Turvadirektiivid

Versioon
7.0

Sisukord

Ettevõtte kontaktandmed
Telia Company AB
16994 Stockholm, Rootsi
Registrijärgne kontor: Stockholm
Ettevõtte registrikood: 556103-4249 KMKR: SE556103424901

Turvadirektiivid

Versioon
7.0

1 Kirjeldus

Käesolevas dokumendis ehk tarnijate turvalisuse direktiivis kirjeldatakse turvanõudeid, mida kohaldatakse tarnijatele ja muudele kolmandatele isikutele, kes tegelevad äritegevusega Telia ettevõttega.

2 Mõisted

1. **Leping** on Telia ja tarnija või Telia Company grupi muu tuvastatud äripartneri vaheline leping, mille alusel kohaldatakse tarnija turvalisuse direktiivi ja mille osa on tarnijate turvalisuse direktiiv.
2. **Kohaldatavad andmekaitsealased õigusnormid** on kõik andmekaitse ja turvalisusega seotud kohaldatavad õigusaktid, muu hulgas eraelu puutumatust ja elektroonilist sidet käsitlev direktiiv (Euroopa Parlamendi ja nõukogu 12. juuli 2002. aasta direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris) ja isikuandmete kaitse üldmäärus (Euroopa Parlamendi ja nõukogu 27. aprilli 2016. aasta määrus (EL) 2016/679 füüsiliste isikute kaitse kohta isikuandmete töötlemisel ja selliste andmete vaba liikumise ning direktiivi 94/46/EÜ kehtetuks tunnistamise kohta) ning nende muudatused, asendused või uuendused (edaspidi kollektiivselt „ELi õigusaktid“), kõik siduvad riigisisesed õigusaktid, millega rakendatakse ELi õigusakte ja muid siduvaid andmekaitsealaseid või andmete turvalisusega seotud direktiive, seaduseid, määrusi ja otsuseid, mis kehtivad asjaomasel ajahetkel.
3. **Ostja andmed** on andmed või muu info, mille ostja või ostja nimel tegutsev isik teeb tarnijale kättesaadavaks, sealhulgas isikuandmed, ning tarnija poolt nende andmete töötlemise tulemus.
4. **Ostja** või **Telia** on Telia Company AB või asjaomane Telia Company kontserni kuuluv ettevõte.
5. **Pilvandmetöötlus** või **pilv** on mudel, mis võimaldab kõikjal kättesaadavat, mugavat ja nõudmisel toimuvat võrgujuurdepääsu konfigureeritavate arvutusressursside (nt võrgud, serverid, salvestusruumid, rakendused ja teenused) jagatud kogule, mida saab kiiresti ja minimaalse haldustegevuse või teenusepakkuja sekkumisega kasutusele võtta ja vabastada.
6. **Tööstusharu parim tava** on tava, meetod, protsess või kriteerium, näiteks tuntud parimad turvatavad, mis toetavad kõrgeid vastupidavuse standardeid ja katkematute protokollide kasutamist jne, mida tööstusharu liikmed üldiselt aktsepteerivad ja järgivad.
7. **Info- ja kommunikatsioonitehnoloogia riistvara** ja **IKT riistvara** on mis tahes tehnoloogiline toode, mis salvestab, otsib, manipuleerib, edastab või võtab vastu teavet elektrooniliselt, samuti selle iseseisvaks toimimiseks vajalik tarkvara ja/või võimaldab asjaomasel personalil toodet kasutada või sellega suhelda.
8. **Infotöötlusvahendid** on infotöötlussüsteem, -teenused või -taristu või füüsilised asukohad, kus need asuvad.
9. **Infoturbe juhtimissüsteem** või **ISMS** on üldise juhtimissüsteemi asjakohane osa, mis põhineb äririskil põhineval lähenemisviisil ja mille eesmärk on luua, rakendada, kasutada, jälgida, läbi vaadata, säilitada ja parandada infoturvet. Juhtimissüsteem hõlmab organisatsioonilist struktuuri, poliitikat, planeerimistegevust, kohustusi, tavasid, menetlusi, protsesse ja ressursse.
10. **Taristu kui teenus** või **IaaS** on teenus, mille võimekus on pakkuda ostjale töötlemis-, salvestus-, võrgu- ja muid põhilisi arvutiressursse, mille puhul saab ostja kasutusele võtta ja käivitada suvalist tarkvara, mis võib hõlmata operatsioonisüsteeme ja rakendusi. Ostja ei halda ega kontrolli aluseks olevat pilvetaristut, kuid tal on kontroll operatsioonisüsteemide, salvestusruumi ja rakenduste üle ning võimalik, et piiratud kontroll valitud võrgukomponentide üle (nt hostide tulemüürid).
11. **Logimine** on info või sündmuste üksikasjade registreerimine organiseeritud registreerimissüsteemi, tavaliselt järjestatuna info või sündmuste toimumise järjekorras.
12. **Isikuandmed** on kogu teave tuvastatud või tuvastatava füüsilise isiku kohta. Tuvastatav füüsiline isik on isik, keda saab otseselt või kaudselt tuvastada selliste näitajate järgi, nagu nimi, aadress, isikukood, tellimisnumber, IP-aadress, asukohaandmed, võrguidentifikaator, andmeliiklusandmed või sõnumi sisu, või ühe või mitme asjaomase füüsilise isiku füüsilise, füsioloogilise, geneetilise, vaimse, majandusliku, kultuurilise või sotsiaalse identiteedi spetsiifilise näitaja alusel.
13. **Platvorm kui teenus** või **PaaS** tähendab teenust, mille ostjale pakutav suutlikkus on juurutada pilvetaristut ostja loodud või omandatud rakendusi, mis on loodud teenusepakkuja poolt toetatud

programmeerimiskeelte, andmekogude, teenuste ja tööriistade abil. Ostja ei halda ega kontrolli aluseks olevat pilvetaristut, sealhulgas võrku, servereid, operatsioonisüsteeme või salvestusruumi, kuid tal on kontroll juurutatud rakenduste ja võimaluse korral rakenduste majutuskeskkonna konfiguratsiooni seadete üle.

14. **Pseudonüümimine** on isikuandmete töötlemine selliselt, et isikuandmeid ei saa enam omistada konkreetsele andmesubjektile lisateavet kasutamata. Seda eeldusel, et vastavat lisateavet hoitakse eraldi ning sellele rakendatakse tehnilisi ja organisatoorseid meetmeid tagamaks, et isikuandmeid ei omistata tuvastatud või tuvastatavale füüsilisele isikule.
15. **Õigusaktidest ja lepingutest tulenevad nõuded** on kõik rahvusvaheliste poliitiliste ja majandusorganisatsioonide (nt Euroopa Liit), riigi, maakonna, haldusasutuse või valitsusasutuse (nt asjaomase finantsteenuste asutuse, andmekaitseasutuse, tarbijakaitseameti või kemikaaliameti) kõik aeg-ajalt kehtivad seadused, eeskirjad, määrused ja lepingud, samuti kohaldatav kohtupraktika, määrused, otsused, litsentsid, soovitused, põhimõtted, standardid ja suunised, mille on välja andnud nimetatud asutused, kohtud ja/või isereguleeruvad või nõuandvad organisatsioonid ja vastava tööstussektori rühmad.
16. **Turvameede** on tehniline turvameede, organisatsiooniline struktuur või protsess, mis aitab hoida IT-süsteemide turvakvaliteediga seotud omadusi.
17. **Turvaintsident** on soovimatud või ootamatud turvasündmused üksikult või sarjana, millel on oluline tõenäosus seada ohtu äritegevust ja ohustada turvalisust.
18. **Tundlikud tooted** ja **tundlikud teenused** on tooted või teenused, mille ostja on määratlenud tundlikuna. Tundlikud tooted või tundlikud teenused dokumenteeritakse selgelt vastavas lepingus.
19. **Teenused** on tarnija või tarnija nimel tegutseva isiku poolt ostjale osutatavad teenused, mis on täpsemalt määratletud poolte vahelises lepingus.
20. **Tarkvara kui teenus** või **SaaS** on teenus, mida tarnija pakub ostjale funktsionaalsusena, mille puhul tarkvara ja sellega seotud andmed asuvad keskselt tarnija juures või mille puhul tarkvara ja sellega seotud andmed on paigaldatud, integreeritud, käitatud, toetatud ja hooldatud tarnija poolt ostja pilvekeskkonnas, selle asemel et anda neid ostjale tarkvaralitsentsi alusel.
21. **Tarnija personal** on kõik isikud, kes töötavad tarnija nimel, näiteks töötajad, konsultandid, töövõtjad ja alltöövõtjad.
22. **Tarnija** viitab asjakohases lepingus teisele poolele, kes tarnib ostjale mis tahes kaupa või teenust, nimetusega tarnija, müüja, partner või muu sarnase nimega.

3 Kohaldamisala

Turvadirektiive kohaldatakse, kui:

1. Tarnija töötleb ostja andmeid, välja arvatud ärisuhte loomiseks või säilitamiseks vajalikud kontaktandmed.
2. tarnijal on lubatud järelevalveta viibida ostja valdustes, välja arvatud väljaspool siseruume;
3. tarnija kasutab ostja võrku või IT-süsteeme, sealhulgas kaugjuurdepääsu;
4. tarnija kasutab ostja infotöötlusseadmeid;
5. ostja on pidanud tarnijat tundlike toodete ja/või tundlike teenuste osutajaks ja määratlenud tarnija sellisena asjaomases lepingus.

4 Tarnija üldine vastutus

1. Tarnija vastutab täielikult selle eest, et tarnija personal järgib tarnijate turvalisuse direktiivi.
2. Tarnija peab rakendama meetmeid, mis on vajalikud tarnijate turvalisuse direktiivi järgimiseks enne mis tahes ülesande alustamist ostja jaoks.
3. Tarnija teavitab ostja nõudmisel ostjat sellest, kuidas tarnija järgib tarnijate turvalisuse direktiivi ja milliseid meetmeid tarnija on võtnud tarnijate turvalisuse direktiivi järgimiseks.
4. Tarnija teavitab ostjat aadressil cert@teliacompany.com kõigist turvaintsidentidest (muu hulgas isikuandmete töötlemisega seotud intsidentidest) niipea kui võimalik, kuid mitte hiljem kui 24 tundi pärast turvaintsidentide tuvastamist. Vt allpool jaotist „Turvaintsidentide haldamine“.
5. Tarnija tagab, et ostja andmete igasugune töötlemine on kooskõlas tarnijate turvalisuse direktiiviga.

6. Tarnija ei võimalda ilma ostja eelneva kirjaliku nõusolekuta ühelegi poolele juurdepääsu ostja andmetele (see võib puudutada ka uut, laiendatud, ajakohastatud, pikendatud või muul viisil muudetud reaalajas võrgujuurdepääsu), mis on vastuolus lepinguga.

5 Turvanõuded

5.1 Riskide juhtimine

5.1.1 Turvariskide juhtimine

1. Tarnija peab perioodiliselt tuvastama, analüüsima, hindama ja kõrvaldama turvariske.

5.2 Infoturbepoliitikad

1. Tarnijal on määratletud ja dokumenteeritud infoturbe juhtimissüsteem (information security management system, ISMS), sealhulgas kehtestatud infoturbepoliitika ja protseduurid, mille peab kinnitama tarnija juhtkond. Need avaldatakse tarnija organisatsioonis ja nendest teavitatakse asjakohast tarnija personali.

5.3 Infoturbe korraldamine

1. Tarnijal on oma organisatsioonis määratletud ja dokumenteeritud turvarollid ja -vastutused.

5.4 Personaliga seotud turve

1. Tarnija tagab, et kõik lepingu alusel ülesandeid täitvad tarnija töötajad on usaldusväärsed ja vastavad mis tahes kehtestatud turvalisuse kriteeriumidele.

5.5 Varahaldus

5.5.1 Materiaalne vara

1. Tarnijal on sätestatud ja dokumenteeritud varahaldussüsteem ning ta peab ajakohastatud registreid kõigi asjakohaste varade ja nende omanike kohta. Varade hulka kuuluvad muu hulgas teave, IT-süsteemid, teavet sisaldavad varukoopiad ja/või eemaldatavad andmekandjad, juurdepääsuõigused, tarkvara ja konfiguratsioon.

5.5.2 Andmed

1. Tarnija rakendab meetmeid, et tagada kaitse juhusliku, volitamata või ebaseadusliku kadumise, hävitamise, muutmise või kahjustamise eest seoses ostja edastatud, salvestatud või muul viisil töödeldud andmetega.
2. Tarnija tagastab või hävitab (vastavalt ostja otsusele) kõik ostja andmed ja nende koopiad lepingu lõppemisel või ostja nõudmisel. Tarnija kinnitab ostjale kirjalikult, et tarnija on selle nõude täitnud.

5.6 Juurdepääsu kontroll

1. Tarnijal peab olema määratletud ja dokumenteeritud juurdepääsukontrolli poliitika rajatiste, tegevuskohtade, võrgu, süsteemi, rakenduste ja teabe/andmete juurdepääsu jaoks (sealhulgas füüsilise, loogilise ja kaugjuurdepääsu kontroll).
2. Tarnija peab kehtestama kasutajate juurdepääsu ja privileegide autoriseerimise protsessi, juurdepääsuõiguste tühistamise korra ja tarnija personali juurdepääsuõiguste aktsepteeritava kasutamise korra.
3. Tarnija määrab kõik juurdepääsuõigused teadmisvajaduse ja vähimate privileegide põhimõtte alusel.

5.7 Krüpteerimine

1. Kui krüpteerimine on nõutav vastavalt 6. jaotisele (infoturbe konfidentsiaalsuse klassifikatsiooni kirjeldus ja käitlemise nõuded) või vastavalt poolte vahel sõlmitud lepingule, tagab tarnija krüpteerimise nõuetekohase ja tõhusa kasutamise vastavalt tööstusharu parimatele tavadele.
2. Tarnija kasutab krüpteerimismeetodeid, mida peetakse turvaliseks vastavalt tööstusharu parimatele tavadele.

5.8 Füüsiline ja keskkonnaturve

1. Tarnija kaitseb oma andmetöötlusrajatisi väliste ja keskkonnaohtude ja ohtude eest, sealhulgas elektri-/kaabeldamishäirete ja muude häirete eest, mis põhjustavad rikkeid toetavates kommunaalteenustes. See hõlmab füüsilist perimeetri ja juurdepääsu kaitsmist.

5.9 Talitluskindlus

1. Tarnija rakendab pahavara kaitset, tagamaks, et tarkvara, mida tarnija kasutab ostjale tarnitavate toodete tarnimiseks, on kaitstud pahavara eest.
2. Tarnija rakendab operatiivseid ja tehnilisi turvakontrolle, nagu logihaldus, tulemüürid, viirusetõrje ja krüpteerimine vastavalt tööstusharu parimatele tavadele.
3. Tarnija teeb kriitilisest teabest varukoopiaid ja testib varukoopiaid, et tagada teabe taastamine vastavalt ostjaga sõlmitud kokkuleppele.

5.10 Side turve

1. Tarnija tagab, et vähemalt kogu sisemiselt konfidentsiaalseks või salajaseks liigitatud teabe edastamine on kaitstud vastavalt ostja teabeklassifikatsiooni kirjeldusele, mis on esitatud 6. jaotises (infoturbe konfidentsiaalsuse klassifikatsiooni kirjeldus ja käitlemise nõuded).

5.11 Tarnija suhe alltöövõtjatega

1. Tarnija peab kajastama tarnijate turvalisuse direktiivi sisu oma lepingutes alltöövõtjatega, kes täidavad lepingu alusel määratud ülesandeid.
2. Tarnija esitab ostja nõudmisel ostjale tõendid selle kohta, et alltöövõtja täidab tarnijate turvalisuse direktiivi.

5.12 Turvaintsidentide haldamine

1. Tarnija peab kehtestama turvaintsidentide haldamise korra.
2. Tarnija teavitab ostjat aadressil cert@teliacompany.com igast turvaintsidendist viivitamata pärast turvaintsidendi tuvastamist.
3. Kõiki turvalisusega seotud vahejuhtumitest teatamisi käsitletakse konfidentsiaalse teabena ja need krüpteeritakse, kasutades selleks tööstusharu parimaid tavasid, nagu PGP või sama tugevaid krüpteerimistehnikaid.

5.13 Äritegevuse järjepidevuse juhtimine

1. Tarnijal peavad olema dokumenteeritud protsessid ja kord talitluspidevuse, sealhulgas avariitaastekava järgimiseks.
2. Tarnija peab regulaarselt tuvastama, analüüsima ja hindama talitluspidevuse riske ning võtma vajalikke meetmeid selliste riskide kontrollimiseks ja leevendamiseks.
3. Tarnija aitab kaasa vastastikuse talitluspidevuse kava (BCP) ja avariitaastekava (DRP) koostamisele või ajakohastamisele ostja nõudmisel.

5.14 Vastavus

1. Tarnija järgib kõiki asjakohaseid õigusaktidest ja lepingutest tulenevaid nõudeid, sealhulgas neid, mis on seotud Isikuandmete kaitsega.
2. Tarnija esitab nõudmisel ostjale põhjendamatu viivituseta aruande turvanõuete täitmise kohta.
3. Tarnija esitab ostjale ISAE3000/SSAE18 SOC2 Type I/II ja/või SOC3 aruande, kui see on olemas.
4. Tarnija teavitab ostja nõudmisel ostjat sellest, kuidas tarnija täidab turvanõudeid ja milliseid meetmeid ta on võtnud turvanõuete täitmiseks.
5. Tarnija jälgib, vaatab läbi ja auditeerib regulaarselt alltöövõtja vastavust turvanõuetele.
6. Tarnija esitab ostja nõudmisel ostjale tõendid selle kohta, et alltöövõtja täidab turvanõudeid.
7. Ostjal on õigus kontrollida, kuidas tarnija ja tema alltöövõtjad täidavad turvanõudeid või vastavaid nõudeid.
8. Kui vahejuhtum kuulub seadusest tulenevate nõuete kohaselt ametiasutustele teatamisele, on ostjal õigus viia läbi vahejuhtumi audit kolme (3) tunni jooksul enne teatamist.
9. Kui vahejuhtum ei kuulu seadusest tulenevate nõuete alla, millest tuleb ametiasutustele teatada, on ostjal õigus viis (5) päeva ette teatades viia läbi vahejuhtumi audit.

6 Infoturbe konfidentsiaalsusklasside kirjeldus ja käitlemise nõuded

6.1 Infoturbe konfidentsiaalsusklasside kirjeldus

Klass	Kirjeldus	Infoliikide näited
Salajane	Loata juurdepääs teabele või selle **avalikustamine võib tõsiselt kahjustada Telia Companyt**, selle korraldust, kriitilisi funktsioone, töötajaid, äripartnereid ja/või kliente.	- Aastaaruanne või finantstulemused enne avalikustamist. - Teatud teave, mis põhineb õiguslikel nõuetel, konkreetsetel kliendikokkulepetel või salastatuse kokkulepetel.
onfidentsiaal e	Loata juurdepääs teabele või selle **avalikustamine võib kahjustada Telia Companyt**, selle korraldusi, kriitilisi funktsioone, töötajaid, äripartnereid ja/või kliente.	- Teatud teave, mis põhineb õiguslikel nõuetel (nt klientide või töötajate isikuandmed). - Tundlikud äriplaanid, strateegiad ja otsused (nt turundusplaanid).
Ettevõttesise seks	Loata juurdepääs teabele või selle **avalikustamine võib tekitada Telia Companyle**, selle korraldusele, kriitilistele funktsioonidele, töötajatele, äripartneritele ja/või klientidele vähest kahju.	- Teave, mis on ette nähtud Telia Company sisekasutuseks. - Kõigile Telia Company töötajatele suunatud kommunikatsioonimaterjalid (st Telia Company korralduse, strateegia, toodete ja töötajate teenustega seotud materjalid).
Avalik	Loata juurdepääs teabele või selle **avalikustamine ei tekita kahju Telia Companyle**, selle korraldusele, kriitilistele funktsioonidele, töötajatele, äripartneritele ja/või klientidele.	- Aastaaruanne ja tulemused pärast nende avaldamist. - Turundusmaterjalid ja avaldatud pressiteated. - Teave, mis tuleb avaldada õiguslike nõuete alusel.

6.2 Infoturbe konfidentsiaalsusklasside käitlemise nõuded

Klass	Kes võib juurdepääsu saada	Kuidas säilitada	Kuidas üle kanda	Kuidas kasutada	Kuidas hinnata kaitse vajadust (riskipõhine lähenemisviis)
Salajane	Ainult määratud isikud	Loogiliselt ja füüsiliselt turvaline säilitamine, st krüpteeritud või lukustatud	Kasutades turvalisi sidekanaleid või turvalist kaasaskantavat salvestusseadet (lukustatult)	Kasutatakse turvalistes ruumides, mis on kaitstud pealtnägemise ja pealtkuulamise eest	Kaitse murdmine peab olema väga raske. Üksnes äärmiselt motiveeritud ja/või leidlikud ründajad suudaksid kaitse maha võtta.

Turvadirektiivid

Versioon
7.0

Konfidentsiaalne	Ainult piiratud *ja kontrollitud* isikute rühm	Loogiliselt ja füüsiliselt kontrollitud ja usaldatav salvestus range juurdepääsukontrolliga	Turvaliste sidekanalite kaudu, kontrollitud ja usaldusväärses võrgus või turvalises kaasaskantavas hoidlas	Kasutatakse üksnes volitatud isikute poolt ärilistel eesmärkidel kontrollitud tööruumis või kohas, mis on kaitstud pealtnägemise ja pealtkuulamise eest	Volitamata isikutel peab olema raske infole juurdepääsu saada. Üksnes hästi motiveeritud ründajad suudaksid kaitse maha võtta.
Ettevõttesisese	Need, kes töötavad Telia Company heaks	Loogilise ja füüsilise juurdepääsukontrolliga	Kasutades kaitstud sidekanaleid või usaldatavas võrgus	Kasutatakse üksnes volitatud isikute poolt ärilistel eesmärkidel kontrollitud tööruumis või kohas, mis on kaitstud pealtnägemise ja pealtkuulamise eest	Volitamata isikutele peab olema infole juurdepääsu saamine ebatõenäoline. Üksnes motiveeritud ründajad suudaksid kaitse maha võtta.
Avalik	Piirangud puuduvad	Piirangud puuduvad	Piirangud puuduvad	Piirangud puuduvad	Piirangud puuduvad

Ettevõtte kontaktandmed
Telia Company AB
16994 Stockholm, Rootsi
Registrijärgne kontor: Stockholm
Ettevõtte registrikood: 556103-4249 KMKR: SE556103424901