatega (NIST CSF 2.0, ISO 27001/2:2022, SCF jne) ja kohaldatavate seaduste nõuetega.

9.VERSIOONID

Versioon	Kuupäev	Muutja	Peamised muudatused
V5	**31.01.2023**	**GRC Security**	• Turvariskide sõnastamine läbi Telia Company eesmärkide • Turvariski määratlemine strateegilise äririskina • Rõhuasetus riskipõhisele turvalisusele • Selgemate ja lühemate turvapõhimõtete uuesti sõnastamine • Viidete ning terminite ja lühendite lisamine
V5	**23.02.2023**	**GRC Security**	• Väiksed sõnastuse muudatused
V6	**24.01.2025**	**Tech Legal and Group Security**	• Poliitika põhimõtete uuendamine, et kajastada NIST CSF 2.0 nõudeid • 5P määratluse eemaldamine

			• NIS2 and DORA viidete lisamine Uue tegevusmudeli kajastamine • Privaatsuspoliitika sisu lisamine ja uuendamine • Terminoloogia täpsustamine

3 TERMINID JA LÜHENDID

Terminid ja lühendid	Definitsioon
Missioonikriitiline (MC) vara	Määratud riiklike reguleerivate asutuste poolt kui riigi julgeoleku seisukohalt oluline, määratletuna kui kriitiline riiklik taristu (CNI) vastavalt reguleerivate asutuste juhistele või teenused osutatud eriklientidele; hõlmab ka riiklikku autonoomiat/reservi, seaduslikku pealtkuulamist, kõrget usaldusväärsust (autentsust) ja väga tundlikke isikuandmeid. Turva- ja privaatsusintsidendid, mis hõlmavad missioonikriitilisi varasid, mõjutavad tõenäoliselt oluliselt ühiskonna toimimist.
Ärikriitiline (BC) vara	Ärilised prioriteedid ja kohaldatavad õiguslikud kohustused (ei kuulu missioonikriitiliste alla). Turva- ja privaatsusintsidendid mõjutavad suure tõenäosusega oluliselt Telia ärieesmärkide ja äriliste ambitsioonide saavutamist.
Standardkriitiline (SC) vara	Varad, mis ei vasta missioonikriitiliste või ärikriitiliste kriteeriumidele (s.t kõik varad, millele kehtivad turva- ja privaatsusstandardid või regulatiivsed nõuded).
Isikuandmete nõuete rikkumine	Isikuandmetega seotud rikkumine on turvanõuete rikkumine, mis põhjustab edastatavate, salvestatud või muul viisil töödeldavate isikuandmete juhusliku või ebaseadusliku hävitamise, kaotsimineku, muutmise või loata avalikustamise või neile juurdepääsu.
Turva- ja privaatsuspõhimõtted	Turva- ja privaatsuspõhimõtted ärieesmärkide toetamiseks ja juhiste ettevalmistamiseks.

Terminid ja lühendid	Definitsioon
ISO/IEC mõisted	ISO/IEC 27000 põhinevad mõisted