Sisukord

Directo OÜ infoturbe põhimõtted 3
1. Üldine info 3
2. Teenuse üldine kirjeldus 3
3. Infoturve Directos 4
3.1. Infoturbe poliitika, protsess, organisatsioon ja riskide haldus 4
3.2. Inimressursiturve 6
3.2. Kliendi infovarade turvalisus 6
3.3. Isikuandmete kaitse Directos 6
3.4. Andmete asukoht 7
3.5. Andmeside 7
3.6. Andmete varundamine 7
3.7. Monitooring ja logimine 7
3.8. Klienditugi ja intsidentide haldus 7
3.9. Directo kaasatud volitatud töötlejad 8
4. Füüsiline turve 8
5. Ligipääsud infosüsteemides 8
6. Vastavus 8
7. Pidev parendamine 8
8. Talitluspidevus 8

Directo OÜ infoturbe põhimõtted

1. Üldine info

Directo missioon on pakkuda oma klientidele vapustavalt võimekat, aga samas uskumatult lihtsalt kasutatavat äritarkvara. Meie missiooni täitmisel on äärmiselt oluline osa infoturbel ning seega suhtume me sellesse äärmise tõsidusega alates juhatusest kuni iga töötajani välja. Oleme pühendunud meie ettevõtte ning klientide infovarade konfidentsiaalsuse, tervikluse ja käideldavuse säilitamisele.

Isikuandmete töötlemisel võib Directo olla nii isikuandmete vastutava töötleja kui ka volitatud töötleja rollis. Isikuandmete kaitse üldmääruse kontekstis on meie peamine ülesanne rakendada oma teenustele piisavalt tehnilisi ja organisatsioonilisi turvameetmeid, et klientide poolt töödeldavad andmed oleksid kaitstud juhusliku või seadusevastase kustutamise, autoriseerimata ligipääsu või avaldamise eest.

Käesoleva infolehega aitamegi sinul paremini aru saada, mida ja kuidas me teeme Directo äritarkvaras töödeldavate andmete (sh isikuandmete) turvamiseks.

Euroopa Parlamendi ja Nõukogu regulatsioon 2016/679 ehk isikuandmete kaitse üldmäärus sedastab järgmist:

- kui isikuandmeid töödeldakse vastutava töötleja nimel, kasutab vastutav töötleja ainult selliseid volitatud töötlejaid, kes annavad piisava tagatise, et nad rakendavad asjakohaseid tehnilisi ja korralduslikke meetmeid sellisel viisil, et töötlemine vastab käesoleva määruse nõuetele ja sealjuures tagatakse andmesubjekti õiguste kaitse.

Vastutav töötleja - see oled sina ehk Directo äritarkvara kasutaja. Directo OÜ on volitatud töötleja ning tegutseb vastavalt sinu antud volitustele. Sinul kui vastutaval töötlejal on vastutus veenduda, et volitatud töötleja ehk Directo kaitseb sinu andmeid. Ühtlasi pead loomulikult ka teadma, millised on sinu ülesanded ja vastutus isikuandmete töötlemisel.

2. Teenuse üldine kirjeldus

Directo äritarkvara teenust pakume me klientidele pilveteenusena. Pilveteenuse pakkujana puudub meil ka kontroll selle üle, milliseid andmeid meie teenusesse laadid või seal töötled. See tähendab, et me ei tea vaikimisi, kas kasutad meie teenust isikuandmete töötlemiseks, milliseid isikuandmeid töötled ja kas selline töötlemine on seaduslik. Vajadusel pead ise hindama andmete töötlemise mõju ja selle vastavust kehtivale seadusandlusele. Vastavalt mõjuhinnangule võib olla vajalik rakendada lisaturvameetmeid nagu näiteks sisselogimise viimine ID-kaardi põhiseks ja/või kasutusõiguste piiramine.

3. Infoturve Directos

3.1. Infoturbe poliitika, protsess, organisatsioon ja riskide haldus

Oleme pühendunud turvalise äritarkvara tagamisele. Selleks on meie juhatus ettevõttes kehtestanud infoturbepoliitika, mida rakendame kogu ettevõtte ulatuses – kehtestatud printsiipide järgimist ootame nii Directo juhtidelt, töötajatelt kui ka töövõtjatelt, kes meie ettevõtte tegevuses osalevad. Infoturbepoliitika ajakohasust hinnatakse vähemalt korra aastas ning poliitika koostamise, täiendamise ja rakendamise eest vastutab Directos infoturbejuht.

Infoturbejuhti toetab tema töös laiapõhjaline infoturbe töörühm.

Infoturbe protsessi on kaasatud kõik ettevõtte struktuuriüksused ja töötajad ning ka töövõtjad.

Oleme oma infoturbepoliitika loonud ja juurutanud standardi ISO/IEC 27001 järgi ning kinnitanud standardiga ühilduvust ka ametliku sertifitseerimisega. Sertifikaadiga saad tutvuda siin:

ISO/IEC 27001:2013 sertifikaat
ISO/IEC 27001:2022 sertifikaat

BUREAU VERITAS

Bureau Veritas Certification

Directo OÜ

Head Office: Mõisa 4, 13522 Tallinn

Bureau Veritas Certification Holding SAS – UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2022

Scope of certification

ERP software development, consultation, sales.

Statement of Applicability Version number and release date: 9.09.2024

Original cycle start date*:	**21-December-2021**
Expiry date of previous cycle**:	**20-December-2024**
Certification / Recertification Audit date**:	**01-November-2024**
Certification / Recertification cycle start date:	**21-January-2025**

Subject to the continued satisfactory operation of the organisation's Management System, this certificate expires on: **20-December-2027**.

Certificate No.IND.24.19034/IS/U *Version:* ***No. 1*** *Issue date:* ***21-January-2025***

Certification body address: ***5th Floor, 100 Lower Thames Street, London, EC3R 6DL , United Kingdom***
Local office: ***Tartu mnt. 24-22, 10115 Tallinn, Estonia***

UKAS MANAGEMENT SYSTEMS
0008

Further clarifications regarding the scope and validity of this certificate, and the applicability of the management system requirements, please call: **+372 667 6610**

CER CERTIF ALL TPL 001 rev 4.3 1 / 1 November 4, 2024

Kuidas Directo kontrollieesmärgid kohalduvad standardi praeguse versiooni ISO/IEC 27001 nõuetega

saab tutvuda: Infoturbe kohaldusmäärang

Meie ettevõttes toimub järjepidevalt ja süsteemselt infoturbealaste riskide seire ning riskihindamise täiendamine koos tegevustega vähendamaks infoturbe alaseid jääkriske.

3.2. Inimressursiturve

Oleme oma töötajatele ning alltöövõtjatele kehtestanud infoturbe reeglid ja nõudmised, mis tagavad et:

- töötajad, töövõtjad ja kolmandatest osapooltest kasutajad mõistavad oma kohustusi
- töötajad, töövõtjad ja kolmandatest osapooltest kasutajad sobivad oma rollidesse
- tehtud on kõik vähendamaks varguse, pettuse ja ressursside või teabe väärkasutuse riski

Tööle asumise eelsete taustakontrollide läbiviimine on värbamisprotsessi oluline osa ja aitab meil tööle võtta ainult neid kandidaate, kes kindlasti oma rolli sobivad.

Alltöövõtjatega sõlmitakse alati konfidentsiaalsuslepingud enne, kui alltöövõtjale tagatakse ligipääs infovaradele.

Turvateadlikkuse tõstmine on pidev protsess. Eesmärk on, et kõik töötajad ja alltöötlejate töötajad mõistaksid ning teaksid Directo OÜ tegevust reguleerivaid seadusi ja määrusi, sise- ja lepingulisi nõudeid, rakendatud kaitsemehhanisme ning nendega seotud intsidentide aruandlusmeetodeid. Turvalisust reguleerivad dokumendid (nt poliitikad, juhised ja parimad tavad) on saadaval ettevõtte siseveebis.

3.2. Kliendi infovarade turvalisus

Directo infosüsteemides säilitatavate ja töödeldavate kliendi infovarade (andmed, dokumendid, failid, e-kirjad jne) vastutav omanik on klient. Kõikide klientide andmeid käsitleme konfidentsiaalsetena, mis on kõrgeim turvalisuse tase Directos.

Directo siseselt kehtiv turvatase ei kandu automaatselt edasi ettevõttest väljapoole. Klient peab oma teavet Directo IT-süsteemides säilitama, töötlema ja edastama vastavalt enda poolt oma infovarale määratud turvatasemetele, kaalutletud riskidele ning korraldama neile vastavate turvameetmete rakendamise, milleks võivad olla kasutajaõiguste või nende ulatuse piiramine jms.

Directo ei müü mitte kunagi Directo äritarkvarasse laaditud, kliendi kasutajate poolt üles laaditud või kliendi poolt teenuse kasutamise käigus serverisse loodud andmeid kellelegi, ega kasuta selliseid andmeid kliendi loata enda otsestes majanduslikes huvides. Directo töötleb selliseid andmeid ainult oma kliendi teenuste või nendega seotud kasutajatoe pakkumiseks vajalikus ulatuses või jagab seaduses ettenähtud juhtudel vastavate õiguskaitseorganitega.

3.3. Isikuandmete kaitse Directos

Isikuandmete kaitseks rakendab Directo OÜ parimaid võimalikke tehnoloogiaid ja meetodeid. Peame arvestust nii töödeldavate isikuandmete kui ka töötlemise mõju üle nendele andmetele. Isikuandmete töötlemise kohta saad lähemalt lugeda Directo OÜ andmekaitsetingimustest:

https://directo.ee/andmekaitsetingimused.

Täpsemalt isikuandmete kaitsest loe siit: https://wiki.directo.ee/et/gdpr

3.4. Andmete asukoht

Directo teenust osutavad serverid asuvad füüsiliselt turvalises andmekeskuses Euroopa Liidu territooriumil.

Infrastruktuuri majutamisel teeb Directo OÜ koostööd ainult tunnustatud partneritega. Andmekeskuse teenust pakub Telia Eesti AS, kelle infoturbe juhtimissüsteem on sertifitseeritud ISO/IEC 27001 standardi alusel:

- ISO/IEC 27001:2013 sertifikaat 20.02.2019 - 25.02.2022
- ISO/IEC 27001:2013 sertifikaat 26.02.2022 – 25.02.2025

3.5. Andmeside

Andmesidega seotud infoturbe-, kestlikkuse ja äririskide maandamiseks teeb Directo koostööd Telia Eesti ASiga. Kõik kliendi andmeside Directoga tarkvaraga toimub üle HTTPS protokolli ja on krüpteeritud.

3.6. Andmete varundamine

Directo litsentsilepingu tingimuste kohaselt koostame varukoopia iga 24 tunni tagant ning säilitame seitset viimast varukoopiat. See tähendab, et juhul, kui andmete töötleja kustutab või anonümiseerib isikuandmeid, kulub seitse kalendripäeva, enne kui muutub võimatuks nende taastamine varukoopiast. Manuste backup tehakse iga 24 tunii tagant ning säilitatakse 1 viimast koopiat.

3.7. Monitooring ja logimine

Directo OÜ koostöös partneritega jälgib teenuseid osutavate serverite tööd 24 tundi ööpäevas ja 7 päeva nädalas.

Jälgitavuse tagamiseks salvestatakse ja säilitatakse infovarade haldamise ja kasutamisega seotud toimingute teostamise kohta kontrolljälgi (logisid), mida ei saa muuta ega kustutada ükski töötaja/kasutaja.

3.8. Klienditugi ja intsidentide haldus

Directo klienditugi pakub telefoni, e-posti ja chati teel abi äripäevadel ajavahemikus 09.00 – 17.00 (ajatsoon EET/EEST).

Klienditoe telefon on: +372 671 8578.

Klienditoe e-posti aadress on: info@directo.ee.

Infoturbe intsidentidest teavitamise eest vastutavad kõik ettevõtte töötjad. Infoturbe intsidentidega tegeleb kasutajatugi koostöös infoturbejuhiga.

3.9. Directo kaasatud volitatud töötlejad

Me võime kaasata kliendi andmete töötlemisse volitatud töötlejaid.

Teeme seda vaid siis, kui oleme saanud piisava kinnituse, et kõik osapooled rakendavad asjakohaseid tehnilisi ja korralduslikke meetmeid sellisel viisil, et andmete töötlemine vastab asjaomastes seadustes esitatud nõuetele.

4. Füüsiline turve

Oleme juurutanud turvalisuse tagamiseks meetmed äritegevuse säilimiseks. Ligipääsud on piiratud ning varustatud vajalike turvaseadmetega.

5. Ligipääsud infosüsteemides

Meie ettevõttes kasutatakse rollipõhist ligipääsu ning juurdepääs antakse üksnes teabele, mis on vajalik oma ülesannete täitmiseks. See kehtib kõikidele Directo töötajatele, töövõtjatele ja kolmandatest osapooltest kasutajatele.

6. Vastavus

Me töötame pidevalt, et järgida asjakohaseid seadusi, määrusi ja lepingulisi nõudmisi. Tagamaks seaduste ja lepinguliste nõuete täitmist, oleme ettevõttes juurutanud sisemised juhtdokumendid, turvanõuded ja ülevaated. Nõuete järgimise hõlbustamiseks korraldame koolitusi ja muid turvateadlikkuse alaseid tegevusi oma töötajatele ja koostööpartneritele.

7. Pidev parendamine

Oleme Directos võtnud endale kohustuse pidevalt täiendada ja arendada Infoturbe juhtimissüsteemi, et ära hoida infoturbeintsidente.

8. Talitluspidevus

Me hoolime väga oma toote töökindlusest ja jätkusuutlikkusest, sest kasutame ka ise täpselt sama äritarkvara. Mõistame, et häireid võib ette tulla, ning seetõttu oleme üles ehitanud süsteemid ja protsessid nii, et häirete esinemisel oleks nende mõju meie klientidele minimaalne. Selleks:

- teostame järjepidevat riskide hindamist ja olukordade parendamist riskide realiseerimise

ennetamiseks
- tagame talitluspidevuse, mis on osa meie teenuse arendamise elutsüklist
- testime oma teenust ning analüüsime ja parendame, et seda täiendada
- töötame parimate tavade ja rahvusvaheliste standardite järgi